Regis University

ePublications at Regis University

Regis University Student Publications (comprehensive collection)

Regis University Student Publications

Fall 2011

The Vulnerability Assessment and Penetration Testing of Two Networks

Steven L. Simpson
Regis University

Follow this and additional works at: https://epublications.regis.edu/theses

Part of the Computer Sciences Commons

Recommended Citation

Simpson, Steven L., "The Vulnerability Assessment and Penetration Testing of Two Networks" (2011). *Regis University Student Publications (comprehensive collection)*. 633.
https://epublications.regis.edu/theses/633

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

THE VULNERABILITY ASSESSMENT AND PENETRATION TESTING

OF TWO NETWORKS

A PROJECT

SUBMITTED ON THE 16th OF DECEMBER, 2011

TO THE DEPARTMENT OF INFORMATION SYSTEMS

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

SYSTEMS ENGINEERING

BY

Steven L. Simpson

APPROVALS

D. M. Likarish

Dan Likarish, Project Advisor

Robert T. Mason

Robert T. Mason, Ph.D.

Nancy Birkenheuer

Nancy Birkenheuer

Abstract

Vulnerability assessments and penetration testing are two approaches available for use by internet security practitioners to determine the security posture of information networks. By assessing network vulnerabilities and attempting to exploit found vulnerabilities through penetration testing security professionals are able to evaluate the effectiveness of their network defenses by identifying defense weaknesses, affirming the defense mechanisms in place, or some combination of the two.

This project is a discussion of the methods and tools used during the vulnerability assessment and penetration testing, and the respective test results of two varied and unique networks. The assessment and testing of the first network occurred from an internal perspective, while the assessment and testing of the second occurred from an external perspective. While the tools and methodologies used across both networks were consistent, the test results differed significantly. The paper concludes with a series of recommendations regarding practical methods and tools that may prove useful to anyone interested in network security, and vulnerability assessments and penetration testing in particular.

Acknowledgements

I would like to thank the following people for their support and help during the pursuit of my graduate education and during the completion of this project. Specifically I would like to thank my wife, Renee Simpson for her continued belief in my abilities for all the projects I have undertaken. I would also like to thank Angus Anderson, Stuart Gentry, Brian Haynie, Ed Richards, Corbit Magby, and Justin McCallister for taking to the time to review my writings and for the edits and suggestions, which made this paper more readable and easier to understand.

I would also like to thank the following people for their continued support during the pursuit of my studies and for always taking the time to ask me how my studies were progressing: Denise Haynie, Jane Richards, Stan and Jeannie Cook, Mark Williams, Davie Costales, Brian and JoAnn Morford, Anita Magby, and Doyle and Judy Warnock. Finally, I would like to thank my son, Matthew Scott Simpson for inspiring me to complete all the work required to finish my Master's education.

Table of Contents

ABSTRACT ..... **II**

ACKNOWLEDGEMENTS ..... **III**

TABLE OF CONTENTS **4**

LIST OF TABLES **6**

CHAPTER 1 – INTRODUCTION **7**

CHAPTER 2 - CANVAS ASSESSMENT AND TESTING **11**

CANVAS PROJECT PURPOSE, REQUIREMENTS, AND DELIVERABLES 11

CANVAS PROJECT TOOLS AND RESOURCES 12

BackTrack 4. ..... *12*

Nmap. *12*

Metasploit. *14*

CANVAS NETWORK TEST METHODOLOGY 15

CANVAS network host discovery. *15*

CANVAS network port analysis. *17*

CANVAS network automated penetration testing. *18*

CANVAS PROJECT SUMMARY 24

CHAPTER 3 - ITS NETWORK VULNERABILITY ASSESSMENT AND PENETRATION TESTING **26**

ITS PROJECT REQUIREMENTS, PROJECT RESTRICTIONS, AND PROJECT DELIVERABLES 26

Project Requirements. *26*

Project Restrictions. *27*

Project Deliverables. *27*

PROJECT TEST PLAN 28

Test Notification Process. *30*

Project Tools and Resources *32*

ITS network assessment and penetration test methodology *33*

ITS Network Assessment and Penetration Test Results Summary 44

CHAPTER 4 - SUMMARY AND RECOMMENDATIONS 49

Summary 49

Recommendations 51

Recommendation 1. 51

Recommendation 2. 52

Recommendation 3. 53

Recommendation 4. 54

Recommendation 5. 54

Recommendation 6. 55

Recommendation Summary 56

REFERENCES 59

APPENDIX A: CANVAS NETWORK ALL HOST/ALL PORTS SCAN RESULTS 61

APPENDIX B: CANVAS AUTO TEST SUMMARY - 031811 64

APPENDIX C: CANVAS TESTING FOR 03222011 65

APPENDIX D: ITS PROJECT TEST PLAN 66

APPENDIX E: ITS NETWORK PING RESULTS 76

APPENDIX F: FILE LISTING OF *EXTERNAL_UP.TXT* 80

APPENDIX G: ITS PORT ANALYSIS SCAN RESULTS – COMPLETE LISTING 82

List of Tables

Table 1: CANVAS Project Requirements, Restrictions, and Deliverables Page 8

Table 2: Active CANVAS Hosts Page 13

Table 3: Port Scan of CANVAS Network Page 15

Table 4: Metasploit db_autopwn results for CANVAS network Page 17

Table 5: Post-hardening Test Results Summary Page 20

Table 6: ITS Project requirements, restrictions, and deliverables Page 24

Table 7: Completed Test Notification Form Page 28

Table 8: ITS Network Ping Scan Results Page 31

Table 9: Partial Listing of external_up.txt Page 33

Table 10: Sample ITS Network Port Analysis Scan Result Page 35

Table 11: Port Analysis Scan Results Summary Page 43

Table 12: Possible Network Irregularity Page 44

Chapter 1 – Introduction

This report presents the methods, tools, and the results of the vulnerability assessment and penetration testing of two separate and unique networks. The assessment and testing of each network was part of the System Engineering and Application Development (SEAD) Practicum in support of a Masters program at Regis University.

Before discussing the details of each project, a definition of the terms "vulnerability assessment" and "penetration testing" is in order. In a broad sense, a vulnerability assessment is any action taken to evaluate the effectiveness of asset protection. Penetration testing usually follows a vulnerability assessment and is the process of verifying identified vulnerabilities by executing tests designed to exploit the vulnerabilities and compromise the target.

A common routine performed by numerous individuals can illustrate the concept of a vulnerability assessment. On a nightly basis, many conduct a vulnerability assessment by checking their dwelling's doors and windows prior to turning in for the night. Verifying the state of external doors and windows (e.g. the determination of whether the external doors and windows are locked, unlocked, open or closed) is a simple example of a common vulnerability assessment. Many people follow the nightly routine of checking the most vulnerable access points of their homes in an effort to determine the safety and security of their possessions and the people inside.

While the concept of checking the most vulnerable access points is applicable to almost any system, when applied to an information network, the process defines a network vulnerability assessment. In terms specific to an information network, a vulnerability assessment is any action taken to evaluate the security of a network. The Red Hat Enterprise Linux 4: Security Guide describes a vulnerability assessment as the "audit of network and system security; the results of

which indicate the confidentiality, integrity, and availability of [the] network" (Red Hat, 2005). Just as the home's resident may check windows and doors for vulnerable points of entry, a network assessor will check the network hosts for vulnerabilities such as unpatched operating system (OS) software, open ports, application flaws, or any number of other security vulnerabilities.

The vulnerability assessment of an information network follows a straightforward and logical series of steps. These steps begin with the broad retrieval of data and narrow to a point of specific action. Commonly, a vulnerability assessment progresses in the following steps:

- Reconnaissance of network hosts
- Enumeration of network devices
- Enumeration of services on each device
- Verification of discovered vulnerabilities

Throughout this report, the phrase "host discovery" will refer to the reconnaissance of network hosts. The phrase "port analysis" will refer to the enumeration of network devices and the operational services of those devices. The phrase "penetration testing" will refer to the verification of discovered vulnerabilities. In the context of this report, the phrase vulnerability assessment will include the processes of host discovery and port analysis while term penetration testing refers to the standalone and unique process of vulnerability verification. Lastly, the term "three-step method" refers to the steps of host discovery, port analysis, and penetration testing and its use is interchangeable with the terms vulnerability assessment(s) and penetration testing throughout this report.

Also of note is the perspective from which these vulnerability assessment and penetration tests occur. All vulnerability assessments and penetration tests occur from a host that is either

external or internal with respect to the network under test. While the methods and tools used for assessment and testing are consistent, the tester's approach and the expectation of the findings is different, dependant on the network's internal or external perspective.

When conducting the vulnerability assessment and penetration test from an external perspective, the tester's view is restricted to the public face of the network. The view usually includes limited network knowledge pertaining to the routable public internet protocol (IP) addresses and the network's web services including file transfer protocol (FTP) services, mail services, and domain name system (DNS) services. The configurations of these services usually block access to the organization's internal local area network (LAN) by any outside untrusted party. As such, the perspective of the external tester is that of someone who is outside of the network looking for any weakness or vulnerability that might provide network access.

Conversely, the perspective of the tester who is internal to the network is that of a trusted party who has the freedom to look around. The trust provided to an internal network user usually translates into an elevated privilege level and increased access to network services and devices. An elevated privilege status may also provide the user configuration rights to various network devices or operational software. Given the level of increased privilege and access, the internal tester is not usually looking for a way into the network. Instead, the internal tester will likely concentrate on finding weaknesses in those operational services or device configurations not accessible to those external to the network.

The projects of this report include one discussion where the vulnerability assessment and penetration testing occurred from an internal perspective, and another where vulnerability assessment and penetration tested occurred from and external perspective. While the tools and

methodologies used in each of the projects was consistent, the outcomes were significantly different.

As the purpose of these projects was to determine the security posture of each network, note that various changes to network IP addresses, stakeholder names, email address, phone numbers, etc. were altered to protect the networks or individuals involved. For example, alpha characters replaced the numeric characters of the network potions of production IP addresses, listed email addresses refer to non-existent recipients, and listed phone numbers are not valid. While these changes protect the networks and people specific to these projects, the changes do not affect the value of the discussion. All of the concepts, methods, or techniques described in this report stand on their own merit and do not rely on the identification of a specific network, host or individual.

Chapter 2 - CANVAS Network Assessment and Testing

The Computer and Networking Visualization and Simulation (CANVAS) security event is a cyber competition providing participants an opportunity to compete in a real-world information security exercise. In April of 2011, Regis University hosted the sixth Annual CANVAS competition (Regis University, 2011). In preparation for the event, testing of the CANVAS network fell on the System Engineering and Applications Development (SEAD) Practicum Penetration Test (Pen Test) group.

CANVAS Project Purpose, Requirements, and Deliverables

The purpose, requirements, restrictions, and deliverables relating to the CANVAS network testing were both straightforward and open-ended. The purpose of the testing was to determine both the vulnerability and exploitability of the CANVAS network with respect to the goals of the competition. The requirements, restrictions, and deliverables relating to the testing of the CANVAS network were as follows:

1. The project required the use of an assigned VMware account to perform an inside network test of the CANVAS network. Any testing of the CANVAS network would originated from the assigned VMware account.
2. The tools used in all CANVAS network assessment and testing were restricted to those loaded on the assigned VMware account.
3. The project deliverable was a report providing as much information as possible regarding the exploitability of any hosts on the CANVAS network.

As the project progressed, the project deliverables expanded to include both pre-hardening and post hardening test findings in the final project report.

A summary listing of the final project purpose, requirements, restrictions, and deliverables are in Table 1: CANVAS Project Purpose, Requirements, Restrictions, and Deliverables.

Table 1: CANVAS Project Purpose, Requirements, Restrictions, and Deliverables

- Identify the exploitability of the pre and post hardened CANVAS networks
- Use the Regis University provided tools to test the CANVAS network
- Enumerate network hosts and services
- Conduct penetration testing to exploit as many hosts as possible on the pre and post hardened network
- Report findings to project stakeholders

CANVAS Project Tools and Resources

BackTrack 4.

The test platform provided by Regis University consisted of an assigned virtual machine (VM) loaded with BackTrack 4 (BT4). BackTrack is a utility that functions as both an operating system (OS) and a comprehensive collection of security-related tools. The tools included with the BackTrack framework are commonly available tools for use by network security practitioners, and support various security tasks including digital forensics, network assessments, and penetration testing. Two tools of note are included with the BT4 tool-set, both proving useful for the testing of the CANVAS network. These tools are Nmap and Metasploit.

Nmap.

Nmap (short for "Network Mapper") is a freely available, open source test utility used for network exploration, network administration, and security auditing. First released in 1997 with

the Phrack Magazine article, *The Art of Port Scanning* (Phrack, 1997), Nmap quickly gained popularity with hackers and network security professionals. Industry periodicals such as the Linux Journal (Linux Journal, 2001), Info World, LinuxQuestions.Org, and Codetalker Digest named Nmap the "Security Product of the Year" (Nmap, 2011). Nmap is consistently one of the top ten most research tools at the freshmeat.net repository. Common uses of Nmap include network host discovery, port scanning, services and applications version detection, and OS fingerprinting (freshmeat.net, 2011).

Nmap training resources.

Although volumes of published information regarding the function and use of Nmap is readily available from books, magazines, technical articles, and websites, an authoritative resource for Nmap is found at the nmap.org website (http://nmap.org). Both the Nmap website and the Nmap tool are maintained by a group of, "…hardcore members (especially programmers) who are interested in helping the [Nmap] project by developing new code and additional features" (Nmap, 2011). Resources provided at the nmap.org home page include links to various urls from which the user can download the Nmap tool, get information regarding Nmap installation, locate the online Nmap reference guide, purchase the Nmap reference book, locate Nmap training, and view examples of where and how Nmap has been portrayed in the media (e.g. movies, books, and television shows).

A resource regarding any technical aspect of Nmap is the book, *NMAP Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning* written by Nmap's creator, Gordon "Fyodor" Lyon. The author regards the work as the "Official Nmap project guide to network discovery and security scanning" (Lyon, 2008). This work provides both experienced and novice users detailed information on all aspects of Nmap including

obtaining the Nmap source code; compiling, installing, and removing Nmap from a given computer; host discovery and port scanning; the Nmap scripting engine; optimizing Nmap performance; and defensive tactics to implement when guarding against internal, or external network scans.

Metasploit.

The second tool used extensively during the vulnerability scanning and penetration testing of the CANVAS network was Metasploit. Like Nmap, the Metasploit Framework is a popular and widely used tool. However, as Nmap's focus is on port scanning, Metasploit's focus is host vulnerability and exploitation.

Since its initial release in 2004, Metasploit has quickly gained significant popularity within the hacker and security communities rising to fifth on the list of the "Top 100 Network Security Tools" according to sectools.org (sectools.org, 2011). As for now, Metasploit Framework is available as freeware downloadable from the Rapid 7 website (Rapid 7, 2011) and is available as part of the BackTrack OS and tool set.

Metasploit training resources.

While a significant amount of information regarding the use and operation of Metasploit is available from books, articles, and websites, a series of informative Metasploit video tutorials is available at the Security Tube website available at http://www.securitytube.net/. In addition to the Metasploit tutorial, Security Tube offers a number of other security-based videos including tutorials on penetration testing, exploit research, assembly language programming, and network and computer hacking.

Security Tube's Metasploit Megaprimer tutorial is a series of 17 videos focusing on the use and capabilities of the Metasploit Framework. The training illustrates how to use BT4,

Nmap, and Metasploit tools to identify and exploit the vulnerabilities of target victim machines. The tutorials spend ample time demonstrating the function and operation of the Metasploit Framework as well as the strategic operation of various exploits.

Security Tube's "Metasploit Megaprimer" video tutorial includes approximately 15 hours of video training over 17 individual videos. Tutorial topics cover various and numerous aspects of the Metasploit Framework's theory of operations and functional usage (SecurityTube, 2011).

CANVAS Network Test Methodology

The CANVAS requirements, restrictions and deliverables all but mandated the test methodology. The project deliverables included a listing of the host IP address and exploitation vectors for the pre-hardened CANVAS network. By using the appropriate command line options, Nmap is capable of producing a list of active network hosts, determining the OS running on each host, an enumerated list of the host's open ports, and determining the software and version of each utility servicing the open ports. Given Nmap's capability for host detection, port discovery, OS finger printing and service detection; as well as Nmap's inclusion in the suite of tools provided with the BT4 tool set made Nmap the logical and available host discovery tool of choice.

CANVAS network host discovery.

The customary first step of host discovery is the enumeration of active IP addresses within an address range. Sending a network "ping", also referred to as "pinging the network", is a function of Internet Control Message Protocol's (ICMP) echo request capabilities. Virtually all TCP/IP based networks use ICMP to relay query messages, respond to query messages, and communicate network status. Echo requests and echo replies are two of the numerous and frequently used network communication features available with ICMP.

Nmap ping scan methodology.

When a host receives a ping, network conformance requirements mandate that the host respond with an ICMP echo reply (Internet Engineering Task Force, 1989). The completed echo request/echo reply cycle verifies that a host exists at a specific network address, and that communication between the initiator and responder is possible. When used by Nmap as a method of network host discovery, the ICMP echo request/echo reply cycle is part of a ping scan, which provides the initiating host discover information regarding which IP addresses are home to an active host, have no hosts, or are attempting to hide from external discovery.

For security reason, some network administrators purposely block an ICMP echo ping request. Even if blocked, most active hosts will respond to either a TCP ACK packet sent to port 80, or a SYN packet sent to a host as a request to establish inter-host communications. As such, an Nmap ping scan not only includes an echo request, but also an ACK packet sent to port 80, and a SYN packet sent to a targeted IP address (Insecure.com LLC, 2004).

By tracking the IP address of responding hosts, the initiator is able to comprise a list IP addresses containing active hosts. Additionally, the host knows that non-responsive addresses indicate either an address at which no host resides, an address at which a host is hiding behind a firewall, or a host that is non-compliant regarding communications between internet hosts per RFC 1122 (IETF, 1989). For purposes of the CANVAS network competition the assumption was that no firewalls were hiding hosts, that a non-responding IP address indicated a lack of a network host, and that all hosts were compliant with RFC 1122.

With the completion of the Ping Scan, network discovery was complete. The value of the information gained through network host discovery is in knowing which IP addresses deserve additional testing, and which IP addresses to ignore.

The project stakeholders provided no information about the CANVAS network concerning size, addresses, or the number of active hosts. The only information about the CANVAS network came from the IP address of test host assigned to the tester. The test host resident at address 10.128.128.123, which led to the following assumptions:

- The test host resided on the CANVAS network
- The CANVAS competition network required no more than 254 hosts
- The CANVAS network address was 10.128.128.0/24

Fortunately, each of the above assumptions proved correct. A ping scan using the Nmap command *nmap –sP 10.128.128.0/24* provided information regarding both network host discovery and an initial enumerated list of active network hosts. See Table 2: *Active CANVAS Hosts* for a listing of the enumerated hosts found by the above Nmap command.

Table 2: Active CANVAS Hosts

10.128.128.1	10.128.128.2
10.128.128.3	10.128.128.50
10.128.128.68	10.128.128.69
10.128.128.71	10.128.128.80
10.128.128.100	10.128.128.121
10.128.128.122	10.128.128.123
10.128.128.124	

While the listing in Table 2 proved accurate for the initial network host enumeration, note that this initial listing is not consistent with host listings taken later in the project. For purposes of the CANVAS competition, the competition organizers included additional network hosts, and changed the IP addresses of others.

CANVAS network port analysis.

With an understanding of the network address range and the network size, the next step included a network scan for open port and the determination of port services. The command

nmap –p0-65535 10.128.128.0/24 executed a port scan across all 65,535 ports of each active host, provided a list of open ports, and determined the port services running on each of the open ports. See Table 3: Port Scan of CANVAS Network, for a partial listing of the above command output and Appendix A: *CANVAS Network All Host/All Ports Scan Results* for a complete listing of the port scan results.

Although the vulnerabilities shown for the majority of the CANVAS hosts were similar to those for hosts 10.128.128.1 and 10.128.128.124, three hosts, 68, 69, and 100, had vulnerabilities similar to that of host 10.128.128.68. The open ports and the running services of hosts 10.128.128.68, 69, and 100 identified these hosts as candidates of interest and targets for additional scanning and possible exploitation.

CANVAS network automated penetration testing.

With network host and port discoveries both complete, enough information regarding the CANVAS network was at hand to initiate exploitation attacks. The tool of choice for the CANVAS network exploitation was Metasploit.

One of Metasploit's useful features is its ability to launch automated exploits using database values as input. This feature allows the output of certain third party tools to load a database with IP addresses. Fortunately, one of these third party tools is Nmap.

Executing Nmap commands from within Metasploit results in a database whose data values include a list of network host IP addresses, a list of open ports, and the services running on each of the open ports. Executing Nmap from within Metasploit and piping the output into a pre-defined database only requires adding the *db_* prefix to any Nmap command.

For example, the command *db_nmap –p0-65535 10.128.128.0/24* executes an Nmap total port scan on all hosts residing on the CANVAS network and saves the results in a previously

Table 3: Port Scan of CANVAS Network

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-03-12 14:39 MST
Nmap scan report for 10.128.128.1
Host is up (0.0057s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:00:0C:07:AC:01 (Cisco Systems)

{Output cut for sake of brevity}

Nmap scan report for 10.128.128.68
Host is up (0.00039s latency).
Not shown: 65509 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
515/tcp  open  printer
548/tcp  open  afp
1046/tcp open  unknown
1063/tcp open  unknown
1065/tcp open  unknown
1070/tcp open  unknown
1074/tcp open  unknown
1076/tcp open  sns_credit
1077/tcp open  unknown
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
3459/tcp open  unknown
MAC Address: 00:50:56:84:00:00 (VMware)

{Output cut for sake of brevity}

Nmap scan report for 10.128.128.124
Host is up (0.00048s latency).
All 65536 scanned ports on 10.128.128.124 are filtered
MAC Address: 00:50:56:84:00:26 (VMware)

Nmap done: 256 IP addresses (13 hosts up) scanned in 1572.98 seconds
```

specified database. Metasploit can then use the database values (e.g. IP addresses, port data, and other values resident in the database) to develop a list of known vulnerabilities and execute automated exploitation attacks against the target network. While automated exploitation may provide only minimal advantages when testing a network the size of CANVAS, the ability to run automated exploitations against a network comprised of thousands of hosts is a significant timesaving feature and provides a handy method for saving and organizing network exploitation results.

Metasploit's *db_autopwn* pipes the values of an existing database into the input queue of the command. The command itself invokes Metasploit's automated capabilities including:

- Automatic choice and launch of exploits against a target host or range of hosts
- Spawning of a Meterpreter session resulting from a successful exploitation
- Creation of multiple Meterpreter sessions from the exploitation of multiple vulnerabilities
- Exploitation of specific targets stored in the database

As with most command line tools, a number of command line options are available. The following options are available for use with the *db_autopwn* command:

- -t Show all matching exploit modules
- -x Select modules based on vulnerability references
- -p Select modules based on open ports
- -e Launch exploits against all matched targets
- -r Use a reverse connect shell
- -b Use a bind shell on a random port
- -h Display this help text (Metasploit, 2006)

- -I [range] Only exploit hosts inside this range

The command *db_autopwn –e –p –t –I 10.128.128.1-122* invoked Metasploit's automated capabilities executing the various command line options (-e, -p, -t and –I) as described above. The results of this command are below in Table 4.

Table 4: Metasploit db_autopwn Results for CANVAS Network

10.128.128.1 > 1 open port, 4 exploits, 0 sessions.
10.128.128.2 > 1 open port, 4 exploits, 0 sessions.
10.128.128.3 > 1 open port, 4 exploits, 0 sessions.
10.128.128.4 > 1 open port, 4 exploits, 0 sessions.
10.128.128.50 > 4 open ports, 50 exploits, 0 sessions.
10.128.128.68 > 23 open ports, 290 exploits, 5 sessions.
10.128.128.69 > 22 open ports, 290 exploits, 9 sessions.
10.128.128.71 > 2 open ports, 50 exploits, 0 sessions.
10.128.128.72 > 21 open ports, 294 exploits, 6 sessions.
10.128.128.100 > 19 open ports, 186 exploits, 0 sessions.
10.128.128.121 > 1 open port, 106 exploits, 0 sessions.
10.128.128.122 > 2 open ports, 50 exploits, 0 sessions

As shown in Table 4, the exploitation of the hosts at 10.128.128.68, 69, and 72 resulted in Meterpreter sessions. Note that the host at 10.128.128.100 was not exploitable contrary to the results given previously and prior to the execution of the automated exploit command.

Initial network and port discoveries identified the host at IP address 10.128.128.100 as both functioning, and having a number of open ports and running services (see Table 2 and Appendix A). Additionally, the initial scans did not detect an operational host at IP address 10.128.128.72. However, as shown in Table 4, the host at IP 10.128.128.100 proved immune from the exploitation while the host at 10.128.128.72 was exploitable. The reason for this inconsistency was not a problem with the test tools or the test methodology. Instead, the inconsistency proved to be the result of network changes made by the project stakeholders to ready the CANVAS network for competition.

Meterpreter sessions.

The establishment of Meterpreter sessions indicates the compromise of the network host. In a white paper written about Metasploit's Meterpreter, the paper's author describes the Meterpreter as

> "an advanced payload that is included in the Metasploit Framework [that allows] developers to write their own extensions in the form of shared object files that can be uploaded and injected into a running process… Meterpreter and all of the extensions that it loads [execute] entirely from memory and never touch the disk, thus allowing them to execute under the radar of standard Anti-Virus detection"(skape, 2004).

Simply stated, when a Metasploit exploit results in a Meterpreter session, the attacker has near, if not total anonymity while on the victim machine. This anonymity provides the attacker the ability to browse file content, create files, delete files, download files from the victim machine, or upload files or software utilities of choice to the victim machine, and do so with near anonymity. Since the Meterpreter only resides in the victim machine's RAM, presence of the Meterpreter session is usually undetectable by anti-virus software. Additionally, all traces of the session may vanish with subsequent data writes to the system RAM, or when the victim system powers down.

To provide evidence regarding the compromise of the hosts at addresses 10.128.128.68, 69, and 72, and to show that user access was elevated to a privileged level during the Metepreter session, a small text file was written in each host's C:\WINDOWS\system32 folder informing the system owner of the compromise. While significant changes to the compromised host were possible, the charter of the project was only to determine host exploitability. As such, the exploitation of the compromised hosts only included the creation of the aforementioned text file.

Note that while each identified host was a target of exploitation, only those hosts that lacked sufficient security protection were victim to the attacks. Hosts containing sufficient hardening were not penetrated and remained uncompromised.

Pre-hardened network test results summary.

The delivery of a summary report to the appropriate stakeholders completed the pre-hardening phase of the CANVAS network test. The report simply listed the command used for the exploitation and that a small number of hosts were vulnerable to the Metasploit automated exploitation. Appendix B: *CANVAS auto test summary – 031811,* includes a copy of the report sent to the top stakeholders summarizing the findings of the pre-hardening CANVAS network testing.

Post Hardening Penetration Testing.

To properly configure the CANVAS network and ready the competition platform, the project stakeholders hardened the network. System hardening is a, "process of securing a system by reducing its surface of vulnerability by the removal of any software, user accounts or services that are not related and required by the planned system functions" (Shortinfosec, 2011). By hardening specific hosts, the stakeholders controlled exploitable network resources while continuing to allow the competitors access to specific information. To confirm the network was hardened per plan, the project stakeholders relied on post-hardening network testing.

Testing of the post-hardened CANVAS network only required a network re-test using Metasploit's automated capabilities as previously described. Neither host, nor port discovery was required. Additionally, retest was only required of the three previously exploitable hosts; those hosts at IP addresses 10.128.128.68, 10.128.128.69, and 10.128.128.72.

As with the testing of the pre-hardened network, the post-hardened network testing would include the automated capabilities of Metasploit. The command *db_autopwn –e –p –t –I <target>***,** where <target> was the IP address of each of the previously failing hosts was again executed. Table 5: *Post-hardening Test Results Summary* shows the results of the test. As shown, hardening occurred on two of the three hosts leaving only the host at IP address 10.128.128.69 susceptible to exploits.

The delivery of the final test results concluded the testing of the CANVAS network. See Appendix C: *Canvas testing for 03222011* for a copy of the final report.

Table 5: *Post-hardening Test Results Summary*

10.128.128.68 > 24 open ports, 382 exploits, 0 sessions
10.128.128.69 > 15 open ports, 60 exploits, 9 sessions
10.128.128.72 > 23 open ports, 382 exploits, 0 sessions

CANVAS Project Summary

The use of a virtual network account and three well known, and widely used, security tools provided the resources and framework allowing the successful test and exploitation of the CANVAS network. Project specifications required the use of a VMware account, BackTrack 4, Nmap, and Metasploit to enumerate network hosts, discover network services, and exploit any vulnerability found on the pre or post hardened CANVAS network. The pre-hardened network included three hosts vulnerable to exploitation, which and was compromised using Metasploit and Meterpreter sessions. The post-hardened network testing resulted in the discovery of only a single host susceptible to compromise. Reports sent to the project stakeholders identified the differences between the pre and post-hardened networks and provided the project stakeholders with information regarding the vulnerabilities and exploitability of the pre and post-hardened networks.

While other tools and methodologies may provide similar results, the resources provided, and the methods developed for this project proved useful. The resources and methods used proved successful for use with network host discovery, host port analysis, port service evaluation, and the exploitation of vulnerable network hosts.

Chapter 3 - ITS network vulnerability assessment and penetration testing

The Information Technology Services (ITS) network vulnerability assessment and penetration-testing project was similar to the CANVAS project in that the purpose of each was to provide a security assessment of a given network. Because of the similarities, many of the overall project methodologies, tools and deliverables were similar, if not identical, to one another. However, the ITS network had significant differences with respect to network purpose, function, and topology, as well as the perspective from which the vulnerability assessments and penetration tests were launched.

CANVAS was a virtual network existing primarily as a network platform for a specific competition. Conversely, the ITS network is a fully functional, physical network of servers, clients, printers, routers, etc. designed, built, and maintained for the on-going use and support of the Regis University administration, faculty, and students. Given the ITS network's intended use, internal testing of the network was not allowed. While the CANVAS assessment and testing occurred only from an internal perspective, the ITS network assessment and testing occurred only from an external perspective. The execution of all assessment and penetration tests occurred from a test host external to the ITS network.

ITS Project Requirements, Project Restrictions, and Project Deliverables

There were two each of project requirements, restriction and deliverables. While some are straightforward and easily understood, others had a significant impact on the project. Those requirements, restrictions, or deliverables that influenced the project results or methodologies are included in the detailed discussions in the appropriate sections of this paper.

Project Requirements.

The overall project requirement was to determine the vulnerability exposure of the ITS

network. While this requirement stopped short of specifying how the exposure was to be determined, the stakeholders and test team jointly decided that conducting a network vulnerability assessment and penetration test was the preferred approach.

The second requirement was that testers were to inform specific university personnel of their intended testing. This requirement obligated testers to provide specific information to the Regis University ITS Security Officer (ITSSO) and project advisors regarding the activities of a network test session. Testers were to provide information prior to the initiation of a test session and again once the session completed. A discussion regarding the specifics of the test notification process (TNP) is in the Project Test Plan section.

Project Restrictions.

Project restrictions pertained to the permitted types of assessments, types of testing, and IP address range of the network under test. Testers were free to implement any form of vulnerability or penetration testing as long as these activities had no adverse impact on any operational aspect of the ITS network. Additionally, if a tester were to uncover a network weakness that resulted in the compromise of a network host, the tester was to suspend any active or planned test execution and immediately inform the ITSSO of the network vulnerability.

The second restriction limited the testing of the network to the IP address range specified by the Regis ITSSO. At the time of the assessment, Regis University operated and maintained at least four networks. Sanctions to test the Regis network applied only to the network specified by the ITSSO.

Project Deliverables.

The deliverables of the ITS project included the development of a formal test plan and the submission of a report summarizing the project test findings. A discussion regarding the

details of the project test plan are in the section that immediately follows, and a summary of the test results are in the section titled ITS Network Assessment and Penetration Test Results Summary.

Table 6: ITS Project requirements, restrictions, and deliverables summarize the project attributes.

Table 6: ITS Project requirements, restrictions, and deliverables

ITS Project Requirements
Determine the security posture of the ITS network
Inform the university ITSSO of all test activity
ITS Project Restrictions
Do not disable or harm any portion of the network during testing
Network testing restricted to IP range specified by ITSSO
ITS Project Deliverables
Provide a summary of findings
Develop a formal project plan

Project Test Plan

The test plan content and format followed the recommendations outlined in documents published by the National Institute of Standards and Technology (NIST) and the Institute for Security and Open Methodologies (ISECOM). Both documents address activities germane to vulnerability scans and penetration testing and served as resources regarding the test plan format, content, and test methodologies utilized during the ITS network project.

NIST's Special Publication 800-115 is part of a series of documents whose purpose is to provide guidance to the computer security industry and to those involved with network security. The NIST commissioned the Information Technology Laboratory (ITL) to write Special Publication 800-115 in order to provide network security practitioners with a proposed guide for network vulnerability assessments (NIST, 2008). Specifically, the NIST charter directs ITL to develop

> [T]ests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. (NIST, 2008)

As reflected in the project test plan, NIST Special Publication 800-115 provided information regarding network host discovery, port analysis, port service identification, and vulnerability scanning. Special Publication 800-115 Appendix B – *Rules of Engagement Template*, and Appendix D - *Remote Access Testing*, provided specific guidance with respect to the ITS network vulnerability scanning methodologies and practices.

The Open Source Security Testing Methodology Manual (OSSTMM), version 3.0, published by the ISECOM was an additional resource. Self advertised as "a peer-reviewed methodology for performing security tests and metrics", the OSSTMM provides information covering multiple aspects of network testing. Specifically, the OSSTMM addresses test topics such as "information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations" (Herzog, 2011).

The content of chapters 2, 6, and 11 of the OSSTMM applied specifically to the project plan for the ITS network. Combined, these chapters provided insight into the definition, scope, common test types, operational test processes, and rules of engagement regarding the ITS network security test.

Test Notification Process.

One project requirement included the notification of project stakeholders at the initiation and at the close of the pending test session. The need for a test notification reflected the ITSSO's concern that a network test might trigger an internal intrusion detection device, or result in network downtime. In either event, the network administrator might spend an inordinate amount of time trying to resolve issues that could result from a sanctioned test activity. To counter this concern, the ITSSO and the author of this paper developed, refined, and implemented the test notification process described below.

Prior to any network scanning or network test action the tester was to complete a Test Notification Form (TNF) supplying the following information:

- The tester's name, phone number and email address at which Regis ITS personnel could reach the tester,
- the IP address of the test host,
- the targeted network IP address, or IP address range,
- the name and version number of the tool(s) used during the test session, and
- the approximate starting time of the test session.

In addition to the above information, the tester was to notify the ITSSO, via a phone text message, at the initiation of the test session and again at the close of the test session.

The test notification process, as it appears in the project test plan, is below and culminates with an example of a completed TNF, as shown in Table 7: *Completed Test Notification Form*.

Test notification process:

1 Fill out your name in the appropriate space

2 Go to a site such as www.whatsmyip.org or www.whatsmyip.com and get your IP address as viewed by the internet. Getting your IP address from a command like ipconfig or ifconfig will provide a private address known only to your ISP.

3 Fill out the network IP address and address range you will be testing. For example, aaa.bbb.ccc.1-30 will target the IP address range 1–30 of the network aaa.bbb.ccc.0.

4 Fill out the name of the tool you will be using for your test.

5 Fill out the tool's revision number

6 Complete the sections regarding the best phone number and email address at which to reach you during your test session.

7 Mail the completed TNF to the following addresses:

- Aaaa@regis.edu;
- ITSO@regis.edu;
- Bbbb@regis.edu;
- Cccc@regis.edu.

8 At the beginning of a test sessions all testers are required to send a phone text to Aaaa at (702) 555-5555 stating your name and your intention to start a test session. An example of an initiating text would be something similar to "Hello Aaaa, This is <tester's first and last name> initiating a test session."

9 Once the tester has completed a test session a closing text must be sent to Aaaa at (702) 555-5555 stating you name and your intention to end a test session. An example of a closing text would be something similar to "Hello Aaaa, This is <tester's first and last name> ending a test session."

An example of a completed form is below:

Table 7: Completed Test Notification Form

Who is doing the PEN Testing:	Student name
What is the source IP address:	xxx.yyy.zzz.115
What address or addresses will be targeted:	aaa.bbb.ccc.0/24
What tool and version will be used:	BackTrack
Version:	Version 5
What is the intended testing time (beginning):	8:30 pm PDT
Phone number where the tester can be reached during the testing:	243 555-5555
Best e-mail address to reach tester:	name123@regis.edu

Project Tools and Resources

The tools and resources used during the test of the ITS network were identical to those used during the CANVAS testing with the following exceptions:

- All testing resources used to test the ITS network were provided by the tester. These resources included computer hardware, software, and internet connections.
- The testing of the network utilized a newer release of the BackTrack OS and security tool set. The public release of BackTrack 5 provided a newer revision of the tool.

Test station configuration.

The computer hardware, software tool set, and internet connection used for the author's test station included the following:

- A Hewlett-Packard Pavilion a250y personal computer configured as follows:
  - Intel P4 3.2 GHz CPU w/Hyper Threading Technology
  - 1 GB Double Data Rate (DDR) memory
  - 200GB hard disk drive (HDD)
  - CD writer and DVD ROM
- BackTrack 5 OS and associated tool set

- Cable-based internet access provided by a local Internet Service Provider (ISP)

Software test tools.

BackTrack is a well-known and widely used open source security framework, which provides a number of tools used for a variety of network and computer security related tasks. Two of these tasks include vulnerability assessments and penetration testing. Additionally, the release of BT5 includes both the Nmap and Metasploit Framework tools.

The choice to use Nmap was the result of the tool's host discovery and port analysis capabilities, but more importantly the following reasons:

- the ability to list the active and responsive host IP addresses
- the OS running on each of the above hosts
- open ports of the hosts
- service identification of the open ports

The choice of Metasploit Framework was due to the tool's ability to execute a suite of automated exploits based on known vulnerabilities. Metasploit also has the ability to use network discovery data generated by Nmap as input to target specific network hosts. The combination of BT5, Nmap, and Metasploit provided a complete tool set, which met all the project objectives.

ITS network assessment and penetration test methodology

The primary object of the project was to determine the vulnerability exposure existing on the ITS network. The project stakeholders jointly agreed that the determination of the network exposure included both a vulnerability assessment and a targeted network penetration test. The network assessment and the resultant testing would occur in three distinct phases, including:

- Host Discovery

- Port analysis
- Penetration testing

The results from the host discovery and port analysis phases would complete the vulnerability assessment requirements, while the results of the penetration testing phase results would confirm the existence of any actual network vulnerability.

Host discovery is the term used to describe the scanning process of finding targets connected to specific network range (Foreman, 2010). As discussed and demonstrated in the CANVAS project discussion, the capabilities of Nmap resulted in Nmap as the author's tool of choice for host discovery.

Port analysis is a combination of OS detection and version detection of port services operating on the open port(s) of an active host. As with host discovery, Nmap provides the capability necessary to meet the port analysis requirements.

Each Nmap scan would address one, or more aspects of the stated deliverables. While the default output for the Nmap tool is the system monitor, a method of saving scan results occurs by redirecting the Nmap output to a text file or by specifying an output file format.

At times, converting the Nmap output into a human readable format requires running the output file through a utility written specifically to convert Nmap output into readable text. A simple PERL script, written by this author, removes unreadable text characters leaving all other information intact. Appendix E is the listing of the PERL script, *replace.plx*. Note that some of the Nmap command outputs displayed in the remainder of this paper have gone through the above conversion process for the sake of readability.

ITS network assessment - host discovery.

The first step in network testing is host discovery. Knowing the active and non-active IP addresses is fundamental to complete network understanding. The output of an Nmap ping scan provides not only a list of the active hosts, but by omission, a list of inactive hosts. As such, the use of an Nmap ping scan is a way to accomplish host discovery.

The command *nmap –sP aaa.bbb.ccc.0/24 > external_ping.txt* specified the ping scan (*-sP*) of the targeted network at *aaa.bbb.ccc.0/24*. The redirection of the output to the file *external_ping.txt* stored the command results allowing further review and analysis.

The ping scan found 89 active hosts on the ITS network. Table 8: *ITS Network Ping Scan Results* is an abbreviated representation of the ping scan output. Appendix F lists the complete result of the ping scan command as executed by the Nmap tool.

Table 8: ITS Network Ping Scan Results

Starting Nmap 5.51 (http://nmap.org) at 2011-06-26 14:31 PDT
Nmap scan report for aaa.bbb.ccc.1
Host is up (0.058s latency).
Nmap scan report for aaa.bbb.ccc.2
Host is up (0.049s latency).
Nmap scan report for www2.regis.edu (aaa.bbb.ccc.33)
Host is up (0.059s latency).

{output cut for the sake of brevity – See Appendix F for complete listing}

Nmap done: 256 IP addresses (89 hosts up) scanned in 17.13 seconds

ITS network assessment - port analysis.

Armed with the knowledge of the active network hosts, the next step included the collection of information necessary for port analysis. Specifically, the required information included:

- operational state of every port of an active host
- software and version providing services on every open port

- OS and version running on each host

Nmap includes command options able to provide each of the above requirements. While individual scans could provide the above requirements, the above requirements resulted from a single scan.

Prior to discussing the command used to collect the above data, note that a complete network vulnerability assessment requires the analysis of all ports on each active network host. Leaving some ports untested while testing others would not provide all information needed for the complete evaluation of a given network. Additionally, omitting the port analysis of any active host could result in the overlooking of network vulnerabilities.

The configuration of computers connected to, and communicating via the internet use the transmission control protocol/internet protocol (TCP/IP) suite of protocols, and require the potential availability of 65,535 ports. While it is theoretically possible to have all 65,535 ports open simultaneously, the common practice is to open only the ports needed for specific communication. To determine which of the 65,535 ports are open on any given host, testing occurs on all ports. The testing of 65,535 ports for each network IP address can require a significant amount of time. To help reduce the time required to analyze all ports of a network range, Nmap provides an option limiting port analysis to specific hosts.

Limiting port analysis to include only active hosts may provide a significant reduction with respect to the time required for the completion of network port analysis. With respect to the ITS network, limiting port analysis to those hosts discovered suing the ping scan reduces the port analysis to 89 known active network hosts (down from 254 possible network hosts). The Nmap option used to leverage this capability is the –iL <filename> option. Using this option will direct Nmap to scan only those IP addresses listed in the named file.

The file *external_up.txt* contains the listing of the 89 ITS network active hosts as determined by the previously run ping scan. Using this file, in conjunction with the *–iL <filename>* option, will limit the port analysis to those IP addresses listed in the file *external_up.txt*.

Table 9 shows a partial listing of the file *external_up.txt* with the full listing of the file in Appendix G.

Table 9: Partial Listing of external_up.txt

aaa.bbb.ccc.1
aaa.bbb.ccc.2
aaa.bbb.ccc.33
aaa.bbb.ccc.34
aaa.bbb.ccc.36
aaa.bbb.ccc.37
aaa.bbb.ccc.38
aaa.bbb.ccc.39
aaa.bbb.ccc.40
aaa.bbb.ccc.41

{output cut for brevity}

aaa.bbb.ccc.218
aaa.bbb.ccc.219
aaa.bbb.ccc.220
aaa.bbb.ccc.222

The Nmap command used to collect the information required for port analysis includes the *–iL <filename>* option, which specifies the scanning of certain IP addresses as listed in the named file. The specific Nmap command follows:

nmap –sS –O –sV –p1-65535 –iL external_up.txt > external_ports_all.txt

The above command

- invokes Nmap *nmap*
- calls the SYN scan *-sS*

- calls remote host fingerprinting *-O*
- calls the version detection option *-sV*
- applies above option to all ports *-p1-65535*
- uses a file as input to scan specific IPs *-iL external_up.txt*
- redirects the output to a specified file *> external_ports_all.txt*

The output of this scan provides each port's operational status, host OS detection/fingerprinting, and port service version detection for all 65,535 ports for each of the 89 known active hosts on the ITS network. This command also redirects its output to the file *external_ports_all.txt* allowing for additional review. Completion of the scan provides all the data meeting the requirements of port analysis. Table 10: *Sample ITS Network Port Analysis Scan Results* is a representative sample of the scan output with Appendix H providing a complete listing of the port scan results.

An analysis of the command results in Table 10 show that the initial three lines include a variety of information pertaining to the host's domain name, IP address, the host's operational state, the observed latency time, and the operational state of the ports not specifically listed with the remainder of the host data.

These three lines of information are common across the results of most Nmap scans and act as a header to the specific host data. A listing of specific ports, the operational state of each listed port, the service running on each port, and the service version, follow the header. Host information concludes with a listing of Nmap's best effort at determining the host's OS, OS version, and device type.

The port's operational status provided by Nmap scan results refer to the state of the port at the time of the scan. Nmap uses six states to describe port operational status defined as follows:

Table 10: Sample ITS Network Port Analysis Scan Result

Nmap scan report for its02.regis.edu (aaa.bbb.ccc.36)
Host is up (0.033s latency).
Not shown: 65520 filtered ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Microsoft ftpd
80/tcp	open	http	Microsoft IIS httpd 7.0
443/tcp	open	ssl/http	Microsoft IIS httpd 7.0
990/tcp	open	ssl/ftp	Microsoft ftpd
4900/tcp	closed	hfcs	
4901/tcp	closed	unknown	
4902/tcp	closed	unknown	

{Output cut for brevity}

4909/tcp	closed	unknown
4910/tcp	closed	unknown

Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

- open – The service operating on an open port is actively accepting transmission control protocol (TCP) connections or user datagram protocol (UDP) packets. In some cases, a TCP wrapper will protect an open port by limiting access to approved IP addresses.
- closed – A closed port is accessible to Nmap in that the port receives an Nmap probe and responds. However, a closed port has no operational, or listening service.

- filtered – Nmap cannot determine if the port is open as packet filtering or other firewall rules block the port.
- unfiltered – Nmap can access the port but is unable to determine if the port is in the open or closed state.
- open|filtered – This state indicates that Nmap sees the port as open, but the port provided no response to an Nmap probe. Since a lack of response could also indicate a filtered port, Nmap is unable to differentiate between a lack of response and a filtered response; it places the port in the open|filtered state.
- closed|filtered – This state indicates that Nmap cannot make the determination between a closed or filtered state.

Note that the port's operational status, in combination with port service and version information, may indicate the presence of one or more vulnerabilities on a given host.

Information specific to device type may also indicate the presence of network or host irregularities. Nmap determined that the host shown in Table 10 has a device type of "general purpose". Other device types found on the ITS network (see Appendix H) include firewall, wireless access point (WAP), broadband router, router, switch, VoIP phone, VoIP adapter, printer, webcam, media device, game console, storage-misc, and remote management. While none of the listed device types identifies specific malicious activity, a device type coupled with an unusual, unauthorized, or unidentified OS or port service, may indicate the need for further investigation.

ITS network automated penetration testing.

While the manual scanning techniques discussed above supported the host discovery and port analysis of the ITS network, there is no direct method of using these scan results to perform

network penetration testing. While Nmap capabilities proved useful for network host discovery and port analysis, the tool has limited penetration-testing capabilities. Instead, the Metasploit Framework was the tool used to perform the penetration testing and network exploitation.

Metasploit has two features that are useful for the penetration testing. These features include Metasploit's ability to automate the execution of exploits and its ability to use database information generated by a third-party tool. Fortunately, Nmap is one of the third-party tools that can populate a database for later use by Metasploit. To use the above features, the tester must first create or select, and then connect to the appropriate database file prior to using any of Metasploit's automated features.

To create or select, and then connect to the database, the following three commands must execute from the Metasploit Framework command line prompt:

- db_driver mysql
- db_connect
- db_connect root:toor@127.0.0.1/<*database filename*>

The *db_driver mysql* command identifies MySQL as the database of choice. While BT5 contains both MySQL and PostgreSQL, familiarity with the former influenced the choice of MySQL for the ITS network penetration testing. The *db_connect* command connects the database to the current instance of the Metasploit Framework, and the *db_connectroot:toor@127.0.0.1/<database filename>* connects the database to the test host.

The use of <*database filename*> will select an existing database, or create a new database file dependant on the existence of the file at the time of the command execution. If the database file exists, subsequent data appends to the existing file. If no file exists, execution of the

command results in the creation of the file. Regardless, the filename chosen for the command is subject to the tester's discretion.

Executing Nmap commands from within Metasploit only requires prefixing *db_* to any valid Nmap command. For example, by prefixing *db_* to the Nmap command below, the command directs the resultant output to the database previously specified by the tester. The command

db_nmap –sP aaa.bbb.ccc.0/24

- invokes Nmap redirecting output to a database db_nmap
- calls the ping scan option -sP
- ping scans the entire network range aaa.bbb.ccc.0/24

As a comparison, the Nmap command used for manual method of host discovery was

nmap –sP aaa.bbb.ccc.0/24 > external_ping.txt

Note that the only difference between the two commands is the lack of the *db_* prefix, and the redirection of the command output (> external_ping.txt) used in the manual version of the command.

The automated version of the port analysis command follows the same format as that of the automated host discovery command. Invoking the automated version of the Nmap command from within the Metasploit Framework is:

db_nmap –sS –O –sV –p1-65535

As with the manual version, the automated version invokes port scanning, version detection, and OS fingerprinting, directing the output to the previously specified database.

The result of the above two Nmap commands is the population of a previously specified database file containing all the host discovery and port analysis information previously discussed

and listed in Appendix F and Appendix H. With the host discovery and port analysis data captured and resident in a database, the automated capabilities of Metasploit could now provide for the execution of the network penetration testing and the attempts at network host exploitation.

Metasploit's *db_autopwn* command takes its input from a database, evaluates the host discovery and port analysis data, and formulates a list of possible host vulnerabilities. The command then uses these vulnerabilities to launch exploits targeted at specific network hosts, host ports, and running port services. If an identified vulnerability proves exploitable, Metasploit will create a Meterpreter session, which in turn, provides a means of intrusion to the network.

A Meterpreter session executes completely out of the host's memory and may provide the intruder the ability to gain control of the compromised host. Host control occurs if the intruder is successful in the execution of various scripts allowing the elevation of the intruder's privilege level to that of root, or system administrator (dependant on the native OS of the compromised host). Elevated privilege levels may also allow the intruder to download or upload files, install a keystroke logger, create a backdoor, install a rootkit, use the compromised host as platform to launch attacks against other network hosts, or any number of other potentially malicious activities. As discussed previously, any compromise to the ITS network during a sanctioned test session requires the tester to cease all test activities and inform the ITSSO of the exploit.

Invoking the automated exploitation capabilities of Metasploit requires the use of the *db_autopwn* and selected command line options. The command launched against the ITS network was:

db_autopwn –p –e –t –I aaa.bbb.ccc.0/24

Specifically, the above command

- invoked the automated capabilities of Metasploit using the connected database as the command input db_autopwn
- selected exploit modules based on open ports -p
- launched exploits against all matched targets -e
- showed all matching exploit modules -t
- only exploited hosts within a given range -I aaa.bbb.ccc.0/24

The result of the above command identified and launched exploits against 15,631 vulnerabilities, spread across the 89 active ITS network hosts. Of the 15,631 vulnerabilities found, none were successful in the exploitation or compromise of any ITS network host.

ITS Network Assessment and Penetration Test Results Summary

The results of the ITS network vulnerability assessment includes the findings of the network host discovery and the host port assessments. Network host discovery found 89 active hosts on the network. The open ports, port services, identified devices, and host operating systems appeared consistent with those of a network designed and maintained to support a diverse group of users. While the port analysis scan did not identify any obvious network vulnerabilities or malicious activity, a review of the scan results indicated that the network usage of a limited number of IP addresses might warrant further investigation.

Security concern criteria.

Several observed aspects of the scan results raised usage and possible security concerns. The identification of any IP addresses, whose scan results raised these concerns, signified a candidate requiring further investigation. Any IP address identified as such exhibited one or more of the following three characteristics:

1) *Any "Device type" that appeared to serve no or little purpose on a business network*. Such a device could be any number of unauthorized devices including entertainment equipment, communication equipment, storage devices, network monitoring equipment, or any of number of other possible devices or equipment installed on the network by a network user. It is likely that any unauthorized device would likely be out of the control of the network administrators in terms of normal device upgrades and regular security software patches. Use of such devices not only include the possible inappropriate use of network resources, but also might provide a means by which outsiders could gain unauthorized access to the network. Additionally, the attachment of such devices might aid the malicious activities of network insiders.

2) *Any IP address for which the list of "Device type" or "OS guesses" appear greater than normal when compared to the results of other IP addresses on the same network.* A large and diverse list indicates that Nmap could not provide a definitive identification of the device type or OS choice at a given IP address. When Nmap is unable to determine the exact OS from a large number of possibilities, the host at the IP warrants further investigation.

3) *Any host who is running an unidentified service or operating system.* While this might not indicate a security weakness, network administrators may want to confirm that the OS operating on these hosts are those intended for the specified IP address.

Ports scan results analysis.

The *Port Analysis Scan Results Summary* in Table 11 is a summary listing of the port analysis results segregated by the above criteria. As can be seen, the following network IP addresses may warrant further investigation:

- aaa.bbb.ccc.196
- aaa.bbb.ccc.198
- aaa.bbb.ccc.199
- aaa.bbb.ccc.203

The flagging of the hosts at IP addresses 196, 198, and 199 are due to the possibility that these addresses may include an unauthorized device, or because OS fingerprinting identified a suspicious OS. Possible devices at these addresses include a switch, wireless access point, printer, webcam, or media device. The possible OS on these addresses include a number of switch, camera, and Tivo operating systems. Additionally, these three network addresses returned information for at least one service not recognized by Nmap. While none of this indicates malicious network activity, the possibility exists regarding the inappropriate use of network resources. Additionally, given the above three addresses met all of the above security concern criteria the addresses warrant the need for further investigation.

The data shown in Table 12: *Possible Network Irregularity* is an edited representation of the data collected from IP address aaa.bbb.ccc.203 (see Appendix H for the full listing of data from IP address aaa.bbb.ccc.203) and is of particular interest from a network security perspective. These findings not only list many of the device types identified as suspicious for the addresses 196, 198, and 199, but also include the additional possible devices types identified as game console, storage-misc, and remote management.

While none of these three devices point to malicious behavior, the presence of a game

Table 11: Port Analysis Scan Results Summary

"Device types" No purpose on network	Device Type / OS Excessive quantity	Unidentified Service or OS
		aaa.bbb.ccc.35
		aaa.bbb.ccc.47
		aaa.bbb.ccc.60
		aaa.bbb.ccc.69
		aaa.bbb.ccc.195
aaa.bbb.ccc.196	aaa.bbb.ccc.196	aaa.bbb.ccc.196
aaa.bbb.ccc.198	aaa.bbb.ccc.198	aaa.bbb.ccc.198
aaa.bbb.ccc.199	aaa.bbb.ccc.199	aaa.bbb.ccc.199
		aaa.bbb.ccc.200
		aaa.bbb.ccc.201
aaa.bbb.ccc.203	aaa.bbb.ccc.203	aaa.bbb.ccc.203
		aaa.bbb.ccc.204
		aaa.bbb.ccc.205
		aaa.bbb.ccc.206
		aaa.bbb.ccc.207
		aaa.bbb.ccc.208
		aaa.bbb.ccc.209
		aaa.bbb.ccc.210
		aaa.bbb.ccc.211
		aaa.bbb.ccc.212
		aaa.bbb.ccc.213
		aaa.bbb.ccc.214
		aaa.bbb.ccc.215
		aaa.bbb.ccc.216
		aaa.bbb.ccc.217
		aaa.bbb.ccc.218
		aaa.bbb.ccc.219
		aaa.bbb.ccc.220

console might be a strong indication regarding the inappropriate use of network resources. Likewise, the presence of a miscellaneous storage device could have a valid use on the network. However, the presence of such a device could also imply the downloading and storage of data unrelated to and unauthorized for network use. Lastly, the presence of a remote management device could indicate unauthorized remote access to the network.

Table 12: Possible Network Irregularity

Nmap scan report for aaa.bbb.ccc.203 Host is up (0.050s latency). Not shown: 65533 filtered ports PORT STATE SERVICE VERSION 80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1) 3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized) 1 service unrecognized despite returning data…… *Output cut* Device type: WAP | general purpose | firewall | game console | storage-misc | switch | remote management | media device Aggressive OS guesses: Netgear DG834G WAP (94%), HP ProCurve MSM422 WAP (93%), Linux 2.4.21 - 2.4.25 (93%), Fortinet FortiGate-60B or -100A firewall (91%), Microsoft Xbox game console (modified, running XboxMediaCenter) (91%)…. TiVo series 1 (Linux 2.1.24-TiVo-2.5) (89%)…

The OS fingerprint data is also of interest. Nmap identified the possibility of a Microsoft Xbox game console OS and, or the possibility of a Tivo OS. As with the other possibilities discussed, either OS may have valid and authorized use on the network. However, the possibilities of their presence meets the criteria listed regarding the need for further identification.

Chapter 4 - Summary and Recommendations

Summary

This report discusses two projects completed during the author's enrollment in the SEAD Practicum at Regis University. Each project was a study of the methodology and tools used for vulnerability assessment and penetration testing of two unique networks. While the networks were diverse with respect to their intended use and function, the tools and methodology during the testing of each project was nearly identical. For each, the vulnerability assessment and penetration testing followed a three-step methodology comprised of host discovery, port analysis, and host exploitation. The tools used in the execution of this methodology included BackTrack, Nmap, and Metasploit.

Host discovery is the term used to describe the process of identifying the active hosts residing on a network. For the purpose of the CANVAS and ITS projects, an active host was any network-connected device capable of responding to a communication request originating from the tester's host.

For the CANVAS project, the communication request originated from a host internal to the responder's network. Conversely, communication requests for the ITS project originated from a host external to the responder's network. The identification or "discovery" of an active host involved sending a communication request to each IP address in the targeted network range and tracking all responses. Nmap's ping scan option proved a quick and effective method of host discovery for both the CANVAS and ITS networks.

Following host discovery was the process of port analysis. Port analysis identifies and evaluates the port status, operating port services, and software revision of all 65,535 ports for each active network host. The port analysis method employed during the CANVAS and ITS

network assessments included the OS fingerprinting and version detection of each active network host. OS fingerprinting is the identification of the operating system (OS) running each active host. Version detection is the determination of the OS revision, service pack, and any software patches included with the OS. Used in conjunction with the host port data, OS fingerprinting and version detection aid in the identification of possible host vulnerabilities.

As with host discovery, Nmap provided the means to collect the port and OS data from each active host on both the CANVAS and ITS networks. Information collected from the CANVAS network showed that both the number of active hosts and the port services operational on the active hosts were minimal. Given that the purpose of the CANVAS network was to provide a platform for a specific competition, the minimalist configuration is understandable.

Conversely, given that the purpose of the ITS network is to support the staff, faculty, and students of Regis University it was not be surprising that the number of port services and the variety of software operating on the ITS network was significantly greater. While the port analysis process identified a minimal number of vulnerabilities on the CANVAS network, the port analysis process identified in excess of 15,000 possible vulnerabilities on the ITS network.

The final process utilized in these projects was that of network penetration testing. Penetration testing uses the vulnerabilities identified via the host discovery and port analysis processes in an attempt to compromise the network and host security defenses. A penetration attempt is successful if the tester is able to compromise the targeted host and establish a running process on the victim. Once the tester establishes a running process on a victim host, the tester will attempt to elevate their privilege to the highest level possible. The goal is to gain “system administrator” or “root” privileges on Windows-based hosts or UNIX/Linux-based hosts respectively by elevating their privilege status to the highest levels. If the tester is successful in

establishing the stated privilege level, they will not only gain complete control over the compromised host but may also be in a position to compromise the entire network. As demonstrated in the discussions specific to each project, host penetration and compromise occurred on the CANVAS network, but proved unsuccessful on the ITS network. This result was not a surprise given the purpose of each network and the nature of each project.

The CANVAS network existed for a cyber competition, the purpose of which was to identify the vulnerabilities that allowed network compromise. Conversely, the ITS network is a fully functioning and operational production network whose primary security goal likely includes the protection of the network from unauthorized access and use. Given the results of the vulnerability assessment and penetration testing of each project, both were successful in meeting their security goals at the time of the tests.

Recommendations

The recommendations resulting from the CANVAS and ITS projects include proposed future guidance regarding network assessment and test methodologies, test tools, tool training, and access to resources. These recommendations are the opinions of the author, and based on the successes, failures, and learning experienced during the CANVAS and ITS projects.

Recommendation 1.

The three-step methodology of host discovery, port analysis, and penetration testing is valid for any project whose goal is the assessment of network vulnerability, or the network's susceptibility to penetration tests.

For both the CANVAS and ITS network projects, the method of host discovery and port analysis proved successful in the identification of active network hosts and the enumeration of possible host vulnerabilities. Additionally, by following the host discovery and port analysis

processes with a penetration test, a network tester is able to determine if the network security measures are sufficient to protect the network hosts from Metasploit and similar penetration tests. As the above three-step process proved valid from both an internal and external network perspective, future testers may want to consider using the processes outlined in this paper for any similar projects.

Recommendation 2.

Consider the use of BackTrack, Nmap, and Metasploit when evaluating tools for network vulnerability assessment or penetration test projects.

The tools used for the security assessments and penetration testing of these networks performed well when used in conjunction with the above methodologies. The Backtrack, Nmap, and Metasploit tools seemed ideally suited for the intent and purpose of the projects. The attractiveness of these tools was not only a result of their performance, but also because each was:

- Free and readily available
- Open source
- Provided for the automated testing of network hosts
- Widely used in the information security and internet technology

Of the attributes listed above, the most significant tool feature includes the support of automated test capabilities. While the advantage of automated test features may not have been apparent during the CANVAS project, the number of hosts resident on the ITS network clearly demonstrated the advantages of automated penetration testing. As the size of the network under test increases, the need for an automated test solution will become more apparent. For any future

network test projects that might benefit from automated testing, project leaders may want to consider leveraging the automated test features of BackTrack, Nmap, and Metasploit.

Recommendation 3.

Investigate the training and tutorial resources outlined in this paper when learning to use BackTrack, Nmap, or Metasploit.

The Metasploit Megaprimer tutorial located at the SecurityTube.net website proved the most informative tutorial found. The Metasploit Megaprimer video series provides the viewer with a systematic demonstration of Backtrack, Nmap, and Metasploit using both manual and automated testing modes. The videos also provide information on how to compromise a host after a successful exploit including how to download files from and upload file to the victim host. The tutorial also provides the viewer with a thorough overview of Metasploit's configuration, Metasploit's theory of operation, and the pairing of Nmap and Metasploit for use when performing network reconnaissance and the execution of automated testing.

Of significant note are the network similarities between the video tutorial and the CANVAS network. These similarities provided the opportunity to view the tutorial on one system while launching exploits against the CANVAS network on another. This method not only provided this author with knowledge specific to the use of BackTrack, Nmap, and Metasploit, but also provided a systematic method to test and exploit the CANVAS and ITS networks.

Web-based education is also available for BackTrack and Nmap. BackTrack training is available online, via live courses, or through the BackTrack Wiki. While both the BackTrack online training and the live courses are fee-based training options, the BackTrack Wiki page

provided all the information needed by this author to complete the testing as described in this paper.

Nmap training is available from the nmap.org website, but the training is limited. For a thorough discussion regarding the capabilities, tool usage, and command options available with Nmap, the publication *NMAP Network Scanning* (Lyon, 2008) is a source worth investigating.

The next three recommendations address resources, which if available to the student tester might provide for a more precise evaluation of network test results as well as increase the knowledge gained by the tester through the completion of a project.

Recommendation 4.

SEAD Practicum students would benefit from a network whose purpose was to allow experimentation with various network test tools and investigative techniques.

The most significant learning experience provided this author was the opportunity to investigate the CANVAS network. The CANVAS project allowed this author to experiment with various network test tools, observing the results of successful and unsuccessful exploitations without the fear of network damage or legal consequences. Additionally, when a host exploit proved successful, further host compromise was possible through the elevation of the attacker's privilege level. In essence, the CANVAS network provided an environment allowing the tester to verify project concepts, test methods, and tool usage. Had the concepts, methods, and tool usage remained unverified, the assessment and testing of the ITS network might have resulted in additional and less answers. The development of a practice network will provide SEAD students a platform on which to test various tools and methods without the fear of network damage or legal repercussions.

Recommendation 5.

Provide a method for the sharing of skills, knowledge, and capabilities between the various practicum classes.

One area where limited knowledge had a negative impact on the outcome of the CANVAS and ITS projects was that of data mining. Even though this author successfully created a database and populated the database with network scan information, efficient use of the database information was not possible. This author lacked the tools and knowledge to evaluate the database information for any possible trends. The identification of data trends might have resulted in the consideration of additional exploit vectors. The availability of a database resource would have proven beneficial for the project.

The recommendation requires the implementation of a method allowing an exchange of knowledge between students from various practicum classes. A possible solution might include a web-based bulletin board listing the projects from the various practicum classes. Project descriptions would include a list of needs in the form of requests for resource support or a call for help with a specific task. It is possible that the availability of this type of resource would have had little impact on the CANVAS or ITS projects. However, a method that encourages the sharing of ideas, projects, and capabilities between the various practicum studies would prove beneficial to everyone involved.

Recommendation 6.

Provide a technical resource experienced with the tools and methods specific to the Practicum project.

While this recommendation may be applicable to any Practicum project, the supporting example for this recommendation is specific to any SEAD group responsible for penetration testing. A resource knowledgeable with the methods, tools, and expected results of network

vulnerability assessments and penetration testing projects would have proven beneficial to the effort. Such a resource could help manage assessment and test methodologies, tool selection, tool usage, result interpretations, and other aspects of the projects.

Unfortunately, no such resource was available during the CANVAS and ITS projects. Instead, team members and stakeholders alike looked to this author for guidance, expertise, and accepted practices regarding network vulnerability assessment and penetration testing. This guidance may have provided a limited benefit to the team members and stakeholders as this author had little prior experience with network vulnerability assessment, penetration testing, or the use of the BackTrack, Nmap, and Metasploit tools. Had a technical resource been available during the CANVAS and ITS projects, guidance with respect to methodology, tool section, results evaluation, or alternative testing may have led the team in a direction more consistent with industry practices.

Recommendation Summary

The recommendations resulting from the CANVAS and ITS projects address the various areas of network security assessment, network test processes, assessment and test tools, tool training, and access to support and technical resources. A summary listing of these recommendations is below:

- Process recommendation: The use of the host discovery, port analysis, and penetration testing process is valid for network vulnerability assessments and/or network penetration test projects.
- Tool recommendation: Consider the use of BackTrack, Nmap, and Metasploit when evaluating tools for any network vulnerability assessment or penetration test projects.

- Tool training recommendation: The Metasploit Megaprimer video tutorial available from SecurityTube.net is a valuable resource for anyone using the methodologies and tools described in this report for network vulnerability assessment and penetration testing. Additionally, the websites specific to Nmap and BackTrack are excellent places to begin a search for training resources specific to each tool.
- Training network recommendation: A network on which students could learn testing methodologies, tools, and results would benefit the practicum students.
- Inter-practicum resource recommendation: A method of sharing knowledge and capabilities between the various practicum projects would be valuable with projects similar to this and allow for the sharing of knowledge and capabilities between the various practicum projects.
- Technical guidance recommendation: Technical resources experienced with industry methodologies and tools used for vulnerability assessment and penetration testing are available to the Pen Test team for consultation and guidance.

The above listings of recommendations provide a balanced approach for the continuation of network security assessments and penetration testing experimentation by SEAD Practicum students. It is the belief of this author that the above recommendations put the burden of learning vulnerability assessment, testing techniques, and methodologies squarely on the shoulders of future students. It is also up to future students to decide if the processes, tools, and training discussed in this paper are valid for their specific projects. Regardless, students will need to be familiar with and understand any process, tool, or training utilized in future projects.

Just as the recommendations regarding the processes, tools, and training point toward future practicum students, the recommendations regarding a training network, the sharing of

inter-practicum resources, and the technical guidance resources point toward the staff and faculty supporting the SEAD Practicum. Resources including an experimentation network, inter-practicum communications, and technical expertise are out of the realm of the student. Instead, these capabilities would best be driven by the staff and, or faculty of Regis University.

References

BackTrack Linux (2011). Roadmap: BackTrack linux – Penetration testing distribution. Retrieved from http://www.backtrack-linux.org/bt/roadmap/

CANVAS student computer security event a success. (2011, May 4). Regis University School of Computer & Information Sciences. Retrieved from http://regis.edu/content/cpcis/pdf/CANVAS%20Success.pdf

Foreman, Park. (© 2010). Vulnerability management. [Books24x7 version] Retrieved from http://common.books24x7.com.dml.regis.edu/toc.aspx?bookid=30514.

freshmeat.net (2011). Welcome to freshmeat.net. Retrieved from http://freshmeat.net/search?q=nmap&submit=Search

Fyodor (1997, September). The Art of port scanning. *Phrack Magazine 7(51).* Retrieved from http://phrack.org/issues.html?issue=51&id=11#article

Herzog, Pete (2011). Open source security testing methodology manual. Retrieved from http://www.isecom.org/osstmm/

Information Security Short Takes (n.d.). *System hardening process checklist.* Retrieved from http://www.shortinfosec.net/2009/01/system-hardening-process-checklist.html

Insecure.org LLC (2004). Nmap. Retrieved from *http://linuxcommand.org/man_pages/nmap1.html*

Internet Engineering Task Force, Network Working Group (1989). *Request for comments 1122. Requirements for internet hosts – Communication layers.* Retrieved from http://tools.ietf.org/html/rfc1122

Linux Journal, December 1, 2001. *Editor's choice awards*. Retrieved from http://www.linuxjournal.com/article/5525

Lyon, Gordon Fyodor, 2008. *NMAP network scanning: Official Nmap project guide to network discovery and security scanning.* Sunnyvale, CA: Insecure.Com LLC

Metasploit (September 17, 2006). *Metasploit 3.0 automated exploitation*. Retrieved from http://blog.metasploit.com/2006/09/metasploit-30-automated-exploitation.html

NIST (2008). *Technical guide to information security testing and assessment*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Nmap (2011). *Nmap free security scanner*. Retrieved from http://nmap.org

Rapid 7, 2011. Download Metasploit. Retrieved from (http://www.metasploit.com/download/)

Red Hat (2005). *Red Hat enterprise Linux 4 security guide.* Retrieved from http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/index.html

Sectools.org (2006). *Top 100 network security tools*. Retrieved from http://sectools.org/

SecurityTube.net (2011). Metasploit Megaprimer. Retrieved from http://www.securitytube.net/groups?operation=view&groupId=8

skape (December, 26, 2004). *Metasploit's Meterpreter.* Retrieved from http://www.nologin.org/Downloads/Papers/meterpreter.pdf

Appendix A: CANVAS Network All Host/All Ports Scan Results

```
This output was created with the command nmap -p0-65535 10.128.128.0/24

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-03-12 14:39 MST
Nmap scan report for 10.128.128.1
Host is up (0.0057s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:00:0C:07:AC:01 (Cisco Systems)

Nmap scan report for 10.128.128.2
Host is up (0.0057s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:07:50:1A:40:C1 (Cisco Systems)

Nmap scan report for 10.128.128.3
Host is up (0.0087s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:05:9B:BF:5E:21 (Cisco Systems)

Nmap scan report for 10.128.128.50
Host is up (0.00018s latency).
All 65536 scanned ports on 10.128.128.50 are filtered
MAC Address: 00:50:56:84:00:16 (VMware)

Nmap scan report for 10.128.128.68
Host is up (0.00039s latency).
Not shown: 65509 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
515/tcp  open  printer
548/tcp  open  afp
1046/tcp open  unknown
1063/tcp open  unknown
1065/tcp open  unknown
1070/tcp open  unknown
1074/tcp open  unknown
```

```
1076/tcp open  sns_credit
1077/tcp open  unknown
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
3459/tcp open  unknown
MAC Address: 00:50:56:84:00:00 (VMware)

Nmap scan report for 10.128.128.69
Host is up (0.00041s latency).
Not shown: 65512 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
515/tcp  open  printer
1042/tcp open  unknown
1062/tcp open  veracity
1065/tcp open  unknown
1072/tcp open  unknown
1084/tcp open  ansoft-lm-2
1723/tcp open  pptp
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
3459/tcp open  unknown
MAC Address: 00:50:56:84:00:1F (VMware)

Nmap scan report for 10.128.128.71
Host is up (0.00050s latency).
All 65536 scanned ports on 10.128.128.71 are filtered
MAC Address: 00:50:56:84:00:19 (VMware)

Nmap scan report for 10.128.128.80
Host is up (0.00036s latency).
All 65536 scanned ports on 10.128.128.80 are closed
MAC Address: 00:50:56:84:00:27 (VMware)

Nmap scan report for 10.128.128.100
Host is up (0.00038s latency).
Not shown: 65517 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
```

```
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
1034/tcp open  zincite-a
1035/tcp open  multidropper
1038/tcp open  unknown
1043/tcp open  boinc
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:50:56:84:00:18 (VMware)

Nmap scan report for 10.128.128.121
Host is up (0.00034s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:84:00:1E (VMware)

Nmap scan report for 10.128.128.122
Host is up (0.00044s latency).
Not shown: 65534 filtered ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:50:56:84:00:24 (VMware)

Nmap scan report for 10.128.128.123
Host is up (0.000014s latency).
All 65536 scanned ports on 10.128.128.123 are closed

Nmap scan report for 10.128.128.124
Host is up (0.00048s latency).
All 65536 scanned ports on 10.128.128.124 are filtered
MAC Address: 00:50:56:84:00:26 (VMware)

Nmap done: 256 IP addresses (13 hosts up) scanned in 1572.98 seconds
```

Appendix B: CANVAS auto test summary - 031811

Sent: Friday, March 18, 2011 7:03 AM
To: H. N., R. C.
Cc: D. L.

Per the plan from Tuesday's Practicum meeting, the following is a summary of the test results from the CANVAS network using the automatic test execution capabilities of Metasploit.

Contact me with any questions you have regarding the findings.

Steve

The automatic test capability of Metasploit was used to test the identified hosts with open ports in the CANVAS network. The command ***db_autopwn –e –p –t –I <target>*** where <*target*> was the IP of each identified host was executed with a summary of the results listed below. The output of the above command yields the number of exploits identified from the Metasploit database and the number of sessions resulting from the execution of the exploits. Note that not all identified hosts could be exploited with the stock Metasploit exploits. For those hosts which were exploited the meterpreter was used to execute a number of commands verifying the compromise.

10.128.128.1 > 1 open port, 4 exploits, 0 sessions.
10.128.128.2 > 1 open port, 4 exploits, 0 sessions.
10.128.128.3 > 1 open port, 4 exploits, 0 sessions.
10.128.128.4 > 1 open port, 4 exploits, 0 sessions.
10.128.128.50 > 4 open ports, 50 exploits, 0 sessions.
10.128.128.68 > 23 open ports, 290 exploits, 5 sessions.
10.128.128.69 > 22 open ports, 290 exploits, 9 sessions.
10.128.128.71 > 2 open ports, 50 exploits, 0 sessions.
10.128.128.72 > 21 open ports, 294 exploits, 6 sessions.
10.128.128.100 > 19 open ports, 186 exploits, 0 sessions.
10.128.128.121 > 1 open port, 106 exploits, 0 sessions.
10.128.128.122 > 2 open ports, 50 exploits, 0 sessions

Appendix C: Canvas testing for 03222011

From Steve Simpson
Sent: Wednesday, March 23, 2011 7:27 PM
To: N, H.; L. D.; J. W.; R. R.;

Automated testing using db_autopwn –p –e –t –I <target>

Heath, Dan,

Per the Canvas meeting of 3/22, exploitation test were run against 3 of the hosts in the CANVAS network with the following results:

10.128.128.68 > 24 open ports, 382 exploits, 0 sessions
10.128.128.69 > 15 open ports, 60 exploits, 9 sessions
10.128.128.72 > 23 open ports, 382 exploits, 0 sessions

I was able to exploit 10.128.1228.69 through the use of the Metasploit automated exploits using the command ***db_autopwn –p –e –t –I 10.128.128.69***. I had the ability to command the system through the exploits but I left the system as I found it (no changes made).

Neither of the other 2 hosts was exploitable using the Metasploit automated exploit command. Both had open ports (as listed above) but neither were exploitable.

Let me know if you have any additional questions or comments.

Steve

Appendix D: ITS Project Test Plan

Document url: https://in2.regis.edu/sites/scis/AAA/BBBB/Cccccc/

1. Introduction

1.1 Purpose

The purpose of this document is to define the Rules of Engagement (ROE) for the vulnerability assessment and penetration testing that will be executed by the Information Assurance (IA) and System Engineering and Application Development (SEAD) Practicum security test team targeting specific Regis University (RU) networks.

1.2 Scope

The scope of this project is limited to the external vulnerability assessment and penetration testing of the following IP network address range:

aaa.bbb.ccc.0/24

The vulnerability assessment and penetration testing of the above network will be conducted by the approved students enrolled in the Regis University Practicum classes, or those authorized by the Regis University Network Security Officer and/or the academic advisor to the IA/SEAD Practicum class.

1.3 Assumptions and Limitations

1.3.1 All testers will use commonly available security tools, or tools approved by Regis University faculty to complete all network vulnerability assessments and penetration testing.

1.3.2 All test equipment and test tools will be supplied by Regis University if possible. In the event that Regis university can not, or will not provide test equipment and tools, the students will be responsible to provide test resources on their own.

1.3.3 All Practicum students executing any vulnerability assessments or penetration testing will be required to complete, and submit the forms included in section 5.1 and follow the Test Notification Form (TNF) submission process outlined in section 5.2.

1.4 Risks

The primary risk with the vulnerability assessment and penetration testing outlined in this plan is the disruption of the Regis University network in it's entirety or any part. For purposes of this plan a disruption is considered any activity that impacts the current capability of the network or any of it's components. If, at any time, the network appears to be at any risk, the tester may be restricted from completing any current or future testing.

1.5 Document Structure

1.5.1 This document contains the following sections

Section 1 – Introduction

1.1 Purpose

1.2 Scope
1.3 Assumptions and Limitation
1.4 Risks
1.5 Document Structure

Section 2 – Logistics
2.1 Personnel
2.2 Test Schedule
2.3 Test Site
2.4 Test Equipment
2.5 Test Tools

Section 3 – Communications
3.1 General Communication
3.2 Incident Handling and response

Section 4 - Target System/Network

Section 5 - Testing Execution
5.1 Volunteer Forms/Procedure
5.2 Test Notification Form/Procedure
5.3 Non Technical Test Components
5.4 Technical Test Components and Test Tools
5.5 Manual Testing
5.6 Automated Testing
5.4 Test Tools
5.5 Test Methodology
5.6 Results Handling

Section 6 - Reporting

Section 7 - Approval Page

2. Logistics

2.1 Personnel

Project stakeholders include the following people:

Aaaaa	ITS Security Officer (ITSSO)	aaaaa@regis.edu
Bbbbb	IA Practicum Advisor	bbbbb@regis.edu
Ddddd	Student security intern	ddddd123@regis.edu

2.2 Test Schedule

Schedules to be negotiated on a term-by-term basis with the project lead, Practicum faculty advisor, and the student test lead. Practicum members change on a regular basis and class student enrollment and student expertise will have a significant impact on the project schedule.

2.3 Test Site

The assumption is that the majority of the vulnerability assessments and penetration testing of the Regis University networks specified in section 1.2 will be conducted from remote locations, e.g. locations where a direct connection to the specified network is not possible. As such, it is assumed that all Practicum students involved in the network tests will launch test execution from any location from which the tester can expect to maintain network access for the length of the test session. Possible test locations includes any Regis campus, the tester's place of employment, the tester's residence, etc.

2.4 Test Equipment

Specific test equipment is not identified for this project. If Regis is to supply the resources necessary to conduct the vulnerability assessment and penetration testing, it is expected that a virtual machine on a specified platform will be used. However, as of this writing no Regis resources have been identified in support of this project. As such, each tester will be required to provide the test equipment and tools necessary to complete the testing.

Any computer hardware available to the tester is approved for use. As long as any equipment used by a tester is capable of establishing and maintain a network connection and can maintain the ability to launch assessments and test scripts from remote locations, the equipment is approved for use. This may include computers whose form factor and capabilities are commonly referred to as server, desktop, laptop, netbook, netpad, etc. Additionally, the operating system (OS) running on any of the above machines may include, but are not limited to Windows, Linux, Apple-OS, or any derivative of the pre-mentioned OS's.

2.5 Test Tools

As with the test equipment requirements, no limitation is being placed on the test tools used to perform the vulnerability assessment and penetration testing. If the tester may use any commercial of proprietary tool to which they have access. The assumption, however, is that most testers will use open source, and commonly available freeware tools for all testing.

This plan specifically discusses the use of the BackTrack OS and suite of security tools included with BackTrack 5 (BT5) including Nmap, and Metasploit. The manual and automated commands listed in Section 5 are command-line invocations of Nmap and Metasploit.

2.5.1 Tool download and training may be found at the following urls:

BackTrack 5 download: http://www.backtrack-linux.org/downloads/
Nmap download (Nmap is include with BT5): http://nmap.org/download
Metasploit download (Metasploit is also included in BT5):
http://metasploit.com/download/

BackTrack 5 training: http://www.backtrack-linux.org/tutorials/

Nmap training: http://nmap.org/bennieston-tutorial/
Metasploit training: http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training

A very good video series that steps the user through the combined use of BT5, Nmap, and Metasploit is found at:
http://www.securitytube.net/groups?operation=view&groupID=8

3. Communication Strategy

3.1 General Communication

The primary means of stakeholder communications will occur via the weekly IA Practicum meeting. This meeting is currently held on Tuesdays at 6:00 pm Mountain Time and is open to all Practicum students and project stakeholders. The Practicum meeting schedule as well as related announcements can be viewed at: https://in2.regis.edu/sites/scis/AAA/BBBB/Cccccc/.

At times additional communications between the stakeholders may be required which may occur through emails, phone or face-to-face conversations, or documents posted on the SEAD SharePoint site found at : https://in2.regis.edu/sites/scis/AAA/BBBB/Cccccc/

3.2 Incident Handling and Response

Should an incident occur at any time during with a tester is conducting an active test session the tester is to cease test execution and contact the ITSSO by phone at the number listed in section5.2 and/or 5.4.

4. Target System/Network

This revision of the test plan covers only the external vulnerability assessment and penetration testing of the network and address range at aaa.bbb.ccc.0/24.

5. Testing Execution

5.1 Volunteer Forms

All testers are required to review, complete (as appropriate), and submit the following forms:

- Criminal Background Policy.pdf
- Volunteer Agreement.pdf
- Volunteer Policy Final.pdf
- Volunteer Services Description.pdf

These forms can be found on the Volunteer Forms folder on the SEAD SharePoint site at : https://in2.regis.edu/sites/scis/AAA/BBBB/Cccccc/

Mail the forms to:

Aaaaaa
Regis University
3333 Regis Blvd. Mail Stop X-1
Denver, CO 80221
O: 303 458-4295
C: 720 810-4612

It is up to each student to complete the volunteer form process as approvals to testing the specified network will not be granted to anyone who has not completed the forms and been approved by Regis University.

5.2 Test Notification Form

The Test Notification Form (TNF) must be filled out and submitted prior to every test sessions. In addition, after completing and submitting a TNF a phone text message must be sent to the ITSSO indicating that a test session is being initiated. Once the test session has completed the tester is required to send a phone text message to the ITSSO indicating that the test session is over.

The TNF is located in same folder as volunteer forms discussed in section 5.1 and the procedure for completing the TNF is listed below:

10 Fill out your name in the appropriate space
11 Go to a site like www.whatsmyip.org or www.whatsmyip.com and get your IP address as viewed by the internet. Getting your IP address from a command like ipconfig or ifconfig will provide a private address which is only known to your ISP.
12 Fill out the network IP address and address range you will be testing. For example aaa.bbb.ccc.1-30 will target the IP address range 1–30 of the network aaa.bbb.ccc.0.
13 Fill out the name of the tool you will be using for your test.
14 Fill out the tool's revision number
15 Complete the sections regarding the best phone number and email address at which you can be reached during your test session.
16 Mail the completed TNF to the following addresses:
- aaaaa@regis.edu;
- ITSO@regis.edu;
- bbbbb@regis.edu;
- ccccc@regis.edu.

17 At the beginning of a test sessions all testers are required to send a phone text to Aaaaa at 702 555-5555 stating your name and your intension to start a test session. An example of a initiating text would be something similar to: "Hello Aaaaa, This is <tester's first and last name> initiating a test session."

18 Once the tester has completed a test sessions a closing session text must be sent to Aaaaa at 702 555-5555 stating you name and your intension to end a test sessions. An example of a closing text would be something similar to: "Hello Aaaaa, This is <tester's first and last name> ending a test session."

An example of a completed form is below:

Who is doing the PEN Testing:	Student Name
What is the source IP Address:	xxx.yyy.zzz.115
What address or address range will be targeted:	aaa.bbb.ccc.1-30
What tool and version will be used:	BackTrack
Version:	5
What is the intended testing time (beginning):	8:30 pm PDT
Phone number where the tester can be reached, if necessary, during the testing:	253 555-5555
Best e-mail address to reach tester:	name123@regis.edu

5.3 Non-technical Test Components

The following websites provide a number of security testing and related information which may prove useful to testers following this test plan or information security personnel in general.

The Security Technical Implementation Guide (STIG) website home provides configuration standards for DOD IA and IA-enabled devices/systems testing. The STIGs and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems and may provide assistance in establishing guidance for the vulnerability assessment and PT testing as part of this test plan: http://iase.disa.mil/stigs/

The NIST Special Publication 800-115 is part of a series of documents which provides guidance to the computer security industry and includes collaborative activities with the security industry, government, and academic organizations. The NIST Special Publication 800-115 provides specific and useful information regarding network discovery, port and service identification, and vulnerability scanning. The NIST document can be found at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

The Open Source Security Testing Methodology Manual (OSSTMM), version 3.0 published by the ISECOM, contains five main sections providing testing information with regards to data controls, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and other topics that could be useful to the vulnerability assessor and PT tester. Chapters 2, 6, and 11 provide information regarding operational test processes such as the enumeration of hosts, ports and services as well as background pertaining to network access, controls, and configuration. The OSSTMM is located at http://www.isecom.org/osstmm/

5.4 Technical Test Components and Test Tools

BackTrack5 (BT5) will be the primary framework and tool set used for the assessment and testing of the defined networks. BackTrack is a well known and widely used open source security framework that provides a number of assessment and penetration tools used for digital forensics, vulnerability assessments, and penetration testing. Specific tools included in the BackTrack framework and used for vulnerability assessment and penetration testing include Nmap and Metasploit.

The network vulnerability assessment will utilize the Nmap security tool found within BT5. Various command line options will be chosen to allow Nmap to determine the following:

- IP addresses of the active hosts on the specified networks,
- The OS of the above hosts,
- Open ports of the hosts, and
- Service identification of the open ports

Network penetration testing will utilize the Metasploit Framework found within BT5. Metasploit contains a significant number of pre-tested exploits that are known to be effective against numerous vulnerabilities. Vulnerabilities identified by Nmap will be the first penetration targets. The results of each penetration test will be recorded as to the port(s) and/or service(s) through which the compromise occurred.

The combined network vulnerability assessment and penetration testing will be conducted in three phases including:

- Host Discovery
- Port scanning, version detection, and OS fingerprinting
- Penetration testing and exploitation

Tools and commands for each of the above phases are listed below.

5.6 Manual Testing

5.6.4 Manual Host Discovery Tool and Command

The Nmap command to be used for host discovery is:

nmap –sP aaa.bbb.ccc.0/24 > external_ping.txt

The above command

• invokes Nmap	nmap
• calls the ping scan option	-sP
• ping scans the entire network range	aaa.bbb.ccc.0/24
• redirects the output to a specified file	> external_ping.txt

The file is to be stored on the tester’s computer and available for retrieval at a later date.

5.6.3 Manual Port Scanning Tool and Command

The Nmap command to be used for port scanning, version detection, and OS fingerprinting is:

nmap –sS –O –sV –p1-65535 –L external_up.txt > external_ports_all.txt

The above command

- invokes Nmap — nmap
- calls the TCP SYN scan — -sS
- calls remote host fingerprinting — -O
- calls the version detection option — -sS
- applies above option to all ports — -p1-65535
- uses a file as input to scan specific IPs — -L external_up.txt
- redirects the output to a specified file — > external_porrs_all.txt

5.5.3 Manual Penetration Testing Tool and Command

No manual penetration testing is expected for this test as the expected number of network hosts will make manual testing in-efficient. See the section on automated testing for information regarding penetration testing.

5.6 Automated Testing

5.6.1 Database Creation

The automated capabilities of the Metasploit Frame allows for it's input to come from a database. The database used must be created prior to the call any automated command call to Metasploit. To create a database for use by Metasploit, start the Metasploit Framework tool and enter the following from the Metasploit Framework command line prompt:

db_driver mysql
db_connect
db_connect root:toor@127.0.0.1/*db_filename*

The above commands will tell Metasploit to

Use the mysql database driver db_driver mysql
Connect the to a database db_connectroot:toor@127.0.0.1/*db_filename*

The database filename (*db_filename*) may be any name chosen by the tester. The tester may connect to an existing database by using the existing database name in place of *db_filename*. If no database of a given name exists at the time the command is invoked, a database will be created and Metasploit will connect to the named database.

Once the tester is through with the database the data base can be erased using the command; db_destroy root:toor@127.0.0.1/*db_filename*

5.6.2 Automated Host Discovery using Nmap from within Metasploit

The output of any Nmap command can be directed to a database from within Metasploit. Using the database created in the step 5.6.1, enter the following command to perform network host discovery and direct the output into the database from the Metasploit command-line prompt:

db_nmap –sP aaa.bbb.ccc.0/24

The above command

- invokes Nmap dumping output to a database db_nmap
- calls the ping scan option -sP
- ping scans the entire network range aaa.bbb.ccc.0/24

5.6.3 Automated Port Scanning Tool and Command

The Nmap command to be used for port scanning, version detection, and OS fingerprinting is:

db_nmap –sS –O –sV –p1-65535

The above command

- invokes Nmap using the existing database data as input regarding the active IP host addresses and dumping output to a database db_nmap
- calls the TCP SYN scan -sS
- calls remote host fingerprinting -O
- calls the version detection option -sS
- applies above option to all ports -p1-65535

5.6.4 Automated Penetration Testing tool and Command

The automated capabilities of Metasploit will use the database to which the Metasploit session is currently attached as input for the command. If the command is successful a Meterpreter session will be opened. The tester can then gain access to the compromised host through one of the associated Meterpreter sessions. Consult the training urls in section 2.5 – Test Tools

To invoke the automated capabilities of Metasploit, execute the following command from the Metasploit Framework command line:

db_autopwn –p –e –t –I aaa.bbb.ccc.0/24

The above command

- invoke the autopwn capabilities of Metasploit using the connected database as the command input db_autopwn
- select modules based on open ports -p
- launch exploits against all matched targets -e
- show all matching exploit modules -t
- only exploit hosts inside this range -I [range]

5.7 Data Handling

At this time data handling and storage will be left to the discretion of the tester. At a future time and under the guidance of the Pen Test lead data may be stored in a specified format on the Regis University SEAD SharePoint site.

6 Reporting

The summary report will include a minimum of the open/active IP addresses found on the Regis ITS network, a summary of the port scan and OS finger printing, and a summary of the exploitation result s of the network.

7 Approval Page

_____/_____
aaaaaaaa - Regis University ITS Security Officer / Date

_____/_____
bbbbbbbb – Faculty Advisor / Date

_____/_____
cccccccc – Project Lead SEAD Practicum / Date

Appendix E: ITS Network Ping Results

Starting Nmap 5.51 (http://nmap.org) at 2011-10-07 12:26 Pacific Daylight Time
Nmap scan report for aaa.bbb.ccc.1
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.2
Host is up (0.031s latency).
Nmap scan report for www2.regis.edu (aaa.bbb.ccc.33)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.34
Host is up (0.031s latency).
Nmap scan report for exchange2.regis.edu (aaa.bbb.ccc.35)
Host is up (0.031s latency).
Nmap scan report for its02.regis.edu (aaa.bbb.ccc.36)
Host is up (0.031s latency).
Nmap scan report for its02.regis.edu (aaa.bbb.ccc.37)
Host is up (0.031s latency).
Nmap scan report for academic.regis.edu (aaa.bbb.ccc.38)
Host is up (0.031s latency).
Nmap scan report for its39.regis.edu (aaa.bbb.ccc.39)
Host is up (0.046s latency).
Nmap scan report for ereserves.regis.edu (aaa.bbb.ccc.40)
Host is up (0.031s latency).
Nmap scan report for its-17.regis.edu (aaa.bbb.ccc.41)
Host is up (0.031s latency).
Nmap scan report for insite.regis.edu (aaa.bbb.ccc.43)
Host is up (0.047s latency).
Nmap scan report for producer.regis.edu (aaa.bbb.ccc.44)
Host is up (0.032s latency).
Nmap scan report for stream.regis.edu (aaa.bbb.ccc.45)
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.47
Host is up (0.047s latency).
Nmap scan report for epicor.regis.edu (aaa.bbb.ccc.49)
Host is up (0.047s latency).
Nmap scan report for its22.regis.edu (aaa.bbb.ccc.51)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.54
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.55
Host is up (0.031s latency).
Nmap scan report for mail1.regis.edu (aaa.bbb.ccc.56)
Host is up (0.047s latency).
Nmap scan report for update.regis.edu (aaa.bbb.ccc.57)
Host is up (0.047s latency).
Nmap scan report for web-classrooms.regis.edu (aaa.bbb.ccc.58)

Host is up (0.031s latency).
Nmap scan report for selfhelp.regis.edu (aaa.bbb.ccc.59)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.60
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.61
Host is up (0.031s latency).
Nmap scan report for communicator.regis.edu (aaa.bbb.ccc.66)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.67
Host is up (0.047s latency).
Nmap scan report for sip.regis.edu (aaa.bbb.ccc.69)
Host is up (0.047s latency).
Nmap scan report for ocswebconf.regis.edu (aaa.bbb.ccc.72)
Host is up (0.047s latency).
Nmap scan report for ocsavedge.regis.edu (aaa.bbb.ccc.73)
Host is up (0.047s latency).
Nmap scan report for spslcalc.regis.edu (aaa.bbb.ccc.75)
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.77
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.78
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.97
Host is up (0.031s latency).
Nmap scan report for in2.regis.edu (aaa.bbb.ccc.98)
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.99
Host is up (0.047s latency).
Nmap scan report for www.regis.edu (aaa.bbb.ccc.100)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.101
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.102
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.103
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.104
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.105
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.106
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.107
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.108

Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.109
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.110
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.111
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.112
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.113
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.114
Host is up (0.031s latency).
Nmap scan report for singtest.regis.edu (aaa.bbb.ccc.115)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.116
Host is up (0.047s latency).
Nmap scan report for maila.regis.edu (aaa.bbb.ccc.120)
Host is up (0.031s latency).
Nmap scan report for mailb.regis.edu (aaa.bbb.ccc.121)
Host is up (0.047s latency).
Nmap scan report for mailc.regis.edu (aaa.bbb.ccc.122)
Host is up (0.031s latency).
Nmap scan report for maild.regis.edu (aaa.bbb.ccc.123)
Host is up (0.031s latency).
Nmap scan report for maile.regis.edu (aaa.bbb.ccc.124)
Host is up (0.031s latency).
Nmap scan report for antispam.regis.edu (aaa.bbb.ccc.125)
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.161
Host is up (0.047s latency).
Nmap scan report for vpn.regis.edu (aaa.bbb.ccc.164)
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.193
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.194
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.195
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.196
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.198
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.199
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.200

Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.201
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.202
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.203
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.204
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.205
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.206
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.207
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.208
Host is up (0.033s latency).
Nmap scan report for aaa.bbb.ccc.209
Host is up (0.033s latency).
Nmap scan report for aaa.bbb.ccc.210
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.211
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.212
Host is up (0.035s latency).
Nmap scan report for aaa.bbb.ccc.213
Host is up (0.043s latency).
Nmap scan report for aaa.bbb.ccc.214
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.215
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.216
Host is up (0.033s latency).
Nmap scan report for aaa.bbb.ccc.217
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.218
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.219
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.220
Host is up (0.045s latency).
Nmap scan report for aaa.bbb.ccc.222
Host is up (0.031s latency).
Nmap done: 256 IP addresses (89 hosts up) scanned in 17.13 seconds

Appendix F: File listing of *external_up.txt*

aaa.bbb.ccc.1
aaa.bbb.ccc.2
aaa.bbb.ccc.33
aaa.bbb.ccc.34
aaa.bbb.ccc.36
aaa.bbb.ccc.37
aaa.bbb.ccc.38
aaa.bbb.ccc.39
aaa.bbb.ccc.40
aaa.bbb.ccc.41
aaa.bbb.ccc.43
aaa.bbb.ccc.44
aaa.bbb.ccc.45
aaa.bbb.ccc.47
aaa.bbb.ccc.49
aaa.bbb.ccc.51
aaa.bbb.ccc.54
aaa.bbb.ccc.55
aaa.bbb.ccc.56
aaa.bbb.ccc.57
aaa.bbb.ccc.58
aaa.bbb.ccc.59
aaa.bbb.ccc.60
aaa.bbb.ccc.61
aaa.bbb.ccc.66
aaa.bbb.ccc.67
aaa.bbb.ccc.69
aaa.bbb.ccc.72
aaa.bbb.ccc.73
aaa.bbb.ccc.75
aaa.bbb.ccc.77
aaa.bbb.ccc.78
aaa.bbb.ccc.97
aaa.bbb.ccc.98
aaa.bbb.ccc.99
aaa.bbb.ccc.100
aaa.bbb.ccc.101
aaa.bbb.ccc.102
aaa.bbb.ccc.103
aaa.bbb.ccc.104
aaa.bbb.ccc.105
aaa.bbb.ccc.106
aaa.bbb.ccc.107
aaa.bbb.ccc.108

aaa.bbb.ccc.109
aaa.bbb.ccc.110
aaa.bbb.ccc.111
aaa.bbb.ccc.112
aaa.bbb.ccc.113
aaa.bbb.ccc.114
aaa.bbb.ccc.115
aaa.bbb.ccc.116
aaa.bbb.ccc.120
aaa.bbb.ccc.121
aaa.bbb.ccc.122
aaa.bbb.ccc.123
aaa.bbb.ccc.124
aaa.bbb.ccc.125
aaa.bbb.ccc.161
aaa.bbb.ccc.164
aaa.bbb.ccc.193
aaa.bbb.ccc.194
aaa.bbb.ccc.195
aaa.bbb.ccc.196
aaa.bbb.ccc.198
aaa.bbb.ccc.199
aaa.bbb.ccc.200
aaa.bbb.ccc.201
aaa.bbb.ccc.202
aaa.bbb.ccc.203
aaa.bbb.ccc.204
aaa.bbb.ccc.205
aaa.bbb.ccc.206
aaa.bbb.ccc.207
aaa.bbb.ccc.208
aaa.bbb.ccc.209
aaa.bbb.ccc.210
aaa.bbb.ccc.211
aaa.bbb.ccc.212
aaa.bbb.ccc.213
aaa.bbb.ccc.214
aaa.bbb.ccc.215
aaa.bbb.ccc.216
aaa.bbb.ccc.217
aaa.bbb.ccc.218
aaa.bbb.ccc.219
aaa.bbb.ccc.220
aaa.bbb.ccc.222

Appendix G: ITS Port Analysis Scan Results – Complete Listing

The following output is the result of the command:
nmap -sP -O -sV -p1-65535 -iL external_up.txt > external_ports_all.txt

Starting Nmap 5.51 (http://nmap.org) at 2011-10-07 13:38 Pacific Daylight Time
Nmap scan report for aaa.bbb.ccc.1
Host is up (0.032s latency).
Not shown: 65529 closed ports
PORT STATE SERVICE VERSION
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: broadband router|router|switch|WAP
Running: Cisco embedded, Cisco IOS 12.X|15.X
OS details: Cisco 827H ADSL router, Cisco 870 router or 2960 switch (IOS 12.2 - 12.4), Cisco Aironet 1250 WAP (IOS 12.4), Cisco C7200 router (IOS 15)

Nmap scan report for aaa.bbb.ccc.2
Host is up (0.034s latency).
Not shown: 65525 closed ports
PORT STATE SERVICE VERSION
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
2001/tcp open telnet Cisco router
4001/tcp open tcpwrapped
6001/tcp open jdwp
9001/tcp open tcpwrapped
Device type: WAP
Running: Cisco IOS 12.X
OS details: Cisco Aironet 1250 WAP (IOS 12.4)
Network Distance: 12 hops
Service Info: OS: IOS; Device: router

Nmap scan report for www2.regis.edu (aaa.bbb.ccc.33)
Host is up (0.043s latency).
All 65535 scanned ports on www2.regis.edu (aaa.bbb.ccc.33) are filtered

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|firewall|general purpose
Running: Cisco embedded, SonicWALL embedded, Sun Solaris 10|9
OS details: Cisco Unified Communications Manager VoIP gateway, SonicWALL Aventail EX-1500 SSL VPN appliance, Sun Solaris 10, Sun Solaris 10 (SPARC), Sun Solaris 9 (SPARC)

Nmap scan report for aaa.bbb.ccc.34
Host is up (0.043s latency).
All 65535 scanned ports on aaa.bbb.ccc.34 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|general purpose|firewall
Running: Cisco embedded, IBM i5/OS V5, IBM z/OS, Linux 2.6.X, SonicWALL embedded
OS details: Cisco Unified Communications Manager VoIP gateway, IBM i5/OS V5R3M0, IBM z/OS v1r8, Linux 2.6.15-28-amd64-server (Ubuntu, x86_64, SMP), Linux 2.6.18.pi (x86), SonicWALL Aventail EX-1500 SSL VPN appliance

Nmap scan report for exchange2.regis.edu (aaa.bbb.ccc.35)
Host is up (0.038s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd
443/tcp open ssl/http Apache httpd
444/tcp open ssl/snpp?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port444-TCP:V=5.51%T=SSL%I=7%D=10/7%Time=4E8F76D7%P=i686-pc-windows-win
SF:dows%r(GetRequest,1A98,"HTTP/1\.1\x20200\x20OK\nDate:\x20Fri,\x207\x20O
SF:ct\x202011\x2022:01:59\x20GMT\nServer:\x20III\x20100\nPragma:\x20no-cac
SF:he\nSet-Cookie:\x20III_EXPT_FILE=aa364;\x20path=/;\x20domain=;\x20path=
SF:/\nSet-Cookie:\x20III_SESSION_ID=8f4adc626ec307eca4db31acf62d9d95;\x20p
SF:ath=/\nSet-Cookie:\x20SESSION_SCOPE=3;\x20path=/\nContent-Type:\x20text
SF:/html\nExpires:\x20Fri,\x207\x20Oct\x202011\x2022:01:59\x20GMT\nCache-c
SF:ontrol:\x20no-cache\n\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtml\
SF:"\x20xml:lang=\"en\"\x20lang=\"en\">\n<!--\x20Rel\x202007\x20\"Skyline\
SF:"\x20Example\x20Set\x20-->\n<!--\x20This\x20File\x20Last\x20Changed:\x2
SF:0June\x202011\x20-->\n<head>\n<link\x20rel=\"stylesheet\"\x20type=\"tex
SF:t/css\"\x20href=\"/scripts/ProStyles\.css\"\x20/>\n<link\x20rel=\"style
SF:sheet\"\x20type=\"text/css\"\x20href=\"/screens/styles\.css\"\x20/>\n<s
SF:cript\x20language=\"JavaScript\"\x20type=\"text/javascript\"\x20src=\"/
SF:scripts/elcontent\.js\"></script>\n<script\x20language=\"JavaScript\"\x
SF:20type=\"text/javascript\"\x20src=\"/scripts/common\.js\"></script>\n<s
SF:cript\x20language=\"JavaScript\"\x20type=\"text/javascript\"\x20src=\"/
SF:scripts/webbridge\.js\"></script>")%r(FourOhFourRequest,D1,"HTTP/1\.1\x
SF:20404\x20Not\x20Found\nServer:\x20III\x20100\nMIME-version:\x201\.0\nCo

SF:ntent-Type:\x20\x20text/html\n\n<HEAD><TITLE>404\x20Not\x20Found</TITLE
SF:></HEAD>\n<BODY><H1>404\x20Not\x20Found</H1>The\x20requested\x20URL\x20
SF:was\x20not\x20found\x20on\x20this\x20server\.\n</BODY>\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Sun Solaris 9|10|5.X (92%), Sun OpenSolaris (88%)
Aggressive OS guesses: Sun Solaris 9 (SPARC) (92%), Sun Solaris 9 or 10 (SPARC) (90%), Sun Solaris 10 (SPARC) (89%), Sun Solaris 9 or 10, or OpenSolaris 2009.06 snv_111b (88%), Sun Solaris 5.10 (85%), Sun Solaris 10 (85%), Sun Solaris 9 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for its02.regis.edu (aaa.bbb.ccc.36)
Host is up (0.033s latency).
Not shown: 65520 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
80/tcp open http Microsoft IIS httpd 7.0
443/tcp open ssl/http Microsoft IIS httpd 7.0
990/tcp open ssl/ftp Microsoft ftpd
4900/tcp closed hfcs
4901/tcp closed unknown
4902/tcp closed unknown
4903/tcp closed unknown
4904/tcp closed unknown
4905/tcp closed unknown
4906/tcp closed unknown
4907/tcp closed unknown
4908/tcp closed unknown
4909/tcp closed unknown
4910/tcp closed unknown
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for its02.regis.edu (aaa.bbb.ccc.37)
Host is up (0.031s latency).
All 65535 scanned ports on its02.regis.edu (aaa.bbb.ccc.37) are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: VoIP adapter|firewall|general purpose
Running: Cisco embedded, SonicWALL embedded, Sun Solaris 10|9
OS details: Cisco Unified Communications Manager VoIP gateway, SonicWALL Aventail EX-1500 SSL VPN appliance, Sun Solaris 10, Sun Solaris 10 (SPARC), Sun Solaris 9 (SPARC)

Nmap scan report for academic.regis.edu (aaa.bbb.ccc.38)
Host is up (0.033s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
25/tcp open tcpwrapped
80/tcp open http Microsoft IIS httpd
110/tcp closed pop3
443/tcp open ssl/http Microsoft IIS httpd 6.0
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for its39.regis.edu (aaa.bbb.ccc.39)
Host is up (0.067s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp closed http
443/tcp closed https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose
Running (JUST GUESSING): SonicWALL embedded (91%), OpenBSD 4.X (87%), DEC Digital UNIX 5.X (87%), FreeBSD 6.X|8.X (86%), Apple Mac OS X 10.6.X (85%), Microsoft Windows 2003|NT (85%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (91%), OpenBSD 4.6 (87%), OpenBSD 4.7 (87%), DEC Digital UNIX 5.X (87%), FreeBSD 6.2-RELEASE-p2 (pf with scrub enabled) (86%), FreeBSD 8.0-CURRENT (86%), OpenBSD 4.2 (86%), OpenBSD 4.3 (86%), Apple Mac OS X 10.6.2 (Snow Leopard) (Darwin 10.2.0) (85%), Microsoft Windows Small Business Server 2003 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for ereserves.regis.edu (aaa.bbb.ccc.40)
Host is up (0.045s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp closed https
3389/tcp open microsoft-rdp Microsoft Terminal Service

Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for its-17.regis.edu (aaa.bbb.ccc.41)
Host is up (0.034s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for insite.regis.edu (aaa.bbb.ccc.43)
Host is up (0.037s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (85%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for producer.regis.edu (aaa.bbb.ccc.44)
Host is up (0.032s latency).
Not shown: 65528 filtered ports
PORT STATE SERVICE VERSION
80/tcp closed http
443/tcp closed https
3389/tcp open microsoft-rdp xrdp
4073/tcp open unknown

8143/tcp closed unknown
8170/tcp closed unknown
8171/tcp closed unknown
Device type: general purpose|phone
Running (JUST GUESSING): Apple Mac OS X 10.5.X|10.6.X (92%), Apple iOS 4.X (88%), Apple iPhone OS 3.X (85%)
Aggressive OS guesses: Apple Mac OS X 10.5.2 - 10.6.2 (Leopard - Snow Leopard) (Darwin 9.2.0 - 10.2.0) (92%), Apple Mac OS X 10.5.5 - 10.6.1 (Leopard - Snow Leopard) (Darwin 9.5.0 - 10.0.0) (89%), Apple Mac OS X 10.5 - 10.6.3 (Leopard - Snow Leopard) or iOS 4.0 - 4.1 (Darwin 9.0.0b5 - 10.2.0) (88%), Apple Mac OS X 10.5.3 - 10.5.4 (Leopard) (Darwin 9.3.0 - 9.4.0) (88%), Apple Mac OS X 10.5.4 (Leopard) (Darwin 9.4.0) (87%), Apple Mac OS X 10.5.5 (Leopard) (Darwin 9.5.0) (87%), Apple Mac OS X 10.6.3 (Snow Leopard) (Darwin 10.3.0) (86%), Apple Mac OS X 10.5 (Leopard) (Darwin 9.0.0b4, x86) (86%), Apple iPhone mobile phone (iPhone OS 3.0 - 3.2.1, Darwin 10.0.0d3) (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for stream.regis.edu (aaa.bbb.ccc.45)
Host is up (0.032s latency).
Not shown: 65529 filtered ports
PORT STATE SERVICE VERSION
80/tcp open rtsp Helix Mobile Server rtspd 14.0.0.348
554/tcp open rtsp Helix Mobile Server rtspd 14.0.0.348
1755/tcp open wms?
7070/tcp closed realserver
8000/tcp open shoutcast SHOUTcast server 1.9.8
8080/tcp closed http-proxy
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.47
Host is up (0.041s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
419/tcp open ftp
422/tcp closed ariel3
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port419-TCP:V=5.51%I=7%D=10/7%Time=4E8F7E21%P=i686-pc-windows-windows%r
SF:(NULL,1A,"220\x20welcome\x20to\x20ftp\x20world\r\n")%r(GenericLines,26,
SF:"220\x20welcome\x20to\x20ftp\x20world\r\n501\x20Error\x20\r\n")%r(Help,
SF:1A,"220\x20welcome\x20to\x20ftp\x20world\r\n")%r(SMBProgNeg,26,"220\x20
SF:welcome\x20to\x20ftp\x20world\r\n501\x20Error\x20\r\n");

Device type: broadband router
Running (JUST GUESSING): XAVi embedded (85%)
Aggressive OS guesses: XAVi 7001 DSL modem (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: welcome

Nmap scan report for epicor.regis.edu (aaa.bbb.ccc.49)
Host is up (0.043s latency).
All 65535 scanned ports on epicor.regis.edu (aaa.bbb.ccc.49) are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|firewall|general purpose
Running: Cisco embedded, SonicWALL embedded, Sun Solaris 10|9
OS details: Cisco Unified Communications Manager VoIP gateway, SonicWALL Aventail EX-1500 SSL VPN appliance, Sun Solaris 10, Sun Solaris 10 (SPARC), Sun Solaris 9 (SPARC)

Nmap scan report for its22.regis.edu (aaa.bbb.ccc.51)
Host is up (0.036s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd
443/tcp open ssl/http Microsoft IIS httpd 6.0
8080/tcp closed http-proxy
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.54
Host is up (0.044s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
25/tcp closed smtp
80/tcp open http Microsoft IIS httpd
443/tcp open ssl/http Microsoft IIS httpd 6.0
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (87%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (87%), Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.55
Host is up (0.047s latency).

Not shown: 65530 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco VPN Concentrator SSHd (protocol 1.5)
80/tcp open http Cisco VPN Concentrator http config
443/tcp open ssl/http Cisco VPN Concentrator http config
1723/tcp open pptp Cisco Systems, Inc. (Firmware: 1025)
10000/tcp open snet-sensor-mgmt?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: router
Running (JUST GUESSING): Juniper embedded (85%)
Aggressive OS guesses: Juniper Networks ERX-700 router (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: Remote; Device: terminal server

Nmap scan report for mail1.regis.edu (aaa.bbb.ccc.56)
Host is up (0.057s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp closed https
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for update.regis.edu (aaa.bbb.ccc.57)
Host is up (0.037s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
443/tcp open ssl/http Microsoft IIS httpd 6.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for web-classrooms.regis.edu (aaa.bbb.ccc.58)
Host is up (0.036s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd
4445/tcp closed upnotifyp
4568/tcp closed unknown
8900/tcp open http Microsoft IIS httpd
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (87%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (87%), Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for selfhelp.regis.edu (aaa.bbb.ccc.59)
Host is up (0.043s latency).
Not shown: 65521 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.0
443/tcp closed https
990/tcp open ssl/ftp Microsoft ftpd
4900/tcp closed hfcs
4901/tcp closed unknown
4902/tcp closed unknown
4903/tcp closed unknown
4904/tcp closed unknown
4905/tcp closed unknown
4906/tcp closed unknown
4907/tcp closed unknown
4908/tcp closed unknown
4909/tcp closed unknown
4910/tcp closed unknown
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008 (85%)
Aggressive OS guesses: Microsoft Windows Server 2008 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.60
Host is up (0.035s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http?
443/tcp open ssl/http VMware View Manager httpd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :

SF-Port80-TCP:V=5.51%I=7%D=10/7%Time=4E8F8A36%P=i686-pc-windows-windows%r(
SF:GetRequest,92B,"HTTP/1\.1\x20505\x20HTTP\x20Version\x20Not\x20Supported
SF:\r\nDate:\x20Fri,\x2007\x20Oct\x202011\x2023:24:37\x20GMT\r\nContent-Le
SF:ngth:\x202220\r\nContent-Type:\x20text/html\r\n\r\n<html>\r\n<head>\r\n
SF:\x20\x20\x20\x20<title>VMware\x20VDM\x20Web\x20Access</title>\r\n\x20\x
SF:20\x20\x20<link\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20href=\"/e
SF:rror/base\.css\"\x20/>\r\n\x20\x20\x20\x20<script\x20language=\"JavaScr
SF:ipt\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20function\x20toggleError\(\)\r
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20var\x20errorElement\x20=\x20document\.getElementById\('
SF:fullErrorStack'\);\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20i
SF:f\x20\(errorElement\x20&&\x20errorElement\.style\.display\x20==\x20'non
SF:e'\)\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20errorElement\.sty
SF:le\.display=\"block\";\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20}\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20else\r\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20errorElement\.style\.display=\"n
SF:one\";\x20\x20\x20\x20\x20\x20\x20\x20\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\x20\x20}\r\n\r\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20function\x20escapeHTML\x20\(str\)\r\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20var\x20div\x20=\x20document\.createElement\('div'\);\r\n\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20var\x20text\x20=\x20document\.cr
SF:eateTextNode\(str\);\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0div\.appendChild\(text\);\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20return\x20div\.inn")%r(HTTPOptions,92B,"HTTP/1\.1\x20505\x20HTTP
SF:\x20Version\x20Not\x20Supported\r\nDate:\x20Fri,\x2007\x20Oct\x202011\x
SF:2023:24:37\x20GMT\r\nContent-Length:\x202220\r\nContent-Type:\x20text/h
SF:tml\r\n\r\n<html>\r\n<head>\r\n\x20\x20\x20\x20<title>VMware\x20VDM\x20
SF:Web\x20Access</title>\r\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x2
SF:0type=\"text/css\"\x20href=\"/error/base\.css\"\x20/>\r\n\x20\x20\x20\x
SF:20<script\x20language=\"JavaScript\">\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20function\x20toggleError\(\)\r\n\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20var\x20errorElement\x20=
SF:\x20document\.getElementById\('fullErrorStack'\);\r\n\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20if\x20\(errorElement\x20&&\x20errorElemen
SF:t\.style\.display\x20==\x20'none'\)\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20errorElement\.style\.display=\"block\";\r\n\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20else\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0{\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20e
SF:rrorElement\.style\.display=\"none\";\x20\x20\x20\x20\x20\x20\x20\x20\r
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20}\r\n\r\n\x20\x20\x20\x20\x20\x20\x20\x20function\x20es

SF:capeHTML\x20\(str\)\r\n\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20var\x20div\x20=\x20document\.creat
SF:eElement\('div'\);\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20v
SF:ar\x20text\x20=\x20document\.createTextNode\(str\);\r\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20div\.appendChild\(text\);\r\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20return\x20div\.inn");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

Nmap scan report for aaa.bbb.ccc.61
Host is up (0.032s latency).
All 65535 scanned ports on aaa.bbb.ccc.61 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|firewall|general purpose
Running: Cisco embedded, SonicWALL embedded, Sun Solaris 10|9
OS details: Cisco Unified Communications Manager VoIP gateway, SonicWALL Aventail EX-1500 SSL VPN appliance, Sun Solaris 10, Sun Solaris 10 (SPARC), Sun Solaris 9 (SPARC)

Nmap scan report for communicator.regis.edu (aaa.bbb.ccc.66)
Host is up (0.041s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http MS ISA httpd
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (86%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.67
Host is up (0.039s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
443/tcp closed https
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%), Microsoft Windows XP SP3 (85%)

No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for sip.regis.edu (aaa.bbb.ccc.69)
Host is up (0.033s latency).
Not shown: 55529 filtered ports, 10004 closed ports
PORT STATE SERVICE VERSION
443/tcp open ssl/sip (SIP end point; Status: 504 Server time-out)
5061/tcp open ssl/sip-tls?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port443-TCP:V=5.51%T=SSL%I=7%D=10/7%Time=4E8F8BD1%P=i686-pc-windows-win
SF:dows%r(SIPOptions,E8,"SIP/2\.0\x20504\x20Server\x20time-out\r\nms-user-
SF:logon-data:\x20RemoteUser\r\nFrom:\x20<sip:nm@nm>;tag=root\r\nTo:\x20<s
SF:ip:nm2@nm2>;tag=0E159298EF9DA3A74EE4141AE5FADD50\r\nCall-ID:\x2050000\r
SF:\nCSeq:\x2042\x20OPTIONS\r\nVia:\x20SIP/2\.0/TCP\x20nm;branch=foo\r\nCo
SF:ntent-Length:\x200\r\n\r\n");
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Server 2008 Beta 3 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for ocswebconf.regis.edu (aaa.bbb.ccc.72)
Host is up (0.033s latency).
Not shown: 55529 filtered ports, 10005 closed ports
PORT STATE SERVICE VERSION
443/tcp open ssl/https?
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for ocsavedge.regis.edu (aaa.bbb.ccc.73)
Host is up (0.032s latency).
Not shown: 55529 filtered ports, 10005 closed ports
PORT STATE SERVICE VERSION
443/tcp open tcpwrapped
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)

Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for spslcalc.regis.edu (aaa.bbb.ccc.75)
Host is up (0.036s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp closed https
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.77
Host is up (0.032s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
8443/tcp closed https-alt
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.78
Host is up (0.049s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (88%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (88%), Microsoft Windows Server 2008 SP1 (86%), Microsoft Windows Server 2008

(85%), Microsoft Windows Server 2008 Beta 3 (85%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.97
Host is up (0.044s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 3.6.1p2 (protocol 2.0)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Aruba A800 wireless LAN switch (89%), Linux 2.4.7 (88%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (88%), Linux 2.4.21 - 2.4.31 (likely embedded) (88%), Linux 2.4.9 (Red Hat Enterprise Linux 2.1 AS) (87%), Netgear DG834GB wireless broadband router (86%), Dell Remote Access Controller 5 (DRAC 5) (86%), SonicWALL Aventail EX-1500 SSL VPN appliance (86%), HP 4200 PSA (Print Server Appliance) model J4117A (85%), Linksys WRV200 wireless broadband router (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for in2.regis.edu (aaa.bbb.ccc.98)
Host is up (0.057s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (86%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.99
Host is up (0.053s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache Tomcat/Coyote JSP engine 1.0
443/tcp closed https
8080/tcp closed http-proxy
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (87%)

Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%), Microsoft Windows XP SP3 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for www.regis.edu (aaa.bbb.ccc.100)
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open https?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (88%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (88%), Microsoft Windows Server 2008 SP1 (85%), Microsoft Windows Server 2008 (85%), Microsoft Windows Server 2008 Beta 3 (85%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.101
Host is up (0.056s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.0.52 ((CentOS))
443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (88%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (88%), Linux 2.6.9 - 2.6.27 (88%), Linux 2.6.11 (Auditor) (86%), Linux 2.6.9 (86%), Linux 2.6.22 (85%), Linux 2.6.9 (CentOS 4.4) (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.102
Host is up (0.060s latency).
Not shown: 65069 filtered ports, 462 closed ports
PORT STATE SERVICE VERSION
80/tcp open http-proxy EZproxy web proxy
443/tcp open ssl/http-proxy EZproxy web proxy
1051/tcp open optima-vnet?
1054/tcp open brvread?
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (87%)

Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.103
Host is up (0.065s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.3 ((CentOS))
443/tcp open ssl/http Apache httpd 2.2.3 ((CentOS))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|WAP
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (89%), ZoneAlarm embedded (87%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (89%), Linux 2.6.9 - 2.6.27 (89%), ZoneAlarm Z100G WAP (87%), Linux 2.6.9 (87%), Linux 2.6.17 (Mandriva) (85%), Linux 2.6.18 (Centos 5.3) (85%), Linux 2.6.22 - 2.6.23 (85%), Linux 2.6.9 - 2.6.30 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.104
Host is up (0.059s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
443/tcp open ssl/http Microsoft IIS httpd 6.0
5060/tcp open sip Microsoft Live SIP client
5061/tcp open ssl/sip Microsoft Office Communications Service 2005
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.105
Host is up (0.058s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
25/tcp closed smtp
80/tcp open http Microsoft IIS httpd 6.0
110/tcp closed pop3
443/tcp open ssl/http Microsoft IIS httpd 6.0

Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (87%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (87%), Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.106
Host is up (0.066s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd
443/tcp open ssl/http Microsoft IIS httpd 6.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (86%), Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows Server 2003 SP1 or SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.107
Host is up (0.070s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|WAP
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (88%), ZoneAlarm embedded (87%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (88%), Linux 2.6.9 - 2.6.27 (88%), ZoneAlarm Z100G WAP (87%), Linux 2.6.9 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.108
Host is up (0.066s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache Tomcat/Coyote JSP engine 1.1
443/tcp open ssl/http Apache Tomcat/Coyote JSP engine 1.1
1935/tcp open rtmp?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.109
Host is up (0.065s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|WAP
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (89%), ZoneAlarm embedded (87%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (89%), Linux 2.6.9 - 2.6.27 (89%), ZoneAlarm Z100G WAP (87%), Linux 2.6.9 (87%), Linux 2.6.17 (Mandriva) (85%), Linux 2.6.18 (Centos 5.3) (85%), Linux 2.6.22 - 2.6.23 (85%), Linux 2.6.9 - 2.6.30 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.110
Host is up (0.075s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (88%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (88%), Microsoft Windows Server 2008 SP1 (85%), Microsoft Windows Server 2008 (85%), Microsoft Windows Server 2008 Beta 3 (85%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.111
Host is up (0.074s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
1935/tcp open rtmp Real-Time Messaging Protocol
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.112
Host is up (0.068s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (85%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.113
Host is up (0.069s latency).
Not shown: 65528 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Microsoft Exchange ESMTP
80/tcp open http Microsoft IIS
143/tcp open imap Microsoft Exchange 2007 imapd
443/tcp open ssl/http Microsoft IIS
587/tcp open smtp Microsoft Exchange ESMTP
993/tcp open ssl/imap Microsoft Exchange 2007 imapd
995/tcp open ssl/pop3 MS Exchange 2007 pop3d
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (85%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (85%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: email.regis.edu; OS: Windows

Nmap scan report for aaa.bbb.ccc.114
Host is up (0.072s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd
443/tcp open https?

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for singtest.regis.edu (aaa.bbb.ccc.115)
Host is up (0.073s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (86%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.116
Host is up (0.050s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp Microsoft ftpd
80/tcp open http Microsoft IIS httpd 6.0
443/tcp closed https
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for maila.regis.edu (aaa.bbb.ccc.120)
Host is up (0.048s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

No OS matches for host
Service Info: OS: Unix

Nmap scan report for mailb.regis.edu (aaa.bbb.ccc.121)
Host is up (0.046s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Unix

Nmap scan report for mailc.regis.edu (aaa.bbb.ccc.122)
Host is up (0.043s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Unix

Nmap scan report for maild.regis.edu (aaa.bbb.ccc.123)
Host is up (0.042s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Unix

Nmap scan report for maile.regis.edu (aaa.bbb.ccc.124)
Host is up (0.031s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (88%)

Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (88%), Linux 2.6.9 - 2.6.27 (88%), Linux 2.6.11 (Auditor) (86%), Linux 2.6.9 (86%), Linux 2.6.22 (85%), Linux 2.6.9 (CentOS 4.4) (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Unix

Nmap scan report for antispam.regis.edu (aaa.bbb.ccc.125)
Host is up (0.038s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.0.52 ((CentOS))
443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (88%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (88%), Linux 2.6.9 - 2.6.27 (88%), Linux 2.6.11 (Auditor) (86%), Linux 2.6.9 (86%), Linux 2.6.22 (85%), Linux 2.6.9 (CentOS 4.4) (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.161
Host is up (0.056s latency).
Not shown: 65529 closed ports
PORT STATE SERVICE VERSION
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: broadband router|router|switch|WAP
Running: Cisco embedded, Cisco IOS 12.X|15.X
OS details: Cisco 827H ADSL router, Cisco 870 router or 2960 switch (IOS 12.2 - 12.4), Cisco Aironet 1250 WAP (IOS 12.4), Cisco C7200 router (IOS 15)

Nmap scan report for vpn.regis.edu (aaa.bbb.ccc.164)
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Cisco ASA firewall http config
443/tcp open ssl/http Cisco ASA firewall http config
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: WAP|switch|webcam|router|VoIP phone
Running (JUST GUESSING): D-Link embedded (96%), TRENDnet embedded (96%), HP embedded (90%), Linksys embedded (89%), Cisco embedded (87%)
Aggressive OS guesses: D-Link DWL-624+ or DWL-2000AP, or TRENDnet TEW-432BRP WAP (96%), HP 4000M ProCurve switch (J4121A) (90%), Linksys BEFSR41 EtherFast router or D-Link DCS-6620G webcam (89%), Cisco IP Phone 7941 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Device: firewall

Nmap scan report for aaa.bbb.ccc.193
Host is up (0.071s latency).
All 65535 scanned ports on aaa.bbb.ccc.193 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.194
Host is up (0.069s latency).
All 65535 scanned ports on aaa.bbb.ccc.194 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.195
Host is up (0.039s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
161/tcp closed snmp
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FAD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,12D,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RegisScience2\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J403-0000-110B-62EB\r\nServer:\x20
SF:Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauth
SF:orized</h1>\n</body>\n</html>")%r(HTTPOptions,12D,"HTTP/1\.0\x20401\x20
SF:Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RegisScienc
SF:e2\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-
SF:Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J
SF:403-0000-110B-62EB\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<
SF:html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSP
SF:Request,12D,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20B
SF:asic\x20realm=\"Admin-RegisScience2\"\r\nContent-Length:\x2056\r\nConte
SF:nt-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-vers
SF:ion:\x202\r\nNiagara-HostId:\x20J403-0000-110B-62EB\r\nServer:\x20Niaga

SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>")%r(FourOhFourRequest,12D,"HTTP/1\.0\x20401\x2
SF:0Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RegisScien
SF:ce2\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara
SF:-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20
SF:J403-0000-110B-62EB\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n
SF:<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIP
SF:Options,12C,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Ba
SF:sic\x20realm=\"Admin-RegisScience2\"\r\nContent-Length:\x2056\r\nConten
SF:t-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-versi
SF:on:\x202\r\nNiagara-HostId:\x20J403-0000-110B-62EB\r\nServer:\x20Niagar
SF:a\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized
SF:</h1>\n</body>\n</html>");
Aggressive OS guesses: Nortel DMS-10 telephony switch (88%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (87%), ReactOS 0.3.7 (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), Konica Minolta bizhub C450 printer with optional Fiery Controller (86%), Netgear DG834G WAP (86%), Siemens SpeedStream 4200 ADSL modem (86%), Lexmark X644e printer (85%), Netgear WGR614v7 wireless broadband router (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.196
Host is up (0.049s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FAD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J404-24737\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J404-0000-0EF0-DEC7\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-24737\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-00
SF:00-0EF0-DEC7\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J404-24737\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J404-0000-0EF0-DEC7\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<

SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-24737\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-0000-0E
SF:F0-DEC7\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J404-24737\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J404-0000-0EF0-DEC7\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.198
Host is up (0.044s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FAD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-11406\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-0A44-8D67\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-11406\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-0A44-8D67\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques

SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-11406\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-0A44-8D67\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-11406\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-0A
SF:44-8D67\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-11406\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-0A44-8D67\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.199
Host is up (0.044s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FAD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-14884\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-0BA1-FFDE\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una

SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-14884\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-0BA1-FFDE\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-14884\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-0BA1-FFDE\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-14884\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-0B
SF:A1-FFDE\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-14884\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-0BA1-FFDE\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.200
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp closed http
3011/tcp open sip Niagara Web Server/3.0 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FB107%P=i686-pc-windows-windows%
SF:r(GetRequest,1A8,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:

SF:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"
SF:MD5\",\x20nonce=\"TovVkzFlODA1ZmZiNDczMTk4MjE2MDhhM2YwNTE4ZWZlYjVj\
"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20QNX\r\nNiagara-Started:\x202010-3-21-3-32-50\r\nBaja-Station-Bran
SF:d:\x20vykon\r\nNiagara-HostId:\x20Qnx-J403-0000-0BA1-95F8\r\nServer:\x2
SF:0Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unaut
SF:horized</h1>\n</body>\n</html>")%r(HTTPOptions,1A8,"HTTP/1\.0\x20401\x2
SF:0Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admin\"
SF:,\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"TovVmDZjZGQ2MzExNjF
SF:kMzA5ZWQxODg0ZjkyZjNkNGJmNWQ0\"\r\nContent-Length:\x2056\r\nContent-Typ
SF:e:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x202010
SF:-3-21-3-32-50\r\nBaja-Station-Brand:\x20vykon\r\nNiagara-HostId:\x20Qnx
SF:-J403-0000-0BA1-95F8\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\
SF:n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RT
SF:SPRequest,1A8,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x2
SF:0Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"MD5
SF:\",\x20nonce=\"TovVnWIyZDkyNDhiOTU4MTE5ODE3YjZkYjU2Mzc5OWMwZmJk\"\r\n
Co
SF:ntent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\
SF:x20QNX\r\nNiagara-Started:\x202010-3-21-3-32-50\r\nBaja-Station-Brand:\
SF:x20vykon\r\nNiagara-HostId:\x20Qnx-J403-0000-0BA1-95F8\r\nServer:\x20Ni
SF:agara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthor
SF:ized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1A8,"HTTP/1\.0\x20401
SF:\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admi
SF:n\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"TovVtGM4ZTk5ZGIy
SF:N2UwNWRiM2U5MGVjNzMyYWRiMWIxM2Yz\"\r\nContent-Length:\x2056\r\nContent-
SF:Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x202
SF:010-3-21-3-32-50\r\nBaja-Station-Brand:\x20vykon\r\nNiagara-HostId:\x20
SF:Qnx-J403-0000-0BA1-95F8\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\r\n
SF:\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Aggressive OS guesses: NRG MP C4500 printer (95%), NRG C7521n printer (93%), Ricoh Aficion SP 4100N printer (92%), Check Point VPN-1 firewall (IPSO 4.1) (90%), Asus RT-N16 WAP (Linux 2.6) (87%), NetBSD 1.4.2 - 1.5.2; Lanier LS232c, NRG DSc428, Ricoh Aficio 2020, Ricoh NRG MP 161, or Savin 8055 printer; or Panasonic Network Camera (BB-HCM331, BB-HCM381, BCL-30A, BL-C1CE, or BL-C10CE) (87%), QNX 6.2.1 (x86) (87%), Netgear DG834G WAP (87%), Ricoh Aficio 1022 copier (87%), Lexmark X644e printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.201
Host is up (0.048s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v2)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FB10A%P=i686-pc-windows-windows%
SF:r(GetRequest,11D,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-NIAGARASERVER\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20NT\r\nniagarad-versi
SF:on:\x202\r\nNiagara-HostId:\x20ECA6-4E73\r\nServer:\x20Niagara\x20Web\x
SF:20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</b
SF:ody>\n</html>")%r(HTTPOptions,11D,"HTTP/1\.0\x20401\x20Unauthorized\r\n
SF:WWW-Authenticate:\x20Basic\x20realm=\"Admin-NIAGARASERVER\"\r\nContent-
SF:Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20NT\
SF:r\nniagarad-version:\x202\r\nNiagara-HostId:\x20ECA6-4E73\r\nServer:\x2
SF:0Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unaut
SF:horized</h1>\n</body>\n</html>")%r(RTSPRequest,11D,"RTSP/1\.0\x20401\x2
SF:0Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-NIAGARASER
SF:VER\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara
SF:-Platform:\x20NT\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20ECA6-4
SF:E73\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n
SF:<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1
SF:1D,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20r
SF:ealm=\"Admin-NIAGARASERVER\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20NT\r\nniagarad-version:\x202\r\nNi
SF:agara-HostId:\x20ECA6-4E73\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\
SF:r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>"
SF:)%r(SIPOptions,11C,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate
SF::\x20Basic\x20realm=\"Admin-NIAGARASERVER\"\r\nContent-Length:\x2056\r\
SF:nContent-Type:\x20text/html\r\nNiagara-Platform:\x20NT\r\nniagarad-vers
SF:ion:\x202\r\nNiagara-HostId:\x20ECA6-4E73\r\nServer:\x20Niagara\x20Web\
SF:x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</
SF:body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2000|2003 (98%)
Aggressive OS guesses: Microsoft Windows XP SP3 (98%), Microsoft Windows XP SP2 or SP3 (96%), Microsoft Windows 2000 SP4 (94%), Microsoft Windows 2000 (93%), Microsoft Windows XP Professional SP2 (91%), Microsoft Windows XP SP 2 (91%), Microsoft Windows XP SP2 (90%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (89%), Microsoft Windows Server 2003 Enterprise Edition (89%), Microsoft Windows XP Professional SP3 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.202
Host is up (0.084s latency).
All 65535 scanned ports on aaa.bbb.ccc.202 are filtered

Too many fingerprints match this host to give specific OS details
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.203
Host is up (0.050s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FB107%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J404-29083\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J404-0000-1225-E4B1\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-29083\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-00
SF:00-1225-E4B1\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J404-29083\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J404-0000-1225-E4B1\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-29083\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-0000-12
SF:25-E4B1\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J404-29083\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J404-0000-1225-E4B1\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose|firewall|game console|storage-misc|switch|remote management|media device

Running (JUST GUESSING): Netgear embedded (94%), HP embedded (93%), Linux 2.4.X|2.1.X|2.6.X (93%), Fortinet embedded (91%), Microsoft embedded (91%), Netgear RAIDiator 4.X (89%), 3Com embedded (89%), Aruba ArubaOS 3.X (89%)
Aggressive OS guesses: Netgear DG834G WAP (94%), HP ProCurve MSM422 WAP (93%), Linux 2.4.21 - 2.4.25 (93%), Fortinet FortiGate-60B or -100A firewall (91%), Microsoft Xbox game console (modified, running XboxMediaCenter) (91%), Netgear ReadyNAS Duo NAS device (RAIDiator 4.1.4) (89%), 3Com SuperStack 3 Switch 3870 (89%), Aruba 200 wireless LAN controller (ArubaOS 3.3.2.5) (89%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (89%), Linux 2.4.20 - 2.4.27 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.204
Host is up (0.045s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J511-4020\"\r\nContent-Length:\x2056\r\nCont
SF:ent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-ver
SF:sion:\x202\r\nNiagara-HostId:\x20J511-AA55-EAAA\r\nServer:\x20Niagara\x
SF:20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h
SF:1>\n</body>\n</html>")%r(HTTPOptions,124,"HTTP/1\.0\x20401\x20Unauthori
SF:zed\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J511-4020\"\r\nConte
SF:nt-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20
SF:JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J511-AA55-EAAA
SF:\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1
SF:>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,124,"RTSP/
SF:1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Ad
SF:min-J511-4020\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\
SF:r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-H
SF:ostId:\x20J511-AA55-EAAA\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\
SF:n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%
SF:r(FourOhFourRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authen
SF:ticate:\x20Basic\x20realm=\"Admin-J511-4020\"\r\nContent-Length:\x2056\
SF:r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniaga
SF:rad-version:\x202\r\nNiagara-HostId:\x20J511-AA55-EAAA\r\nServer:\x20Ni
SF:agara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthor
SF:ized</h1>\n</body>\n</html>")%r(SIPOptions,123,"SIP/2\.0\x20401\x20Unau
SF:thorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J511-4020\"\r\n
SF:Content-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform
SF::\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J511-AA55

SF:-EAAA\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>
SF:\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.205
Host is up (0.050s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-JACE-27583\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J404-0000-110B-5737\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-JACE-27583\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-00
SF:00-110B-5737\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-JACE-27583\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J404-0000-110B-5737\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-JACE-27583\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-0000-11
SF:0B-5737\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod

SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-JACE-27583\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J404-0000-110B-5737\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.206
Host is up (0.044s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-29073\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-1225-F54F\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29073\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-1225-F54F\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-29073\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-1225-F54F\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<

SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29073\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-12
SF:25-F54F\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-29073\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-1225-F54F\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|switch|printer|webcam|general purpose|media device
Running (JUST GUESSING): Netgear embedded (88%), Nortel embedded (87%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Netgear DG834G WAP (88%), Nortel DMS-10 telephony switch (87%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.207
Host is up (0.039s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-29067\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-1226-0673\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29067\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-1226-0673\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques

SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-29067\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-1226-0673\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29067\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-12
SF:26-0673\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-29067\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-1226-0673\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.208
Host is up (0.055s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,127,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-REGISLIBRARY\"\r\nContent-Length:\x2056\r\nC
SF:ontent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-
SF:version:\x202\r\nNiagara-HostId:\x20J512-2041-C820\r\nServer:\x20Niagar
SF:a\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized
SF:</h1>\n</body>\n</html>")%r(HTTPOptions,127,"HTTP/1\.0\x20401\x20Unauth

SF:orized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-REGISLIBRARY\"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J512-204
SF:1-C820\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body
SF:>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,127,
SF:"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20real
SF:m=\"Admin-REGISLIBRARY\"\r\nContent-Length:\x2056\r\nContent-Type:\x20t
SF:ext/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\n
SF:Niagara-HostId:\x20J512-2041-C820\r\nServer:\x20Niagara\x20Web\x20Serve
SF:r/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n<
SF:/html>")%r(FourOhFourRequest,127,"HTTP/1\.0\x20401\x20Unauthorized\r\nW
SF:WW-Authenticate:\x20Basic\x20realm=\"Admin-REGISLIBRARY\"\r\nContent-Le
SF:ngth:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_
SF:51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J512-2041-C820\r\nS
SF:erver:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:
SF:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,126,"SIP/2\.0\x2
SF:0401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-REG
SF:ISLIBRARY\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nN
SF:iagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostI
SF:d:\x20J512-2041-C820\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\
SF:n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.209
Host is up (0.049s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12D,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RegisScience1\"\r\nContent-Length:\x2056\r\n

SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J403-0000-110B-6226\r\nServer:\x20
SF:Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauth
SF:orized</h1>\n</body>\n</html>")%r(HTTPOptions,12D,"HTTP/1\.0\x20401\x20
SF:Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RegisScienc
SF:e1\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-
SF:Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J
SF:403-0000-110B-6226\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<
SF:html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSP
SF:Request,12D,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20B
SF:asic\x20realm=\"Admin-RegisScience1\"\r\nContent-Length:\x2056\r\nConte
SF:nt-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-vers
SF:ion:\x202\r\nNiagara-HostId:\x20J403-0000-110B-6226\r\nServer:\x20Niaga
SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>")%r(FourOhFourRequest,12D,"HTTP/1\.0\x20401\x2
SF:0Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RegisScien
SF:ce1\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara
SF:-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20
SF:J403-0000-110B-6226\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n
SF:<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIP
SF:Options,12C,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Ba
SF:sic\x20realm=\"Admin-RegisScience1\"\r\nContent-Length:\x2056\r\nConten
SF:t-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-versi
SF:on:\x202\r\nNiagara-HostId:\x20J403-0000-110B-6226\r\nServer:\x20Niagar
SF:a\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized
SF:</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.210
Host is up (0.047s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-29066\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-1225-E8C8\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29066\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-1225-E8C8\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-29066\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-1225-E8C8\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29066\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-12
SF:25-E8C8\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-29066\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-1225-E8C8\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.211

Host is up (0.051s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-28929\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-1225-0B4E\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-28929\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-1225-0B4E\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-28929\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-1225-0B4E\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-28929\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-12
SF:25-0B4E\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-28929\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-1225-0B4E\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera

(Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.212
Host is up (0.050s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J404-31225\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J404-0000-1225-0882\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-31225\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-00
SF:00-1225-0882\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J404-31225\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J404-0000-1225-0882\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-31225\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-0000-12
SF:25-0882\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J404-31225\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J404-0000-1225-0882\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|switch|printer|webcam|general purpose|media device

Running (JUST GUESSING): Netgear embedded (88%), Nortel embedded (87%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Netgear DG834G WAP (88%), Nortel DMS-10 telephony switch (87%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.213
Host is up (0.052s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
1911/tcp open mtp?
3012/tcp open sip Niagara Web Server/3.0 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3012-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,1AB,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"
SF:MD5\",\x20nonce=\"To/MB2RjZTUzOWJhYmZjYWI5YWY5MWViYjYxMTQ4ZjgxYW
M0\"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20QNX\r\nNiagara-Started:\x202011-8-22-23-36-50\r\nBaja-Station-Bra
SF:nd:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-68E6\r\nServer:
SF:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Un
SF:authorized</h1>\n</body>\n</html>")%r(HTTPOptions,1AB,"HTTP/1\.0\x20401
SF:\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admi
SF:n\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/MDDk3YzNjM2Fk
SF:YTU5ZGQwZTFiMjkxMDg3N2MyNjFhOTdk\"\r\nContent-Length:\x2056\r\nContent-
SF:Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x202
SF:011-8-22-23-36-50\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara-HostId:\
SF:x20Qnx-NPM2-0000-0E56-68E6\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\
SF:r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>"
SF:)%r(RTSPRequest,1AB,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authentica
SF:te:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm
SF:=\"MD5\",\x20nonce=\"To/MEWRjYThkYmE2ODMzY2RjZTVmZWRlZjViYzhjM2M0M
WEz\"
SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat
SF:form:\x20QNX\r\nNiagara-Started:\x202011-8-22-23-36-50\r\nBaja-Station-
SF:Brand:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-68E6\r\nServ
SF:er:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x2
SF:0Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1AB,"HTTP/1\
SF:.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Nia

SF:gara-Admin\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/MKDN
SF:iYTBmMGZmM2JjYjJkNjJkM2M3N2YzZmQ0ZmI2OTRj\"\r\nContent-Length:\x2056\r\
SF:nContent-Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Star
SF:ted:\x202011-8-22-23-36-50\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara
SF:-HostId:\x20Qnx-NPM2-0000-0E56-68E6\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: NRG MP C4500 printer (94%), NRG C7521n printer (92%), Ricoh Aficion SP 4100N printer (91%), Netgear DG834G WAP (89%), Asus RT-N16 WAP (Linux 2.6) (88%), AXIS 211A Network Camera (Linux 2.6) (88%), AXIS 211A Network Camera (Linux 2.6.20) (88%), Linux 2.6.24 (88%), Check Point VPN-1 firewall (IPSO 4.1) (87%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.214
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
1911/tcp open mtp?
3012/tcp open sip Niagara Web Server/3.0 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3012-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD25%P=i686-pc-windows-windows%
SF:r(GetRequest,1AB,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"
SF:MD5\",\x20nonce=\"To/DpWFiYmM3NzFmYTk0MDkzNDA3NzUyZWYzMTJmODhlYT
Q5\"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20QNX\r\nNiagara-Started:\x202011-8-17-11-38-58\r\nBaja-Station-Bra
SF:nd:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-3926\r\nServer:
SF:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Un
SF:authorized</h1>\n</body>\n</html>")%r(HTTPOptions,1AB,"HTTP/1\.0\x20401
SF:\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admi
SF:n\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/DqjEyOTFiODIw
SF:MDkzY2U2MDdmZDg3NDhjOGQzOTMwOWFi\"\r\nContent-Length:\x2056\r\nContent-
SF:Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x202
SF:011-8-17-11-38-58\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara-HostId:\
SF:x20Qnx-NPM2-0000-0E56-3926\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\
SF:r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>"
SF:)%r(RTSPRequest,1AB,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authentica
SF:te:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm
SF:=\"MD5\",\x20nonce=\"To/Drzk1M2U1NzI4MmZlNzFlYmIzZWQxNjU4NGU4ZjYwMGFj
\"

SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat
SF:form:\x20QNX\r\nNiagara-Started:\x202011-8-17-11-38-58\r\nBaja-Station-
SF:Brand:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-3926\r\nServ
SF:er:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x2
SF:0Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1AB,"HTTP/1\
SF:.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Nia
SF:gara-Admin\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/DxjY
SF:wNzU3NGE0ZGE1NzRjYTFmNmY2ZTlmNTE0ZWJiODVj\"\r\nContent-Length:\x2056\r\
SF:nContent-Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Star
SF:ted:\x202011-8-17-11-38-58\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara
SF:-HostId:\x20Qnx-NPM2-0000-0E56-3926\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: NRG MP C4500 printer (94%), NRG C7521n printer (92%), Ricoh Aficion SP 4100N printer (90%), Netgear DG834G WAP (89%), Asus RT-N16 WAP (Linux 2.6) (88%), AXIS 211A Network Camera (Linux 2.6) (88%), AXIS 211A Network Camera (Linux 2.6.20) (88%), Linux 2.6.24 (88%), Check Point VPN-1 firewall (IPSO 4.1) (87%), NetBSD 1.4.2 - 1.5.2; Lanier LS232c, NRG DSc428, Ricoh Aficio 2020, Ricoh NRG MP 161, or Savin 8055 printer; or Panasonic Network Camera (BB-HCM331, BB-HCM381, BCL-30A, BL-C1CE, or BL-C10CE) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.215
Host is up (0.045s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD25%P=i686-pc-windows-windows%
SF:r(GetRequest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RV_1\"\r\nContent-Length:\x2056\r\nContent-T
SF:ype:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:
SF:\x202\r\nNiagara-HostId:\x20J501-0001-C000\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(HTTPOptions,11F,"HTTP/1\.0\x20401\x20Unauthorized\r
SF:\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_1\"\r\nContent-Length:
SF:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r
SF:\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-0001-C000\r\nServer
SF::\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20U
SF:nauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,11F,"RTSP/1\.0\x2040
SF:1\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_1\"

SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat
SF:form:\x20JACE_50x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-
SF:0001-C000\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<b
SF:ody>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourReq
SF:uest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basi
SF:c\x20realm=\"Admin-RV_1\"\r\nContent-Length:\x2056\r\nContent-Type:\x20
SF:text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\x202\r\
SF:nNiagara-HostId:\x20J501-0001-C000\r\nServer:\x20Niagara\x20Web\x20Serv
SF:er/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n
SF:</html>")%r(SIPOptions,11E,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Auth
SF:enticate:\x20Basic\x20realm=\"Admin-RV_1\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J501-0001-C000\r\nServer:\x20Niaga
SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|printer|WAP|general purpose|webcam
Running (JUST GUESSING): Nortel embedded (94%), Konica Minolta embedded (92%), Netgear embedded (88%), ReactOS 0.3.X (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (94%), Konica Minolta bizhub C450 printer with optional Fiery Controller (92%), Netgear DG834G WAP (88%), ReactOS 0.3.7 (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.216
Host is up (0.055s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
1911/tcp open mtp?
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
3012/tcp open sip Niagara Web Server/3.0 (Status: 401 Unauthorized)
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD25%P=i686-pc-windows-windows%
SF:r(GetRequest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RV_2\"\r\nContent-Length:\x2056\r\nContent-T
SF:ype:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:
SF:\x202\r\nNiagara-HostId:\x20J501-70E1-DC70\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<

SF:/body>\n</html>")%r(HTTPOptions,11F,"HTTP/1\.0\x20401\x20Unauthorized\r
SF:\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_2\"\r\nContent-Length:
SF:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r
SF:\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-70E1-DC70\r\nServer
SF::\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20U
SF:nauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,11F,"RTSP/1\.0\x2040
SF:1\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_2\"
SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat
SF:form:\x20JACE_50x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-
SF:70E1-DC70\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<b
SF:ody>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourReq
SF:uest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basi
SF:c\x20realm=\"Admin-RV_2\"\r\nContent-Length:\x2056\r\nContent-Type:\x20
SF:text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\x202\r\
SF:nNiagara-HostId:\x20J501-70E1-DC70\r\nServer:\x20Niagara\x20Web\x20Serv
SF:er/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n
SF:</html>")%r(SIPOptions,11E,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Auth
SF:enticate:\x20Basic\x20realm=\"Admin-RV_2\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J501-70E1-DC70\r\nServer:\x20Niaga
SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT
INDIVIDUALLY)==============
SF-Port3012-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD25%P=i686-pc-windows-windows%
SF:r(GetRequest,1AA,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"
SF:MD5\",\x20nonce=\"To/JGDM2NDA2ZjkxY2E1MDZkYzI1YTVmZDYxN2NiZjkzYTk3\"\
r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20QNX\r\nNiagara-Started:\x202011-6-20-10-2-29\r\nBaja-Station-Bran
SF:d:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-6AB9\r\nServer:\
SF:x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Una
SF:uthorized</h1>\n</body>\n</html>")%r(HTTPOptions,1AA,"HTTP/1\.0\x20401\
SF:x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admin
SF:\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/JHTI2MjBlYjU0Y
SF:zAzNjYxNjMzNGEyYjljYzI3NmUxYWRi\"\r\nContent-Length:\x2056\r\nContent-T
SF:ype:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x2020
SF:11-6-20-10-2-29\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara-HostId:\x2
SF:0Qnx-NPM2-0000-0E56-6AB9\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\r\
SF:n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%
SF:r(RTSPRequest,1AA,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate
SF::\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\
SF:"MD5\",\x20nonce=\"To/JIjJkMTRlYjRjOTZmZTc5OWVmMTE2YThiZmVlY2ZlNmIz\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20QNX\r\nNiagara-Started:\x202011-6-20-10-2-29\r\nBaja-Station-Bra

SF:nd:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-6AB9\r\nServer:
SF:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Un
SF:authorized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1AA,"HTTP/1\.0\
SF:x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagar
SF:a-Admin\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/JOWQ3NG
SF:JkOTY4ZTgzNDY3NmVlZjk2ZjUzYWMxN2M0YTcz\"\r\nContent-Length:\x2056\r\nCo
SF:ntent-Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started
SF::\x202011-6-20-10-2-29\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara-Hos
SF:tId:\x20Qnx-NPM2-0000-0E56-6AB9\r\nServer:\x20Niagara\x20Web\x20Server/
SF:3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</h
SF:tml>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|printer|WAP|general purpose|webcam
Running (JUST GUESSING): Nortel embedded (94%), Konica Minolta embedded (92%), Netgear embedded (88%), ReactOS 0.3.X (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (94%), Konica Minolta bizhub C450 printer with optional Fiery Controller (92%), Netgear DG834G WAP (88%), ReactOS 0.3.7 (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.217
Host is up (0.050s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RV_3\"\r\nContent-Length:\x2056\r\nContent-T
SF:ype:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:
SF:\x202\r\nNiagara-HostId:\x20J501-77EF-DD77\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(HTTPOptions,11F,"HTTP/1\.0\x20401\x20Unauthorized\r
SF:\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_3\"\r\nContent-Length:
SF:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r
SF:\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-77EF-DD77\r\nServer
SF::\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20U
SF:nauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,11F,"RTSP/1\.0\x2040
SF:1\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_3\"
SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat

SF:form:\x20JACE_50x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-
SF:77EF-DD77\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<b
SF:ody>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourReq
SF:uest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basi
SF:c\x20realm=\"Admin-RV_3\"\r\nContent-Length:\x2056\r\nContent-Type:\x20
SF:text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\x202\r\
SF:nNiagara-HostId:\x20J501-77EF-DD77\r\nServer:\x20Niagara\x20Web\x20Serv
SF:er/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n
SF:</html>")%r(SIPOptions,11E,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Auth
SF:enticate:\x20Basic\x20realm=\"Admin-RV_3\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J501-77EF-DD77\r\nServer:\x20Niaga
SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|printer|WAP|general purpose|webcam
Running (JUST GUESSING): Nortel embedded (94%), Konica Minolta embedded (92%), Netgear embedded (88%), ReactOS 0.3.X (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (94%), Konica Minolta bizhub C450 printer with optional Fiery Controller (92%), Netgear DG834G WAP (88%), ReactOS 0.3.7 (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.218
Host is up (0.046s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,11E,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RV4\"\r\nContent-Length:\x2056\r\nContent-Ty
SF:pe:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\
SF:x202\r\nNiagara-HostId:\x20J501-71E3-DC71\r\nServer:\x20Niagara\x20Web\
SF:x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</
SF:body>\n</html>")%r(HTTPOptions,11E,"HTTP/1\.0\x20401\x20Unauthorized\r\
SF:nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV4\"\r\nContent-Length:\x
SF:2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\n
SF:niagarad-version:\x202\r\nNiagara-HostId:\x20J501-71E3-DC71\r\nServer:\
SF:x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Una

SF:uthorized</h1>\n</body>\n</html>")%r(RTSPRequest,11E,"RTSP/1\.0\x20401\
SF:x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV4\"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20JACE_50x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-71E
SF:3-DC71\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body
SF:>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourReques
SF:t,11E,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-RV4\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J501-71E3-DC71\r\nServer:\x20Niagara\x20Web\x20Server/1
SF:\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</ht
SF:ml>")%r(SIPOptions,11D,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenti
SF:cate:\x20Basic\x20realm=\"Admin-RV4\"\r\nContent-Length:\x2056\r\nConte
SF:nt-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-vers
SF:ion:\x202\r\nNiagara-HostId:\x20J501-71E3-DC71\r\nServer:\x20Niagara\x2
SF:0Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1
SF:>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|printer|WAP|general purpose|webcam
Running (JUST GUESSING): Nortel embedded (94%), Konica Minolta embedded (92%), Netgear embedded (88%), ReactOS 0.3.X (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (94%), Konica Minolta bizhub C450 printer with optional Fiery Controller (92%), Netgear DG834G WAP (88%), ReactOS 0.3.7 (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.219
Host is up (0.051s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD30%P=i686-pc-windows-windows%
SF:r(GetRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-REGISALC2\"\r\nContent-Length:\x2056\r\nCont
SF:ent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-ver
SF:sion:\x202\r\nNiagara-HostId:\x20J511-AD5B-EBAD\r\nServer:\x20Niagara\x
SF:20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h
SF:1>\n</body>\n</html>")%r(HTTPOptions,124,"HTTP/1\.0\x20401\x20Unauthori
SF:zed\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-REGISALC2\"\r\nConte

SF:nt-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20
SF:JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J511-AD5B-EBAD
SF:\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1
SF:>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,124,"RTSP/
SF:1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Ad
SF:min-REGISALC2\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\
SF:r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-H
SF:ostId:\x20J511-AD5B-EBAD\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\
SF:n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%
SF:r(FourOhFourRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authen
SF:ticate:\x20Basic\x20realm=\"Admin-REGISALC2\"\r\nContent-Length:\x2056\
SF:r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniaga
SF:rad-version:\x202\r\nNiagara-HostId:\x20J511-AD5B-EBAD\r\nServer:\x20Ni
SF:agara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthor
SF:ized</h1>\n</body>\n</html>")%r(SIPOptions,123,"SIP/2\.0\x20401\x20Unau
SF:thorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-REGISALC2\"\r\n
SF:Content-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform
SF::\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J511-AD5B
SF:-EBAD\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>
SF:\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.220
Host is up (0.054s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD32%P=i686-pc-windows-windows%
SF:r(GetRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J512-8894\"\r\nContent-Length:\x2056\r\nCont
SF:ent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-ver

SF:sion:\x202\r\nNiagara-HostId:\x20J512-9327-E493\r\nServer:\x20Niagara\x
SF:20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h
SF:1>\n</body>\n</html>")%r(HTTPOptions,124,"HTTP/1\.0\x20401\x20Unauthori
SF:zed\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J512-8894\"\r\nConte
SF:nt-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20
SF:JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J512-9327-E493
SF:\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1
SF:>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,124,"RTSP/
SF:1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Ad
SF:min-J512-8894\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\
SF:r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-H
SF:ostId:\x20J512-9327-E493\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\
SF:n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%
SF:r(FourOhFourRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authen
SF:ticate:\x20Basic\x20realm=\"Admin-J512-8894\"\r\nContent-Length:\x2056\
SF:r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniaga
SF:rad-version:\x202\r\nNiagara-HostId:\x20J512-9327-E493\r\nServer:\x20Ni
SF:agara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthor
SF:ized</h1>\n</body>\n</html>")%r(SIPOptions,123,"SIP/2\.0\x20401\x20Unau
SF:thorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J512-8894\"\r\n
SF:Content-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform
SF::\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J512-9327
SF:-E493\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>
SF:\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.222
Host is up (0.049s latency).
Not shown: 65529 closed ports
PORT STATE SERVICE VERSION
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm

139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: broadband router|router|switch|WAP
Running: Cisco embedded, Cisco IOS 12.X|15.X
OS details: Cisco 827H ADSL router, Cisco 870 router or 2960 switch (IOS 12.2 - 12.4), Cisco Aironet 1250 WAP (IOS 12.4), Cisco C7200 router (IOS 15)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 89 IP addresses (89 hosts up) scanned in 15409.94 seconds

THE VULNERABILITY ASSESSMENT AND PENTRATION TESTING

OF TWO NETWORKS

A PROJECT

SUBMITTED ON THE 16th OF DECEMBER, 2011

TO THE DEPARTMENT OF INFORMATION SYSTEMS

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

SYSTEMS ENGINEERING

BY

Steven L. Simpson

APPROVALS

D. M. Likarish

Dan Likarish, Project Advisor

Robert T. Mason

Robert T. Mason, Ph.D.

Nancy Birkenheuer

Nancy Birkenheuer

Abstract

Vulnerability assessments and penetration testing are two approaches available for use by internet security practitioners to determine the security posture of information networks. By assessing network vulnerabilities and attempting to exploit found vulnerabilities through penetration testing security professionals are able to evaluate the effectiveness of their network defenses by identifying defense weaknesses, affirming the defense mechanisms in place, or some combination of the two.

This project is a discussion of the methods and tools used during the vulnerability assessment and penetration testing, and the respective test results of two varied and unique networks. The assessment and testing of the first network occurred from an internal perspective, while the assessment and testing of the second occurred from an external perspective. While the tools and methodologies used across both networks were consistent, the test results differed significantly. The paper concludes with a series of recommendations regarding practical methods and tools that may prove useful to anyone interested in network security, and vulnerability assessments and penetration testing in particular.

Acknowledgements

I would like to thank the following people for their support and help during the pursuit of my graduate education and during the completion of this project. Specifically I would like to thank my wife, Renee Simpson for her continued belief in my abilities for all the projects I have undertaken. I would also like to thank Angus Anderson, Stuart Gentry, Brian Haynie, Ed Richards, Corbit Magby, and Justin McCallister for taking to the time to review my writings and for the edits and suggestions, which made this paper more readable and easier to understand.

I would also like to thank the following people for their continued support during the pursuit of my studies and for always taking the time to ask me how my studies were progressing: Denise Haynie, Jane Richards, Stan and Jeannie Cook, Mark Williams, Davie Costales, Brian and JoAnn Morford, Anita Magby, and Doyle and Judy Warnock. Finally, I would like to thank my son, Matthew Scott Simpson for inspiring me to complete all the work required to finish my Master's education.

Table of Contents

ABSTRACT ..... **II**

ACKNOWLEDGEMENTS ..... **III**

TABLE OF CONTENTS **4**

LIST OF TABLES **6**

CHAPTER 1 – INTRODUCTION **7**

CHAPTER 2 - CANVAS ASSESSMENT AND TESTING **11**

CANVAS PROJECT PURPOSE, REQUIREMENTS, AND DELIVERABLES 11

CANVAS PROJECT TOOLS AND RESOURCES 12

BackTrack 4. ..... *12*

Nmap. *12*

Metasploit. *14*

CANVAS NETWORK TEST METHODOLOGY 15

CANVAS network host discovery. *15*

CANVAS network port analysis *17*

CANVAS network automated penetration testing *18*

CANVAS PROJECT SUMMARY 24

CHAPTER 3 - ITS NETWORK VULNERABILITY ASSESSMENT AND PENETRATION TESTING **26**

ITS PROJECT REQUIREMENTS, PROJECT RESTRICTIONS, AND PROJECT DELIVERABLES 26

Project Requirements. *26*

Project Restrictions. *27*

Project Deliverables. *27*

PROJECT TEST PLAN 28

Test Notification Process. *30*

Project Tools and Resources *32*

ITS network assessment and penetration test methodology *33*

ITS Network Assessment and Penetration Test Results Summary 44

CHAPTER 4 - SUMMARY AND RECOMMENDATIONS 49

Summary 49

Recommendations 51

Recommendation 1. 51

Recommendation 2. 52

Recommendation 3. 53

Recommendation 4. 54

Recommendation 5. 54

Recommendation 6. 55

Recommendation Summary 56

REFERENCES 59

APPENDIX A: CANVAS NETWORK ALL HOST/ALL PORTS SCAN RESULTS 61

APPENDIX B: CANVAS AUTO TEST SUMMARY - 031811 64

APPENDIX C: CANVAS TESTING FOR 03222011 65

APPENDIX D: ITS PROJECT TEST PLAN 66

APPENDIX E: ITS NETWORK PING RESULTS 76

APPENDIX F: FILE LISTING OF *EXTERNAL_UP.TXT* 80

APPENDIX G: ITS PORT ANALYSIS SCAN RESULTS – COMPLETE LISTING 82

List of Tables

Table 1: CANVAS Project Requirements, Restrictions, and Deliverables Page 8

Table 2: Active CANVAS Hosts Page 13

Table 3: Port Scan of CANVAS Network Page 15

Table 4: Metasploit db_autopwn results for CANVAS network Page 17

Table 5: Post-hardening Test Results Summary Page 20

Table 6: ITS Project requirements, restrictions, and deliverables Page 24

Table 7: Completed Test Notification Form Page 28

Table 8: ITS Network Ping Scan Results Page 31

Table 9: Partial Listing of external_up.txt Page 33

Table 10: Sample ITS Network Port Analysis Scan Result Page 35

Table 11: Port Analysis Scan Results Summary Page 43

Table 12: Possible Network Irregularity Page 44

Chapter 1 – Introduction

This report presents the methods, tools, and the results of the vulnerability assessment and penetration testing of two separate and unique networks. The assessment and testing of each network was part of the System Engineering and Application Development (SEAD) Practicum in support of a Masters program at Regis University.

Before discussing the details of each project, a definition of the terms "vulnerability assessment" and "penetration testing" is in order. In a broad sense, a vulnerability assessment is any action taken to evaluate the effectiveness of asset protection. Penetration testing usually follows a vulnerability assessment and is the process of verifying identified vulnerabilities by executing tests designed to exploit the vulnerabilities and compromise the target.

A common routine performed by numerous individuals can illustrate the concept of a vulnerability assessment. On a nightly basis, many conduct a vulnerability assessment by checking their dwelling's doors and windows prior to turning in for the night. Verifying the state of external doors and windows (e.g. the determination of whether the external doors and windows are locked, unlocked, open or closed) is a simple example of a common vulnerability assessment. Many people follow the nightly routine of checking the most vulnerable access points of their homes in an effort to determine the safety and security of their possessions and the people inside.

While the concept of checking the most vulnerable access points is applicable to almost any system, when applied to an information network, the process defines a network vulnerability assessment. In terms specific to an information network, a vulnerability assessment is any action taken to evaluate the security of a network. The Red Hat Enterprise Linux 4: Security Guide describes a vulnerability assessment as the "audit of network and system security; the results of

which indicate the confidentiality, integrity, and availability of [the] network" (Red Hat, 2005). Just as the home's resident may check windows and doors for vulnerable points of entry, a network assessor will check the network hosts for vulnerabilities such as unpatched operating system (OS) software, open ports, application flaws, or any number of other security vulnerabilities.

The vulnerability assessment of an information network follows a straightforward and logical series of steps. These steps begin with the broad retrieval of data and narrow to a point of specific action. Commonly, a vulnerability assessment progresses in the following steps:

- Reconnaissance of network hosts
- Enumeration of network devices
- Enumeration of services on each device
- Verification of discovered vulnerabilities

Throughout this report, the phrase "host discovery" will refer to the reconnaissance of network hosts. The phrase "port analysis" will refer to the enumeration of network devices and the operational services of those devices. The phrase "penetration testing" will refer to the verification of discovered vulnerabilities. In the context of this report, the phrase vulnerability assessment will include the processes of host discovery and port analysis while term penetration testing refers to the standalone and unique process of vulnerability verification. Lastly, the term "three-step method" refers to the steps of host discovery, port analysis, and penetration testing and its use is interchangeable with the terms vulnerability assessment(s) and penetration testing throughout this report.

Also of note is the perspective from which these vulnerability assessment and penetration tests occur. All vulnerability assessments and penetration tests occur from a host that is either

external or internal with respect to the network under test. While the methods and tools used for assessment and testing are consistent, the tester's approach and the expectation of the findings is different, dependant on the network's internal or external perspective.

When conducting the vulnerability assessment and penetration test from an external perspective, the tester's view is restricted to the public face of the network. The view usually includes limited network knowledge pertaining to the routable public internet protocol (IP) addresses and the network's web services including file transfer protocol (FTP) services, mail services, and domain name system (DNS) services. The configurations of these services usually block access to the organization's internal local area network (LAN) by any outside untrusted party. As such, the perspective of the external tester is that of someone who is outside of the network looking for any weakness or vulnerability that might provide network access.

Conversely, the perspective of the tester who is internal to the network is that of a trusted party who has the freedom to look around. The trust provided to an internal network user usually translates into an elevated privilege level and increased access to network services and devices. An elevated privilege status may also provide the user configuration rights to various network devices or operational software. Given the level of increased privilege and access, the internal tester is not usually looking for a way into the network. Instead, the internal tester will likely concentrate on finding weaknesses in those operational services or device configurations not accessible to those external to the network.

The projects of this report include one discussion where the vulnerability assessment and penetration testing occurred from an internal perspective, and another where vulnerability assessment and penetration tested occurred from and external perspective. While the tools and

methodologies used in each of the projects was consistent, the outcomes were significantly different.

As the purpose of these projects was to determine the security posture of each network, note that various changes to network IP addresses, stakeholder names, email address, phone numbers, etc. were altered to protect the networks or individuals involved. For example, alpha characters replaced the numeric characters of the network potions of production IP addresses, listed email addresses refer to non-existent recipients, and listed phone numbers are not valid. While these changes protect the networks and people specific to these projects, the changes do not affect the value of the discussion. All of the concepts, methods, or techniques described in this report stand on their own merit and do not rely on the identification of a specific network, host or individual.

Chapter 2 - CANVAS Network Assessment and Testing

The Computer and Networking Visualization and Simulation (CANVAS) security event is a cyber competition providing participants an opportunity to compete in a real-world information security exercise. In April of 2011, Regis University hosted the sixth Annual CANVAS competition (Regis University, 2011). In preparation for the event, testing of the CANVAS network fell on the System Engineering and Applications Development (SEAD) Practicum Penetration Test (Pen Test) group.

CANVAS Project Purpose, Requirements, and Deliverables

The purpose, requirements, restrictions, and deliverables relating to the CANVAS network testing were both straightforward and open-ended. The purpose of the testing was to determine both the vulnerability and exploitability of the CANVAS network with respect to the goals of the competition. The requirements, restrictions, and deliverables relating to the testing of the CANVAS network were as follows:

1. The project required the use of an assigned VMware account to perform an inside network test of the CANVAS network. Any testing of the CANVAS network would originated from the assigned VMware account.
2. The tools used in all CANVAS network assessment and testing were restricted to those loaded on the assigned VMware account.
3. The project deliverable was a report providing as much information as possible regarding the exploitability of any hosts on the CANVAS network.

As the project progressed, the project deliverables expanded to include both pre-hardening and post hardening test findings in the final project report.

A summary listing of the final project purpose, requirements, restrictions, and deliverables are in Table 1: CANVAS Project Purpose, Requirements, Restrictions, and Deliverables.

Table 1: CANVAS Project Purpose, Requirements, Restrictions, and Deliverables

- Identify the exploitability of the pre and post hardened CANVAS networks
- Use the Regis University provided tools to test the CANVAS network
- Enumerate network hosts and services
- Conduct penetration testing to exploit as many hosts as possible on the pre and post hardened network
- Report findings to project stakeholders

CANVAS Project Tools and Resources

BackTrack 4.

The test platform provided by Regis University consisted of an assigned virtual machine (VM) loaded with BackTrack 4 (BT4). BackTrack is a utility that functions as both an operating system (OS) and a comprehensive collection of security-related tools. The tools included with the BackTrack framework are commonly available tools for use by network security practitioners, and support various security tasks including digital forensics, network assessments, and penetration testing. Two tools of note are included with the BT4 tool-set, both proving useful for the testing of the CANVAS network. These tools are Nmap and Metasploit.

Nmap.

Nmap (short for “Network Mapper”) is a freely available, open source test utility used for network exploration, network administration, and security auditing. First released in 1997 with

the Phrack Magazine article, *The Art of Port Scanning* (Phrack, 1997), Nmap quickly gained popularity with hackers and network security professionals. Industry periodicals such as the Linux Journal (Linux Journal, 2001), Info World, LinuxQuestions.Org, and Codetalker Digest named Nmap the "Security Product of the Year" (Nmap, 2011). Nmap is consistently one of the top ten most research tools at the freshmeat.net repository. Common uses of Nmap include network host discovery, port scanning, services and applications version detection, and OS fingerprinting (freshmeat.net, 2011).

Nmap training resources.

Although volumes of published information regarding the function and use of Nmap is readily available from books, magazines, technical articles, and websites, an authoritative resource for Nmap is found at the nmap.org website (http://nmap.org). Both the Nmap website and the Nmap tool are maintained by a group of, "…hardcore members (especially programmers) who are interested in helping the [Nmap] project by developing new code and additional features" (Nmap, 2011). Resources provided at the nmap.org home page include links to various urls from which the user can download the Nmap tool, get information regarding Nmap installation, locate the online Nmap reference guide, purchase the Nmap reference book, locate Nmap training, and view examples of where and how Nmap has been portrayed in the media (e.g. movies, books, and television shows).

A resource regarding any technical aspect of Nmap is the book, *NMAP Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning* written by Nmap's creator, Gordon "Fyodor" Lyon. The author regards the work as the "Official Nmap project guide to network discovery and security scanning" (Lyon, 2008). This work provides both experienced and novice users detailed information on all aspects of Nmap including

obtaining the Nmap source code; compiling, installing, and removing Nmap from a given computer; host discovery and port scanning; the Nmap scripting engine; optimizing Nmap performance; and defensive tactics to implement when guarding against internal, or external network scans.

Metasploit.

The second tool used extensively during the vulnerability scanning and penetration testing of the CANVAS network was Metasploit. Like Nmap, the Metasploit Framework is a popular and widely used tool. However, as Nmap's focus is on port scanning, Metasploit's focus is host vulnerability and exploitation.

Since its initial release in 2004, Metasploit has quickly gained significant popularity within the hacker and security communities rising to fifth on the list of the "Top 100 Network Security Tools" according to sectools.org (sectools.org, 2011). As for now, Metasploit Framework is available as freeware downloadable from the Rapid 7 website (Rapid 7, 2011) and is available as part of the BackTrack OS and tool set.

Metasploit training resources.

While a significant amount of information regarding the use and operation of Metasploit is available from books, articles, and websites, a series of informative Metasploit video tutorials is available at the Security Tube website available at http://www.securitytube.net/. In addition to the Metasploit tutorial, Security Tube offers a number of other security-based videos including tutorials on penetration testing, exploit research, assembly language programming, and network and computer hacking.

Security Tube's Metasploit Megaprimer tutorial is a series of 17 videos focusing on the use and capabilities of the Metasploit Framework. The training illustrates how to use BT4,

Nmap, and Metasploit tools to identify and exploit the vulnerabilities of target victim machines. The tutorials spend ample time demonstrating the function and operation of the Metasploit Framework as well as the strategic operation of various exploits.

Security Tube's "Metasploit Megaprimer" video tutorial includes approximately 15 hours of video training over 17 individual videos. Tutorial topics cover various and numerous aspects of the Metasploit Framework's theory of operations and functional usage (SecurityTube, 2011).

CANVAS Network Test Methodology

The CANVAS requirements, restrictions and deliverables all but mandated the test methodology. The project deliverables included a listing of the host IP address and exploitation vectors for the pre-hardened CANVAS network. By using the appropriate command line options, Nmap is capable of producing a list of active network hosts, determining the OS running on each host, an enumerated list of the host's open ports, and determining the software and version of each utility servicing the open ports. Given Nmap's capability for host detection, port discovery, OS finger printing and service detection; as well as Nmap's inclusion in the suite of tools provided with the BT4 tool set made Nmap the logical and available host discovery tool of choice.

CANVAS network host discovery.

The customary first step of host discovery is the enumeration of active IP addresses within an address range. Sending a network "ping", also referred to as "pinging the network", is a function of Internet Control Message Protocol's (ICMP) echo request capabilities. Virtually all TCP/IP based networks use ICMP to relay query messages, respond to query messages, and communicate network status. Echo requests and echo replies are two of the numerous and frequently used network communication features available with ICMP.

Nmap ping scan methodology.

When a host receives a ping, network conformance requirements mandate that the host respond with an ICMP echo reply (Internet Engineering Task Force, 1989). The completed echo request/echo reply cycle verifies that a host exists at a specific network address, and that communication between the initiator and responder is possible. When used by Nmap as a method of network host discovery, the ICMP echo request/echo reply cycle is part of a ping scan, which provides the initiating host discover information regarding which IP addresses are home to an active host, have no hosts, or are attempting to hide from external discovery.

For security reason, some network administrators purposely block an ICMP echo ping request. Even if blocked, most active hosts will respond to either a TCP ACK packet sent to port 80, or a SYN packet sent to a host as a request to establish inter-host communications. As such, an Nmap ping scan not only includes an echo request, but also an ACK packet sent to port 80, and a SYN packet sent to a targeted IP address (Insecure.com LLC, 2004).

By tracking the IP address of responding hosts, the initiator is able to comprise a list IP addresses containing active hosts. Additionally, the host knows that non-responsive addresses indicate either an address at which no host resides, an address at which a host is hiding behind a firewall, or a host that is non-compliant regarding communications between internet hosts per RFC 1122 (IETF, 1989). For purposes of the CANVAS network competition the assumption was that no firewalls were hiding hosts, that a non-responding IP address indicated a lack of a network host, and that all hosts were compliant with RFC 1122.

With the completion of the Ping Scan, network discovery was complete. The value of the information gained through network host discovery is in knowing which IP addresses deserve additional testing, and which IP addresses to ignore.

The project stakeholders provided no information about the CANVAS network concerning size, addresses, or the number of active hosts. The only information about the CANVAS network came from the IP address of test host assigned to the tester. The test host resident at address 10.128.128.123, which led to the following assumptions:

- The test host resided on the CANVAS network
- The CANVAS competition network required no more than 254 hosts
- The CANVAS network address was 10.128.128.0/24

Fortunately, each of the above assumptions proved correct. A ping scan using the Nmap command *nmap –sP 10.128.128.0/24* provided information regarding both network host discovery and an initial enumerated list of active network hosts. See Table 2: *Active CANVAS Hosts* for a listing of the enumerated hosts found by the above Nmap command.

Table 2: Active CANVAS Hosts

10.128.128.1	10.128.128.2
10.128.128.3	10.128.128.50
10.128.128.68	10.128.128.69
10.128.128.71	10.128.128.80
10.128.128.100	10.128.128.121
10.128.128.122	10.128.128.123
10.128.128.124	

While the listing in Table 2 proved accurate for the initial network host enumeration, note that this initial listing is not consistent with host listings taken later in the project. For purposes of the CANVAS competition, the competition organizers included additional network hosts, and changed the IP addresses of others.

CANVAS network port analysis.

With an understanding of the network address range and the network size, the next step included a network scan for open port and the determination of port services. The command

nmap –p0-65535 10.128.128.0/24 executed a port scan across all 65,535 ports of each active host, provided a list of open ports, and determined the port services running on each of the open ports. See Table 3: Port Scan of CANVAS Network, for a partial listing of the above command output and Appendix A: *CANVAS Network All Host/All Ports Scan Results* for a complete listing of the port scan results.

Although the vulnerabilities shown for the majority of the CANVAS hosts were similar to those for hosts 10.128.128.1 and 10.128.128.124, three hosts, 68, 69, and 100, had vulnerabilities similar to that of host 10.128.128.68. The open ports and the running services of hosts 10.128.128.68, 69, and 100 identified these hosts as candidates of interest and targets for additional scanning and possible exploitation.

CANVAS network automated penetration testing.

With network host and port discoveries both complete, enough information regarding the CANVAS network was at hand to initiate exploitation attacks. The tool of choice for the CANVAS network exploitation was Metasploit.

One of Metasploit's useful features is its ability to launch automated exploits using database values as input. This feature allows the output of certain third party tools to load a database with IP addresses. Fortunately, one of these third party tools is Nmap.

Executing Nmap commands from within Metasploit results in a database whose data values include a list of network host IP addresses, a list of open ports, and the services running on each of the open ports. Executing Nmap from within Metasploit and piping the output into a pre-defined database only requires adding the *db_* prefix to any Nmap command.

For example, the command *db_nmap –p0-65535 10.128.128.0/24* executes an Nmap total port scan on all hosts residing on the CANVAS network and saves the results in a previously

Table 3: Port Scan of CANVAS Network

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-03-12 14:39 MST
Nmap scan report for 10.128.128.1
Host is up (0.0057s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:00:0C:07:AC:01 (Cisco Systems)

{Output cut for sake of brevity}

Nmap scan report for 10.128.128.68
Host is up (0.00039s latency).
Not shown: 65509 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
515/tcp  open  printer
548/tcp  open  afp
1046/tcp open  unknown
1063/tcp open  unknown
1065/tcp open  unknown
1070/tcp open  unknown
1074/tcp open  unknown
1076/tcp open  sns_credit
1077/tcp open  unknown
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
3459/tcp open  unknown
MAC Address: 00:50:56:84:00:00 (VMware)

{Output cut for sake of brevity}

Nmap scan report for 10.128.128.124
Host is up (0.00048s latency).
All 65536 scanned ports on 10.128.128.124 are filtered
MAC Address: 00:50:56:84:00:26 (VMware)

Nmap done: 256 IP addresses (13 hosts up) scanned in 1572.98 seconds
```

specified database. Metasploit can then use the database values (e.g. IP addresses, port data, and other values resident in the database) to develop a list of known vulnerabilities and execute automated exploitation attacks against the target network. While automated exploitation may provide only minimal advantages when testing a network the size of CANVAS, the ability to run automated exploitations against a network comprised of thousands of hosts is a significant timesaving feature and provides a handy method for saving and organizing network exploitation results.

Metasploit's *db_autopwn* pipes the values of an existing database into the input queue of the command. The command itself invokes Metasploit's automated capabilities including:

- Automatic choice and launch of exploits against a target host or range of hosts
- Spawning of a Meterpreter session resulting from a successful exploitation
- Creation of multiple Meterpreter sessions from the exploitation of multiple vulnerabilities
- Exploitation of specific targets stored in the database

As with most command line tools, a number of command line options are available. The following options are available for use with the *db_autopwn* command:

- -t Show all matching exploit modules
- -x Select modules based on vulnerability references
- -p Select modules based on open ports
- -e Launch exploits against all matched targets
- -r Use a reverse connect shell
- -b Use a bind shell on a random port
- -h Display this help text (Metasploit, 2006)

- -I [range] Only exploit hosts inside this range

The command *db_autopwn –e –p –t –I 10.128.128.1-122* invoked Metasploit's automated capabilities executing the various command line options (-e, -p, -t and –I) as described above. The results of this command are below in Table 4.

Table 4: Metasploit db_autopwn Results for CANVAS Network

10.128.128.1 > 1 open port, 4 exploits, 0 sessions.
10.128.128.2 > 1 open port, 4 exploits, 0 sessions.
10.128.128.3 > 1 open port, 4 exploits, 0 sessions.
10.128.128.4 > 1 open port, 4 exploits, 0 sessions.
10.128.128.50 > 4 open ports, 50 exploits, 0 sessions.
10.128.128.68 > 23 open ports, 290 exploits, 5 sessions.
10.128.128.69 > 22 open ports, 290 exploits, 9 sessions.
10.128.128.71 > 2 open ports, 50 exploits, 0 sessions.
10.128.128.72 > 21 open ports, 294 exploits, 6 sessions.
10.128.128.100 > 19 open ports, 186 exploits, 0 sessions.
10.128.128.121 > 1 open port, 106 exploits, 0 sessions.
10.128.128.122 > 2 open ports, 50 exploits, 0 sessions

As shown in Table 4, the exploitation of the hosts at 10.128.128.68, 69, and 72 resulted in Meterpreter sessions. Note that the host at 10.128.128.100 was not exploitable contrary to the results given previously and prior to the execution of the automated exploit command.

Initial network and port discoveries identified the host at IP address 10.128.128.100 as both functioning, and having a number of open ports and running services (see Table 2 and Appendix A). Additionally, the initial scans did not detect an operational host at IP address 10.128.128.72. However, as shown in Table 4, the host at IP 10.128.128.100 proved immune from the exploitation while the host at 10.128.128.72 was exploitable. The reason for this inconsistency was not a problem with the test tools or the test methodology. Instead, the inconsistency proved to be the result of network changes made by the project stakeholders to ready the CANVAS network for competition.

Meterpreter sessions.

The establishment of Meterpreter sessions indicates the compromise of the network host. In a white paper written about Metasploit's Meterpreter, the paper's author describes the Meterpreter as

> "an advanced payload that is included in the Metasploit Framework [that allows] developers to write their own extensions in the form of shared object files that can be uploaded and injected into a running process… Meterpreter and all of the extensions that it loads [execute] entirely from memory and never touch the disk, thus allowing them to execute under the radar of standard Anti-Virus detection"(skape, 2004).

Simply stated, when a Metasploit exploit results in a Meterpreter session, the attacker has near, if not total anonymity while on the victim machine. This anonymity provides the attacker the ability to browse file content, create files, delete files, download files from the victim machine, or upload files or software utilities of choice to the victim machine, and do so with near anonymity. Since the Meterpreter only resides in the victim machine's RAM, presence of the Meterpreter session is usually undetectable by anti-virus software. Additionally, all traces of the session may vanish with subsequent data writes to the system RAM, or when the victim system powers down.

To provide evidence regarding the compromise of the hosts at addresses 10.128.128.68, 69, and 72, and to show that user access was elevated to a privileged level during the Metepreter session, a small text file was written in each host's C:\WINDOWS\system32 folder informing the system owner of the compromise. While significant changes to the compromised host were possible, the charter of the project was only to determine host exploitability. As such, the exploitation of the compromised hosts only included the creation of the aforementioned text file.

Note that while each identified host was a target of exploitation, only those hosts that lacked sufficient security protection were victim to the attacks. Hosts containing sufficient hardening were not penetrated and remained uncompromised.

Pre-hardened network test results summary.

The delivery of a summary report to the appropriate stakeholders completed the pre-hardening phase of the CANVAS network test. The report simply listed the command used for the exploitation and that a small number of hosts were vulnerable to the Metasploit automated exploitation. Appendix B: *CANVAS auto test summary – 031811,* includes a copy of the report sent to the top stakeholders summarizing the findings of the pre-hardening CANVAS network testing.

Post Hardening Penetration Testing.

To properly configure the CANVAS network and ready the competition platform, the project stakeholders hardened the network. System hardening is a, "process of securing a system by reducing its surface of vulnerability by the removal of any software, user accounts or services that are not related and required by the planned system functions" (Shortinfosec, 2011). By hardening specific hosts, the stakeholders controlled exploitable network resources while continuing to allow the competitors access to specific information. To confirm the network was hardened per plan, the project stakeholders relied on post-hardening network testing.

Testing of the post-hardened CANVAS network only required a network re-test using Metasploit's automated capabilities as previously described. Neither host, nor port discovery was required. Additionally, retest was only required of the three previously exploitable hosts; those hosts at IP addresses 10.128.128.68, 10.128.128.69, and 10.128.128.72.

As with the testing of the pre-hardened network, the post-hardened network testing would include the automated capabilities of Metasploit. The command *db_autopwn –e –p –t –I <target>***,** where <target> was the IP address of each of the previously failing hosts was again executed. Table 5: *Post-hardening Test Results Summary* shows the results of the test. As shown, hardening occurred on two of the three hosts leaving only the host at IP address 10.128.128.69 susceptible to exploits.

The delivery of the final test results concluded the testing of the CANVAS network. See Appendix C: *Canvas testing for 03222011* for a copy of the final report.

Table 5: *Post-hardening Test Results Summary*

10.128.128.68 > 24 open ports, 382 exploits, 0 sessions
10.128.128.69 > 15 open ports, 60 exploits, 9 sessions
10.128.128.72 > 23 open ports, 382 exploits, 0 sessions

CANVAS Project Summary

The use of a virtual network account and three well known, and widely used, security tools provided the resources and framework allowing the successful test and exploitation of the CANVAS network. Project specifications required the use of a VMware account, BackTrack 4, Nmap, and Metasploit to enumerate network hosts, discover network services, and exploit any vulnerability found on the pre or post hardened CANVAS network. The pre-hardened network included three hosts vulnerable to exploitation, which and was compromised using Metasploit and Meterpreter sessions. The post-hardened network testing resulted in the discovery of only a single host susceptible to compromise. Reports sent to the project stakeholders identified the differences between the pre and post-hardened networks and provided the project stakeholders with information regarding the vulnerabilities and exploitability of the pre and post-hardened networks.

While other tools and methodologies may provide similar results, the resources provided, and the methods developed for this project proved useful. The resources and methods used proved successful for use with network host discovery, host port analysis, port service evaluation, and the exploitation of vulnerable network hosts.

Chapter 3 - ITS network vulnerability assessment and penetration testing

The Information Technology Services (ITS) network vulnerability assessment and penetration-testing project was similar to the CANVAS project in that the purpose of each was to provide a security assessment of a given network. Because of the similarities, many of the overall project methodologies, tools and deliverables were similar, if not identical, to one another. However, the ITS network had significant differences with respect to network purpose, function, and topology, as well as the perspective from which the vulnerability assessments and penetration tests were launched.

CANVAS was a virtual network existing primarily as a network platform for a specific competition. Conversely, the ITS network is a fully functional, physical network of servers, clients, printers, routers, etc. designed, built, and maintained for the on-going use and support of the Regis University administration, faculty, and students. Given the ITS network's intended use, internal testing of the network was not allowed. While the CANVAS assessment and testing occurred only from an internal perspective, the ITS network assessment and testing occurred only from an external perspective. The execution of all assessment and penetration tests occurred from a test host external to the ITS network.

ITS Project Requirements, Project Restrictions, and Project Deliverables

There were two each of project requirements, restriction and deliverables. While some are straightforward and easily understood, others had a significant impact on the project. Those requirements, restrictions, or deliverables that influenced the project results or methodologies are included in the detailed discussions in the appropriate sections of this paper.

Project Requirements.

The overall project requirement was to determine the vulnerability exposure of the ITS

network. While this requirement stopped short of specifying how the exposure was to be determined, the stakeholders and test team jointly decided that conducting a network vulnerability assessment and penetration test was the preferred approach.

The second requirement was that testers were to inform specific university personnel of their intended testing. This requirement obligated testers to provide specific information to the Regis University ITS Security Officer (ITSSO) and project advisors regarding the activities of a network test session. Testers were to provide information prior to the initiation of a test session and again once the session completed. A discussion regarding the specifics of the test notification process (TNP) is in the Project Test Plan section.

Project Restrictions.

Project restrictions pertained to the permitted types of assessments, types of testing, and IP address range of the network under test. Testers were free to implement any form of vulnerability or penetration testing as long as these activities had no adverse impact on any operational aspect of the ITS network. Additionally, if a tester were to uncover a network weakness that resulted in the compromise of a network host, the tester was to suspend any active or planned test execution and immediately inform the ITSSO of the network vulnerability.

The second restriction limited the testing of the network to the IP address range specified by the Regis ITSSO. At the time of the assessment, Regis University operated and maintained at least four networks. Sanctions to test the Regis network applied only to the network specified by the ITSSO.

Project Deliverables.

The deliverables of the ITS project included the development of a formal test plan and the submission of a report summarizing the project test findings. A discussion regarding the

details of the project test plan are in the section that immediately follows, and a summary of the test results are in the section titled ITS Network Assessment and Penetration Test Results Summary.

Table 6: ITS Project requirements, restrictions, and deliverables summarize the project attributes.

Table 6: ITS Project requirements, restrictions, and deliverables

ITS Project Requirements
Determine the security posture of the ITS network
Inform the university ITSSO of all test activity
ITS Project Restrictions
Do not disable or harm any portion of the network during testing
Network testing restricted to IP range specified by ITSSO
ITS Project Deliverables
Provide a summary of findings
Develop a formal project plan

Project Test Plan

The test plan content and format followed the recommendations outlined in documents published by the National Institute of Standards and Technology (NIST) and the Institute for Security and Open Methodologies (ISECOM). Both documents address activities germane to vulnerability scans and penetration testing and served as resources regarding the test plan format, content, and test methodologies utilized during the ITS network project.

NIST's Special Publication 800-115 is part of a series of documents whose purpose is to provide guidance to the computer security industry and to those involved with network security. The NIST commissioned the Information Technology Laboratory (ITL) to write Special Publication 800-115 in order to provide network security practitioners with a proposed guide for network vulnerability assessments (NIST, 2008). Specifically, the NIST charter directs ITL to develop

> [T]ests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. (NIST, 2008)

As reflected in the project test plan, NIST Special Publication 800-115 provided information regarding network host discovery, port analysis, port service identification, and vulnerability scanning. Special Publication 800-115 Appendix B – *Rules of Engagement Template*, and Appendix D - *Remote Access Testing*, provided specific guidance with respect to the ITS network vulnerability scanning methodologies and practices.

The Open Source Security Testing Methodology Manual (OSSTMM), version 3.0, published by the ISECOM was an additional resource. Self advertised as "a peer-reviewed methodology for performing security tests and metrics", the OSSTMM provides information covering multiple aspects of network testing. Specifically, the OSSTMM addresses test topics such as "information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations" (Herzog, 2011).

The content of chapters 2, 6, and 11 of the OSSTMM applied specifically to the project plan for the ITS network. Combined, these chapters provided insight into the definition, scope, common test types, operational test processes, and rules of engagement regarding the ITS network security test.

Test Notification Process.

One project requirement included the notification of project stakeholders at the initiation and at the close of the pending test session. The need for a test notification reflected the ITSSO's concern that a network test might trigger an internal intrusion detection device, or result in network downtime. In either event, the network administrator might spend an inordinate amount of time trying to resolve issues that could result from a sanctioned test activity. To counter this concern, the ITSSO and the author of this paper developed, refined, and implemented the test notification process described below.

Prior to any network scanning or network test action the tester was to complete a Test Notification Form (TNF) supplying the following information:

- The tester's name, phone number and email address at which Regis ITS personnel could reach the tester,
- the IP address of the test host,
- the targeted network IP address, or IP address range,
- the name and version number of the tool(s) used during the test session, and
- the approximate starting time of the test session.

In addition to the above information, the tester was to notify the ITSSO, via a phone text message, at the initiation of the test session and again at the close of the test session.

The test notification process, as it appears in the project test plan, is below and culminates with an example of a completed TNF, as shown in Table 7: *Completed Test Notification Form*.

Test notification process:

1 Fill out your name in the appropriate space

2 Go to a site such as www.whatsmyip.org or www.whatsmyip.com and get your IP address as viewed by the internet. Getting your IP address from a command like ipconfig or ifconfig will provide a private address known only to your ISP.

3 Fill out the network IP address and address range you will be testing. For example, aaa.bbb.ccc.1-30 will target the IP address range 1–30 of the network aaa.bbb.ccc.0.

4 Fill out the name of the tool you will be using for your test.

5 Fill out the tool's revision number

6 Complete the sections regarding the best phone number and email address at which to reach you during your test session.

7 Mail the completed TNF to the following addresses:

- Aaaa@regis.edu;
- ITSO@regis.edu;
- Bbbb@regis.edu;
- Cccc@regis.edu.

8 At the beginning of a test sessions all testers are required to send a phone text to Aaaa at (702) 555-5555 stating your name and your intention to start a test session. An example of an initiating text would be something similar to "Hello Aaaa, This is <tester's first and last name> initiating a test session."

9 Once the tester has completed a test session a closing text must be sent to Aaaa at (702) 555-5555 stating you name and your intention to end a test session. An example of a closing text would be something similar to "Hello Aaaa, This is <tester's first and last name> ending a test session."

An example of a completed form is below:

Table 7: Completed Test Notification Form

Who is doing the PEN Testing:	Student name
What is the source IP address:	xxx.yyy.zzz.115
What address or addresses will be targeted:	aaa.bbb.ccc.0/24
What tool and version will be used:	BackTrack
Version:	Version 5
What is the intended testing time (beginning):	8:30 pm PDT
Phone number where the tester can be reached during the testing:	243 555-5555
Best e-mail address to reach tester:	name123@regis.edu

Project Tools and Resources

The tools and resources used during the test of the ITS network were identical to those used during the CANVAS testing with the following exceptions:

- All testing resources used to test the ITS network were provided by the tester. These resources included computer hardware, software, and internet connections.
- The testing of the network utilized a newer release of the BackTrack OS and security tool set. The public release of BackTrack 5 provided a newer revision of the tool.

Test station configuration.

The computer hardware, software tool set, and internet connection used for the author's test station included the following:

- A Hewlett-Packard Pavilion a250y personal computer configured as follows:
  - Intel P4 3.2 GHz CPU w/Hyper Threading Technology
  - 1 GB Double Data Rate (DDR) memory
  - 200GB hard disk drive (HDD)
  - CD writer and DVD ROM
- BackTrack 5 OS and associated tool set

- Cable-based internet access provided by a local Internet Service Provider (ISP)

Software test tools.

BackTrack is a well-known and widely used open source security framework, which provides a number of tools used for a variety of network and computer security related tasks. Two of these tasks include vulnerability assessments and penetration testing. Additionally, the release of BT5 includes both the Nmap and Metasploit Framework tools.

The choice to use Nmap was the result of the tool's host discovery and port analysis capabilities, but more importantly the following reasons:

- the ability to list the active and responsive host IP addresses
- the OS running on each of the above hosts
- open ports of the hosts
- service identification of the open ports

The choice of Metasploit Framework was due to the tool's ability to execute a suite of automated exploits based on known vulnerabilities. Metasploit also has the ability to use network discovery data generated by Nmap as input to target specific network hosts. The combination of BT5, Nmap, and Metasploit provided a complete tool set, which met all the project objectives.

ITS network assessment and penetration test methodology

The primary object of the project was to determine the vulnerability exposure existing on the ITS network. The project stakeholders jointly agreed that the determination of the network exposure included both a vulnerability assessment and a targeted network penetration test. The network assessment and the resultant testing would occur in three distinct phases, including:

- Host Discovery

- Port analysis
- Penetration testing

The results from the host discovery and port analysis phases would complete the vulnerability assessment requirements, while the results of the penetration testing phase results would confirm the existence of any actual network vulnerability.

Host discovery is the term used to describe the scanning process of finding targets connected to specific network range (Foreman, 2010). As discussed and demonstrated in the CANVAS project discussion, the capabilities of Nmap resulted in Nmap as the author's tool of choice for host discovery.

Port analysis is a combination of OS detection and version detection of port services operating on the open port(s) of an active host. As with host discovery, Nmap provides the capability necessary to meet the port analysis requirements.

Each Nmap scan would address one, or more aspects of the stated deliverables. While the default output for the Nmap tool is the system monitor, a method of saving scan results occurs by redirecting the Nmap output to a text file or by specifying an output file format.

At times, converting the Nmap output into a human readable format requires running the output file through a utility written specifically to convert Nmap output into readable text. A simple PERL script, written by this author, removes unreadable text characters leaving all other information intact. Appendix E is the listing of the PERL script, *replace.plx*. Note that some of the Nmap command outputs displayed in the remainder of this paper have gone through the above conversion process for the sake of readability.

ITS network assessment - host discovery.

The first step in network testing is host discovery. Knowing the active and non-active IP addresses is fundamental to complete network understanding. The output of an Nmap ping scan provides not only a list of the active hosts, but by omission, a list of inactive hosts. As such, the use of an Nmap ping scan is a way to accomplish host discovery.

The command *nmap –sP aaa.bbb.ccc.0/24 > external_ping.txt* specified the ping scan (*-sP*) of the targeted network at *aaa.bbb.ccc.0/24*. The redirection of the output to the file *external_ping.txt* stored the command results allowing further review and analysis.

The ping scan found 89 active hosts on the ITS network. Table 8: *ITS Network Ping Scan Results* is an abbreviated representation of the ping scan output. Appendix F lists the complete result of the ping scan command as executed by the Nmap tool.

Table 8: ITS Network Ping Scan Results

```
Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-26 14:31 PDT
Nmap scan report for aaa.bbb.ccc.1
Host is up (0.058s latency).
Nmap scan report for aaa.bbb.ccc.2
Host is up (0.049s latency).
Nmap scan report for www2.regis.edu (aaa.bbb.ccc.33)
Host is up (0.059s latency).

{output cut for the sake of brevity – See Appendix F for complete listing}

Nmap done: 256 IP addresses (89 hosts up) scanned in 17.13 seconds
```

ITS network assessment - port analysis.

Armed with the knowledge of the active network hosts, the next step included the collection of information necessary for port analysis. Specifically, the required information included:

- operational state of every port of an active host
- software and version providing services on every open port

- OS and version running on each host

Nmap includes command options able to provide each of the above requirements. While individual scans could provide the above requirements, the above requirements resulted from a single scan.

Prior to discussing the command used to collect the above data, note that a complete network vulnerability assessment requires the analysis of all ports on each active network host. Leaving some ports untested while testing others would not provide all information needed for the complete evaluation of a given network. Additionally, omitting the port analysis of any active host could result in the overlooking of network vulnerabilities.

The configuration of computers connected to, and communicating via the internet use the transmission control protocol/internet protocol (TCP/IP) suite of protocols, and require the potential availability of 65,535 ports. While it is theoretically possible to have all 65,535 ports open simultaneously, the common practice is to open only the ports needed for specific communication. To determine which of the 65,535 ports are open on any given host, testing occurs on all ports. The testing of 65,535 ports for each network IP address can require a significant amount of time. To help reduce the time required to analyze all ports of a network range, Nmap provides an option limiting port analysis to specific hosts.

Limiting port analysis to include only active hosts may provide a significant reduction with respect to the time required for the completion of network port analysis. With respect to the ITS network, limiting port analysis to those hosts discovered suing the ping scan reduces the port analysis to 89 known active network hosts (down from 254 possible network hosts). The Nmap option used to leverage this capability is the –iL <filename> option. Using this option will direct Nmap to scan only those IP addresses listed in the named file.

The file *external_up.txt* contains the listing of the 89 ITS network active hosts as determined by the previously run ping scan. Using this file, in conjunction with the *–iL <filename>* option, will limit the port analysis to those IP addresses listed in the file *external_up.txt*.

Table 9 shows a partial listing of the file *external_up.txt* with the full listing of the file in Appendix G.

Table 9: Partial Listing of external_up.txt

aaa.bbb.ccc.1
aaa.bbb.ccc.2
aaa.bbb.ccc.33
aaa.bbb.ccc.34
aaa.bbb.ccc.36
aaa.bbb.ccc.37
aaa.bbb.ccc.38
aaa.bbb.ccc.39
aaa.bbb.ccc.40
aaa.bbb.ccc.41

{output cut for brevity}

aaa.bbb.ccc.218
aaa.bbb.ccc.219
aaa.bbb.ccc.220
aaa.bbb.ccc.222

The Nmap command used to collect the information required for port analysis includes the *–iL <filename>* option, which specifies the scanning of certain IP addresses as listed in the named file. The specific Nmap command follows:

nmap –sS –O –sV –p1-65535 –iL external_up.txt > external_ports_all.txt

The above command

- invokes Nmap *nmap*
- calls the SYN scan *-sS*

- calls remote host fingerprinting *-O*
- calls the version detection option *-sV*
- applies above option to all ports *-p1-65535*
- uses a file as input to scan specific IPs *-iL external_up.txt*
- redirects the output to a specified file *> external_ports_all.txt*

The output of this scan provides each port's operational status, host OS detection/fingerprinting, and port service version detection for all 65,535 ports for each of the 89 known active hosts on the ITS network. This command also redirects its output to the file *external_ports_all.txt* allowing for additional review. Completion of the scan provides all the data meeting the requirements of port analysis. Table 10: *Sample ITS Network Port Analysis Scan Results* is a representative sample of the scan output with Appendix H providing a complete listing of the port scan results.

An analysis of the command results in Table 10 show that the initial three lines include a variety of information pertaining to the host's domain name, IP address, the host's operational state, the observed latency time, and the operational state of the ports not specifically listed with the remainder of the host data.

These three lines of information are common across the results of most Nmap scans and act as a header to the specific host data. A listing of specific ports, the operational state of each listed port, the service running on each port, and the service version, follow the header. Host information concludes with a listing of Nmap's best effort at determining the host's OS, OS version, and device type.

The port's operational status provided by Nmap scan results refer to the state of the port at the time of the scan. Nmap uses six states to describe port operational status defined as follows:

Table 10: Sample ITS Network Port Analysis Scan Result

Nmap scan report for its02.regis.edu (aaa.bbb.ccc.36)
Host is up (0.033s latency).
Not shown: 65520 filtered ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Microsoft ftpd
80/tcp	open	http	Microsoft IIS httpd 7.0
443/tcp	open	ssl/http	Microsoft IIS httpd 7.0
990/tcp	open	ssl/ftp	Microsoft ftpd
4900/tcp	closed	hfcs	
4901/tcp	closed	unknown	
4902/tcp	closed	unknown	

{Output cut for brevity}

4909/tcp	closed	unknown
4910/tcp	closed	unknown

Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

- open – The service operating on an open port is actively accepting transmission control protocol (TCP) connections or user datagram protocol (UDP) packets. In some cases, a TCP wrapper will protect an open port by limiting access to approved IP addresses.
- closed – A closed port is accessible to Nmap in that the port receives an Nmap probe and responds. However, a closed port has no operational, or listening service.

- filtered – Nmap cannot determine if the port is open as packet filtering or other firewall rules block the port.
- unfiltered – Nmap can access the port but is unable to determine if the port is in the open or closed state.
- open|filtered – This state indicates that Nmap sees the port as open, but the port provided no response to an Nmap probe. Since a lack of response could also indicate a filtered port, Nmap is unable to differentiate between a lack of response and a filtered response; it places the port in the open|filtered state.
- closed|filtered – This state indicates that Nmap cannot make the determination between a closed or filtered state.

Note that the port's operational status, in combination with port service and version information, may indicate the presence of one or more vulnerabilities on a given host.

Information specific to device type may also indicate the presence of network or host irregularities. Nmap determined that the host shown in Table 10 has a device type of "general purpose". Other device types found on the ITS network (see Appendix H) include firewall, wireless access point (WAP), broadband router, router, switch, VoIP phone, VoIP adapter, printer, webcam, media device, game console, storage-misc, and remote management. While none of the listed device types identifies specific malicious activity, a device type coupled with an unusual, unauthorized, or unidentified OS or port service, may indicate the need for further investigation.

ITS network automated penetration testing.

While the manual scanning techniques discussed above supported the host discovery and port analysis of the ITS network, there is no direct method of using these scan results to perform

network penetration testing. While Nmap capabilities proved useful for network host discovery and port analysis, the tool has limited penetration-testing capabilities. Instead, the Metasploit Framework was the tool used to perform the penetration testing and network exploitation.

Metasploit has two features that are useful for the penetration testing. These features include Metasploit's ability to automate the execution of exploits and its ability to use database information generated by a third-party tool. Fortunately, Nmap is one of the third-party tools that can populate a database for later use by Metasploit. To use the above features, the tester must first create or select, and then connect to the appropriate database file prior to using any of Metasploit's automated features.

To create or select, and then connect to the database, the following three commands must execute from the Metasploit Framework command line prompt:

- db_driver mysql
- db_connect
- db_connect root:toor@127.0.0.1/<*database filename*>

The *db_driver mysql* command identifies MySQL as the database of choice. While BT5 contains both MySQL and PostgreSQL, familiarity with the former influenced the choice of MySQL for the ITS network penetration testing. The *db_connect* command connects the database to the current instance of the Metasploit Framework, and the *db_connectroot:toor@127.0.0.1/<database filename>* connects the database to the test host.

The use of <*database filename*> will select an existing database, or create a new database file dependant on the existence of the file at the time of the command execution. If the database file exists, subsequent data appends to the existing file. If no file exists, execution of the

command results in the creation of the file. Regardless, the filename chosen for the command is subject to the tester's discretion.

Executing Nmap commands from within Metasploit only requires prefixing *db_* to any valid Nmap command. For example, by prefixing *db_* to the Nmap command below, the command directs the resultant output to the database previously specified by the tester. The command

db_nmap –sP aaa.bbb.ccc.0/24

- invokes Nmap redirecting output to a database db_nmap
- calls the ping scan option -sP
- ping scans the entire network range aaa.bbb.ccc.0/24

As a comparison, the Nmap command used for manual method of host discovery was

nmap –sP aaa.bbb.ccc.0/24 > external_ping.txt

Note that the only difference between the two commands is the lack of the *db_* prefix, and the redirection of the command output (> external_ping.txt) used in the manual version of the command.

The automated version of the port analysis command follows the same format as that of the automated host discovery command. Invoking the automated version of the Nmap command from within the Metasploit Framework is:

db_nmap –sS –O –sV –p1-65535

As with the manual version, the automated version invokes port scanning, version detection, and OS fingerprinting, directing the output to the previously specified database.

The result of the above two Nmap commands is the population of a previously specified database file containing all the host discovery and port analysis information previously discussed

and listed in Appendix F and Appendix H. With the host discovery and port analysis data captured and resident in a database, the automated capabilities of Metasploit could now provide for the execution of the network penetration testing and the attempts at network host exploitation.

Metasploit's *db_autopwn* command takes its input from a database, evaluates the host discovery and port analysis data, and formulates a list of possible host vulnerabilities. The command then uses these vulnerabilities to launch exploits targeted at specific network hosts, host ports, and running port services. If an identified vulnerability proves exploitable, Metasploit will create a Meterpreter session, which in turn, provides a means of intrusion to the network.

A Meterpreter session executes completely out of the host's memory and may provide the intruder the ability to gain control of the compromised host. Host control occurs if the intruder is successful in the execution of various scripts allowing the elevation of the intruder's privilege level to that of root, or system administrator (dependant on the native OS of the compromised host). Elevated privilege levels may also allow the intruder to download or upload files, install a keystroke logger, create a backdoor, install a rootkit, use the compromised host as platform to launch attacks against other network hosts, or any number of other potentially malicious activities. As discussed previously, any compromise to the ITS network during a sanctioned test session requires the tester to cease all test activities and inform the ITSSO of the exploit.

Invoking the automated exploitation capabilities of Metasploit requires the use of the *db_autopwn* and selected command line options. The command launched against the ITS network was:

db_autopwn –p –e –t –I aaa.bbb.ccc.0/24

Specifically, the above command

- invoked the automated capabilities of Metasploit using the connected database as the command input db_autopwn
- selected exploit modules based on open ports -p
- launched exploits against all matched targets -e
- showed all matching exploit modules -t
- only exploited hosts within a given range -I aaa.bbb.ccc.0/24

The result of the above command identified and launched exploits against 15,631 vulnerabilities, spread across the 89 active ITS network hosts. Of the 15,631 vulnerabilities found, none were successful in the exploitation or compromise of any ITS network host.

ITS Network Assessment and Penetration Test Results Summary

The results of the ITS network vulnerability assessment includes the findings of the network host discovery and the host port assessments. Network host discovery found 89 active hosts on the network. The open ports, port services, identified devices, and host operating systems appeared consistent with those of a network designed and maintained to support a diverse group of users. While the port analysis scan did not identify any obvious network vulnerabilities or malicious activity, a review of the scan results indicated that the network usage of a limited number of IP addresses might warrant further investigation.

Security concern criteria.

Several observed aspects of the scan results raised usage and possible security concerns. The identification of any IP addresses, whose scan results raised these concerns, signified a candidate requiring further investigation. Any IP address identified as such exhibited one or more of the following three characteristics:

1) *Any "Device type" that appeared to serve no or little purpose on a business network*. Such a device could be any number of unauthorized devices including entertainment equipment, communication equipment, storage devices, network monitoring equipment, or any of number of other possible devices or equipment installed on the network by a network user. It is likely that any unauthorized device would likely be out of the control of the network administrators in terms of normal device upgrades and regular security software patches. Use of such devices not only include the possible inappropriate use of network resources, but also might provide a means by which outsiders could gain unauthorized access to the network. Additionally, the attachment of such devices might aid the malicious activities of network insiders.

2) *Any IP address for which the list of "Device type" or "OS guesses" appear greater than normal when compared to the results of other IP addresses on the same network.* A large and diverse list indicates that Nmap could not provide a definitive identification of the device type or OS choice at a given IP address. When Nmap is unable to determine the exact OS from a large number of possibilities, the host at the IP warrants further investigation.

3) *Any host who is running an unidentified service or operating system.* While this might not indicate a security weakness, network administrators may want to confirm that the OS operating on these hosts are those intended for the specified IP address.

Ports scan results analysis.

The *Port Analysis Scan Results Summary* in Table 11 is a summary listing of the port analysis results segregated by the above criteria. As can be seen, the following network IP addresses may warrant further investigation:

- aaa.bbb.ccc.196
- aaa.bbb.ccc.198
- aaa.bbb.ccc.199
- aaa.bbb.ccc.203

The flagging of the hosts at IP addresses 196, 198, and 199 are due to the possibility that these addresses may include an unauthorized device, or because OS fingerprinting identified a suspicious OS. Possible devices at these addresses include a switch, wireless access point, printer, webcam, or media device. The possible OS on these addresses include a number of switch, camera, and Tivo operating systems. Additionally, these three network addresses returned information for at least one service not recognized by Nmap. While none of this indicates malicious network activity, the possibility exists regarding the inappropriate use of network resources. Additionally, given the above three addresses met all of the above security concern criteria the addresses warrant the need for further investigation.

The data shown in Table 12: *Possible Network Irregularity* is an edited representation of the data collected from IP address aaa.bbb.ccc.203 (see Appendix H for the full listing of data from IP address aaa.bbb.ccc.203) and is of particular interest from a network security perspective. These findings not only list many of the device types identified as suspicious for the addresses 196, 198, and 199, but also include the additional possible devices types identified as game console, storage-misc, and remote management.

While none of these three devices point to malicious behavior, the presence of a game

Table 11: Port Analysis Scan Results Summary

"Device types" No purpose on network	Device Type / OS Excessive quantity	Unidentified Service or OS
		aaa.bbb.ccc.35
		aaa.bbb.ccc.47
		aaa.bbb.ccc.60
		aaa.bbb.ccc.69
		aaa.bbb.ccc.195
aaa.bbb.ccc.196	aaa.bbb.ccc.196	aaa.bbb.ccc.196
aaa.bbb.ccc.198	aaa.bbb.ccc.198	aaa.bbb.ccc.198
aaa.bbb.ccc.199	aaa.bbb.ccc.199	aaa.bbb.ccc.199
		aaa.bbb.ccc.200
		aaa.bbb.ccc.201
aaa.bbb.ccc.203	aaa.bbb.ccc.203	aaa.bbb.ccc.203
		aaa.bbb.ccc.204
		aaa.bbb.ccc.205
		aaa.bbb.ccc.206
		aaa.bbb.ccc.207
		aaa.bbb.ccc.208
		aaa.bbb.ccc.209
		aaa.bbb.ccc.210
		aaa.bbb.ccc.211
		aaa.bbb.ccc.212
		aaa.bbb.ccc.213
		aaa.bbb.ccc.214
		aaa.bbb.ccc.215
		aaa.bbb.ccc.216
		aaa.bbb.ccc.217
		aaa.bbb.ccc.218
		aaa.bbb.ccc.219
		aaa.bbb.ccc.220

console might be a strong indication regarding the inappropriate use of network resources. Likewise, the presence of a miscellaneous storage device could have a valid use on the network. However, the presence of such a device could also imply the downloading and storage of data unrelated to and unauthorized for network use. Lastly, the presence of a remote management device could indicate unauthorized remote access to the network.

Table 12: Possible Network Irregularity

Nmap scan report for aaa.bbb.ccc.203 Host is up (0.050s latency). Not shown: 65533 filtered ports PORT STATE SERVICE VERSION 80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1) 3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized) 1 service unrecognized despite returning data…… *Output cut* Device type: WAP | general purpose | firewall | game console | storage-misc | switch | remote management | media device Aggressive OS guesses: Netgear DG834G WAP (94%), HP ProCurve MSM422 WAP (93%), Linux 2.4.21 - 2.4.25 (93%), Fortinet FortiGate-60B or -100A firewall (91%), Microsoft Xbox game console (modified, running XboxMediaCenter) (91%)…. TiVo series 1 (Linux 2.1.24-TiVo-2.5) (89%)…

The OS fingerprint data is also of interest. Nmap identified the possibility of a Microsoft Xbox game console OS and, or the possibility of a Tivo OS. As with the other possibilities discussed, either OS may have valid and authorized use on the network. However, the possibilities of their presence meets the criteria listed regarding the need for further identification.

Chapter 4 - Summary and Recommendations

Summary

This report discusses two projects completed during the author's enrollment in the SEAD Practicum at Regis University. Each project was a study of the methodology and tools used for vulnerability assessment and penetration testing of two unique networks. While the networks were diverse with respect to their intended use and function, the tools and methodology during the testing of each project was nearly identical. For each, the vulnerability assessment and penetration testing followed a three-step methodology comprised of host discovery, port analysis, and host exploitation. The tools used in the execution of this methodology included BackTrack, Nmap, and Metasploit.

Host discovery is the term used to describe the process of identifying the active hosts residing on a network. For the purpose of the CANVAS and ITS projects, an active host was any network-connected device capable of responding to a communication request originating from the tester's host.

For the CANVAS project, the communication request originated from a host internal to the responder's network. Conversely, communication requests for the ITS project originated from a host external to the responder's network. The identification or "discovery" of an active host involved sending a communication request to each IP address in the targeted network range and tracking all responses. Nmap's ping scan option proved a quick and effective method of host discovery for both the CANVAS and ITS networks.

Following host discovery was the process of port analysis. Port analysis identifies and evaluates the port status, operating port services, and software revision of all 65,535 ports for each active network host. The port analysis method employed during the CANVAS and ITS

network assessments included the OS fingerprinting and version detection of each active network host. OS fingerprinting is the identification of the operating system (OS) running each active host. Version detection is the determination of the OS revision, service pack, and any software patches included with the OS. Used in conjunction with the host port data, OS fingerprinting and version detection aid in the identification of possible host vulnerabilities.

As with host discovery, Nmap provided the means to collect the port and OS data from each active host on both the CANVAS and ITS networks. Information collected from the CANVAS network showed that both the number of active hosts and the port services operational on the active hosts were minimal. Given that the purpose of the CANVAS network was to provide a platform for a specific competition, the minimalist configuration is understandable.

Conversely, given that the purpose of the ITS network is to support the staff, faculty, and students of Regis University it was not be surprising that the number of port services and the variety of software operating on the ITS network was significantly greater. While the port analysis process identified a minimal number of vulnerabilities on the CANVAS network, the port analysis process identified in excess of 15,000 possible vulnerabilities on the ITS network.

The final process utilized in these projects was that of network penetration testing. Penetration testing uses the vulnerabilities identified via the host discovery and port analysis processes in an attempt to compromise the network and host security defenses. A penetration attempt is successful if the tester is able to compromise the targeted host and establish a running process on the victim. Once the tester establishes a running process on a victim host, the tester will attempt to elevate their privilege to the highest level possible. The goal is to gain “system administrator” or “root” privileges on Windows-based hosts or UNIX/Linux-based hosts respectively by elevating their privilege status to the highest levels. If the tester is successful in

establishing the stated privilege level, they will not only gain complete control over the compromised host but may also be in a position to compromise the entire network. As demonstrated in the discussions specific to each project, host penetration and compromise occurred on the CANVAS network, but proved unsuccessful on the ITS network. This result was not a surprise given the purpose of each network and the nature of each project.

The CANVAS network existed for a cyber competition, the purpose of which was to identify the vulnerabilities that allowed network compromise. Conversely, the ITS network is a fully functioning and operational production network whose primary security goal likely includes the protection of the network from unauthorized access and use. Given the results of the vulnerability assessment and penetration testing of each project, both were successful in meeting their security goals at the time of the tests.

Recommendations

The recommendations resulting from the CANVAS and ITS projects include proposed future guidance regarding network assessment and test methodologies, test tools, tool training, and access to resources. These recommendations are the opinions of the author, and based on the successes, failures, and learning experienced during the CANVAS and ITS projects.

Recommendation 1.

The three-step methodology of host discovery, port analysis, and penetration testing is valid for any project whose goal is the assessment of network vulnerability, or the network's susceptibility to penetration tests.

For both the CANVAS and ITS network projects, the method of host discovery and port analysis proved successful in the identification of active network hosts and the enumeration of possible host vulnerabilities. Additionally, by following the host discovery and port analysis

processes with a penetration test, a network tester is able to determine if the network security measures are sufficient to protect the network hosts from Metasploit and similar penetration tests. As the above three-step process proved valid from both an internal and external network perspective, future testers may want to consider using the processes outlined in this paper for any similar projects.

Recommendation 2.

Consider the use of BackTrack, Nmap, and Metasploit when evaluating tools for network vulnerability assessment or penetration test projects.

The tools used for the security assessments and penetration testing of these networks performed well when used in conjunction with the above methodologies. The Backtrack, Nmap, and Metasploit tools seemed ideally suited for the intent and purpose of the projects. The attractiveness of these tools was not only a result of their performance, but also because each was:

- Free and readily available
- Open source
- Provided for the automated testing of network hosts
- Widely used in the information security and internet technology

Of the attributes listed above, the most significant tool feature includes the support of automated test capabilities. While the advantage of automated test features may not have been apparent during the CANVAS project, the number of hosts resident on the ITS network clearly demonstrated the advantages of automated penetration testing. As the size of the network under test increases, the need for an automated test solution will become more apparent. For any future

network test projects that might benefit from automated testing, project leaders may want to consider leveraging the automated test features of BackTrack, Nmap, and Metasploit.

Recommendation 3.

Investigate the training and tutorial resources outlined in this paper when learning to use BackTrack, Nmap, or Metasploit.

The Metasploit Megaprimer tutorial located at the SecurityTube.net website proved the most informative tutorial found. The Metasploit Megaprimer video series provides the viewer with a systematic demonstration of Backtrack, Nmap, and Metasploit using both manual and automated testing modes. The videos also provide information on how to compromise a host after a successful exploit including how to download files from and upload file to the victim host. The tutorial also provides the viewer with a thorough overview of Metasploit's configuration, Metasploit's theory of operation, and the pairing of Nmap and Metasploit for use when performing network reconnaissance and the execution of automated testing.

Of significant note are the network similarities between the video tutorial and the CANVAS network. These similarities provided the opportunity to view the tutorial on one system while launching exploits against the CANVAS network on another. This method not only provided this author with knowledge specific to the use of BackTrack, Nmap, and Metasploit, but also provided a systematic method to test and exploit the CANVAS and ITS networks.

Web-based education is also available for BackTrack and Nmap. BackTrack training is available online, via live courses, or through the BackTrack Wiki. While both the BackTrack online training and the live courses are fee-based training options, the BackTrack Wiki page

provided all the information needed by this author to complete the testing as described in this paper.

Nmap training is available from the nmap.org website, but the training is limited. For a thorough discussion regarding the capabilities, tool usage, and command options available with Nmap, the publication *NMAP Network Scanning* (Lyon, 2008) is a source worth investigating.

The next three recommendations address resources, which if available to the student tester might provide for a more precise evaluation of network test results as well as increase the knowledge gained by the tester through the completion of a project.

Recommendation 4.

SEAD Practicum students would benefit from a network whose purpose was to allow experimentation with various network test tools and investigative techniques.

The most significant learning experience provided this author was the opportunity to investigate the CANVAS network. The CANVAS project allowed this author to experiment with various network test tools, observing the results of successful and unsuccessful exploitations without the fear of network damage or legal consequences. Additionally, when a host exploit proved successful, further host compromise was possible through the elevation of the attacker's privilege level. In essence, the CANVAS network provided an environment allowing the tester to verify project concepts, test methods, and tool usage. Had the concepts, methods, and tool usage remained unverified, the assessment and testing of the ITS network might have resulted in additional and less answers. The development of a practice network will provide SEAD students a platform on which to test various tools and methods without the fear of network damage or legal repercussions.

Recommendation 5.

Provide a method for the sharing of skills, knowledge, and capabilities between the various practicum classes.

One area where limited knowledge had a negative impact on the outcome of the CANVAS and ITS projects was that of data mining. Even though this author successfully created a database and populated the database with network scan information, efficient use of the database information was not possible. This author lacked the tools and knowledge to evaluate the database information for any possible trends. The identification of data trends might have resulted in the consideration of additional exploit vectors. The availability of a database resource would have proven beneficial for the project.

The recommendation requires the implementation of a method allowing an exchange of knowledge between students from various practicum classes. A possible solution might include a web-based bulletin board listing the projects from the various practicum classes. Project descriptions would include a list of needs in the form of requests for resource support or a call for help with a specific task. It is possible that the availability of this type of resource would have had little impact on the CANVAS or ITS projects. However, a method that encourages the sharing of ideas, projects, and capabilities between the various practicum studies would prove beneficial to everyone involved.

Recommendation 6.

Provide a technical resource experienced with the tools and methods specific to the Practicum project.

While this recommendation may be applicable to any Practicum project, the supporting example for this recommendation is specific to any SEAD group responsible for penetration testing. A resource knowledgeable with the methods, tools, and expected results of network

vulnerability assessments and penetration testing projects would have proven beneficial to the effort. Such a resource could help manage assessment and test methodologies, tool selection, tool usage, result interpretations, and other aspects of the projects.

Unfortunately, no such resource was available during the CANVAS and ITS projects. Instead, team members and stakeholders alike looked to this author for guidance, expertise, and accepted practices regarding network vulnerability assessment and penetration testing. This guidance may have provided a limited benefit to the team members and stakeholders as this author had little prior experience with network vulnerability assessment, penetration testing, or the use of the BackTrack, Nmap, and Metasploit tools. Had a technical resource been available during the CANVAS and ITS projects, guidance with respect to methodology, tool section, results evaluation, or alternative testing may have led the team in a direction more consistent with industry practices.

Recommendation Summary

The recommendations resulting from the CANVAS and ITS projects address the various areas of network security assessment, network test processes, assessment and test tools, tool training, and access to support and technical resources. A summary listing of these recommendations is below:

- Process recommendation: The use of the host discovery, port analysis, and penetration testing process is valid for network vulnerability assessments and/or network penetration test projects.
- Tool recommendation: Consider the use of BackTrack, Nmap, and Metasploit when evaluating tools for any network vulnerability assessment or penetration test projects.

- Tool training recommendation: The Metasploit Megaprimer video tutorial available from SecurityTube.net is a valuable resource for anyone using the methodologies and tools described in this report for network vulnerability assessment and penetration testing. Additionally, the websites specific to Nmap and BackTrack are excellent places to begin a search for training resources specific to each tool.
- Training network recommendation: A network on which students could learn testing methodologies, tools, and results would benefit the practicum students.
- Inter-practicum resource recommendation: A method of sharing knowledge and capabilities between the various practicum projects would be valuable with projects similar to this and allow for the sharing of knowledge and capabilities between the various practicum projects.
- Technical guidance recommendation: Technical resources experienced with industry methodologies and tools used for vulnerability assessment and penetration testing are available to the Pen Test team for consultation and guidance.

The above listings of recommendations provide a balanced approach for the continuation of network security assessments and penetration testing experimentation by SEAD Practicum students. It is the belief of this author that the above recommendations put the burden of learning vulnerability assessment, testing techniques, and methodologies squarely on the shoulders of future students. It is also up to future students to decide if the processes, tools, and training discussed in this paper are valid for their specific projects. Regardless, students will need to be familiar with and understand any process, tool, or training utilized in future projects.

Just as the recommendations regarding the processes, tools, and training point toward future practicum students, the recommendations regarding a training network, the sharing of

inter-practicum resources, and the technical guidance resources point toward the staff and faculty supporting the SEAD Practicum. Resources including an experimentation network, inter-practicum communications, and technical expertise are out of the realm of the student. Instead, these capabilities would best be driven by the staff and, or faculty of Regis University.

References

BackTrack Linux (2011). Roadmap: BackTrack linux – Penetration testing distribution. Retrieved from http://www.backtrack-linux.org/bt/roadmap/

CANVAS student computer security event a success. (2011, May 4). Regis University School of Computer & Information Sciences. Retrieved from http://regis.edu/content/cpcis/pdf/CANVAS%20Success.pdf

Foreman, Park. (© 2010). Vulnerability management. [Books24x7 version] Retrieved from http://common.books24x7.com.dml.regis.edu/toc.aspx?bookid=30514.

freshmeat.net (2011). Welcome to freshmeat.net. Retrieved from http://freshmeat.net/search?q=nmap&submit=Search

Fyodor (1997, September). The Art of port scanning. *Phrack Magazine 7(51).* Retrieved from http://phrack.org/issues.html?issue=51&id=11#article

Herzog, Pete (2011). Open source security testing methodology manual. Retrieved from http://www.isecom.org/osstmm/

Information Security Short Takes (n.d.). *System hardening process checklist.* Retrieved from http://www.shortinfosec.net/2009/01/system-hardening-process-checklist.html

Insecure.org LLC (2004). Nmap. Retrieved from *http://linuxcommand.org/man_pages/nmap1.html*

Internet Engineering Task Force, Network Working Group (1989). *Request for comments 1122. Requirements for internet hosts – Communication layers.* Retrieved from http://tools.ietf.org/html/rfc1122

Linux Journal, December 1, 2001. *Editor's choice awards.* Retrieved from http://www.linuxjournal.com/article/5525

Lyon, Gordon Fyodor, 2008. *NMAP network scanning: Official Nmap project guide to network discovery and security scanning.* Sunnyvale, CA: Insecure.Com LLC

Metasploit (September 17, 2006). *Metasploit 3.0 automated exploitation*. Retrieved from http://blog.metasploit.com/2006/09/metasploit-30-automated-exploitation.html

NIST (2008). *Technical guide to information security testing and assessment*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Nmap (2011). *Nmap free security scanner*. Retrieved from http://nmap.org

Rapid 7, 2011. Download Metasploit. Retrieved from (http://www.metasploit.com/download/)

Red Hat (2005). *Red Hat enterprise Linux 4 security guide*. Retrieved from http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/index.html

Sectools.org (2006). *Top 100 network security tools*. Retrieved from http://sectools.org/

SecurityTube.net (2011). Metasploit Megaprimer. Retrieved from http://www.securitytube.net/groups?operation=view&groupId=8

skape (December, 26, 2004). *Metasploit's Meterpreter*. Retrieved from http://www.nologin.org/Downloads/Papers/meterpreter.pdf

Appendix A: CANVAS Network All Host/All Ports Scan Results

```
This output was created with the command nmap -p0-65535 10.128.128.0/24

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-03-12 14:39 MST
Nmap scan report for 10.128.128.1
Host is up (0.0057s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:00:0C:07:AC:01 (Cisco Systems)

Nmap scan report for 10.128.128.2
Host is up (0.0057s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:07:50:1A:40:C1 (Cisco Systems)

Nmap scan report for 10.128.128.3
Host is up (0.0087s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:05:9B:BF:5E:21 (Cisco Systems)

Nmap scan report for 10.128.128.50
Host is up (0.00018s latency).
All 65536 scanned ports on 10.128.128.50 are filtered
MAC Address: 00:50:56:84:00:16 (VMware)

Nmap scan report for 10.128.128.68
Host is up (0.00039s latency).
Not shown: 65509 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
515/tcp  open  printer
548/tcp  open  afp
1046/tcp open  unknown
1063/tcp open  unknown
1065/tcp open  unknown
1070/tcp open  unknown
1074/tcp open  unknown
```

```
1076/tcp open  sns_credit
1077/tcp open  unknown
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
3459/tcp open  unknown
MAC Address: 00:50:56:84:00:00 (VMware)

Nmap scan report for 10.128.128.69
Host is up (0.00041s latency).
Not shown: 65512 closed ports
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
21/tcp   open  ftp
25/tcp   open  smtp
42/tcp   open  nameserver
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
515/tcp  open  printer
1042/tcp open  unknown
1062/tcp open  veracity
1065/tcp open  unknown
1072/tcp open  unknown
1084/tcp open  ansoft-lm-2
1723/tcp open  pptp
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
3459/tcp open  unknown
MAC Address: 00:50:56:84:00:1F (VMware)

Nmap scan report for 10.128.128.71
Host is up (0.00050s latency).
All 65536 scanned ports on 10.128.128.71 are filtered
MAC Address: 00:50:56:84:00:19 (VMware)

Nmap scan report for 10.128.128.80
Host is up (0.00036s latency).
All 65536 scanned ports on 10.128.128.80 are closed
MAC Address: 00:50:56:84:00:27 (VMware)

Nmap scan report for 10.128.128.100
Host is up (0.00038s latency).
Not shown: 65517 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
```

```
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
1034/tcp open  zincite-a
1035/tcp open  multidropper
1038/tcp open  unknown
1043/tcp open  boinc
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:50:56:84:00:18 (VMware)

Nmap scan report for 10.128.128.121
Host is up (0.00034s latency).
Not shown: 65535 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:84:00:1E (VMware)

Nmap scan report for 10.128.128.122
Host is up (0.00044s latency).
Not shown: 65534 filtered ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:50:56:84:00:24 (VMware)

Nmap scan report for 10.128.128.123
Host is up (0.000014s latency).
All 65536 scanned ports on 10.128.128.123 are closed

Nmap scan report for 10.128.128.124
Host is up (0.00048s latency).
All 65536 scanned ports on 10.128.128.124 are filtered
MAC Address: 00:50:56:84:00:26 (VMware)

Nmap done: 256 IP addresses (13 hosts up) scanned in 1572.98 seconds
```

Appendix B: CANVAS auto test summary - 031811

Sent: Friday, March 18, 2011 7:03 AM
To: H. N., R. C.
Cc: D. L.

Per the plan from Tuesday's Practicum meeting, the following is a summary of the test results from the CANVAS network using the automatic test execution capabilities of Metasploit.

Contact me with any questions you have regarding the findings.

Steve

The automatic test capability of Metasploit was used to test the identified hosts with open ports in the CANVAS network. The command ***db_autopwn –e –p –t –I <target>*** where <*target*> was the IP of each identified host was executed with a summary of the results listed below. The output of the above command yields the number of exploits identified from the Metasploit database and the number of sessions resulting from the execution of the exploits. Note that not all identified hosts could be exploited with the stock Metasploit exploits. For those hosts which were exploited the meterpreter was used to execute a number of commands verifying the compromise.

10.128.128.1 > 1 open port, 4 exploits, 0 sessions.
10.128.128.2 > 1 open port, 4 exploits, 0 sessions.
10.128.128.3 > 1 open port, 4 exploits, 0 sessions.
10.128.128.4 > 1 open port, 4 exploits, 0 sessions.
10.128.128.50 > 4 open ports, 50 exploits, 0 sessions.
10.128.128.68 > 23 open ports, 290 exploits, 5 sessions.
10.128.128.69 > 22 open ports, 290 exploits, 9 sessions.
10.128.128.71 > 2 open ports, 50 exploits, 0 sessions.
10.128.128.72 > 21 open ports, 294 exploits, 6 sessions.
10.128.128.100 > 19 open ports, 186 exploits, 0 sessions.
10.128.128.121 > 1 open port, 106 exploits, 0 sessions.
10.128.128.122 > 2 open ports, 50 exploits, 0 sessions

Appendix C: Canvas testing for 03222011

From Steve Simpson
Sent: Wednesday, March 23, 2011 7:27 PM
To: N, H.; L. D.; J. W.; R. R.;

Automated testing using db_autopwn –p –e –t –I <target>

Heath, Dan,

Per the Canvas meeting of 3/22, exploitation test were run against 3 of the hosts in the CANVAS network with the following results:

10.128.128.68 > 24 open ports, 382 exploits, 0 sessions
10.128.128.69 > 15 open ports, 60 exploits, 9 sessions
10.128.128.72 > 23 open ports, 382 exploits, 0 sessions

I was able to exploit 10.128.1228.69 through the use of the Metasploit automated exploits using the command ***db_autopwn –p –e –t –I 10.128.128.69***. I had the ability to command the system through the exploits but I left the system as I found it (no changes made).

Neither of the other 2 hosts was exploitable using the Metasploit automated exploit command. Both had open ports (as listed above) but neither were exploitable.

Let me know if you have any additional questions or comments.

Steve

Appendix D: ITS Project Test Plan

Document url: https://in2.regis.edu/sites/scis/AAA/BBBB/Cccccc/

1. Introduction

1.1 Purpose

The purpose of this document is to define the Rules of Engagement (ROE) for the vulnerability assessment and penetration testing that will be executed by the Information Assurance (IA) and System Engineering and Application Development (SEAD) Practicum security test team targeting specific Regis University (RU) networks.

1.2 Scope

The scope of this project is limited to the external vulnerability assessment and penetration testing of the following IP network address range:

aaa.bbb.ccc.0/24

The vulnerability assessment and penetration testing of the above network will be conducted by the approved students enrolled in the Regis University Practicum classes, or those authorized by the Regis University Network Security Officer and/or the academic advisor to the IA/SEAD Practicum class.

1.3 Assumptions and Limitations

1.3.1 All testers will use commonly available security tools, or tools approved by Regis University faculty to complete all network vulnerability assessments and penetration testing.

1.3.2 All test equipment and test tools will be supplied by Regis University if possible. In the event that Regis university can not, or will not provide test equipment and tools, the students will be responsible to provide test resources on their own.

1.3.3 All Practicum students executing any vulnerability assessments or penetration testing will be required to complete, and submit the forms included in section 5.1 and follow the Test Notification Form (TNF) submission process outlined in section 5.2.

1.4 Risks

The primary risk with the vulnerability assessment and penetration testing outlined in this plan is the disruption of the Regis University network in it's entirety or any part. For purposes of this plan a disruption is considered any activity that impacts the current capability of the network or any of it's components. If, at any time, the network appears to be at any risk, the tester may be restricted from completing any current or future testing.

1.5 Document Structure

1.5.1 This document contains the following sections

Section 1 – Introduction

1.1 Purpose

1.2 Scope
1.3 Assumptions and Limitation
1.4 Risks
1.5 Document Structure

Section 2 – Logistics
2.1 Personnel
2.2 Test Schedule
2.3 Test Site
2.4 Test Equipment
2.5 Test Tools

Section 3 – Communications
3.1 General Communication
3.2 Incident Handling and response

Section 4 - Target System/Network

Section 5 - Testing Execution
5.1 Volunteer Forms/Procedure
5.2 Test Notification Form/Procedure
5.3 Non Technical Test Components
5.4 Technical Test Components and Test Tools
5.5 Manual Testing
5.6 Automated Testing
5.4 Test Tools
5.5 Test Methodology
5.6 Results Handling

Section 6 - Reporting

Section 7 - Approval Page

2. Logistics

2.1 Personnel

Project stakeholders include the following people:

Aaaaa	ITS Security Officer (ITSSO)	aaaaa@regis.edu
Bbbbb	IA Practicum Advisor	bbbbb@regis.edu
Ddddd	Student security intern	ddddd123@regis.edu

2.2 Test Schedule

Schedules to be negotiated on a term-by-term basis with the project lead, Practicum faculty advisor, and the student test lead. Practicum members change on a regular basis and class student enrollment and student expertise will have a significant impact on the project schedule.

2.3 Test Site

The assumption is that the majority of the vulnerability assessments and penetration testing of the Regis University networks specified in section 1.2 will be conducted from remote locations, e.g. locations where a direct connection to the specified network is not possible. As such, it is assumed that all Practicum students involved in the network tests will launch test execution from any location from which the tester can expect to maintain network access for the length of the test session. Possible test locations includes any Regis campus, the tester's place of employment, the tester's residence, etc.

2.4 Test Equipment

Specific test equipment is not identified for this project. If Regis is to supply the resources necessary to conduct the vulnerability assessment and penetration testing, it is expected that a virtual machine on a specified platform will be used. However, as of this writing no Regis resources have been identified in support of this project. As such, each tester will be required to provide the test equipment and tools necessary to complete the testing.

Any computer hardware available to the tester is approved for use. As long as any equipment used by a tester is capable of establishing and maintain a network connection and can maintain the ability to launch assessments and test scripts from remote locations, the equipment is approved for use. This may include computers whose form factor and capabilities are commonly referred to as server, desktop, laptop, netbook, netpad, etc. Additionally, the operating system (OS) running on any of the above machines may include, but are not limited to Windows, Linux, Apple-OS, or any derivative of the pre-mentioned OS's.

2.5 Test Tools

As with the test equipment requirements, no limitation is being placed on the test tools used to perform the vulnerability assessment and penetration testing. If the tester may use any commercial of proprietary tool to which they have access. The assumption, however, is that most testers will use open source, and commonly available freeware tools for all testing.

This plan specifically discusses the use of the BackTrack OS and suite of security tools included with BackTrack 5 (BT5) including Nmap, and Metasploit. The manual and automated commands listed in Section 5 are command-line invocations of Nmap and Metasploit.

2.5.1 Tool download and training may be found at the following urls:

BackTrack 5 download: http://www.backtrack-linux.org/downloads/
Nmap download (Nmap is include with BT5): http://nmap.org/download
Metasploit download (Metasploit is also included in BT5):
http://metasploit.com/download/

BackTrack 5 training: http://www.backtrack-linux.org/tutorials/

Nmap training: http://nmap.org/bennieston-tutorial/
Metasploit training: http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training

A very good video series that steps the user through the combined use of BT5, Nmap, and Metasploit is found at:
http://www.securitytube.net/groups?operation=view&groupID=8

3. Communication Strategy

3.1 General Communication

The primary means of stakeholder communications will occur via the weekly IA Practicum meeting. This meeting is currently held on Tuesdays at 6:00 pm Mountain Time and is open to all Practicum students and project stakeholders. The Practicum meeting schedule as well as related announcements can be viewed at: https://in2.regis.edu/sites/scis/AAA/BBBB/Cccccc/.

At times additional communications between the stakeholders may be required which may occur through emails, phone or face-to-face conversations, or documents posted on the SEAD SharePoint site found at : https://in2.regis.edu/sites/scis/AAA/BBBB/Cccccc/

3.2 Incident Handling and Response

Should an incident occur at any time during with a tester is conducting an active test session the tester is to cease test execution and contact the ITSSO by phone at the number listed in section5.2 and/or 5.4.

4. Target System/Network

This revision of the test plan covers only the external vulnerability assessment and penetration testing of the network and address range at aaa.bbb.ccc.0/24.

5. Testing Execution

5.1 Volunteer Forms

All testers are required to review, complete (as appropriate), and submit the following forms:

- Criminal Background Policy.pdf
- Volunteer Agreement.pdf
- Volunteer Policy Final.pdf
- Volunteer Services Description.pdf

These forms can be found on the Volunteer Forms folder on the SEAD SharePoint site at : https://in2.regis.edu/sites/scis/AAA/BBBB/Cccccc/

Mail the forms to:

Aaaaaa
Regis University
3333 Regis Blvd. Mail Stop X-1
Denver, CO 80221
O: 303 458-4295
C: 720 810-4612

It is up to each student to complete the volunteer form process as approvals to testing the specified network will not be granted to anyone who has not completed the forms and been approved by Regis University.

5.2 Test Notification Form

The Test Notification Form (TNF) must be filled out and submitted prior to every test sessions. In addition, after completing and submitting a TNF a phone text message must be sent to the ITSSO indicating that a test session is being initiated. Once the test session has completed the tester is required to send a phone text message to the ITSSO indicating that the test session is over.

The TNF is located in same folder as volunteer forms discussed in section 5.1 and the procedure for completing the TNF is listed below:

10 Fill out your name in the appropriate space
11 Go to a site like www.whatsmyip.org or www.whatsmyip.com and get your IP address as viewed by the internet. Getting your IP address from a command like ipconfig or ifconfig will provide a private address which is only known to your ISP.
12 Fill out the network IP address and address range you will be testing. For example aaa.bbb.ccc.1-30 will target the IP address range 1–30 of the network aaa.bbb.ccc.0.
13 Fill out the name of the tool you will be using for your test.
14 Fill out the tool's revision number
15 Complete the sections regarding the best phone number and email address at which you can be reached during your test session.
16 Mail the completed TNF to the following addresses:
- aaaaa@regis.edu;
- ITSO@regis.edu;
- bbbbb@regis.edu;
- ccccc@regis.edu.

17 At the beginning of a test sessions all testers are required to send a phone text to Aaaaa at 702 555-5555 stating your name and your intension to start a test session. An example of a initiating text would be something similar to: "Hello Aaaaa, This is <tester's first and last name> initiating a test session."

18 Once the tester has completed a test sessions a closing session text must be sent to Aaaaa at 702 555-5555 stating you name and your intension to end a test sessions. An example of a closing text would be something similar to: "Hello Aaaaa, This is <tester's first and last name> ending a test session."

An example of a completed form is below:

Who is doing the PEN Testing:	Student Name
What is the source IP Address:	xxx.yyy.zzz.115
What address or address range will be targeted:	aaa.bbb.ccc.1-30
What tool and version will be used:	BackTrack
Version:	5
What is the intended testing time (beginning):	8:30 pm PDT
Phone number where the tester can be reached, if necessary, during the testing:	253 555-5555
Best e-mail address to reach tester:	name123@regis.edu

5.3 Non-technical Test Components

The following websites provide a number of security testing and related information which may prove useful to testers following this test plan or information security personnel in general.

The Security Technical Implementation Guide (STIG) website home provides configuration standards for DOD IA and IA-enabled devices/systems testing. The STIGs and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems and may provide assistance in establishing guidance for the vulnerability assessment and PT testing as part of this test plan: http://iase.disa.mil/stigs/

The NIST Special Publication 800-115 is part of a series of documents which provides guidance to the computer security industry and includes collaborative activities with the security industry, government, and academic organizations. The NIST Special Publication 800-115 provides specific and useful information regarding network discovery, port and service identification, and vulnerability scanning. The NIST document can be found at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

The Open Source Security Testing Methodology Manual (OSSTMM), version 3.0 published by the ISECOM, contains five main sections providing testing information with regards to data controls, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and other topics that could be useful to the vulnerability assessor and PT tester. Chapters 2, 6, and 11 provide information regarding operational test processes such as the enumeration of hosts, ports and services as well as background pertaining to network access, controls, and configuration. The OSSTMM is located at http://www.isecom.org/osstmm/

5.4 Technical Test Components and Test Tools

BackTrack5 (BT5) will be the primary framework and tool set used for the assessment and testing of the defined networks. BackTrack is a well known and widely used open source security framework that provides a number of assessment and penetration tools used for digital forensics, vulnerability assessments, and penetration testing. Specific tools included in the BackTrack framework and used for vulnerability assessment and penetration testing include Nmap and Metasploit.

The network vulnerability assessment will utilize the Nmap security tool found within BT5. Various command line options will be chosen to allow Nmap to determine the following:

- IP addresses of the active hosts on the specified networks,
- The OS of the above hosts,
- Open ports of the hosts, and
- Service identification of the open ports

Network penetration testing will utilize the Metasploit Framework found within BT5. Metasploit contains a significant number of pre-tested exploits that are known to be effective against numerous vulnerabilities. Vulnerabilities identified by Nmap will be the first penetration targets. The results of each penetration test will be recorded as to the port(s) and/or service(s) through which the compromise occurred.

The combined network vulnerability assessment and penetration testing will be conducted in three phases including:

- Host Discovery
- Port scanning, version detection, and OS fingerprinting
- Penetration testing and exploitation

Tools and commands for each of the above phases are listed below.

5.6 Manual Testing

5.6.4 Manual Host Discovery Tool and Command

The Nmap command to be used for host discovery is:

nmap –sP aaa.bbb.ccc.0/24 > external_ping.txt

The above command

• invokes Nmap	nmap
• calls the ping scan option	-sP
• ping scans the entire network range	aaa.bbb.ccc.0/24
• redirects the output to a specified file	> external_ping.txt

The file is to be stored on the tester’s computer and available for retrieval at a later date.

5.6.3 Manual Port Scanning Tool and Command

The Nmap command to be used for port scanning, version detection, and OS fingerprinting is:

nmap –sS –O –sV –p1-65535 –L external_up.txt > external_ports_all.txt

The above command

- invokes Nmap — nmap
- calls the TCP SYN scan — -sS
- calls remote host fingerprinting — -O
- calls the version detection option — -sS
- applies above option to all ports — -p1-65535
- uses a file as input to scan specific IPs — -L external_up.txt
- redirects the output to a specified file — > external_porrs_all.txt

5.5.3 Manual Penetration Testing Tool and Command

No manual penetration testing is expected for this test as the expected number of network hosts will make manual testing in-efficient. See the section on automated testing for information regarding penetration testing.

5.6 Automated Testing

5.6.1 Database Creation

The automated capabilities of the Metasploit Frame allows for it's input to come from a database. The database used must be created prior to the call any automated command call to Metasploit. To create a database for use by Metasploit, start the Metasploit Framework tool and enter the following from the Metasploit Framework command line prompt:

db_driver mysql
db_connect
db_connect root:toor@127.0.0.1/*db_filename*

The above commands will tell Metasploit to

Use the mysql database driver db_driver mysql
Connect the to a database db_connectroot:toor@127.0.0.1/*db_filename*

The database filename (*db_filename*) may be any name chosen by the tester. The tester may connect to an existing database by using the existing database name in place of *db_filename*. If no database of a given name exists at the time the command is invoked, a database will be created and Metasploit will connect to the named database.

Once the tester is through with the database the data base can be erased using the command; db_destroy root:toor@127.0.0.1/*db_filename*

5.6.2 Automated Host Discovery using Nmap from within Metasploit

The output of any Nmap command can be directed to a database from within Metasploit. Using the database created in the step 5.6.1, enter the following command to perform network host discovery and direct the output into the database from the Metasploit command-line prompt:

db_nmap –sP aaa.bbb.ccc.0/24

The above command

- invokes Nmap dumping output to a database db_nmap
- calls the ping scan option -sP
- ping scans the entire network range aaa.bbb.ccc.0/24

5.6.3 Automated Port Scanning Tool and Command

The Nmap command to be used for port scanning, version detection, and OS fingerprinting is:

db_nmap –sS –O –sV –p1-65535

The above command

- invokes Nmap using the existing database data as input regarding the active IP host addresses and dumping output to a database db_nmap
- calls the TCP SYN scan -sS
- calls remote host fingerprinting -O
- calls the version detection option -sS
- applies above option to all ports -p1-65535

5.6.4 Automated Penetration Testing tool and Command

The automated capabilities of Metasploit will use the database to which the Metasploit session is currently attached as input for the command. If the command is successful a Meterpreter session will be opened. The tester can then gain access to the compromised host through one of the associated Meterpreter sessions. Consult the training urls in section 2.5 – Test Tools

To invoke the automated capabilities of Metasploit, execute the following command from the Metasploit Framework command line:

db_autopwn –p –e –t –I aaa.bbb.ccc.0/24

The above command

- invoke the autopwn capabilities of Metasploit using the connected database as the command input db_autopwn
- select modules based on open ports -p
- launch exploits against all matched targets -e
- show all matching exploit modules -t
- only exploit hosts inside this range -I [range]

5.7 Data Handling

At this time data handling and storage will be left to the discretion of the tester. At a future time and under the guidance of the Pen Test lead data may be stored in a specified format on the Regis University SEAD SharePoint site.

6 Reporting

The summary report will include a minimum of the open/active IP addresses found on the Regis ITS network, a summary of the port scan and OS finger printing, and a summary of the exploitation result s of the network.

7 Approval Page

_____/_____
aaaaaaaa - Regis University ITS Security Officer / Date

_____/_____
bbbbbbbb – Faculty Advisor / Date

_____/_____
cccccccc – Project Lead SEAD Practicum / Date

Appendix E: ITS Network Ping Results

Starting Nmap 5.51 (http://nmap.org) at 2011-10-07 12:26 Pacific Daylight Time
Nmap scan report for aaa.bbb.ccc.1
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.2
Host is up (0.031s latency).
Nmap scan report for www2.regis.edu (aaa.bbb.ccc.33)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.34
Host is up (0.031s latency).
Nmap scan report for exchange2.regis.edu (aaa.bbb.ccc.35)
Host is up (0.031s latency).
Nmap scan report for its02.regis.edu (aaa.bbb.ccc.36)
Host is up (0.031s latency).
Nmap scan report for its02.regis.edu (aaa.bbb.ccc.37)
Host is up (0.031s latency).
Nmap scan report for academic.regis.edu (aaa.bbb.ccc.38)
Host is up (0.031s latency).
Nmap scan report for its39.regis.edu (aaa.bbb.ccc.39)
Host is up (0.046s latency).
Nmap scan report for ereserves.regis.edu (aaa.bbb.ccc.40)
Host is up (0.031s latency).
Nmap scan report for its-17.regis.edu (aaa.bbb.ccc.41)
Host is up (0.031s latency).
Nmap scan report for insite.regis.edu (aaa.bbb.ccc.43)
Host is up (0.047s latency).
Nmap scan report for producer.regis.edu (aaa.bbb.ccc.44)
Host is up (0.032s latency).
Nmap scan report for stream.regis.edu (aaa.bbb.ccc.45)
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.47
Host is up (0.047s latency).
Nmap scan report for epicor.regis.edu (aaa.bbb.ccc.49)
Host is up (0.047s latency).
Nmap scan report for its22.regis.edu (aaa.bbb.ccc.51)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.54
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.55
Host is up (0.031s latency).
Nmap scan report for mail1.regis.edu (aaa.bbb.ccc.56)
Host is up (0.047s latency).
Nmap scan report for update.regis.edu (aaa.bbb.ccc.57)
Host is up (0.047s latency).
Nmap scan report for web-classrooms.regis.edu (aaa.bbb.ccc.58)

Host is up (0.031s latency).
Nmap scan report for selfhelp.regis.edu (aaa.bbb.ccc.59)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.60
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.61
Host is up (0.031s latency).
Nmap scan report for communicator.regis.edu (aaa.bbb.ccc.66)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.67
Host is up (0.047s latency).
Nmap scan report for sip.regis.edu (aaa.bbb.ccc.69)
Host is up (0.047s latency).
Nmap scan report for ocswebconf.regis.edu (aaa.bbb.ccc.72)
Host is up (0.047s latency).
Nmap scan report for ocsavedge.regis.edu (aaa.bbb.ccc.73)
Host is up (0.047s latency).
Nmap scan report for spslcalc.regis.edu (aaa.bbb.ccc.75)
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.77
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.78
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.97
Host is up (0.031s latency).
Nmap scan report for in2.regis.edu (aaa.bbb.ccc.98)
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.99
Host is up (0.047s latency).
Nmap scan report for www.regis.edu (aaa.bbb.ccc.100)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.101
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.102
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.103
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.104
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.105
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.106
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.107
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.108

Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.109
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.110
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.111
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.112
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.113
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.114
Host is up (0.031s latency).
Nmap scan report for singtest.regis.edu (aaa.bbb.ccc.115)
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.116
Host is up (0.047s latency).
Nmap scan report for maila.regis.edu (aaa.bbb.ccc.120)
Host is up (0.031s latency).
Nmap scan report for mailb.regis.edu (aaa.bbb.ccc.121)
Host is up (0.047s latency).
Nmap scan report for mailc.regis.edu (aaa.bbb.ccc.122)
Host is up (0.031s latency).
Nmap scan report for maild.regis.edu (aaa.bbb.ccc.123)
Host is up (0.031s latency).
Nmap scan report for maile.regis.edu (aaa.bbb.ccc.124)
Host is up (0.031s latency).
Nmap scan report for antispam.regis.edu (aaa.bbb.ccc.125)
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.161
Host is up (0.047s latency).
Nmap scan report for vpn.regis.edu (aaa.bbb.ccc.164)
Host is up (0.047s latency).
Nmap scan report for aaa.bbb.ccc.193
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.194
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.195
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.196
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.198
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.199
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.200

Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.201
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.202
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.203
Host is up (0.032s latency).
Nmap scan report for aaa.bbb.ccc.204
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.205
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.206
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.207
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.208
Host is up (0.033s latency).
Nmap scan report for aaa.bbb.ccc.209
Host is up (0.033s latency).
Nmap scan report for aaa.bbb.ccc.210
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.211
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.212
Host is up (0.035s latency).
Nmap scan report for aaa.bbb.ccc.213
Host is up (0.043s latency).
Nmap scan report for aaa.bbb.ccc.214
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.215
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.216
Host is up (0.033s latency).
Nmap scan report for aaa.bbb.ccc.217
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.218
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.219
Host is up (0.031s latency).
Nmap scan report for aaa.bbb.ccc.220
Host is up (0.045s latency).
Nmap scan report for aaa.bbb.ccc.222
Host is up (0.031s latency).
Nmap done: 256 IP addresses (89 hosts up) scanned in 17.13 seconds

Appendix F: File listing of *external_up.txt*

aaa.bbb.ccc.1
aaa.bbb.ccc.2
aaa.bbb.ccc.33
aaa.bbb.ccc.34
aaa.bbb.ccc.36
aaa.bbb.ccc.37
aaa.bbb.ccc.38
aaa.bbb.ccc.39
aaa.bbb.ccc.40
aaa.bbb.ccc.41
aaa.bbb.ccc.43
aaa.bbb.ccc.44
aaa.bbb.ccc.45
aaa.bbb.ccc.47
aaa.bbb.ccc.49
aaa.bbb.ccc.51
aaa.bbb.ccc.54
aaa.bbb.ccc.55
aaa.bbb.ccc.56
aaa.bbb.ccc.57
aaa.bbb.ccc.58
aaa.bbb.ccc.59
aaa.bbb.ccc.60
aaa.bbb.ccc.61
aaa.bbb.ccc.66
aaa.bbb.ccc.67
aaa.bbb.ccc.69
aaa.bbb.ccc.72
aaa.bbb.ccc.73
aaa.bbb.ccc.75
aaa.bbb.ccc.77
aaa.bbb.ccc.78
aaa.bbb.ccc.97
aaa.bbb.ccc.98
aaa.bbb.ccc.99
aaa.bbb.ccc.100
aaa.bbb.ccc.101
aaa.bbb.ccc.102
aaa.bbb.ccc.103
aaa.bbb.ccc.104
aaa.bbb.ccc.105
aaa.bbb.ccc.106
aaa.bbb.ccc.107
aaa.bbb.ccc.108

aaa.bbb.ccc.109
aaa.bbb.ccc.110
aaa.bbb.ccc.111
aaa.bbb.ccc.112
aaa.bbb.ccc.113
aaa.bbb.ccc.114
aaa.bbb.ccc.115
aaa.bbb.ccc.116
aaa.bbb.ccc.120
aaa.bbb.ccc.121
aaa.bbb.ccc.122
aaa.bbb.ccc.123
aaa.bbb.ccc.124
aaa.bbb.ccc.125
aaa.bbb.ccc.161
aaa.bbb.ccc.164
aaa.bbb.ccc.193
aaa.bbb.ccc.194
aaa.bbb.ccc.195
aaa.bbb.ccc.196
aaa.bbb.ccc.198
aaa.bbb.ccc.199
aaa.bbb.ccc.200
aaa.bbb.ccc.201
aaa.bbb.ccc.202
aaa.bbb.ccc.203
aaa.bbb.ccc.204
aaa.bbb.ccc.205
aaa.bbb.ccc.206
aaa.bbb.ccc.207
aaa.bbb.ccc.208
aaa.bbb.ccc.209
aaa.bbb.ccc.210
aaa.bbb.ccc.211
aaa.bbb.ccc.212
aaa.bbb.ccc.213
aaa.bbb.ccc.214
aaa.bbb.ccc.215
aaa.bbb.ccc.216
aaa.bbb.ccc.217
aaa.bbb.ccc.218
aaa.bbb.ccc.219
aaa.bbb.ccc.220
aaa.bbb.ccc.222

Appendix G: ITS Port Analysis Scan Results – Complete Listing

The following output is the result of the command:
nmap -sP -O -sV -p1-65535 -iL external_up.txt > external_ports_all.txt

Starting Nmap 5.51 (http://nmap.org) at 2011-10-07 13:38 Pacific Daylight Time
Nmap scan report for aaa.bbb.ccc.1
Host is up (0.032s latency).
Not shown: 65529 closed ports
PORT STATE SERVICE VERSION
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: broadband router|router|switch|WAP
Running: Cisco embedded, Cisco IOS 12.X|15.X
OS details: Cisco 827H ADSL router, Cisco 870 router or 2960 switch (IOS 12.2 - 12.4), Cisco Aironet 1250 WAP (IOS 12.4), Cisco C7200 router (IOS 15)

Nmap scan report for aaa.bbb.ccc.2
Host is up (0.034s latency).
Not shown: 65525 closed ports
PORT STATE SERVICE VERSION
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
2001/tcp open telnet Cisco router
4001/tcp open tcpwrapped
6001/tcp open jdwp
9001/tcp open tcpwrapped
Device type: WAP
Running: Cisco IOS 12.X
OS details: Cisco Aironet 1250 WAP (IOS 12.4)
Network Distance: 12 hops
Service Info: OS: IOS; Device: router

Nmap scan report for www2.regis.edu (aaa.bbb.ccc.33)
Host is up (0.043s latency).
All 65535 scanned ports on www2.regis.edu (aaa.bbb.ccc.33) are filtered

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|firewall|general purpose
Running: Cisco embedded, SonicWALL embedded, Sun Solaris 10|9
OS details: Cisco Unified Communications Manager VoIP gateway, SonicWALL Aventail EX-1500 SSL VPN appliance, Sun Solaris 10, Sun Solaris 10 (SPARC), Sun Solaris 9 (SPARC)

Nmap scan report for aaa.bbb.ccc.34
Host is up (0.043s latency).
All 65535 scanned ports on aaa.bbb.ccc.34 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|general purpose|firewall
Running: Cisco embedded, IBM i5/OS V5, IBM z/OS, Linux 2.6.X, SonicWALL embedded
OS details: Cisco Unified Communications Manager VoIP gateway, IBM i5/OS V5R3M0, IBM z/OS v1r8, Linux 2.6.15-28-amd64-server (Ubuntu, x86_64, SMP), Linux 2.6.18.pi (x86), SonicWALL Aventail EX-1500 SSL VPN appliance

Nmap scan report for exchange2.regis.edu (aaa.bbb.ccc.35)
Host is up (0.038s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd
443/tcp open ssl/http Apache httpd
444/tcp open ssl/snpp?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port444-TCP:V=5.51%T=SSL%I=7%D=10/7%Time=4E8F76D7%P=i686-pc-windows-win
SF:dows%r(GetRequest,1A98,"HTTP/1\.1\x20200\x20OK\nDate:\x20Fri,\x207\x20O
SF:ct\x202011\x2022:01:59\x20GMT\nServer:\x20III\x20100\nPragma:\x20no-cac
SF:he\nSet-Cookie:\x20III_EXPT_FILE=aa364;\x20path=/;\x20domain=;\x20path=
SF:/\nSet-Cookie:\x20III_SESSION_ID=8f4adc626ec307eca4db31acf62d9d95;\x20p
SF:ath=/\nSet-Cookie:\x20SESSION_SCOPE=3;\x20path=/\nContent-Type:\x20text
SF:/html\nExpires:\x20Fri,\x207\x20Oct\x202011\x2022:01:59\x20GMT\nCache-c
SF:ontrol:\x20no-cache\n\n<html\x20xmlns=\"http://www\.w3\.org/1999/xhtml\
SF:"\x20xml:lang=\"en\"\x20lang=\"en\">\n<!--\x20Rel\x202007\x20\"Skyline\
SF:"\x20Example\x20Set\x20-->\n<!--\x20This\x20File\x20Last\x20Changed:\x2
SF:0June\x202011\x20-->\n<head>\n<link\x20rel=\"stylesheet\"\x20type=\"tex
SF:t/css\"\x20href=\"/scripts/ProStyles\.css\"\x20/>\n<link\x20rel=\"style
SF:sheet\"\x20type=\"text/css\"\x20href=\"/screens/styles\.css\"\x20/>\n<s
SF:cript\x20language=\"JavaScript\"\x20type=\"text/javascript\"\x20src=\"/
SF:scripts/elcontent\.js\"></script>\n<script\x20language=\"JavaScript\"\x
SF:20type=\"text/javascript\"\x20src=\"/scripts/common\.js\"></script>\n<s
SF:cript\x20language=\"JavaScript\"\x20type=\"text/javascript\"\x20src=\"/
SF:scripts/webbridge\.js\"></script>")%r(FourOhFourRequest,D1,"HTTP/1\.1\x
SF:20404\x20Not\x20Found\nServer:\x20III\x20100\nMIME-version:\x201\.0\nCo

SF:ntent-Type:\x20\x20text/html\n\n<HEAD><TITLE>404\x20Not\x20Found</TITLE
SF:></HEAD>\n<BODY><H1>404\x20Not\x20Found</H1>The\x20requested\x20URL\x20
SF:was\x20not\x20found\x20on\x20this\x20server\.\n</BODY>\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Sun Solaris 9|10|5.X (92%), Sun OpenSolaris (88%)
Aggressive OS guesses: Sun Solaris 9 (SPARC) (92%), Sun Solaris 9 or 10 (SPARC) (90%), Sun Solaris 10 (SPARC) (89%), Sun Solaris 9 or 10, or OpenSolaris 2009.06 snv_111b (88%), Sun Solaris 5.10 (85%), Sun Solaris 10 (85%), Sun Solaris 9 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for its02.regis.edu (aaa.bbb.ccc.36)
Host is up (0.033s latency).
Not shown: 65520 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd
80/tcp open http Microsoft IIS httpd 7.0
443/tcp open ssl/http Microsoft IIS httpd 7.0
990/tcp open ssl/ftp Microsoft ftpd
4900/tcp closed hfcs
4901/tcp closed unknown
4902/tcp closed unknown
4903/tcp closed unknown
4904/tcp closed unknown
4905/tcp closed unknown
4906/tcp closed unknown
4907/tcp closed unknown
4908/tcp closed unknown
4909/tcp closed unknown
4910/tcp closed unknown
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for its02.regis.edu (aaa.bbb.ccc.37)
Host is up (0.031s latency).
All 65535 scanned ports on its02.regis.edu (aaa.bbb.ccc.37) are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: VoIP adapter|firewall|general purpose
Running: Cisco embedded, SonicWALL embedded, Sun Solaris 10|9
OS details: Cisco Unified Communications Manager VoIP gateway, SonicWALL Aventail EX-1500 SSL VPN appliance, Sun Solaris 10, Sun Solaris 10 (SPARC), Sun Solaris 9 (SPARC)

Nmap scan report for academic.regis.edu (aaa.bbb.ccc.38)
Host is up (0.033s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
25/tcp open tcpwrapped
80/tcp open http Microsoft IIS httpd
110/tcp closed pop3
443/tcp open ssl/http Microsoft IIS httpd 6.0
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for its39.regis.edu (aaa.bbb.ccc.39)
Host is up (0.067s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp closed http
443/tcp closed https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose
Running (JUST GUESSING): SonicWALL embedded (91%), OpenBSD 4.X (87%), DEC Digital UNIX 5.X (87%), FreeBSD 6.X|8.X (86%), Apple Mac OS X 10.6.X (85%), Microsoft Windows 2003|NT (85%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (91%), OpenBSD 4.6 (87%), OpenBSD 4.7 (87%), DEC Digital UNIX 5.X (87%), FreeBSD 6.2-RELEASE-p2 (pf with scrub enabled) (86%), FreeBSD 8.0-CURRENT (86%), OpenBSD 4.2 (86%), OpenBSD 4.3 (86%), Apple Mac OS X 10.6.2 (Snow Leopard) (Darwin 10.2.0) (85%), Microsoft Windows Small Business Server 2003 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for ereserves.regis.edu (aaa.bbb.ccc.40)
Host is up (0.045s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp closed https
3389/tcp open microsoft-rdp Microsoft Terminal Service

Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for its-17.regis.edu (aaa.bbb.ccc.41)
Host is up (0.034s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for insite.regis.edu (aaa.bbb.ccc.43)
Host is up (0.037s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (85%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for producer.regis.edu (aaa.bbb.ccc.44)
Host is up (0.032s latency).
Not shown: 65528 filtered ports
PORT STATE SERVICE VERSION
80/tcp closed http
443/tcp closed https
3389/tcp open microsoft-rdp xrdp
4073/tcp open unknown

8143/tcp closed unknown
8170/tcp closed unknown
8171/tcp closed unknown
Device type: general purpose|phone
Running (JUST GUESSING): Apple Mac OS X 10.5.X|10.6.X (92%), Apple iOS 4.X (88%), Apple iPhone OS 3.X (85%)
Aggressive OS guesses: Apple Mac OS X 10.5.2 - 10.6.2 (Leopard - Snow Leopard) (Darwin 9.2.0 - 10.2.0) (92%), Apple Mac OS X 10.5.5 - 10.6.1 (Leopard - Snow Leopard) (Darwin 9.5.0 - 10.0.0) (89%), Apple Mac OS X 10.5 - 10.6.3 (Leopard - Snow Leopard) or iOS 4.0 - 4.1 (Darwin 9.0.0b5 - 10.2.0) (88%), Apple Mac OS X 10.5.3 - 10.5.4 (Leopard) (Darwin 9.3.0 - 9.4.0) (88%), Apple Mac OS X 10.5.4 (Leopard) (Darwin 9.4.0) (87%), Apple Mac OS X 10.5.5 (Leopard) (Darwin 9.5.0) (87%), Apple Mac OS X 10.6.3 (Snow Leopard) (Darwin 10.3.0) (86%), Apple Mac OS X 10.5 (Leopard) (Darwin 9.0.0b4, x86) (86%), Apple iPhone mobile phone (iPhone OS 3.0 - 3.2.1, Darwin 10.0.0d3) (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for stream.regis.edu (aaa.bbb.ccc.45)
Host is up (0.032s latency).
Not shown: 65529 filtered ports
PORT STATE SERVICE VERSION
80/tcp open rtsp Helix Mobile Server rtspd 14.0.0.348
554/tcp open rtsp Helix Mobile Server rtspd 14.0.0.348
1755/tcp open wms?
7070/tcp closed realserver
8000/tcp open shoutcast SHOUTcast server 1.9.8
8080/tcp closed http-proxy
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.47
Host is up (0.041s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
419/tcp open ftp
422/tcp closed ariel3
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port419-TCP:V=5.51%I=7%D=10/7%Time=4E8F7E21%P=i686-pc-windows-windows%r
SF:(NULL,1A,"220\x20welcome\x20to\x20ftp\x20world\r\n")%r(GenericLines,26,
SF:"220\x20welcome\x20to\x20ftp\x20world\r\n501\x20Error\x20\r\n")%r(Help,
SF:1A,"220\x20welcome\x20to\x20ftp\x20world\r\n")%r(SMBProgNeg,26,"220\x20
SF:welcome\x20to\x20ftp\x20world\r\n501\x20Error\x20\r\n");

Device type: broadband router
Running (JUST GUESSING): XAVi embedded (85%)
Aggressive OS guesses: XAVi 7001 DSL modem (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: welcome

Nmap scan report for epicor.regis.edu (aaa.bbb.ccc.49)
Host is up (0.043s latency).
All 65535 scanned ports on epicor.regis.edu (aaa.bbb.ccc.49) are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|firewall|general purpose
Running: Cisco embedded, SonicWALL embedded, Sun Solaris 10|9
OS details: Cisco Unified Communications Manager VoIP gateway, SonicWALL Aventail EX-1500 SSL VPN appliance, Sun Solaris 10, Sun Solaris 10 (SPARC), Sun Solaris 9 (SPARC)

Nmap scan report for its22.regis.edu (aaa.bbb.ccc.51)
Host is up (0.036s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd
443/tcp open ssl/http Microsoft IIS httpd 6.0
8080/tcp closed http-proxy
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.54
Host is up (0.044s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
25/tcp closed smtp
80/tcp open http Microsoft IIS httpd
443/tcp open ssl/http Microsoft IIS httpd 6.0
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (87%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (87%), Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.55
Host is up (0.047s latency).

Not shown: 65530 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco VPN Concentrator SSHd (protocol 1.5)
80/tcp open http Cisco VPN Concentrator http config
443/tcp open ssl/http Cisco VPN Concentrator http config
1723/tcp open pptp Cisco Systems, Inc. (Firmware: 1025)
10000/tcp open snet-sensor-mgmt?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: router
Running (JUST GUESSING): Juniper embedded (85%)
Aggressive OS guesses: Juniper Networks ERX-700 router (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: Remote; Device: terminal server

Nmap scan report for mail1.regis.edu (aaa.bbb.ccc.56)
Host is up (0.057s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp closed https
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%), Microsoft Windows Server 2008 SP1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for update.regis.edu (aaa.bbb.ccc.57)
Host is up (0.037s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
443/tcp open ssl/http Microsoft IIS httpd 6.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for web-classrooms.regis.edu (aaa.bbb.ccc.58)
Host is up (0.036s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd
4445/tcp closed upnotifyp
4568/tcp closed unknown
8900/tcp open http Microsoft IIS httpd
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (87%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (87%), Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for selfhelp.regis.edu (aaa.bbb.ccc.59)
Host is up (0.043s latency).
Not shown: 65521 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.0
443/tcp closed https
990/tcp open ssl/ftp Microsoft ftpd
4900/tcp closed hfcs
4901/tcp closed unknown
4902/tcp closed unknown
4903/tcp closed unknown
4904/tcp closed unknown
4905/tcp closed unknown
4906/tcp closed unknown
4907/tcp closed unknown
4908/tcp closed unknown
4909/tcp closed unknown
4910/tcp closed unknown
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2008 (85%)
Aggressive OS guesses: Microsoft Windows Server 2008 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.60
Host is up (0.035s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http?
443/tcp open ssl/http VMware View Manager httpd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :

SF-Port80-TCP:V=5.51%I=7%D=10/7%Time=4E8F8A36%P=i686-pc-windows-windows%r(
SF:GetRequest,92B,"HTTP/1\.1\x20505\x20HTTP\x20Version\x20Not\x20Supported
SF:\r\nDate:\x20Fri,\x2007\x20Oct\x202011\x2023:24:37\x20GMT\r\nContent-Le
SF:ngth:\x202220\r\nContent-Type:\x20text/html\r\n\r\n<html>\r\n<head>\r\n
SF:\x20\x20\x20\x20<title>VMware\x20VDM\x20Web\x20Access</title>\r\n\x20\x
SF:20\x20\x20<link\x20rel=\"stylesheet\"\x20type=\"text/css\"\x20href=\"/e
SF:rror/base\.css\"\x20/>\r\n\x20\x20\x20\x20<script\x20language=\"JavaScr
SF:ipt\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20function\x20toggleError\(\)\r
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20var\x20errorElement\x20=\x20document\.getElementById\('
SF:fullErrorStack'\);\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20i
SF:f\x20\(errorElement\x20&&\x20errorElement\.style\.display\x20==\x20'non
SF:e'\)\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20errorElement\.sty
SF:le\.display=\"block\";\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20}\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20else\r\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20errorElement\.style\.display=\"n
SF:one\";\x20\x20\x20\x20\x20\x20\x20\x20\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\x20\x20}\r\n\r\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20function\x20escapeHTML\x20\(str\)\r\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20var\x20div\x20=\x20document\.createElement\('div'\);\r\n\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20var\x20text\x20=\x20document\.cr
SF:eateTextNode\(str\);\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0div\.appendChild\(text\);\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20return\x20div\.inn")%r(HTTPOptions,92B,"HTTP/1\.1\x20505\x20HTTP
SF:\x20Version\x20Not\x20Supported\r\nDate:\x20Fri,\x2007\x20Oct\x202011\x
SF:2023:24:37\x20GMT\r\nContent-Length:\x202220\r\nContent-Type:\x20text/h
SF:tml\r\n\r\n<html>\r\n<head>\r\n\x20\x20\x20\x20<title>VMware\x20VDM\x20
SF:Web\x20Access</title>\r\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x2
SF:0type=\"text/css\"\x20href=\"/error/base\.css\"\x20/>\r\n\x20\x20\x20\x
SF:20<script\x20language=\"JavaScript\">\r\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20function\x20toggleError\(\)\r\n\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20var\x20errorElement\x20=
SF:\x20document\.getElementById\('fullErrorStack'\);\r\n\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20if\x20\(errorElement\x20&&\x20errorElemen
SF:t\.style\.display\x20==\x20'none'\)\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20{\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20errorElement\.style\.display=\"block\";\r\n\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20else\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0{\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20e
SF:rrorElement\.style\.display=\"none\";\x20\x20\x20\x20\x20\x20\x20\x20\r
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20}\r\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20}\r\n\r\n\x20\x20\x20\x20\x20\x20\x20\x20function\x20es

SF:capeHTML\x20\(str\)\r\n\x20\x20\x20\x20\x20\x20\x20\x20{\r\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20var\x20div\x20=\x20document\.creat
SF:eElement\('div'\);\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20v
SF:ar\x20text\x20=\x20document\.createTextNode\(str\);\r\n\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20div\.appendChild\(text\);\r\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20return\x20div\.inn");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

Nmap scan report for aaa.bbb.ccc.61
Host is up (0.032s latency).
All 65535 scanned ports on aaa.bbb.ccc.61 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP adapter|firewall|general purpose
Running: Cisco embedded, SonicWALL embedded, Sun Solaris 10|9
OS details: Cisco Unified Communications Manager VoIP gateway, SonicWALL Aventail EX-1500 SSL VPN appliance, Sun Solaris 10, Sun Solaris 10 (SPARC), Sun Solaris 9 (SPARC)

Nmap scan report for communicator.regis.edu (aaa.bbb.ccc.66)
Host is up (0.041s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http MS ISA httpd
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (86%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.67
Host is up (0.039s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
443/tcp closed https
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%), Microsoft Windows XP SP3 (85%)

No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for sip.regis.edu (aaa.bbb.ccc.69)
Host is up (0.033s latency).
Not shown: 55529 filtered ports, 10004 closed ports
PORT STATE SERVICE VERSION
443/tcp open ssl/sip (SIP end point; Status: 504 Server time-out)
5061/tcp open ssl/sip-tls?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port443-TCP:V=5.51%T=SSL%I=7%D=10/7%Time=4E8F8BD1%P=i686-pc-windows-win
SF:dows%r(SIPOptions,E8,"SIP/2\.0\x20504\x20Server\x20time-out\r\nms-user-
SF:logon-data:\x20RemoteUser\r\nFrom:\x20<sip:nm@nm>;tag=root\r\nTo:\x20<s
SF:ip:nm2@nm2>;tag=0E159298EF9DA3A74EE4141AE5FADD50\r\nCall-ID:\x2050000\r
SF:\nCSeq:\x2042\x20OPTIONS\r\nVia:\x20SIP/2\.0/TCP\x20nm;branch=foo\r\nCo
SF:ntent-Length:\x200\r\n\r\n");
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Server 2008 Beta 3 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for ocswebconf.regis.edu (aaa.bbb.ccc.72)
Host is up (0.033s latency).
Not shown: 55529 filtered ports, 10005 closed ports
PORT STATE SERVICE VERSION
443/tcp open ssl/https?
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for ocsavedge.regis.edu (aaa.bbb.ccc.73)
Host is up (0.032s latency).
Not shown: 55529 filtered ports, 10005 closed ports
PORT STATE SERVICE VERSION
443/tcp open tcpwrapped
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)

Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for spslcalc.regis.edu (aaa.bbb.ccc.75)
Host is up (0.036s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp closed https
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.77
Host is up (0.032s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
8443/tcp closed https-alt
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (87%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (87%), Microsoft Windows Server 2008 (87%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (87%), Microsoft Windows Server 2008 Beta 3 (86%), Microsoft Windows 7 Professional (86%), Microsoft Windows Vista Enterprise (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.78
Host is up (0.049s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (88%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (88%), Microsoft Windows Server 2008 SP1 (86%), Microsoft Windows Server 2008

(85%), Microsoft Windows Server 2008 Beta 3 (85%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.97
Host is up (0.044s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 3.6.1p2 (protocol 2.0)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Aruba A800 wireless LAN switch (89%), Linux 2.4.7 (88%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or Xerox WorkCentre Pro 265 printer (88%), Linux 2.4.21 - 2.4.31 (likely embedded) (88%), Linux 2.4.9 (Red Hat Enterprise Linux 2.1 AS) (87%), Netgear DG834GB wireless broadband router (86%), Dell Remote Access Controller 5 (DRAC 5) (86%), SonicWALL Aventail EX-1500 SSL VPN appliance (86%), HP 4200 PSA (Print Server Appliance) model J4117A (85%), Linksys WRV200 wireless broadband router (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for in2.regis.edu (aaa.bbb.ccc.98)
Host is up (0.057s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (86%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.99
Host is up (0.053s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache Tomcat/Coyote JSP engine 1.0
443/tcp closed https
8080/tcp closed http-proxy
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (87%)

Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%), Microsoft Windows XP SP3 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for www.regis.edu (aaa.bbb.ccc.100)
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open https?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (88%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (88%), Microsoft Windows Server 2008 SP1 (85%), Microsoft Windows Server 2008 (85%), Microsoft Windows Server 2008 Beta 3 (85%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.101
Host is up (0.056s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.0.52 ((CentOS))
443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (88%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (88%), Linux 2.6.9 - 2.6.27 (88%), Linux 2.6.11 (Auditor) (86%), Linux 2.6.9 (86%), Linux 2.6.22 (85%), Linux 2.6.9 (CentOS 4.4) (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.102
Host is up (0.060s latency).
Not shown: 65069 filtered ports, 462 closed ports
PORT STATE SERVICE VERSION
80/tcp open http-proxy EZproxy web proxy
443/tcp open ssl/http-proxy EZproxy web proxy
1051/tcp open optima-vnet?
1054/tcp open brvread?
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (87%)

Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.103
Host is up (0.065s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.2.3 ((CentOS))
443/tcp open ssl/http Apache httpd 2.2.3 ((CentOS))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|WAP
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (89%), ZoneAlarm embedded (87%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (89%), Linux 2.6.9 - 2.6.27 (89%), ZoneAlarm Z100G WAP (87%), Linux 2.6.9 (87%), Linux 2.6.17 (Mandriva) (85%), Linux 2.6.18 (Centos 5.3) (85%), Linux 2.6.22 - 2.6.23 (85%), Linux 2.6.9 - 2.6.30 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.104
Host is up (0.059s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 6.0
443/tcp open ssl/http Microsoft IIS httpd 6.0
5060/tcp open sip Microsoft Live SIP client
5061/tcp open ssl/sip Microsoft Office Communications Service 2005
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.105
Host is up (0.058s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
25/tcp closed smtp
80/tcp open http Microsoft IIS httpd 6.0
110/tcp closed pop3
443/tcp open ssl/http Microsoft IIS httpd 6.0

Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (87%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (87%), Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.106
Host is up (0.066s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd
443/tcp open ssl/http Microsoft IIS httpd 6.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (86%), Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows Server 2003 SP1 or SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.107
Host is up (0.070s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|WAP
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (88%), ZoneAlarm embedded (87%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (88%), Linux 2.6.9 - 2.6.27 (88%), ZoneAlarm Z100G WAP (87%), Linux 2.6.9 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.108
Host is up (0.066s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache Tomcat/Coyote JSP engine 1.1
443/tcp open ssl/http Apache Tomcat/Coyote JSP engine 1.1
1935/tcp open rtmp?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.109
Host is up (0.065s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|WAP
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (89%), ZoneAlarm embedded (87%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (89%), Linux 2.6.9 - 2.6.27 (89%), ZoneAlarm Z100G WAP (87%), Linux 2.6.9 (87%), Linux 2.6.17 (Mandriva) (85%), Linux 2.6.18 (Centos 5.3) (85%), Linux 2.6.22 - 2.6.23 (85%), Linux 2.6.9 - 2.6.30 (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.110
Host is up (0.075s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008 (88%)
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1, Windows 7, or Server 2008 (88%), Microsoft Windows Server 2008 SP1 (85%), Microsoft Windows Server 2008 (85%), Microsoft Windows Server 2008 Beta 3 (85%), Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.111
Host is up (0.074s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
1935/tcp open rtmp Real-Time Messaging Protocol
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.112
Host is up (0.068s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (85%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.113
Host is up (0.069s latency).
Not shown: 65528 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Microsoft Exchange ESMTP
80/tcp open http Microsoft IIS
143/tcp open imap Microsoft Exchange 2007 imapd
443/tcp open ssl/http Microsoft IIS
587/tcp open smtp Microsoft Exchange ESMTP
993/tcp open ssl/imap Microsoft Exchange 2007 imapd
995/tcp open ssl/pop3 MS Exchange 2007 pop3d
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (85%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (85%), Microsoft Windows Server 2003 SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: email.regis.edu; OS: Windows

Nmap scan report for aaa.bbb.ccc.114
Host is up (0.072s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd
443/tcp open https?

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (86%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (86%), Microsoft Windows Server 2003 SP2 (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for singtest.regis.edu (aaa.bbb.ccc.115)
Host is up (0.073s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS
443/tcp open ssl/http Microsoft IIS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2003 (86%)
Aggressive OS guesses: Microsoft Windows XP SP2 or Server 2003 SP2 (86%), Microsoft Windows XP SP2 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for aaa.bbb.ccc.116
Host is up (0.050s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp Microsoft ftpd
80/tcp open http Microsoft IIS httpd 6.0
443/tcp closed https
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003 (87%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (87%), Microsoft Windows Server 2003 SP2 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows

Nmap scan report for maila.regis.edu (aaa.bbb.ccc.120)
Host is up (0.048s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete

No OS matches for host
Service Info: OS: Unix

Nmap scan report for mailb.regis.edu (aaa.bbb.ccc.121)
Host is up (0.046s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Unix

Nmap scan report for mailc.regis.edu (aaa.bbb.ccc.122)
Host is up (0.043s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Unix

Nmap scan report for maild.regis.edu (aaa.bbb.ccc.123)
Host is up (0.042s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Unix

Nmap scan report for maile.regis.edu (aaa.bbb.ccc.124)
Host is up (0.031s latency).
Not shown: 65534 filtered ports
PORT STATE SERVICE VERSION
25/tcp open smtp Sendmail 8.13.1/8.13.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (88%)

Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (88%), Linux 2.6.9 - 2.6.27 (88%), Linux 2.6.11 (Auditor) (86%), Linux 2.6.9 (86%), Linux 2.6.22 (85%), Linux 2.6.9 (CentOS 4.4) (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Unix

Nmap scan report for antispam.regis.edu (aaa.bbb.ccc.125)
Host is up (0.038s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.0.52 ((CentOS))
443/tcp open ssl/http Apache httpd 2.0.52 ((CentOS))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose
Running (JUST GUESSING): SonicWALL embedded (90%), Linux 2.6.X (88%)
Aggressive OS guesses: SonicWALL Aventail EX-1500 SSL VPN appliance (90%), Linux 2.6.9 - 2.6.18 (88%), Linux 2.6.9 - 2.6.27 (88%), Linux 2.6.11 (Auditor) (86%), Linux 2.6.9 (86%), Linux 2.6.22 (85%), Linux 2.6.9 (CentOS 4.4) (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for aaa.bbb.ccc.161
Host is up (0.056s latency).
Not shown: 65529 closed ports
PORT STATE SERVICE VERSION
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: broadband router|router|switch|WAP
Running: Cisco embedded, Cisco IOS 12.X|15.X
OS details: Cisco 827H ADSL router, Cisco 870 router or 2960 switch (IOS 12.2 - 12.4), Cisco Aironet 1250 WAP (IOS 12.4), Cisco C7200 router (IOS 15)

Nmap scan report for vpn.regis.edu (aaa.bbb.ccc.164)
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Cisco ASA firewall http config
443/tcp open ssl/http Cisco ASA firewall http config
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: WAP|switch|webcam|router|VoIP phone
Running (JUST GUESSING): D-Link embedded (96%), TRENDnet embedded (96%), HP embedded (90%), Linksys embedded (89%), Cisco embedded (87%)
Aggressive OS guesses: D-Link DWL-624+ or DWL-2000AP, or TRENDnet TEW-432BRP WAP (96%), HP 4000M ProCurve switch (J4121A) (90%), Linksys BEFSR41 EtherFast router or D-Link DCS-6620G webcam (89%), Cisco IP Phone 7941 (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Device: firewall

Nmap scan report for aaa.bbb.ccc.193
Host is up (0.071s latency).
All 65535 scanned ports on aaa.bbb.ccc.193 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.194
Host is up (0.069s latency).
All 65535 scanned ports on aaa.bbb.ccc.194 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.195
Host is up (0.039s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
161/tcp closed snmp
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FAD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,12D,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RegisScience2\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J403-0000-110B-62EB\r\nServer:\x20
SF:Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauth
SF:orized</h1>\n</body>\n</html>")%r(HTTPOptions,12D,"HTTP/1\.0\x20401\x20
SF:Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RegisScienc
SF:e2\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-
SF:Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J
SF:403-0000-110B-62EB\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<
SF:html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSP
SF:Request,12D,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20B
SF:asic\x20realm=\"Admin-RegisScience2\"\r\nContent-Length:\x2056\r\nConte
SF:nt-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-vers
SF:ion:\x202\r\nNiagara-HostId:\x20J403-0000-110B-62EB\r\nServer:\x20Niaga

SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>")%r(FourOhFourRequest,12D,"HTTP/1\.0\x20401\x2
SF:0Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RegisScien
SF:ce2\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara
SF:-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20
SF:J403-0000-110B-62EB\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n
SF:<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIP
SF:Options,12C,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Ba
SF:sic\x20realm=\"Admin-RegisScience2\"\r\nContent-Length:\x2056\r\nConten
SF:t-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-versi
SF:on:\x202\r\nNiagara-HostId:\x20J403-0000-110B-62EB\r\nServer:\x20Niagar
SF:a\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized
SF:</h1>\n</body>\n</html>");
Aggressive OS guesses: Nortel DMS-10 telephony switch (88%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (87%), ReactOS 0.3.7 (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), Konica Minolta bizhub C450 printer with optional Fiery Controller (86%), Netgear DG834G WAP (86%), Siemens SpeedStream 4200 ADSL modem (86%), Lexmark X644e printer (85%), Netgear WGR614v7 wireless broadband router (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.196
Host is up (0.049s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FAD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J404-24737\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J404-0000-0EF0-DEC7\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-24737\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-00
SF:00-0EF0-DEC7\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J404-24737\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J404-0000-0EF0-DEC7\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<

SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-24737\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-0000-0E
SF:F0-DEC7\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J404-24737\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J404-0000-0EF0-DEC7\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.198
Host is up (0.044s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FAD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-11406\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-0A44-8D67\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-11406\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-0A44-8D67\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques

SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-11406\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-0A44-8D67\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-11406\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-0A
SF:44-8D67\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-11406\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-0A44-8D67\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.199
Host is up (0.044s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FAD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-14884\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-0BA1-FFDE\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una

SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-14884\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-0BA1-FFDE\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-14884\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-0BA1-FFDE\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-14884\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-0B
SF:A1-FFDE\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-14884\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-0BA1-FFDE\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.200
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp closed http
3011/tcp open sip Niagara Web Server/3.0 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FB107%P=i686-pc-windows-windows%
SF:r(GetRequest,1A8,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:

SF:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"
SF:MD5\",\x20nonce=\"TovVkzFlODA1ZmZiNDczMTk4MjE2MDhhM2YwNTE4ZWZlYjVj\
"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20QNX\r\nNiagara-Started:\x202010-3-21-3-32-50\r\nBaja-Station-Bran
SF:d:\x20vykon\r\nNiagara-HostId:\x20Qnx-J403-0000-0BA1-95F8\r\nServer:\x2
SF:0Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unaut
SF:horized</h1>\n</body>\n</html>")%r(HTTPOptions,1A8,"HTTP/1\.0\x20401\x2
SF:0Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admin\"
SF:,\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"TovVmDZjZGQ2MzExNjF
SF:kMzA5ZWQxODg0ZjkyZjNkNGJmNWQ0\"\r\nContent-Length:\x2056\r\nContent-Typ
SF:e:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x202010
SF:-3-21-3-32-50\r\nBaja-Station-Brand:\x20vykon\r\nNiagara-HostId:\x20Qnx
SF:-J403-0000-0BA1-95F8\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\
SF:n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RT
SF:SPRequest,1A8,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x2
SF:0Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"MD5
SF:\",\x20nonce=\"TovVnWIyZDkyNDhiOTU4MTE5ODE3YjZkYjU2Mzc5OWMwZmJk\"\r\n
Co
SF:ntent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\
SF:x20QNX\r\nNiagara-Started:\x202010-3-21-3-32-50\r\nBaja-Station-Brand:\
SF:x20vykon\r\nNiagara-HostId:\x20Qnx-J403-0000-0BA1-95F8\r\nServer:\x20Ni
SF:agara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthor
SF:ized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1A8,"HTTP/1\.0\x20401
SF:\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admi
SF:n\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"TovVtGM4ZTk5ZGIy
SF:N2UwNWRiM2U5MGVjNzMyYWRiMWIxM2Yz\"\r\nContent-Length:\x2056\r\nContent-
SF:Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x202
SF:010-3-21-3-32-50\r\nBaja-Station-Brand:\x20vykon\r\nNiagara-HostId:\x20
SF:Qnx-J403-0000-0BA1-95F8\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\r\n
SF:\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Aggressive OS guesses: NRG MP C4500 printer (95%), NRG C7521n printer (93%), Ricoh Aficion SP 4100N printer (92%), Check Point VPN-1 firewall (IPSO 4.1) (90%), Asus RT-N16 WAP (Linux 2.6) (87%), NetBSD 1.4.2 - 1.5.2; Lanier LS232c, NRG DSc428, Ricoh Aficio 2020, Ricoh NRG MP 161, or Savin 8055 printer; or Panasonic Network Camera (BB-HCM331, BB-HCM381, BCL-30A, BL-C1CE, or BL-C10CE) (87%), QNX 6.2.1 (x86) (87%), Netgear DG834G WAP (87%), Ricoh Aficio 1022 copier (87%), Lexmark X644e printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.201
Host is up (0.048s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v2)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FB10A%P=i686-pc-windows-windows%
SF:r(GetRequest,11D,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-NIAGARASERVER\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20NT\r\nniagarad-versi
SF:on:\x202\r\nNiagara-HostId:\x20ECA6-4E73\r\nServer:\x20Niagara\x20Web\x
SF:20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</b
SF:ody>\n</html>")%r(HTTPOptions,11D,"HTTP/1\.0\x20401\x20Unauthorized\r\n
SF:WWW-Authenticate:\x20Basic\x20realm=\"Admin-NIAGARASERVER\"\r\nContent-
SF:Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20NT\
SF:r\nniagarad-version:\x202\r\nNiagara-HostId:\x20ECA6-4E73\r\nServer:\x2
SF:0Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unaut
SF:horized</h1>\n</body>\n</html>")%r(RTSPRequest,11D,"RTSP/1\.0\x20401\x2
SF:0Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-NIAGARASER
SF:VER\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara
SF:-Platform:\x20NT\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20ECA6-4
SF:E73\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n
SF:<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1
SF:1D,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20r
SF:ealm=\"Admin-NIAGARASERVER\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20NT\r\nniagarad-version:\x202\r\nNi
SF:agara-HostId:\x20ECA6-4E73\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\
SF:r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>"
SF:)%r(SIPOptions,11C,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate
SF::\x20Basic\x20realm=\"Admin-NIAGARASERVER\"\r\nContent-Length:\x2056\r\
SF:nContent-Type:\x20text/html\r\nNiagara-Platform:\x20NT\r\nniagarad-vers
SF:ion:\x202\r\nNiagara-HostId:\x20ECA6-4E73\r\nServer:\x20Niagara\x20Web\
SF:x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</
SF:body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2000|2003 (98%)
Aggressive OS guesses: Microsoft Windows XP SP3 (98%), Microsoft Windows XP SP2 or SP3 (96%), Microsoft Windows 2000 SP4 (94%), Microsoft Windows 2000 (93%), Microsoft Windows XP Professional SP2 (91%), Microsoft Windows XP SP 2 (91%), Microsoft Windows XP SP2 (90%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (89%), Microsoft Windows Server 2003 Enterprise Edition (89%), Microsoft Windows XP Professional SP3 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.202
Host is up (0.084s latency).
All 65535 scanned ports on aaa.bbb.ccc.202 are filtered

Too many fingerprints match this host to give specific OS details
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.203
Host is up (0.050s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FB107%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J404-29083\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J404-0000-1225-E4B1\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-29083\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-00
SF:00-1225-E4B1\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J404-29083\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J404-0000-1225-E4B1\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-29083\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-0000-12
SF:25-E4B1\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J404-29083\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J404-0000-1225-E4B1\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose|firewall|game console|storage-misc|switch|remote management|media device

Running (JUST GUESSING): Netgear embedded (94%), HP embedded (93%), Linux 2.4.X|2.1.X|2.6.X (93%), Fortinet embedded (91%), Microsoft embedded (91%), Netgear RAIDiator 4.X (89%), 3Com embedded (89%), Aruba ArubaOS 3.X (89%)
Aggressive OS guesses: Netgear DG834G WAP (94%), HP ProCurve MSM422 WAP (93%), Linux 2.4.21 - 2.4.25 (93%), Fortinet FortiGate-60B or -100A firewall (91%), Microsoft Xbox game console (modified, running XboxMediaCenter) (91%), Netgear ReadyNAS Duo NAS device (RAIDiator 4.1.4) (89%), 3Com SuperStack 3 Switch 3870 (89%), Aruba 200 wireless LAN controller (ArubaOS 3.3.2.5) (89%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (89%), Linux 2.4.20 - 2.4.27 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.204
Host is up (0.045s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J511-4020\"\r\nContent-Length:\x2056\r\nCont
SF:ent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-ver
SF:sion:\x202\r\nNiagara-HostId:\x20J511-AA55-EAAA\r\nServer:\x20Niagara\x
SF:20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h
SF:1>\n</body>\n</html>")%r(HTTPOptions,124,"HTTP/1\.0\x20401\x20Unauthori
SF:zed\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J511-4020\"\r\nConte
SF:nt-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20
SF:JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J511-AA55-EAAA
SF:\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1
SF:>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,124,"RTSP/
SF:1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Ad
SF:min-J511-4020\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\
SF:r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-H
SF:ostId:\x20J511-AA55-EAAA\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\
SF:n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%
SF:r(FourOhFourRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authen
SF:ticate:\x20Basic\x20realm=\"Admin-J511-4020\"\r\nContent-Length:\x2056\
SF:r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniaga
SF:rad-version:\x202\r\nNiagara-HostId:\x20J511-AA55-EAAA\r\nServer:\x20Ni
SF:agara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthor
SF:ized</h1>\n</body>\n</html>")%r(SIPOptions,123,"SIP/2\.0\x20401\x20Unau
SF:thorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J511-4020\"\r\n
SF:Content-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform
SF::\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J511-AA55

SF:-EAAA\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>
SF:\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.205
Host is up (0.050s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-JACE-27583\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J404-0000-110B-5737\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-JACE-27583\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-00
SF:00-110B-5737\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-JACE-27583\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J404-0000-110B-5737\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-JACE-27583\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-0000-11
SF:0B-5737\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod

SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-JACE-27583\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J404-0000-110B-5737\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.206
Host is up (0.044s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-29073\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-1225-F54F\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29073\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-1225-F54F\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-29073\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-1225-F54F\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<

SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29073\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-12
SF:25-F54F\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-29073\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-1225-F54F\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|switch|printer|webcam|general purpose|media device
Running (JUST GUESSING): Netgear embedded (88%), Nortel embedded (87%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Netgear DG834G WAP (88%), Nortel DMS-10 telephony switch (87%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.207
Host is up (0.039s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-29067\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-1226-0673\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29067\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-1226-0673\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques

SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-29067\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-1226-0673\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29067\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-12
SF:26-0673\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-29067\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-1226-0673\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.208
Host is up (0.055s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,127,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-REGISLIBRARY\"\r\nContent-Length:\x2056\r\nC
SF:ontent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-
SF:version:\x202\r\nNiagara-HostId:\x20J512-2041-C820\r\nServer:\x20Niagar
SF:a\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized
SF:</h1>\n</body>\n</html>")%r(HTTPOptions,127,"HTTP/1\.0\x20401\x20Unauth

SF:orized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-REGISLIBRARY\"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J512-204
SF:1-C820\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body
SF:>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,127,
SF:"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20real
SF:m=\"Admin-REGISLIBRARY\"\r\nContent-Length:\x2056\r\nContent-Type:\x20t
SF:ext/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\n
SF:Niagara-HostId:\x20J512-2041-C820\r\nServer:\x20Niagara\x20Web\x20Serve
SF:r/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n<
SF:/html>")%r(FourOhFourRequest,127,"HTTP/1\.0\x20401\x20Unauthorized\r\nW
SF:WW-Authenticate:\x20Basic\x20realm=\"Admin-REGISLIBRARY\"\r\nContent-Le
SF:ngth:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_
SF:51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J512-2041-C820\r\nS
SF:erver:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:
SF:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,126,"SIP/2\.0\x2
SF:0401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-REG
SF:ISLIBRARY\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nN
SF:iagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostI
SF:d:\x20J512-2041-C820\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\
SF:n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.209
Host is up (0.049s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12D,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RegisScience1\"\r\nContent-Length:\x2056\r\n

SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J403-0000-110B-6226\r\nServer:\x20
SF:Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauth
SF:orized</h1>\n</body>\n</html>")%r(HTTPOptions,12D,"HTTP/1\.0\x20401\x20
SF:Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RegisScienc
SF:e1\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-
SF:Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J
SF:403-0000-110B-6226\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<
SF:html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSP
SF:Request,12D,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20B
SF:asic\x20realm=\"Admin-RegisScience1\"\r\nContent-Length:\x2056\r\nConte
SF:nt-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-vers
SF:ion:\x202\r\nNiagara-HostId:\x20J403-0000-110B-6226\r\nServer:\x20Niaga
SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>")%r(FourOhFourRequest,12D,"HTTP/1\.0\x20401\x2
SF:0Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RegisScien
SF:ce1\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara
SF:-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20
SF:J403-0000-110B-6226\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n
SF:<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIP
SF:Options,12C,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Ba
SF:sic\x20realm=\"Admin-RegisScience1\"\r\nContent-Length:\x2056\r\nConten
SF:t-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-versi
SF:on:\x202\r\nNiagara-HostId:\x20J403-0000-110B-6226\r\nServer:\x20Niagar
SF:a\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized
SF:</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.210
Host is up (0.047s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-29066\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-1225-E8C8\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29066\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-1225-E8C8\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-29066\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-1225-E8C8\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-29066\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-12
SF:25-E8C8\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-29066\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-1225-E8C8\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.211

Host is up (0.051s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J403-28929\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J403-0000-1225-0B4E\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-28929\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-00
SF:00-1225-0B4E\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J403-28929\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J403-0000-1225-0B4E\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J403-28929\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_403\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J403-0000-12
SF:25-0B4E\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J403-28929\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_403\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J403-0000-1225-0B4E\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera

(Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.212
Host is up (0.050s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,12A,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J404-31225\"\r\nContent-Length:\x2056\r\nCon
SF:tent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-ve
SF:rsion:\x202\r\nNiagara-HostId:\x20J404-0000-1225-0882\r\nServer:\x20Nia
SF:gara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthori
SF:zed</h1>\n</body>\n</html>")%r(HTTPOptions,12A,"HTTP/1\.0\x20401\x20Una
SF:uthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-31225\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-00
SF:00-1225-0882\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\
SF:n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPReques
SF:t,12A,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-J404-31225\"\r\nContent-Length:\x2056\r\nContent-Type:\
SF:x20text/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202
SF:\r\nNiagara-HostId:\x20J404-0000-1225-0882\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(FourOhFourRequest,12A,"HTTP/1\.0\x20401\x20Unauthor
SF:ized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J404-31225\"\r\nCon
SF:tent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x
SF:20JACE_404\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J404-0000-12
SF:25-0882\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<bod
SF:y>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(SIPOptions,129,
SF:"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm
SF:=\"Admin-J404-31225\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_404\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J404-0000-1225-0882\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|switch|printer|webcam|general purpose|media device

Running (JUST GUESSING): Netgear embedded (88%), Nortel embedded (87%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Netgear DG834G WAP (88%), Nortel DMS-10 telephony switch (87%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.213
Host is up (0.052s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
1911/tcp open mtp?
3012/tcp open sip Niagara Web Server/3.0 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3012-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD1F%P=i686-pc-windows-windows%
SF:r(GetRequest,1AB,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"
SF:MD5\",\x20nonce=\"To/MB2RjZTUzOWJhYmZjYWI5YWY5MWViYjYxMTQ4ZjgxYW
M0\"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20QNX\r\nNiagara-Started:\x202011-8-22-23-36-50\r\nBaja-Station-Bra
SF:nd:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-68E6\r\nServer:
SF:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Un
SF:authorized</h1>\n</body>\n</html>")%r(HTTPOptions,1AB,"HTTP/1\.0\x20401
SF:\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admi
SF:n\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/MDDk3YzNjM2Fk
SF:YTU5ZGQwZTFiMjkxMDg3N2MyNjFhOTdk\"\r\nContent-Length:\x2056\r\nContent-
SF:Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x202
SF:011-8-22-23-36-50\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara-HostId:\
SF:x20Qnx-NPM2-0000-0E56-68E6\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\
SF:r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>"
SF:)%r(RTSPRequest,1AB,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authentica
SF:te:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm
SF:=\"MD5\",\x20nonce=\"To/MEWRjYThkYmE2ODMzY2RjZTVmZWRlZjViYzhjM2M0M
WEz\"
SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat
SF:form:\x20QNX\r\nNiagara-Started:\x202011-8-22-23-36-50\r\nBaja-Station-
SF:Brand:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-68E6\r\nServ
SF:er:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x2
SF:0Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1AB,"HTTP/1\
SF:.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Nia

SF:gara-Admin\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/MKDN
SF:iYTBmMGZmM2JjYjJkNjJkM2M3N2YzZmQ0ZmI2OTRj\"\r\nContent-Length:\x2056\r\
SF:nContent-Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Star
SF:ted:\x202011-8-22-23-36-50\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara
SF:-HostId:\x20Qnx-NPM2-0000-0E56-68E6\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: NRG MP C4500 printer (94%), NRG C7521n printer (92%), Ricoh Aficion SP 4100N printer (91%), Netgear DG834G WAP (89%), Asus RT-N16 WAP (Linux 2.6) (88%), AXIS 211A Network Camera (Linux 2.6) (88%), AXIS 211A Network Camera (Linux 2.6.20) (88%), Linux 2.6.24 (88%), Check Point VPN-1 firewall (IPSO 4.1) (87%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.214
Host is up (0.043s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
1911/tcp open mtp?
3012/tcp open sip Niagara Web Server/3.0 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3012-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD25%P=i686-pc-windows-windows%
SF:r(GetRequest,1AB,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"
SF:MD5\",\x20nonce=\"To/DpWFiYmM3NzFmYTk0MDkzNDA3NzUyZWYzMTJmODhlYT
Q5\"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20QNX\r\nNiagara-Started:\x202011-8-17-11-38-58\r\nBaja-Station-Bra
SF:nd:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-3926\r\nServer:
SF:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Un
SF:authorized</h1>\n</body>\n</html>")%r(HTTPOptions,1AB,"HTTP/1\.0\x20401
SF:\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admi
SF:n\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/DqjEyOTFiODIw
SF:MDkzY2U2MDdmZDg3NDhjOGQzOTMwOWFi\"\r\nContent-Length:\x2056\r\nContent-
SF:Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x202
SF:011-8-17-11-38-58\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara-HostId:\
SF:x20Qnx-NPM2-0000-0E56-3926\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\
SF:r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>"
SF:)%r(RTSPRequest,1AB,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authentica
SF:te:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm
SF:=\"MD5\",\x20nonce=\"To/Drzk1M2U1NzI4MmZlNzFlYmIzZWQxNjU4NGU4ZjYwMGFj
\"

SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat
SF:form:\x20QNX\r\nNiagara-Started:\x202011-8-17-11-38-58\r\nBaja-Station-
SF:Brand:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-3926\r\nServ
SF:er:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x2
SF:0Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1AB,"HTTP/1\
SF:.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Nia
SF:gara-Admin\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/DxjY
SF:wNzU3NGE0ZGE1NzRjYTFmNmY2ZTlmNTE0ZWJiODVj\"\r\nContent-Length:\x2056\r\
SF:nContent-Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Star
SF:ted:\x202011-8-17-11-38-58\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara
SF:-HostId:\x20Qnx-NPM2-0000-0E56-3926\r\nServer:\x20Niagara\x20Web\x20Ser
SF:ver/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\
SF:n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: NRG MP C4500 printer (94%), NRG C7521n printer (92%), Ricoh Aficion SP 4100N printer (90%), Netgear DG834G WAP (89%), Asus RT-N16 WAP (Linux 2.6) (88%), AXIS 211A Network Camera (Linux 2.6) (88%), AXIS 211A Network Camera (Linux 2.6.20) (88%), Linux 2.6.24 (88%), Check Point VPN-1 firewall (IPSO 4.1) (87%), NetBSD 1.4.2 - 1.5.2; Lanier LS232c, NRG DSc428, Ricoh Aficio 2020, Ricoh NRG MP 161, or Savin 8055 printer; or Panasonic Network Camera (BB-HCM331, BB-HCM381, BCL-30A, BL-C1CE, or BL-C10CE) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.215
Host is up (0.045s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD25%P=i686-pc-windows-windows%
SF:r(GetRequest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RV_1\"\r\nContent-Length:\x2056\r\nContent-T
SF:ype:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:
SF:\x202\r\nNiagara-HostId:\x20J501-0001-C000\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(HTTPOptions,11F,"HTTP/1\.0\x20401\x20Unauthorized\r
SF:\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_1\"\r\nContent-Length:
SF:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r
SF:\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-0001-C000\r\nServer
SF::\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20U
SF:nauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,11F,"RTSP/1\.0\x2040
SF:1\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_1\"

SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat
SF:form:\x20JACE_50x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-
SF:0001-C000\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<b
SF:ody>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourReq
SF:uest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basi
SF:c\x20realm=\"Admin-RV_1\"\r\nContent-Length:\x2056\r\nContent-Type:\x20
SF:text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\x202\r\
SF:nNiagara-HostId:\x20J501-0001-C000\r\nServer:\x20Niagara\x20Web\x20Serv
SF:er/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n
SF:</html>")%r(SIPOptions,11E,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Auth
SF:enticate:\x20Basic\x20realm=\"Admin-RV_1\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J501-0001-C000\r\nServer:\x20Niaga
SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|printer|WAP|general purpose|webcam
Running (JUST GUESSING): Nortel embedded (94%), Konica Minolta embedded (92%), Netgear embedded (88%), ReactOS 0.3.X (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (94%), Konica Minolta bizhub C450 printer with optional Fiery Controller (92%), Netgear DG834G WAP (88%), ReactOS 0.3.7 (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.216
Host is up (0.055s latency).
Not shown: 65531 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
1911/tcp open mtp?
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
3012/tcp open sip Niagara Web Server/3.0 (Status: 401 Unauthorized)
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD25%P=i686-pc-windows-windows%
SF:r(GetRequest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RV_2\"\r\nContent-Length:\x2056\r\nContent-T
SF:ype:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:
SF:\x202\r\nNiagara-HostId:\x20J501-70E1-DC70\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<

SF:/body>\n</html>")%r(HTTPOptions,11F,"HTTP/1\.0\x20401\x20Unauthorized\r
SF:\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_2\"\r\nContent-Length:
SF:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r
SF:\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-70E1-DC70\r\nServer
SF::\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20U
SF:nauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,11F,"RTSP/1\.0\x2040
SF:1\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_2\"
SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat
SF:form:\x20JACE_50x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-
SF:70E1-DC70\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<b
SF:ody>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourReq
SF:uest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basi
SF:c\x20realm=\"Admin-RV_2\"\r\nContent-Length:\x2056\r\nContent-Type:\x20
SF:text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\x202\r\
SF:nNiagara-HostId:\x20J501-70E1-DC70\r\nServer:\x20Niagara\x20Web\x20Serv
SF:er/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n
SF:</html>")%r(SIPOptions,11E,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Auth
SF:enticate:\x20Basic\x20realm=\"Admin-RV_2\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J501-70E1-DC70\r\nServer:\x20Niaga
SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>");
==============NEXT SERVICE FINGERPRINT (SUBMIT
INDIVIDUALLY)==============
SF-Port3012-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD25%P=i686-pc-windows-windows%
SF:r(GetRequest,1AA,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\"
SF:MD5\",\x20nonce=\"To/JGDM2NDA2ZjkxY2E1MDZkYzI1YTVmZDYxN2NiZjkzYTk3\"\
r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20QNX\r\nNiagara-Started:\x202011-6-20-10-2-29\r\nBaja-Station-Bran
SF:d:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-6AB9\r\nServer:\
SF:x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Una
SF:uthorized</h1>\n</body>\n</html>")%r(HTTPOptions,1AA,"HTTP/1\.0\x20401\
SF:x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagara-Admin
SF:\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/JHTI2MjBlYjU0Y
SF:zAzNjYxNjMzNGEyYjljYzI3NmUxYWRi\"\r\nContent-Length:\x2056\r\nContent-T
SF:ype:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started:\x2020
SF:11-6-20-10-2-29\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara-HostId:\x2
SF:0Qnx-NPM2-0000-0E56-6AB9\r\nServer:\x20Niagara\x20Web\x20Server/3\.0\r\
SF:n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%
SF:r(RTSPRequest,1AA,"RTSP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate
SF::\x20Digest\x20realm=\"Niagara-Admin\",\x20qop=\"auth\",\x20algorithm=\
SF:"MD5\",\x20nonce=\"To/JIjJkMTRlYjRjOTZmZTc5OWVmMTE2YThiZmVlY2ZlNmIz\"\r
SF:\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfo
SF:rm:\x20QNX\r\nNiagara-Started:\x202011-6-20-10-2-29\r\nBaja-Station-Bra

SF:nd:\x20JENEsys\r\nNiagara-HostId:\x20Qnx-NPM2-0000-0E56-6AB9\r\nServer:
SF:\x20Niagara\x20Web\x20Server/3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Un
SF:authorized</h1>\n</body>\n</html>")%r(FourOhFourRequest,1AA,"HTTP/1\.0\
SF:x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Digest\x20realm=\"Niagar
SF:a-Admin\",\x20qop=\"auth\",\x20algorithm=\"MD5\",\x20nonce=\"To/JOWQ3NG
SF:JkOTY4ZTgzNDY3NmVlZjk2ZjUzYWMxN2M0YTcz\"\r\nContent-Length:\x2056\r\nCo
SF:ntent-Type:\x20text/html\r\nNiagara-Platform:\x20QNX\r\nNiagara-Started
SF::\x202011-6-20-10-2-29\r\nBaja-Station-Brand:\x20JENEsys\r\nNiagara-Hos
SF:tId:\x20Qnx-NPM2-0000-0E56-6AB9\r\nServer:\x20Niagara\x20Web\x20Server/
SF:3\.0\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</h
SF:tml>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|printer|WAP|general purpose|webcam
Running (JUST GUESSING): Nortel embedded (94%), Konica Minolta embedded (92%), Netgear embedded (88%), ReactOS 0.3.X (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (94%), Konica Minolta bizhub C450 printer with optional Fiery Controller (92%), Netgear DG834G WAP (88%), ReactOS 0.3.7 (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.217
Host is up (0.050s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RV_3\"\r\nContent-Length:\x2056\r\nContent-T
SF:ype:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:
SF:\x202\r\nNiagara-HostId:\x20J501-77EF-DD77\r\nServer:\x20Niagara\x20Web
SF:\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n<
SF:/body>\n</html>")%r(HTTPOptions,11F,"HTTP/1\.0\x20401\x20Unauthorized\r
SF:\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_3\"\r\nContent-Length:
SF:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r
SF:\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-77EF-DD77\r\nServer
SF::\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20U
SF:nauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,11F,"RTSP/1\.0\x2040
SF:1\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV_3\"
SF:\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Plat

SF:form:\x20JACE_50x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-
SF:77EF-DD77\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<b
SF:ody>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourReq
SF:uest,11F,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basi
SF:c\x20realm=\"Admin-RV_3\"\r\nContent-Length:\x2056\r\nContent-Type:\x20
SF:text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\x202\r\
SF:nNiagara-HostId:\x20J501-77EF-DD77\r\nServer:\x20Niagara\x20Web\x20Serv
SF:er/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n
SF:</html>")%r(SIPOptions,11E,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Auth
SF:enticate:\x20Basic\x20realm=\"Admin-RV_3\"\r\nContent-Length:\x2056\r\n
SF:Content-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad
SF:-version:\x202\r\nNiagara-HostId:\x20J501-77EF-DD77\r\nServer:\x20Niaga
SF:ra\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorize
SF:d</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|printer|WAP|general purpose|webcam
Running (JUST GUESSING): Nortel embedded (94%), Konica Minolta embedded (92%), Netgear embedded (88%), ReactOS 0.3.X (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (94%), Konica Minolta bizhub C450 printer with optional Fiery Controller (92%), Netgear DG834G WAP (88%), ReactOS 0.3.7 (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.218
Host is up (0.046s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD2C%P=i686-pc-windows-windows%
SF:r(GetRequest,11E,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-RV4\"\r\nContent-Length:\x2056\r\nContent-Ty
SF:pe:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\
SF:x202\r\nNiagara-HostId:\x20J501-71E3-DC71\r\nServer:\x20Niagara\x20Web\
SF:x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</
SF:body>\n</html>")%r(HTTPOptions,11E,"HTTP/1\.0\x20401\x20Unauthorized\r\
SF:nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV4\"\r\nContent-Length:\x
SF:2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\n
SF:niagarad-version:\x202\r\nNiagara-HostId:\x20J501-71E3-DC71\r\nServer:\
SF:x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Una

SF:uthorized</h1>\n</body>\n</html>")%r(RTSPRequest,11E,"RTSP/1\.0\x20401\
SF:x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-RV4\"\r\
SF:nContent-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platfor
SF:m:\x20JACE_50x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J501-71E
SF:3-DC71\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body
SF:>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(FourOhFourReques
SF:t,11E,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x
SF:20realm=\"Admin-RV4\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text
SF:/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-version:\x202\r\nNia
SF:gara-HostId:\x20J501-71E3-DC71\r\nServer:\x20Niagara\x20Web\x20Server/1
SF:\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</ht
SF:ml>")%r(SIPOptions,11D,"SIP/2\.0\x20401\x20Unauthorized\r\nWWW-Authenti
SF:cate:\x20Basic\x20realm=\"Admin-RV4\"\r\nContent-Length:\x2056\r\nConte
SF:nt-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_50x\r\nniagarad-vers
SF:ion:\x202\r\nNiagara-HostId:\x20J501-71E3-DC71\r\nServer:\x20Niagara\x2
SF:0Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1
SF:>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|printer|WAP|general purpose|webcam
Running (JUST GUESSING): Nortel embedded (94%), Konica Minolta embedded (92%), Netgear embedded (88%), ReactOS 0.3.X (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (94%), Konica Minolta bizhub C450 printer with optional Fiery Controller (92%), Netgear DG834G WAP (88%), ReactOS 0.3.7 (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.219
Host is up (0.051s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD30%P=i686-pc-windows-windows%
SF:r(GetRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-REGISALC2\"\r\nContent-Length:\x2056\r\nCont
SF:ent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-ver
SF:sion:\x202\r\nNiagara-HostId:\x20J511-AD5B-EBAD\r\nServer:\x20Niagara\x
SF:20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h
SF:1>\n</body>\n</html>")%r(HTTPOptions,124,"HTTP/1\.0\x20401\x20Unauthori
SF:zed\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-REGISALC2\"\r\nConte

SF:nt-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20
SF:JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J511-AD5B-EBAD
SF:\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1
SF:>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,124,"RTSP/
SF:1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Ad
SF:min-REGISALC2\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\
SF:r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-H
SF:ostId:\x20J511-AD5B-EBAD\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\
SF:n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%
SF:r(FourOhFourRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authen
SF:ticate:\x20Basic\x20realm=\"Admin-REGISALC2\"\r\nContent-Length:\x2056\
SF:r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniaga
SF:rad-version:\x202\r\nNiagara-HostId:\x20J511-AD5B-EBAD\r\nServer:\x20Ni
SF:agara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthor
SF:ized</h1>\n</body>\n</html>")%r(SIPOptions,123,"SIP/2\.0\x20401\x20Unau
SF:thorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-REGISALC2\"\r\n
SF:Content-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform
SF::\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J511-AD5B
SF:-EBAD\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>
SF:\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

Nmap scan report for aaa.bbb.ccc.220
Host is up (0.054s latency).
Not shown: 65533 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http Sun Niagara httpd 1.1 (Niagara release 2.301.522.v1)
3011/tcp open sip Niagara Web Server/1.1 (Status: 401 Unauthorized)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port3011-TCP:V=5.51%I=7%D=10/7%Time=4E8FBD32%P=i686-pc-windows-windows%
SF:r(GetRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"Admin-J512-8894\"\r\nContent-Length:\x2056\r\nCont
SF:ent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-ver

SF:sion:\x202\r\nNiagara-HostId:\x20J512-9327-E493\r\nServer:\x20Niagara\x
SF:20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h
SF:1>\n</body>\n</html>")%r(HTTPOptions,124,"HTTP/1\.0\x20401\x20Unauthori
SF:zed\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J512-8894\"\r\nConte
SF:nt-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20
SF:JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J512-9327-E493
SF:\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1
SF:>401:\x20Unauthorized</h1>\n</body>\n</html>")%r(RTSPRequest,124,"RTSP/
SF:1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Ad
SF:min-J512-8894\"\r\nContent-Length:\x2056\r\nContent-Type:\x20text/html\
SF:r\nNiagara-Platform:\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-H
SF:ostId:\x20J512-9327-E493\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\
SF:n\r\n<html>\n<body>\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>")%
SF:r(FourOhFourRequest,124,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authen
SF:ticate:\x20Basic\x20realm=\"Admin-J512-8894\"\r\nContent-Length:\x2056\
SF:r\nContent-Type:\x20text/html\r\nNiagara-Platform:\x20JACE_51x\r\nniaga
SF:rad-version:\x202\r\nNiagara-HostId:\x20J512-9327-E493\r\nServer:\x20Ni
SF:agara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>\n<h1>401:\x20Unauthor
SF:ized</h1>\n</body>\n</html>")%r(SIPOptions,123,"SIP/2\.0\x20401\x20Unau
SF:thorized\r\nWWW-Authenticate:\x20Basic\x20realm=\"Admin-J512-8894\"\r\n
SF:Content-Length:\x2056\r\nContent-Type:\x20text/html\r\nNiagara-Platform
SF::\x20JACE_51x\r\nniagarad-version:\x202\r\nNiagara-HostId:\x20J512-9327
SF:-E493\r\nServer:\x20Niagara\x20Web\x20Server/1\.1\r\n\r\n<html>\n<body>
SF:\n<h1>401:\x20Unauthorized</h1>\n</body>\n</html>");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch|WAP|printer|webcam|general purpose|media device
Running (JUST GUESSING): Nortel embedded (89%), Netgear embedded (88%), Konica Minolta embedded (87%), Enterasys embedded (87%), Asus Linux 2.6.X (86%), AXIS Linux 2.6.X (86%), Linux 2.6.X|2.1.X (86%)
Aggressive OS guesses: Nortel DMS-10 telephony switch (89%), Netgear DG834G WAP (88%), Konica Minolta bizhub C450 printer with optional Fiery Controller (87%), Enterasys Matrix N7 switch (87%), Asus RT-N16 WAP (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6) (86%), AXIS 211A Network Camera (Linux 2.6.20) (86%), Linux 2.6.24 (86%), TiVo series 1 (Linux 2.1.24-TiVo-2.5) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 11 hops

Nmap scan report for aaa.bbb.ccc.222
Host is up (0.049s latency).
Not shown: 65529 closed ports
PORT STATE SERVICE VERSION
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm

139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: broadband router|router|switch|WAP
Running: Cisco embedded, Cisco IOS 12.X|15.X
OS details: Cisco 827H ADSL router, Cisco 870 router or 2960 switch (IOS 12.2 - 12.4), Cisco Aironet 1250 WAP (IOS 12.4), Cisco C7200 router (IOS 15)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 89 IP addresses (89 hosts up) scanned in 15409.94 seconds