Summer 2011

Uncovering Network Perimeter Vulnerabilities in Cisco Routers According to Requirements Defined in Pci Dss 2.0

David E. Naples
Regis University

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

Disclaimer

UNCOVERING NETWORK PERIMETER VULNERABILITIES IN CISCO ROUTERS ACCORDING TO REQUIREMENTS DEFINED IN PCI DSS 2.0

A THESIS SUBMITTED ON 7 OF

JUNE, 2011

TO THE DEPARTMENT OF INFORMATION TECHNOLOGY

OF THE SCHOOL OF COMPUTER & INFORMATION

SCIENCES OF REGIS UNIVERSITY

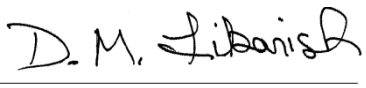
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF

SCIENCE IN INFORMATION ASSURANCE

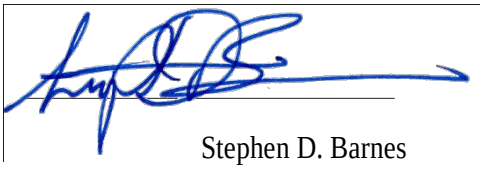
BY

David E. Naples

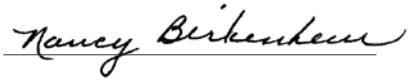
APPROVALS



Dan Likarish, Thesis Advisor



Stephen D. Barnes



Nancy Birkenheuer

Abstract

According to the Payment Card Industry (PCI), over 500 million records containing sensitive cardholder data have been breached since January 2005. Merchants accepting credit and debit cards are at the center of payment card transactions, making it crucial that standard security procedures and technologies are employed to thwart cardholder data theft. Numerous organizations have experienced embarrassing breaches, which lead to losses of credit card data, including Starbucks, California Pizza Kitchen, and TJX Companies. This paper examined an action research methodology to test the security of a network router and remediate all the vulnerabilities that caused it to fail the requirements of the Payment Card Industry Data Security Standards (PCI DSS). The basic functions of a router include packet forwarding, sharing routing information with adjacent routers, packet filtering, network address translation (NAT), and encrypting or decrypting packets. Since a router is traditionally installed at the perimeter of a network, it plays an important role in network security. By following the approach of this study, administrators should understand how employing a network vulnerability scanner to test a host can illuminate hidden security risks. This study also demonstrated how to use the results of the vulnerability scan to harden a host to ensure it complied with the Payment Card Industry's (PCI DSS) requirements.

Table of Contents

List of Figures

Chapter 1 – Introduction

Protecting cardholder data is definitely a serious concern for many merchants. Over 510 million records containing sensitive cardholder data have been compromised in the past six years (PCI Security Standards Council, 2010). This problem can be greatly attributed to insufficient security measures employed by a number of merchants. One only needs to consider the large amount of data stored by businesses in order to understand the importance of maintaining effective security solutions when handling cardholder data. According to a Forrester Consulting survey (as cited in PCI Security Standards Council, 2010), 81% of businesses polled store payment card numbers, 73% store payment card expiration dates, 71% store payment card verification codes, 57% store customer data from the payment card magnetic stripe, and 16% store other personal data. Sustained compliance with the Payment Card Industry Data Security Standards (PCI DSS) will help alleviate many of the vulnerabilities found in today's networks and will, in effect, reduce risks to sensitive cardholder information.

The Payment Card Industry Data Security Standards necessitate that merchants follow a set of documented requirements when configuring network devices used with card processing activities. Several examples of the PCI DSS requirements include specifications on firewall implementation parameters at the network perimeter, as well as the creation of a demilitarized zone (DMZ); implementing a single function per server; disabling unnecessary and insecure services, ports, and protocols; and configuring security according to the organization's business requirements and best practices. The best practice of changing any vendor-supplied default passwords or accounts before installing a host on the network is also a PCI DSS requirement. In addition, PCI DSS demands secure administrative access to all network devices. This standard can be met by implementing secure shell (SSH) for a protected command line interface or

HTTPS to secure the Web interface on network hosts. PCI DSS requires all firewalls to implement stateful packet inspection to meet compliance. Another PCI DSS requirement, and one that is often overlooked by administrators, is the use of RFC 1918 private Internet Protocol (IP) addresses on the internal network (Chapple, 2010).

Regular security testing of network components and processes is required since malicious attackers are extremely persistent at discovering new host vulnerabilities. To compound this problem, new software and updates to existing software oftentimes introduce additional vulnerabilities. Regular network vulnerability testing is a highly effective method of locating new vulnerabilities introduced by hardware and software changes. Network components, processes, and newly added applications should be tested on a frequent basis to ensure new weaknesses have not been introduced into the network. PCI DSS requires a scanning frequency of at least once per quarter to discover the presence of wireless access points and rogue wireless devices. Quarterly scans are also required for discovery of internal and external network vulnerabilities. In addition, these vulnerability scans must be completed any time significant network changes are made. An organization must pass four consecutive scans to attain PCI DSS compliance and PCI DSS requires that the quarterly external scans are performed only by an Approved Scanning Vendor (ASV). Vulnerability scans are considered passing if no high-level vulnerabilities are discovered in any section of the cardholder data environment. An organization is considered compliant only if no components contain vulnerabilities with a National Institute of Standards and Technology (NIST) assigned Common Vulnerability Scoring System (CVSS) base score that is equal to or greater than 4.0 (PCI Security Standards Council, 2010).

PCI DSS defines several steps to help organizations meet their established requirements. The first recommended step is to fully assess the network and all information resources for

vulnerabilities. Next, the vulnerabilities found during the assessment that may permit unauthorized access to sensitive cardholder data must be remediated. As a final step, the organization must report compliance to PCI DSS and show evidence that controls to protect cardholder data are in place (PCI Security Standards Council, 2010).

This study followed an action research approach to conduct the PCI DSS required external vulnerability scan on one example network device, a Cisco router. A router was chosen for this study because routers are typically installed at the perimeter of a network, controlling access to and from each network, making them susceptible to all sorts of attacks from external networks. Since routers are the first device on a network that packets traverse, they can become easy targets of attack if proper steps are not followed to secure them. Hardening network devices, such as routers, is not a complicated task, but it is a task that is frequently disregarded by administrators (Northcutt, et al., 2003). To help make routers more resistant to attacks, Roland (2004) suggested that router administrators should, at a minimum, lock down insecure management access to all routers, use a secure version of Simple Network Management Protocol (SNMP), use a central server to control access to router management, turn off unnecessary services, enable logging, and authenticate routing table updates.

The vulnerability assessment conducted for this study was performed by initiating scans using the QualysGuard PCI scanning tool. The QualysGuard PCI tool is a commercially available vulnerability scanning application that provides a cost-effective, automated method to scan network hosts for vulnerabilities. QualysGuard PCI was chosen for this study because of its thoroughness in testing hosts for vulnerabilities, its ability to create easy-to-understand results and reports, and because it was made available for use in this study. The QualysGuard tool was used to test a Cisco 2800 series router for vulnerabilities as defined by the requirements of PCI

DSS version 2.0. The report produced by QualysGuard PCI was reviewed for any vulnerabilities that had a CVSS rating of 4.0 and higher. Research was conducted on each of these vulnerabilities to find solutions that would potentially remediate the vulnerabilities in the report. The recommended solutions were applied to the device, and then the device was scanned once again using the same standards as the initial scan. This process was repeated until the Cisco router's vulnerabilities were reduced to an acceptable level to meet PCI DSS compliance. Several of the questions this study attempted to answer include: How can administrators test network devices for PCI DSS compliance? What makes a network component PCI DSS compliant? What are some of the vulnerabilities PCI DSS will look for in a device? What is an example of how vulnerabilities can be properly remediated on a network host in order to achieve PCI DSS compliance? What is an example process that security professionals can follow to make a device PCI DSS compliant?

Chapter 2 – Review of Literature

According to the Payment Card Industry (PCI), over 500 million records containing sensitive cardholder data have been breached since January 2005. Merchants accepting credit and debit cards are at the center of payment card transactions, making it crucial that standard security procedures and technologies are employed to thwart cardholder data theft. Vulnerabilities can typically present themselves anywhere in the payment card processing system (PCI Security Standards Council, 2010) and can be especially dangerous when multiple vulnerabilities are present in the Internet-facing (perimeter) routers.

This paper will look at using an action research methodology to test the security of a network router and remediate all the vulnerabilities that cause it to fail the requirements of the Payment Card Industry Data Security Standards (PCI DSS). A Cisco router, configured with a standard setup that does not take security or hardening into consideration, will be employed for testing. The router will first undergo a thorough scan according to the requirements of PCI and the vulnerabilities will be noted. Each vulnerability will be researched for a resolution, the resolution shall be applied, and the router scanned once again to ensure it complies with the PCI standards.

What is PCI DSS?

Attackers often target credit card information due to the profits an attacker can reap on the black market. Card companies quickly realized that the threats to their payment systems were on the rise and they needed to do something to lessen the potential risks. The major card companies decided to come together to form the Payment Card Industry Data Security Standards (PCI DSS). As described by Chuvakin and Williams (2010), PCI is not a legal requirement like other requirements, such as HIPAA or Sarbanes-Oxley, that can impose penalties backed by a

law enforcing agency. However PCI may be even more effective in other ways. For instance, noncompliance with PCI can lead to financial fines or even having the merchant status revoked, effectively stopping the organization from being able to accept any payment cards. The loss of the ability to process credit card payments could have a drastic effect on some organizations, possibly leading to the failure of the business entirely (Chuvakin & Williams, 2010).

The Payment Card Industry Data Security Standards (PCI DSS) consists of twelve common sense steps that mirror security best-practices. The PCI standards include both technical and operational requirements designed to help protect cardholder data. PCI standards apply to all organizations that store, process, or transmit cardholder data. In other words, any organization or retailer performing any of the above functions is required to comply with PCI DSS (PCI Security Standards Council, 2010). As Chuvakin and Williams (2010) stated, **"**The scope of PCI DSS affects almost every business, from the largest retail megastores down to a self-employed single mother working from her home computer. If the business accepts, processes, transmits, or in any other way handles credit card transactions, they must comply with PCI DSS."

The Importance of Compliance

Compliance with PCI is not an easy task, both for large organizations and small organizations alike. The time and monetary resources required to comply with PCI can make compliance difficult for smaller organizations. Large organizations may experience difficulty due to their sheer size and complexity. However, non-compliance can lead to the organization paying fines and even a loss of credit card processing rights, according to Sophos (n.d.). The loss of customer financial data can lead to undesirable press releases, a loss of consumer confidence, and a loss of business. Sophos (n.d.) added that there are many examples of large organizations that have experienced such negative impacts, such as Starbucks, California Pizza Kitchen, and 7-

Eleven. Sophos (2008) also discussed the example of how the auto parts retailer, Advance Auto Parts, fell victim to an attack in which hackers accessed financial information for 56,000 customers in 14 stores covering 7 different states.

According to Ciampa (2009), another embarrassing incident in which customer data was compromised involved TJX Companies, Inc. TJX is the retailer that owns T. J. Maxx, Marshalls, HomeGoods, A. J. Wright, and HomeSense stores. Ciampa (2009) stated how hackers broke the Wired Equivalent Privacy (WEP) encryption that a particular store was using and proceeded to steal cardholder data over a period of 18 months. Once the breach was discovered, it was estimated that the attackers stole data on 45.6 million credit and debit cards. Several lawsuits were initiated against TJX, including a class-action suit by the customers. By the time TJX settles this breach with all parties, the cost is expected to surpass $1 billion. Adding to the list of data breaches is the incident concerning CardSystems in June 2005, where 40 million individual records were exposed by hackers. The organizations involved in loss of cardholder data also includes DSW Retail in 2005, The U.S. Department of Veterans' Affairs in 2006, and Heartland Payment Systems in 2009 (Chuvakin & Williams, 2010).

If an organization is unsure whether or not it should comply with the regulations established by PCI, Sophos (n.d.) recommended that businesses ask themselves the following questions: To what extent would business be affected if customer data was lost or stolen? What would the impact to business be if Visa, MasterCard, etc. revoked authorization to accept and process credit cards? How would non-compliance with PCI affect the overall business? According to Sophos (2010), the reputation of a business and its credibility are only as good as the processes, precautions, and protective solutions it put in place to guard sensitive data.

As suggested by the Payment Card Industry Security Standards Council (PCI SSC) (n.d.), compliance may not be as difficult as some organizations think. PCI SSC (n.d.) noted that compliance can bring major benefits to businesses, while a failure to comply can come with several serious, long-term consequences. Several benefits that compliance can provide include a better reputation with acquirers and payment brands, better customer confidence, and the prevention of security breaches and loss of payment card data. Compliance with PCI may even improve compliance with other regulations, such as HIPAA and SOX. PCI SSC (n.d.) also described several of the negative effects organizations may experience through non-compliance as lawsuits, insurance claims, cancelled accounts, payment card issuer fines, and government fines. According to PCI SSC (n.d.), compromised data may affect consumers, merchants, as well as financial institutions. One incident can severely impact an organization's reputation and ability to continue business as usual.

The Importance of Routers in Security Architecture

According to Northcutt, Zeltser, Winters, Frederick, & Ritchey (2003), routers are used to connect two or more networks together and many times one of those networks is the public Internet. Because routers face the Internet, they are at the frontline of a network's defense and should be the focal point of the network's security. Hardening routers is of utmost importance since they are placed in a vulnerable position. Northcutt, et al. (2003) recommended disabling all unnecessary services, blocking all unneeded traffic types, locking down router management methods, and monitoring the traffic that travels through a router in order to properly harden these devices.

According to Wilhelm (2009), router attacks are the most common form of attacks in network penetration tests. This is due to a router's physical and logical location in a network

design and the potential gains an attacker could experience if a router is exploited. Vladimirov, Gavrilenko, Vizulis, and Mikhailovsky (2006) noted that once an attacker controls a router, he or she controls the entire network. Vladimirov, et al. (2006) suggested that an attacker would then have the ability to control all traffic on the network and could perform any of the following actions:

- Completely map the network
- Forward any type of traffic to hosts on the network under control
- Sniff and modify any or all traffic passing through the router
- Force traffic that would not normally flow through the router to pass through it
- Establish an encrypted backdoor to the network
- Attack other networks from or through the router
- Cause connectivity problems on the attacked network that are very difficult to troubleshoot

The seriousness of the attacker's actions as described above shows how vital it is to ensure routers are properly hardened when installed on any network.

Routers are normally configured with access control lists (ACLs) to filter specific packets from entering the network. Paquet (2009) noted that routers implemented at the network perimeter and configured with traffic filtering ACLs are performing as an integral part of an overall defense-in-depth approach to network security rather than being the sole provider of perimeter security. This effectively establishes their importance and position in most any security architecture. According to Northcutt, et al. (2003), a best practice is to allow a router to concentrate on what it is good at (such as routing and packet filtering) and not require it to do ancillary tasks. As part of a defense-in-depth approach, a router should not include the roles of a

stateful firewall, an intrusion detection system, etc. However, as Northcutt, et al. (2003) asserted, packet filtering at the router level makes excellent sense since routers can perform this function quickly and easily.

As previously mentioned, routers are located at the perimeter of the network and provide the initial layer of network defense. If an attacker exploits the router, then that attacker takes one step closer to the critical systems of the organization. Convery (2004) described many of the weaknesses inherent in routers and current router technology. As Convery noted, the number of attacks targeting routers has been on the rise. Convery suggested that administrators take the necessary steps to properly harden routers by disabling unneeded services and ensuring passwords are encrypted. Paquet (2009) reinforced Convery's assertion and also pointed out that many extraneous services are enabled on routers by default or unnecessarily by administrators. It is imperative that specific configuration changes are be made to routers, especially when deployed at the perimeter, to improve security (Paquet, 2009).

As Pacquet (2009) mentioned, a router's operating system is not that much different from that of a computer. Routers have numerous services enabled by default just as with their computer counterparts. A large number of those services are unnecessary and can be exploited by attackers to gather information or launch a router exploitation attack. Pacquet (2009), as well as Arregoces and Portolani (2004), asserted that all unnecessary services should be disabled in order to harden a router's operating system. Arregoces and Portolani (2004) also went on to show the exact commands that can be implemented in Cisco routers to disable unnecessary services. Hucaby, McQuerry and Whitaker (2010) described the unnecessary services on Cisco routers as well as a description of their inherent weaknesses. According to Hucaby, McQuerry and Whitaker (2010), these unnecessary services can leave a router vulnerable to numerous

attacks and should almost always be disabled at the global level, the interface level, or both. According to Cisco Systems (2003), many router services are known by attackers and are commonly exploited. Cisco (2003) recommended that administrators keep in mind the important task of disabling unused and commonly exploited router services. Cisco (2003) also provided a list of the vulnerable services, along with a number of commands to properly execute the necessary configuration changes (Cisco Systems, 2003).

PCI Requirements and Testing

PCI realizes that routers are an integral part of most all networks and recognizes the importance of their role in network and security architectures. In response to this understanding, PCI has developed requirement 11.2 to specify that all Internet-facing devices must be scanned from an external source on a quarterly basis to expose any security vulnerabilities. Additionally, if any significant network changes are made, PCI requirement 11.2 also requires an external scan of the same network to ensure all components affected by the modifications continue to meet PCI guidelines. Requirement 11.2.1.b specifies that the network must be rescanned until passing results are obtained if the network did not pass on the first scan. PCI requires that only an Approved Scanning Vendor (ASV) is permitted to perform the quarterly scans, otherwise the results are not valid (PCI DSS, 2010).

PCI requires administrators to change all vendor-supplied default passwords before installing any equipment on the network (PCI DSS, 2010). This requirement follows industry best-practices and is confirmed by Donahue and Swan (2007). Donahue and Swan suggested changing the password, adjusting minimum password-length settings as well as storing passwords using a one-way hash, such as Message Digest 5 (MD5). To show the extent of the vulnerability of using default passwords, Basta and Halton (2008) pointed out that the default

password set by many router vendors are very simple. Basta and Halton (2008) showed that even some of the larger router manufacturers configure new devices with easily guessed default passwords, such as "*cisco*", "*admin*", or "*password*".

According to PCI DSS (2010), malicious individuals use default passwords, along with other vendor supplied information, to help compromise network devices since the passwords and settings are easily obtained and well-known in hacker communities. In fact, Northcutt (2007) mentioned that an even bigger issue concerns worms that are capable of automatically propagating and searching systems for default usernames and passwords. Northcutt (2007) also noted that many administrators believe default usernames and passwords are not generally known. However, this is not always the case. One Website contains hundreds of device models from different vendors, showing not only the usernames and passwords, but also the level and method of access (CIRT, 2010).

The Importance of PCI

Basta and Halton (2008) asserted that the sheer complexity of router configurations can have a positive or negative effect on router vulnerability. Hackers are able to perform many different attacks on routers even if they cannot gain physical access to them. Adding protection to one area of a router can inadvertently open another area to attack. By following the common sense steps outlined in the PCI standards, organizations can ensure they are following security best-practices as well as maintaining compliance with PCI DSS (PCI Security Standards Council, 2010).

PCI remains relevant to the field of security since it is periodically updated as networks and the payment card landscape progress. The latest version of PCI, version 2.0, was recently released in October 2010 to incorporate additional requirements and modifications to existing

requirements. According to Hoelzer (2010), the PCI standard has evolved into an effective approach for protecting the handling and processing of card transactions. Hoelzer (2010) also showed that PCI is doing a good job at keeping up with technological changes with the recent adjustments to the requirements.

The Action Research Approach

This project will use an action research methodology to examine the multiple facets of this project. The main reason for this approach is, as Avison, Lau, Myers, and Nielsen (1999) explained, action research emphasizes what practitioners do more than what they say. That idea applies to this research project because the research will attempt to prove that vulnerabilities will be found in a sample router and that, through specific actions, the discovered vulnerabilities will be remediated.

Avison, et al. also discussed how action research is an iterative process that involves problem diagnosis, action intervention, and reflective learning. According to Avison, et al., the researcher investigates a theory in an actual real-world situation (in our case, on a Cisco router), obtain feedback from the experiment (the results from the vulnerability scans), modify the theory according to the feedback (make modifications to the router's configuration to remediate the vulnerabilities discovered by the scan) and repeat the process. The iterative part of this process includes performing the above actions as many times as necessary. This is done to reduce the router vulnerabilities to a level that allows the router to pass a subsequent vulnerability scan that compares the state of the device with the requirements established by PCI.

All steps will be documented and thoroughly explained so the experiment can be duplicated on most any Cisco router. Upon project completion, the results should provide a

comprehensive guideline for any network or security administrator to apply toward a given network to enhance the security of its network components.

Chapter 3 – Methodology

Action Research

This study was conducted according to an action research methodology. The study tested the security of a network router by scanning it for security vulnerabilities. Next, all vulnerabilities that caused it to fail when measured against the requirements of the Payment Card Industry Data Security Standards (PCI DSS) were remediated. A Cisco router, configured with a conventional configuration that did not take security or device hardening into consideration, was employed for the subject of this study. The router was placed on a test network, then thoroughly tested for vulnerabilities according to the requirements developed by PCI DSS. All vulnerabilities discovered by the scan were thoroughly documented and described in the results of this study. Each vulnerability was also researched for a resolution and the corresponding recommended resolutions were applied to the test router. Once all router configuration changes were applied, the router was subject to an identical scan to determine if each vulnerability was indeed remediated and that it complied with the PCI standards. It is feasible to assume that the results from this initial iteration could have resulted in a satisfactory conclusion (Järvinen, 2007). However, in the case of this study, additional research and intervention were necessary to fully harden the test router.

Place

The router under test was located on the primary network at the commercial location of The Company in Houston, Texas. The router was physically mounted in an existing 19” equipment rack and connected to an existing Cisco 3560 switch. Access to test and manage the router was provided by the existing network infrastructure. Router management access was

available through the console port, direct network connection, and through VPN access to the host network. The network equipment was located in an access-restricted server room within a secure office environment to ensure physical security of the testing equipment.

Participants

Since the study was based upon the use of one hardware component and several software applications, hardware set up was minimized, allowing it to be entirely researched by the primary researcher. I was the main participant in this study from creation of the proposal, to designing the artifact, performing the tests, and researching and interpreting the test results (Vaishnavi & Kuechler, 2004/5). Intermittent assistance was provided by The Company's senior network engineer to help determine where to physically locate the router, as well as which switch and switch port to connect to the router. The senior network engineer also provided a reserved IP address on the host network to apply to the test router.

Materials

The materials needed for the project consisted of both hardware and software. Hardware requirements were very minimal because only one network component was tested and all supporting network infrastructure was already in place. The existing equipment included the server room, the 19" equipment rack, power, cooling, lighting, cabling, and the network switch. A laptop with network and Internet access was required for connecting to the Qualys Website for running the test scans, configuring the router, storing and interpreting the results, and researching solutions to problems discovered on the router. The laptop was manufactured by HP and used Windows 7 Professional as its operating system. This laptop did not contain any serial ports, so a USB-to-serial adapter was required for console access in order to perform the initial configuration set up.

The test router selected for this study was a Cisco 2800 Series router running Cisco IOS version 12.4(3e). It was determined that this router was fairly representative of that found in a small business or small branch office. The router contained a typical configuration used to perform the normal routing functions for an organization, running standard services and protocols that would normally be found on a router not configured with security as a top priority. As this router represented one that has been in service for several years within a typical organization, unused services and unnecessary ports were found to have been left open and running by previous administrators. The Cisco 2800 series router only required one rack unit of space in a standard 19" network equipment/server rack. Power was provided by the power outlets mounted in the rack in which the router was installed. A single Ethernet port was made available on a Cisco 3560 switch in which the router's Gigabit Ethernet port G0/0 was connected in order to provide network connectivity. A standard Ethernet category 5E cable was used to connect from the test router to the Cisco 3560 switch and a normal Cisco rollover type, RJ-45 to DB-9 console cable was used for console port access.

The test router employed a static default route through the Gigabit Ethernet 0/0 (G0/0) port to accomplish the routing function rather than configuring a more complex interior gateway protocol (IGP), such as Open Shortest Path First (OSPF), Router Information Protocol (RIP), or Enhanced Interior Gateway Routing Protocol (EIGRP). This configuration helped simplify the test set up since the test network consisted of only a single device connected to the host network. This configuration was also preferred because it is more representative of a router in a small office or small branch office location that may only have one route to access an outside network or the Internet. In addition, a static route used in situations such as this is a much more efficient method of routing compared to using one of the routing protocols described above (Teare, 2008).

The primary software application utilized to complete this project was the *QualysGuard IT Security and Compliance* suite of software. QualysGuard is an on-demand web application that uses a Software-as-a-Service (SaaS) approach to provide organizations with a cost-effective, automated method of scanning network assets for vulnerabilities. QualysGuard contains several useful components in its suite of applications, including vulnerability management, policy compliance, Web application scanning, PCI compliance, and malware detection. The element from QualysGuard's assortment of products employed for this study was the *QualysGuard PCI Compliance* component. QualysGuard designed this tool to provide businesses, online merchants, and Member Service Providers an effective method of achieving compliance with the Payment Card Industry Data Security Standard (PCI DSS). QualysGuard PCI is used to conduct network and web application security scans to help organizations identify security vulnerabilities in its network assets (Qualys, n.d.) and it was used in the study for that exact purpose. QualysGuard PCI effectively discovered all vulnerabilities in the project's test router that violated the current standards established by PCI DSS.

Access to the commercially available QualysGuard PCI product was made possible through the researcher's employment with The Company. The Company maintains a licensed corporate account with QualysGuard, allowing authorized members to scan a certain range of IP addresses on the network. The Company also maintains a licensed Qualys scanning device that is located on the internal corporate network. This hardware device permits the scanning of internal network hosts with a private IP address, as in the case of the study's test router. RFC 1918 defines private IP addresses as those addresses that are designed to be used only on an internal network. Private IP addresses cannot be routed outside a private network onto the public Internet. The address space reserved for private addresses are listed below:

- 10.0.0.0 to 10.255.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255 (Teare, 2008)

The network used for this project employed the private address range of 172.16.0.0/16. The private IP address assigned to the test router was 172.16.0.32. This meant that in order to scan the test router with QualysGuard PCI, we needed to use the internal scanning device rather than the main QualysGuard scanning servers. This is because the main scanning services originate from servers on the QualysGuard network and are assigned and attached to the public IP address space. The QualysGuard hosted servers can only communicate with and scan publically addressed hosts. To further clarify the point, the QualysGuard external scanners are located in the following public address space:

- 64.39.96.1to 64.39.111.254
- 62.210.136.129 to 62.210.136.254
- 167.216.252.1to 167.216.252.62 (QualysGuard, n.d.)

Since the test router was installed on a private network, it could not be reached from any publically addressed host. Therefore, the internal scanning device was the only option available for performing the vulnerability scans on the test router.

Procedure

The research utilized QualysGuard PCI to scan the test router and generate a report that displayed all the vulnerabilities discovered during the scan. QualysGuard PCI also supplied a score that showed the severity level assigned to each of the vulnerabilities and whether or not the device under test passed or failed the scan according to the Payment Card Industry's standards.

Since the router was not initially configured as a secure, hardened network component, it was expected that vulnerabilities would be found and that it would not meet PCI requirements on its preliminary scan. The initial scan results did, in fact, indicate that the test router was not yet properly hardened. Research was conducted on each of the vulnerabilities to locate potential solutions. Research indicated that the possible fixes included software updates, patches, configuration changes, etc. to remediate the vulnerabilities. Upon discovery of potential resolutions for each specific vulnerability, changes to the software or the configuration were made to eliminate each weakness that was detailed in the QualysGuard PCI scan report. The final solutions included shutting down services, modifying services, closing particular TCP or UDP ports, software updates, and changing passwords.

The research report provided full descriptions of the vulnerabilities discovered by the scan in order to describe to the reader the inherent problems with each vulnerability. Additionally, when available, the documentation also included a description of why the vulnerabilities were severe enough to require action to be taken, along with the prospective problems they could lead to if left unattended. This information should help the research reader understand why the actions taken to harden the router were necessary for such a device that is installed in a production network and required to follow PCI DSS requirements.

Chapter 4 – Background, Analysis, and Results

Background

PCI DSS requirements.

The PCI DSS requirements include many facets of securing a network. For example, requirement 1 sets the guidelines for establishing router and firewall configuration standards. This requirement defines implementing a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network. Requirement 1 sets the constraints for restricting inbound and outbound traffic, perimeter firewalls between wireless networks and the cardholder data, the prohibition of public access to any network area containing cardholder data, the use of stateful inspection, the non-disclosure of private IP addresses and routing information, among other requirements (PCI DSS, 2010).

PCI DSS requirement 2 necessitates changing vendor-supplied defaults on all systems attached to the network. This includes vendor-supplied accounts and passwords, SNMP community strings, and unused accounts. Requirement 2 also defines the requirements pertaining to the implementation of security features for any necessary services and protocols. For example, this requirement establishes the use of secure services such as SSH, S-FTP, SSL, and IPSec rather than using the insecure services of Telnet, FTP, etc. (PCI DSS, 2010).

Requirement 6 states that organizations must ensure all system components and software are protected from vulnerabilities through a process of applying the latest vendor security patches. This requirement also defines the necessity of developing secure software applications. All applications must be developed according to the PCI DSS standards and based on industry best practices. Requirement 6 requires that software applications are developed to be resistant to

such attacks as injection flaws, buffer overflows, cross-site scripting (XSS), and cross-site request forgery (CSRF) (PCI DSS, 2010).

The PCI DSS requirements involve every device on a network. In addition to defining requirements for hardware, PCI DSS also includes requirements pertaining to design, processes, access control, as well as software applications. However, since routers are at the forefront of a network, they are more at risk of attack than most other devices. For this reason, routers must be thoroughly tested for vulnerabilities, regularly updated and properly hardened to resist attacks.

Discussion on Routers.

The role of a router.

A router functions at the OSI (Open Systems Interconnection) network layer to direct the flow of network packets using headers and routing tables to determine the direction each packet should be sent. Specific protocols are used for communications and for selecting the best path between hosts or networks. The basic functions of a router include packet forwarding, sharing routing information with adjacent routers, packet filtering, network address translation (NAT), and encrypting or decrypting packets as in the case of virtual private networks (VPNs) (EC Council, 2010). A router is a multifunctional device with the primary duty of forwarding packets between two or more networks or network segments. Little initial configuration is needed to begin routing and the routing function can be employed using either dynamic routing protocols or by configuring static routes. Dynamic routing allows the router to receive and maintain routes automatically from its neighboring routers through periodic routing updates. Manually adding static routes can easily be accomplished in smaller networks by a network administrator, but this task quickly becomes overwhelming in a larger network environment (Northcutt, Zeltser, Winters, Frederick, & Ritchey, 2003).

Since a router is traditionally installed at the perimeter of a network, it plays an important role in security. The best implementation of a router with regard to security is to use it simply as a single component of a larger defense-in-depth security structure. This implementation allows a router to focus on what it was designed to do – route packets – rather than on security-specific concerns, such as intrusion detection/prevention, or as a firewall. However, in very small networks, this is not always possible. Sometimes routers must perform multiple functions, including that of a single perimeter security solution in addition to routing packets. A router's ability to be flexible enough to fill this need is an excellent example of the value routers can bring to an organization. In certain environments, a router may be effective as a perimeter security device on its own. This requires a properly configured device to provide a solid foundation of perimeter defense. This scenario makes it even more important to apply defense-in-depth principles behind the router, such as NAT and host-based solutions. The practice of implementing a single line of network perimeter defense is an undesirable practice since an attacker only needs to exploit one defense layer before an entire network becomes vulnerable to compromise (Northcutt, et al., 2003).

Why harden routers?

As Cole (2010) suggested, there are three things attackers will typically look for on a network when planning an attack:

1. Visible hosts
2. Open ports
3. Vulnerable services

An attacker can search for hosts using any of several different tools, such as *ping*, *hping2,* etc. This is normally an attack step in which the attacker performs the discovery function to find

exploitable hosts. Next, open ports can be illuminated on the hosts discovered in the previous step. One example of a free, open source, port scanning tool attackers commonly use for this purpose is *Nmap*. An Nmap scan will show the TCP and UDP ports that are open and can indicate the type of operating system on a specific host. To look for vulnerable services, an attacker may employ a tool such as *Nessus* to scan the visible hosts. The information gained from these steps can provide a would-be attacker with valuable, exploitable information about the hosts on a network.

The strategy behind hardening routers is to eliminate one source of vulnerabilities on the network, thereby reducing overall risk. By closing unneeded ports on the router, vulnerabilities are removed because if an attacker cannot connect to a device, that device cannot be attacked. In addition, removing vulnerable services prevents an attacker from exploiting certain weaknesses since they are no longer available (Cole, 2010). Using a router as a filtering device employing NAT or using access control lists (ACLs) to filter external scans and effectively hiding internal hosts will greatly impact the effort on reducing visible hosts to potential attackers.

Statistics indicate that attackers still rely heavily on misconfigurations and functional vulnerabilities when targeting network infrastructure equipment (Lindner, 2009). Vulnerabilities in open network services, such as a service with a memory corruption vulnerability, tend to be the primary entry targets for attackers (Lindner, 2009). Deal (2005) recommended manually disabling all services that are not being used on a router. Another method is to use the Cisco AutoSecure feature to dynamically disable the unused ports. Either method is a valid, acceptable practice when ensuring that these services are in fact disabled. Certain Cisco IOS (Internetwork Operating System) releases disable specific services by default and require the administrator to enable them when they are needed. However, when an IOS is upgraded, an administrator may

not realize that previously disabled ports and services have become enabled with the new release. Manually or dynamically ensuring unused services are disabled will help protect the router and the network from the issue of services and ports inadvertently being re-enabled. Deal (2005) advised that administrators try to refrain from making any assumptions about what services are running on a router and always assume unused services need to be disabled.

Router attacks and vulnerabilities.

Similar to typical computer systems, routers contain a number of common innate vulnerabilities, many of which depend on the specific configuration. Conceptually, a router is created with three separate operational planes – the management plane, the control plane, and the data plane. Administration, configuration, and the state of the router are organized by the management plane. The control plane ensures that monitoring, routing table updates, and the dynamic operations of the router are properly handled. The data plane controls the forwarding of packets onto the attached network(s). To maintain a secure router, threats to each of these planes must be considered because exploitation of any one plane can easily lead to all planes becoming compromised (Antoine, et al., 2005).

According to Antoine, et al. (2005), attacks on routers may include unauthorized access, session hijacking, denial of service (DoS), eavesdropping, as well as information theft. Several techniques of attack used against routers are password guessing, routing protocol attacks, IP fragmentation attacks, and attacks against specific vulnerable services.

In the case of password guessing, most networking devices (including Cisco routers) are shipped with a preconfigured default username and password. It is up to the administrator to change the default settings to use more secure credentials. Many Cisco routers use the default username and password of *admin*/*admin* (Basta & Halton, 2008). It would not take an attacker

long to break this username/password combination, especially since these credentials are well-known and highly published.

Administrators must also be aware of the methods attackers employ to obtain credentials for a device in order to take the appropriate steps to prevent compromise. For example, an attacker can use an open source tool to crack a weak password. If an attacker obtains the running configuration, the password will be shown as a hash, an encrypted value, or the actual plain-text password. The password can be encrypted using Cisco's own cryptographic algorithm known as Type-7. A Type-7 password can be easily decrypted using one of several different tools, such as Cain and Abel, Cisco Password 7 Hash Decoder, and GetPass. Most passwords in modern routers are stored in an MD 5 hash representation of the password. This creates a one-way hash of the password and makes the reversal of the hash extremely difficult. Since cracking an MD 5 password could prove to be highly complex, another method of cracking the password is to use a dictionary attack. Many tools exist that are capable of performing dictionary attacks by trying different password combinations until the correct one is found (Vladimirov, Gavrilenko, Vizulis, & Mikhailovsky, 2006). One of the more popular tools is John the Ripper. John the Ripper is an open source password-cracking tool that incorporates a number of password crackers into one package (DHS/FEMA, 2008). John the Ripper may be run in several different modes; however, by default it will use a dictionary attack. John contains its own password files that can be employed for the attack or the attacker can load a customized file that may be more adept at breaking into the type of device being attacked (Whitaker, & Newman, 2006).

Using a rainbow table is another alternative if an attacker wishes to crack a hashed password without actually performing any action against the hash. Rainbow tables are created by others that have already broken a hash and obtained the corresponding password. An attacker can

take the MD 5 hash of the password and compare it against the values in the rainbow table to find the correct password. This is a method used to crack hashed passwords that also saves time and processing power, as long as the attacker can locate a rainbow table containing the hash in question (Whitaker, & Newman, 2006).

Methods of hardening routers.

According to the EC Council (2011), router security best practices include using the most secure services to accomplish a task. For example, enable SSH on a router instead of the insecure Telnet service, which is discussed in more detail below. In addition, it is a good practice to disable the router's HTTP server if Web access is not needed. Best practices also include using the more secure SNMP version 2 rather than version 1, and using access control lists to help secure NTP if it must be used. The EC Council also recommends disabling all unneeded services, such as TCP and UDP small services, CDP, and Finger since many of these services are not needed on today's networks.

Turning off unneeded ports and services.

As mentioned, security best practices suggest disabling any unnecessary services. Many services that use UDP are not frequently used for legitimate purposes on modern networks, but they are commonly used to launch denial of service (DoS) as well as other attacks. Cisco Systems (2008) recommends disabling the TCP and UDP small services, which include *echo*, *discard*, *daytime*, and *chargen*. These services are located on TCP/UDP ports 7, 9, 13, and 19 respectively. All of these services are now outdated. They were once used in UNIX environments to provide information such as date and time, connectivity testing, and to generate a stream of characters. If left open, hackers can use these services to their advantage. For

example, the chargen service (TCP or UDP port 19) can permit an attacker to send a flood of traffic directed at this port, effectively causing a Fraggle DoS attack (Deal, 2005).

The *Finger* service (TCP port 79) is also an old UNIX application that was used to determine who was logged into a device. Today, the same information can be provided from many other sources, diminishing the need for Finger. When the Finger command is used on a Cisco router, the router responds with the output from the **`show users`** command. This output could allow an attacker to see the current users logged onto the router as well as being able to acquire valid user identification credentials (Deal, 2005). According to Stevens (1995), the Finger service had a programming error in an earlier version of the service that facilitated the infection of the password cracking Internet worm of 1988. The Finger protocol can also reveal detailed user information such as login names, phone numbers, last login, etc. Probably the most famous cracker to date, Kevin Mitnick, also used Finger as one of his targeted services when he attacked Shimomura's network in 1994 (Smith, 2005).

The PCI DSS (2010) documentation lists the Telnet service as an insecure service in multiple locations of requirements 1 and 2. Telnet is considered insecure because all communications conducted under it are completed in clear text. Numerous attacks are known to capture the traffic of a Telnet session with a packet sniffer, permitting the attacker to view the information contained in the session. The captured information may include such sensitive data as the device configuration, passwords, usernames, IP addresses, etc. (Roland, 2004). PCI DSS requires that Telnet be disabled and the more secure service – the Secure Shell (SSH) protocol – be used in its place. SSH operates on TCP port 22 and provides strong authentication and encryption of the session (Bhaiji, 2008).

The HTTP server protocol is supported on all newer Cisco IOS releases to provide a Web interface for device administration. A very common router vulnerability is present when the HTTP server service is enabled. Attackers have discovered numerous methods of exploiting it to gain unauthorized access (Deal, 2005). Several of the weaknesses in the HTTP server include passwords being revealed in plain-text, and the requirement that administrators log on at full (level 15) privilege (Antoine, et al., 2005). Another HTTP exploit involves an attacker taking advantage of the HTTP authentication vulnerability. This exploit can allow a remote user to gain full administrative access to a router (EC Council, 2010). Careful consideration should be given to the use of HTTP on a router and, unless it is used in conjunction with a secure authentication method such as AAA (AAA refers to Authentication, Authorization, and Accounting), it should be disabled. An additional HTTP hardening measure includes configuring access control lists to limit HTTP router management access to specific hosts (Hucaby, McQuerry, & Whitaker, 2010).

Cisco routers and many other network hosts utilize the Network Time Protocol (NTP) to synchronize all the time-of-day clocks (Antoine, et al., 2005) with a remote time server or other reliable time source. It is good practice to synchronize the time on all network devices down to the second if possible. Network time stamps assist administrators with recognizing problems such as lost connections, network crashes, buffer overflows, and missing packets. NTP also helps with network forensics investigations since time synchronization can affect log file accuracy, auditing precision, network fault diagnosis and recovery, as well as file time stamps (EC Council, 2011). If NTP is employed on a network, the router can be configured with specific trusted addresses for the time source. Additionally, NTP authentication should be used whenever possible. However, if NTP is not needed on a network, it is important to disable this service to remove the vulnerabilities it presents.

The Cisco Discovery Protocol (CDP) is a data link layer protocol used to discover information about neighboring Cisco devices. CDP can show the Cisco IOS software version, network layer addresses, and the platform type of any neighboring Cisco devices. This information is not encrypted and CDP does not offer any mechanisms for authentication between devices. A malicious attacker can connect a rogue router or switch to a network and obtain information about the network devices. In addition, a router using an IOS version earlier than 12.2(3) may crash or reboot if battered with a flood of CDP frames by an attacker (Whitaker, & Newman, 2006). CDP is enabled by default on Cisco routers and can be disabled globally or on specific interfaces. The recommended practice is to disable CDP to prevent router information from being transmitted to untrusted hosts outside the network (Hucaby, McQuerry, & Whitaker, 2010).

If the Simple Network Management Protocol (SNMP) is needed on a router, the more secure SNMP version 2 should be used. Version 2 provides support for MD 5 authentication rather than the clear text community string as used in version 1. If version 1 must be used due to compatibility restrictions, administrators should ensure the default “public” and “private” community strings are changed to community strings that are much more difficult to guess. Standard IP access lists can also be implemented to limit the router’s SNMP access to specific network hosts (Hucaby, McQuerry, & Whitaker, 2010).

Routing protocol security.

Routing and routing protocols can raise several important security concerns. Routing security should be considered a high priority to prevent unauthorized access to network resources, to protect critical data, and to prevent network failures and service interruptions. Unprotected routers make painless targets for skilled attackers that can falsify routing update

packets and corrupt the route tables. This attack can allow the attacker to reroute network traffic in any direction desired. The best way to prevent this type of attack is to implement only static routes. This is a very effective solution for smaller networks. However, static routes can create an administrative nightmare for administrators managing medium to large networks (Antoine, et al., 2005).

The use of routing protocols that can implement authentication is a better solution for larger networks. According to Northcutt, et al. (2003), an important rule when employing dynamic routing protocols such as RIP (versions 1 and 2), OSPF, BGP, and EIGRP is to configure the protocols to ensure they are implemented in a secure fashion. These routing protocols can become an easily exploited security hole if due care is not taken. For example, several routing protocols include numbering schemes (such as an autonomous system [AS] number or area number) (Lewis, 2006) providing several specific details of the network that are transmitted in plain-text and easily captured by an attacker. To help prevent this security issue, administrators can implement route authentication. The process of route authentication includes the use of a secret keyword that is hashed with Message Digest 5 (MD 5) and is used with all routing updates. The routing protocols that support this feature include RIPv2, OSPF, EIGRP, IS-IS, and BGP. Another method of securing dynamic routing protocols is to prevent tampering of the routing tables. This can be done by blocking updates from untrusted networks. To accomplish this task on a Cisco router, the command `passive interface [interface]` can be applied to the appropriate interface configuration (Northcutt, et al., 2003).

AutoSecure.

To automatically secure a router with the recommended security settings, an administrator can use the Cisco *AutoSecure* feature. When using full mode, AutoSecure will

automatically apply more than 80 commands to a router to configure additional security features. AutoSecure will lock down the management plane services, the data plane services, firewall services, login functions, NTP, SSH, and TCP services. This feature may be useful for easy security implementation on a Cisco router, but it is only available on Cisco IOS Release 12.3(8)T and above. The AutoSecure feature can be run in full mode, noninteractive mode, or only for select services. Full mode will prompt the administrator with questions concerning how to secure the router. Noninteractive mode allows the router to automatically apply the recommended commands to the configuration. Another option is to specify the management plane, data plane, NTP service, etc. to apply the proper commands to the router in order to secure only the desired service or plane (Hucaby, McQuerry, & Whitaker, 2010).

Analysis

Initial results from the QualysGuard PCI report.

The test router was scanned to check if any vulnerabilities existed and, if so, how severe they were when measured against PCI DSS standards. QualysGuard PCI was used for this scan and it delivered a report detailing the vulnerabilities discovered and the severity of each. The report also showed the average security risk rating of the device, as well as whether or not the vulnerabilities were confirmed. As figure 1 shows, the security risk rating of the test router after

Summary of Vulnerabilities

Total: 56 Security Risk (Avg): 4.0

by Severity	
Severity	**Confirmed**
5	0
4	1
3	5
2	3
1	0
Total	**9**

Figure 1. QualysGuard PCI report indicating the security risk rating and the number of vulnerabilities confirmed on the device after the first scan (QualysGuard PCI Report, 2011).

the initial scan was 4.0 out of 5.0. This indicates a high security risk and falls outside the acceptable range required by PCI DSS. PCI DSS requires each device to fall below an average NIST CVSS rating of 4.0. In other words, if the CVSS rating on any specific device is 4.0 or above, remediation of the vulnerabilities must be completed to bring the risk rating down to an acceptable level. Figure 1 also signifies that a total of 56 vulnerabilities were discovered, however only 9 were listed as confirmed. The remaining 47 vulnerabilities fell into the categories of "potential" and "information gathered." None of the 9 vulnerabilities rated at the highest severity. Nevertheless, several were rated well above the acceptable severity levels. Figure 2 displays the discovered vulnerabilities organized by assigned severity level.

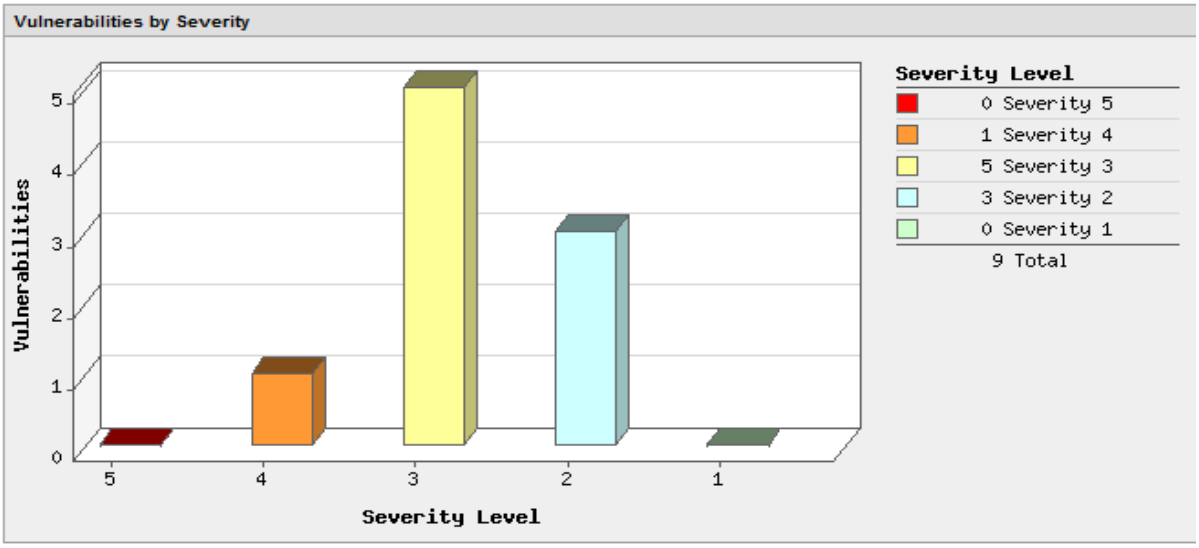


Figure 2: QualysGuard PCI report graphically displaying how the severity levels compare with each other (QualysGuard PCI Report, 2011).

Remediating the vulnerabilities.

The vulnerabilities were addressed according to severity, with the most severe vulnerabilities addressed first. General security best practices were also followed to address several other vulnerabilities not specifically listed on the report.

Hardening default passwords.

The first and most severe vulnerability listed on the QualysGuard report addresses the Cisco router default password. Because default passwords are widely published and easily accessible, PCI DSS requires all passwords to be changed from those set as default by the manufacturer. This requirement is described in PCI DSS requirement 2.1, stating that vendor-supplied default passwords must always be changed before installing a device on the network (PCI DSS, 2010). This vulnerability carries a CVSS score of 7.5 and to remediate this high severity vulnerability on the test router, the enable secret and line passwords were changed from the default setting to a more secure password. Below is the command used to change the enable secret password:

```
Security_Router(config)#enable secret regis#1
```

To verify that the enable secret password was set and hashed using the default hashing algorithm, MD 5, the following command was used:

```
Security_Router#sh run | include enable secret
enable secret 5 $1$JmSy$OVjEpSHjvHFn8PV.XUyW7/
```

The above output indicates that the enable secret password is represented by a string of random-looking characters. This is seen in the second line beginning with **“**`enable secret 5`.” The final password change involves the setting for the console port. Below are the commands used to make this configuration change and to save all password changes:

```
Security_Router# configure terminal
Security_Router(config)#line console 0
Security_Router(config-line)#password regis#1
Security_Router(config-line)#login
```

```
Security_Router(config-line)#^Z
Security_Router#write memory
Building configuration...
[OK]
```

IKE and IPSec denial of service vulnerabilities.

These two vulnerabilities were reported by QualysGuard with a NIST CVSS rating of 5 and 7.8 respectively and apply to the Cisco IOS version installed on the router. These vulnerabilities were caused by a malformed Internet Key Exchange (IKE) packet that could lead to a denial of service issue. The denial of service attack could be caused by an attacker exploiting this vulnerability by sending malicious IKE packets to the Cisco device (Cisco, 2008). Cisco's recommended fix for these issues is to upgrade the IOS image to a later version that has addressed the vulnerability (Cisco, 2010). Following the recommended course of action, the router was upgraded to the latest version of IP Basic Cisco IOS – version 15.1.4M(ED) – which was released by Cisco on March 25, 2011 (Cisco, n.d.). This update should address the two vulnerabilities and improve the overall security of the router since, as Vladimirov, et al. (2006) suggested, newer IOS versions are typically more secure, have fewer open ports, and are more difficult for an attacker to fingerprint.

Disabling the Finger service.

The QualysGuard PCI vulnerability report indicated the Finger service can disclose logged on users and details about those users. This service has a CVSS score of 5 and can make the test router vulnerable to an attacker exploiting user names, especially if weak passwords are used. QualysGuard's suggested solution for this vulnerability is to disable the service. The following command was used to disable the Finger service:

```
Security_Router(config)#no ip finger
```

Securing the management interfaces.

Most Cisco administrators prefer using the command line interface to configure network devices and don't place an overly high value on the HTTP interface for this purpose, making the HTTP server service unnecessary. In addition, HTTP offers another weakness to the router's security. The HTTP server service was disabled on the test router to alleviate this vulnerability with following two commands:

```
Security_Router(config)#no ip http server
Security_Router(config)#no ip http secure-server
```

Telnet is another method for network device management that offers no authentication. PCI DSS requires the more secure SSH protocol to be implemented instead of Telnet. The commands below were used to replace Telnet with SSH (Watkins, 2008):

```
Security_Router(config)#crypto key generate rsa general-keys modulus
1024
Security_Router(config)#ip ssh time-out 60
Security_Router(config)#ip ssh authentication-retries 3
Security_Router(config)#line vty 0 15
Security_Router(config-line)#transport input ssh
Security_Router(config-line)#login local
```

Hardening the NTP service.

Next, the NTP service was hardened by configuring NTP authentication. This was done as a best practice and was not required by PCI DSS since the vulnerability was rated with a CVSS score of only 2.6. This service was hardened rather than disabled because most networks use NTP to correlate logging information among the numerous network devices. Below are the commands used to configure authentication and eliminate this vulnerability:

```
Security_Router(config)#access-list 25 permit host 172.16.2.5
Security_Router(config)#ntp trusted-key 1
Security_Router(config)#ntp authentication-key 1 md5 key1
Security_Router(config)#ntp authenticate
Security_Router(config)#ntp server 172.16.2.5 key 1
Security_Router(config)#ntp access-group peer 25
```

Disabling TCP and UDP small services.

This group of vulnerabilities is noted as “TCP test-services” on the QualysGuard report and listed as a confirmed vulnerability with a CVSS rating of 5. These services were turned off on the test router in order to work toward PCI DSS compliance and because they are no longer needed in today’s networks. The commands below were used to disable these services:

```
Security_Router(config)#no service tcp-small-servers
Security_Router(config)#no service udp-small-servers
```

Applying AutoSecure.

To automatically disable the vulnerable services using Cisco AutoSecure in full mode, the command shown below can be used. Following the command is a list of all the services automatically disabled by the AutoSecure feature. This one command, along with the answers provided to the prompted questions, offers a much simpler method of applying the security features as compared to individually hardening or disabling each service as shown in the previous steps. The drawback to using AutoSecure is that the administrator has less control over the commands applied to the router and the changes made.

```
Security_Router#auto secure management full
Securing Management plane services...
Disabling service finger
Disabling service pad
```

```
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol
Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Disabling SNMP
          ...
!
End
```

Results

Second scan.

After going through the process of either disabling or hardening specific vulnerabilities and upgrading the Cisco IOS version, a second vulnerability scan was performed. However, even though many vulnerabilities were mitigated, the second scan indicated an average security risk level of 4. According to PCI DSS, the router still did not meet the standards. As seen in figure 3, the two vulnerabilities producing the high severity level were related to SSH. SSH version 1 was

Figure 3: Detail of vulnerabilities from second QualysGuard PCI scan (QualysGuard PCI Report, 2011).

configured on the router initially while remediating the Telnet vulnerability. SSH is available in both version 1 and version 2 and the command shown below was used to secure the test router

with SSH version 2 because it is the more secure, improved version. Version 2 first became available on Cisco IOS 12.3(4)T and was incorporated on all later images (Watkins, 2008). Figure 3 shows that one of the SSH vulnerabilities was caused by the use of version 1 and the second vulnerability was from a weak cipher. The QualysGuard report indicated that SSH version 2 needed to be enabled and that DES (Data Encryption Standard) should not be used. Implementing 3DES or AES (Advanced Encryption Standard) would resolve the weak cipher issue. Performing the following command to enable SSH version 2 remediated both vulnerabilities.

```
Security_Router(config)#ip ssh version 2
```

Third scan.

The only remediation effort made after the second scan was to configure SSH version 2 to replace SSH version 1. Once this change was made and the configuration saved, a third scan was performed to ensure the problem was corrected. The third scan indicated an average security risk rating of only 2 (shown in figure 4). Figure 5 shows that only one confirmed vulnerability

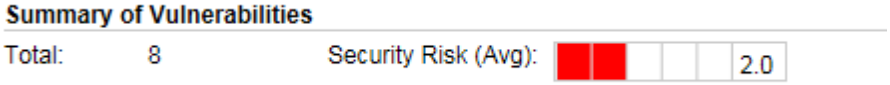


Figure 4: Summary of vulnerabilities from third QualysGuard PCI scan (QualysGuard PCI Report, 2011).

was found by QualysGuard. The remaining vulnerability could allow an attacker to discover the host operating system, which could then be used to launch additional attacks against the host. This vulnerability however, was not resolved for two reasons. First, it was rated at a severity level of 2 and was rated with a permissible score according to PCI DSS requirements. Second, no solutions were currently available to fix this vulnerability.

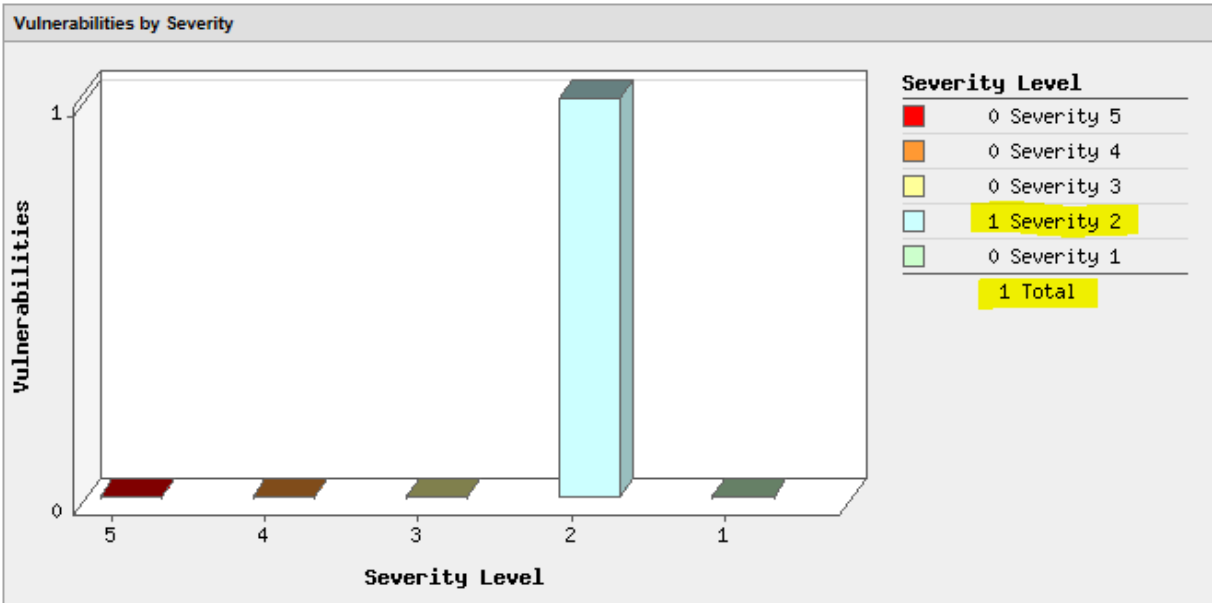


Figure 5: Detail of vulnerabilities from third QualysGuard PCI scan (QualysGuard PCI Report, 2011).

Additional steps.

This study showed how to approach a device from a security perspective and ensure it can pass PCI DSS requirements. However, it does not serve as a guide to provide all the steps necessary to make sure a router is as secure as possible. Several items were not specifically indicated in the QualysGuard scans that security best practices may suggest. One change that could help secure router access is to implement authentication, authorization and accounting (AAA). AAA implemented through a centralized server allows better account management and improves consistency of access control (The Center for Internet Security, 2010).

Best practices also dictate limiting the source addresses of hosts that are able to access a network device or specific services on a device. This task can normally be accomplished by implementing standard access control lists (ACLs) on the router interfaces. One use of standard ACLs is to restrict NTP access to the configured NTP server. Another use for standard ACLs is during the process of hardening the SNMP service. An ACL can be used to define the SNMP

agents that will query the management agents on network devices, effectively blocking unauthorized devices from trying to use this service to connect to hosts.

The test router was configured with a direct connection, a static route, a RIP process and an OSPF process during the entire study. QualysGuard was not able to determine whether the router needed all these processes running and did not suggest that they presented vulnerabilities. In the case of the test router, only the direct connection was needed to forward packets to the default network and all other routing processes could have been disabled to save on CPU cycles as well as to minimize several vulnerabilities. It would be considered a best practice to disable the RIP and OSPF routing processes or, if they are needed, to implement them in a more secure way. If RIP is needed on a network device, it should be implemented using RIP version 2 because version 1 has no mechanism to authenticate routing messages. RIP version 2 allows the implementation of router authentication by adding MD 5 hash capabilities to the authentication process. If the OSPF routing protocol is necessary on a network, it should also be configured to employ router authentication. Although not enabled on the test router, the routing protocols EIGRP, IS-IS, and BGP should always use router authentication as well (Cisco Systems, 2008).

Chapter 5 – Conclusion

Vulnerabilities can be found anywhere in a network and these vulnerabilities can become particularly dangerous to the security of a network when they are on Internet-facing routers. However, what types of threats are associated with these vulnerabilities? Do the vulnerabilities have any effect on a network's ability to comply with PCI DSS requirements? What can administrators do to harden perimeter routers? This study has demonstrated how routers function in a network, their importance in network architecture, and the significance of ensuring that they are properly secured. Many variables contribute to a router's vulnerability to threats, including outdated Cisco IOS software, misconfigurations, unnecessary/unused ports and services left enabled, weak or default passwords, and the use of insecure protocols. This study has gone through the process of uncovering the vulnerabilities on a typical Cisco router and shown the configuration modifications necessary to properly harden the router to meet the requirements of PCI DSS.

The QualysGuard PCI report showed that the test router was configured with a default password. This is a direct violation of PCI DSS requirement 2.1, which states that all vendor-supplied defaults must be changed (PCI DSS, 2010). The password was changed from the default and the new password was hashed using the MD 5 algorithm.

The study showed that certain services may be active on a network host, but these services may not be the most secure methods to accomplish a specific function. For instance, the test router initially had the Telnet service enabled to allow remote administration. PCI DSS indicates that this service is insecure because all information conducted while using this protocol is transmitted across the network in plain-text. An attacker can easily view this information if traffic is captured with a network sniffer (Roland, 2004). Telnet was disabled on the test router

and Secure Shell (SSH) was configured to permit remote device management. However, even after enabling SSH, the second QualysGuard scan showed that SSH was still causing a severity 4 and a severity 3 vulnerability. Both vulnerabilities were related to the use of SSH version 1. One of the issues with SSH version 1 included multiple vulnerabilities that could only be addressed by upgrading to SSH version 2. The other vulnerability was caused by the use of a weak cipher in SSH version 1. The QualysGuard report recommended using 3DES or AES (Advanced Encryption Standard) rather than the less secure DES (Data Encryption Standard). Enabling SSH version 2 on the router resolved both of these vulnerabilities.

In addition to changing to more secure services, some services that were active on the test router were completely unnecessary and created additional holes in the router's security. The Finger service was one such service that provided no benefit, but left the router vulnerable to an attacker exploiting user names. The HTTP server service provides an HTML interface for router management. However, HTTP is considered an insecure service and an administrator would have the same functionality through the command line interface (CLI). TCP and UDP small services were enabled, but they are outdated services that were once useful in UNIX environments. All of the above listed services were unneeded and consequently disabled on the test router with no loss in functionality.

The Cisco Discovery Protocol (CDP) was also initially enabled on the router. CDP can be a useful tool for administrators because it can discover information about neighboring Cisco devices that is helpful in managing the network. The information CDP provides includes Cisco IOS version, network layer addresses, and the platform of neighboring Cisco devices. Nevertheless, the information CDP provides is unencrypted and does not offer any form of authentication. These weaknesses make it a target for attackers wishing to gather information

about the network (Whitaker, & Newman, 2006). PCI DSS and best practices suggested that this service is best left disabled (Hucaby, McQuerry, & Whitaker, 2010) and, therefore, was disabled on the test router.

The first QualysGuard PCI scan included two vulnerabilities rated at a severity level of 3 that included weaknesses in the Cisco IOS causing an Internet Key Exchange (IKE) denial of service vulnerability. According to QualysGuard, as well as security best practices, the course of action required to remediate this vulnerability was to upgrade the IOS software to a later version that has addressed multiple security issues. Following this advice, the router was upgraded to version 15.1.4M(ED), which was the latest release of IP Basic Cisco IOS (Cisco, n.d.). The subsequent QualysGuard PCI scan indicated that this upgrade did indeed relieve the router of the two related vulnerabilities.

Network and security administrators may not always be aware of the best practices to follow or which ports, services, IOS software, etc. are the best from a security perspective. By following the approach of this study, administrators should understand how employing a network vulnerability scanner to test a host can illuminate hidden security risks. The same methodology can be adapted for use on all the hosts of an entire network to gain a device listing and each device's respective vulnerabilities. This is possible because the steps outlined apply to multiple hosts just as well as with the individual router. This logical approach to remediating vulnerabilities can help secure an organization's network and reduce its overall IT risk.

This study showed that a methodology for ensuring that a device meets the PCI DSS requirements can include several logical steps. Once a specific network device is targeted for testing, employing a vulnerability scanner to locate hidden weaknesses should be accomplished. The results of the vulnerability scan must be compared against the requirements of PCI DSS to

determine if action is necessary to secure the device. If vulnerabilities are present, gaining an understanding the vulnerabilities, learning how each vulnerability may have an impact on the integrity of the device and on overall security, as well as deciding how to mitigate the vulnerabilities should be performed next. During the administrator's research of the vulnerabilities, information regarding the best methods of mitigating each one should have been collected for use in creating a plan of action to detail the steps that should be applied to the device to resolve each weakness. Once the plan has been fully implemented, the administrator should perform another vulnerability scan to ensure nothing had been overlooked and that the modifications performed as expected. The results of this scan should also be reviewed to determine if the device meets PCI DSS requirements. If it does not, the above steps should be completed once again. Once PCI DSS compliance has been met, the next course of action would be to move on to another device and repeat the entire process. Once all hosts have been addressed in this fashion, an entire network should be able to pass a quarterly PCI DSS vulnerability scan and obtain PCI certification.

The approach shown in this study was an example of one method of providing a fairly high level of security for a single network component. The approach was demonstrated using one device, but the concepts apply equally well to multiple network hosts since PCI DSS is based on many common sense security practices as well as industry best practices. For instance, disabling or removing unnecessary services, using the latest software, and maintaining updates is applicable to virtually all hosts. The devices on a network that may benefit from the methods in this study include additional network routers and switches (from Cisco or any other vendors), servers, virtual machines, and workstations. What the study does not show is how to provide complete security for an enterprise or an acceptable level of security appropriate for *all*

organizations. In addition, this study did not attempt to meet the requirements of other standards, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act of 1999, etc. It is the researcher's hope that the approach taken in this study will serve as a general outline to guide administrators to research the best methods of hardening network devices to suit the requirements of their respective organizations.

References

Antoine, V., Bongiorni, R., Borza, A., Bosmajian, P., Deusterhaus, D., Dransfield, M., … Ziring, N. (2005, December 15). Router security configuration guide. Fort Meade, MD: National Security Agency.

Arregoces, M., & Portolani, M. (2004). *Data center fundamentals*. Indianapolis, IN: Cisco Press.

Avison, D, Lau, F., Myers, M., & Nielsen, P. A. (1999, January). Action research. *Communications of the ACM, 42*(1), 94-97.

Basta, A., & Halton, W. (2008). *Computer security and penetration testing*. Boston: Course Technology.

Bhaiji, Y. (2008). *Network security technologies and solutions (CCIE professional development series)*. Indianapolis, IN: Cisco Press.

Chapple, M. (2010, April). PCI DSS requirement: Building and maintaining a secure network. Retrieved from http://searchmidmarketsecurity.techtarget.com/tip/PCI-DSS-requirement-Building-and-maintaining-a-secure-network

Chuvakin, A, & Williams, B. R. (2010). *PCI compliance: Understand and implement effective PCI data security standard compliance* (2nd ed.). Burlington, MA: Elsevier.

Ciampa, M. (2009). Security+ *guide to network security fundamentals* (3rd ed.). Boston: Course Technology.

CIRT (2010). Default passwords. Retrieved from http://www.cirt.net/passwords

Cisco (2008, July 25). Cisco security response: Internet key exchange resource exhaustion vulnerability. Retrieved from http://www.cisco.com/warp/public/707/cisco-sr-20060726-ike.shtml

Cisco (2010, March 24). Cisco security advisory: Cisco IOS software IPSec vulnerability. Retrieved from http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee5.shtml

Cisco (n.d.). Cisco 2821 integrated services router: Download software. Retrieved from http://www.cisco.com/cisco/software/release.html?mdfid=279120798&flowid=7533&softwareid=280805680&release=15.1.4M&relind=AVAILABLE&rellifecycle=ED&reltype=latest

Cisco Systems (2003). *CCIE security, version 1.1*. Cisco Systems.

Cisco Systems (2008). Cisco guide to harden Cisco IOS devices. Retrieved from http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Cole, E. (2010). Security 401: SANS security essentials bootcamp style. Bethesda, MD: The SANS Institute.

Convery, S. (2004). *Network security architectures*. Indianapolis, IN: Cisco Press.

Deal, R. A. (2005). *Cisco router firewall security*. Indianapolis, IN: Cisco Press.

DHS/FEMA (2008, October). *Comprehensive cyberterrorism defense training support package: Participant guide*.

Donahue, D, & Swan, J. (2007). CCNP ISCW quick reference sheets. Indianapolis, IN: Cisco Press.

EC Council (2010). *Computer forensics: Investigating network intrusions and cybercrime*. Clifton Park, NY: Cengage Learning.

EC Council (2011). *Penetration testing: Security analysis*. Clifton Park, NY: Cengage Learning.

Hoelzer, D. (2010, November). PCI 2.0: What's new? What matters? What's left? Retrieved from http://www.secureworks.com/research/articles/sans-pci

Hucaby, D., McQuerry, S., & Whitaker, A. (2010). *Cisco router configuration handbook* (2nd ed.). Indianapolis, IN: Cisco Press.

Järvinen, P. (2007). Action Research is Similar to Design Science. *Quality & Quantity*, 41, 37-54.

Lewis, W. (2006). *Switching basics and intermediate routing: CCNA 3 companion guide.* Indianapolis, IN: Cisco Press.

Lindner, F. (2009, July 26). Cisco IOS router exploitation: A map of the problem space. Retrieved from http://www.recurity-labs.com

Northcutt, S., Zeltser, L., Winters, S., Frederick, K. K., & Ritchey, R. W. (2003). *Inside network perimeter security*. Indianapolis, IN: New Riders.

Northcutt, S. (2007, May 11). The risk of default passwords. Retrieved from http://www.sans.edu/research/security-laboratory/article/default-psswd

Paquet, C. (2009). *Implementing Cisco IOS network security (IINS): (CCNA security exam 640-553) (authorized self-study guide)*. Retrieved from http://library.books24x7.com.dml.regis.edu/books.asp?task=query

PCI DSS (2010, October). Requirements and security assessment procedures, version 2.0. Retrieved from https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

PCI Security Standards Council (2010, October). PCI DSS quick reference guide: Understanding the Payment Card Industry Data Security Standard version 2.0. Retrieved from https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

PCI SSC (n.d.). Why comply with PCI security standards? Retrieved from https://www.pcisecuritystandards.org/security_standards/why_comply.php

Qualys (n.d.). QualysGuard PCI compliance. Retrieved from http://www.qualys.com/products/qg_suite/pci/

QualysGuard (n.d.). About QualysGuard Enterprise suite. Retrieved from https://qualysguard.qualys.com/fo/scan/scanList.php#

Roland, J. F. (2004). *CCSP self-study: Securing Cisco IOS networks (SECUR)*. Indianapolis, IN: Cisco Press.

Smith, P. G. (2005). *Linux network security*. Hingham, MA: Charles River Media.

Sophos (n.d.). PCI compliance. Retrieved from www.sophos.com

Sophos (2008, April 1). Hackers steal financial information from auto parts retailer. Retrieved from http://www.sophos.com/pressoffice/news/articles/2008/04/advance.html

Sophos (2010). Security threat report: Mid-year 2010. Retrieved from www.sophos.com

Stevens, W. R. (1994). *TCP/IP illustrated: The protocols*. Reading, MA: Addison Wesley Longman.

Teare, D. (2008). *Designing for Cisco internetwork solutions (DESGN) (authorized CCDA self-study Guide) (exam 640-863)* (2nd ed.) Indianapolis, IN: Cisco Press

The Center for Internet Security (2010, December 31). Security configuration benchmark for Cisco IOS. Retrieved from http://cisecurity.com

Vaishnavi, V., & Kuechler, W. (2004/5). *Design Research in Information Systems*. Retrieved from http://www.isworld.org/Researchdesign/drisISworld.htm

Vladimirov, A. A., Gavrilenko, K. V., Vizulis, J. N., & Mikhailovsky, A. A. (2006). *Hacking exposed Cisco networks: Cisco security secrets & solutions*. Retrieved from

http://library.books24x7.com.dml.regis.edu/book/id_13193/viewer.asp?bookid=13193&chunkid=345492183

Watkins, M. (2008). *CCNA security official exam certification guide*. Indianapolis, IN: Cisco Press.

Whitaker, A, & Newman, D. P. (2006). *Penetration testing and network defense*. Indianapolis, IN: Cisco Press.

Wilhelm, T. (2009). *Professional penetration testing*. Burlington, MA: Syngress.