https://doi.org/10.48009/4_iis_2017_91-98

Issues in Information Systems
Volume 18, Issue 4, pp. 91-98, 2017

CYBERSECURITY VULNERABILITY ANALYSIS VIA VIRTUALIZATION

Jorge Savaglia, University of Maryland, jorge.savaglia@gmail.com
Ping Wang, Robert Morris University, wangp@rmu.edu

ABSTRACT

Cybersecurity has become a significant issue for users and organizations. Penetration testing by scanning computer networks and systems to identify and analyze cybersecurity vulnerabilities is essential to defending the networks and systems against cyber threats and attacks. It is ideal to conduct such tests, scans, and analysis in a virtualized or simulated environment to minimize interruptions and security risks to live production networks and systems. This paper presents simulated vulnerability test scans and analysis using a virtualized network lab environment to demonstrate the effectiveness and benefits of virtualization in cybersecurity testing. The paper also discusses important implications for cybersecurity workforce training and preparation.

Keywords: Cybersecurity, vulnerability, virtualization, simulation, Nmap, Nessus

INTRODUCTION

Cybersecurity has become a significant issue for individual users and organizations whose business operations are increasingly dependent on the services and data on their computer and network systems. The goals of cybersecurity are to protect the confidentiality, integrity, and availability of computer and network systems, services, and data residing on the systems (Ciampa, 2015). Cyber threats such as viruses, worms, Trojan horses, backdoors, spyware, ransomware, phishing attacks, injection attacks, distributed denial of service (DDoS) attacks, and zero day attacks are becoming increasingly frequent and sophisticated. Computer systems and networks have become victims of cyber attacks because of their vulnerabilities or weaknesses that are exposed to and exploited by cyber threats. Therefore, proactive penetration testing by scanning and analyzing vulnerabilities is essential to addressing and hardening system and network weaknesses for protection and prevention against cyber threats and attacks.

Vulnerability analysis and system weakness assessment depend on penetration testing, which is "a set of tests and evaluations that simulate attacks" by a hacker or other malicious sources (Whitman & Mattord, 2015). The security tests have to be simulated due to the potential risks, harms, and interruptions to live production networks and systems. Many cyber threats to be tested, such as mutating malware and zero day attacks, have unknown or unpredictable and uncontrollable signature patterns and consequences, making it unsafe to test in a real production environment. Therefore, a lab for simulation and experimentation is the ideal isolated and controlled environment for security testing and analysis where unexpected events and consequences are minimized (Greg, 2015).

A virtualized lab environment is preferred over a physical lab for cybersecurity testing and training. Virtualization brings the benefits of high availability and performance testing (Ali, 2016). "A virtual lab infrastructure can provide a flexible and cost-effective platform that allows for running multiple operating systems and for sharing computing resources" (Son, Irrechukwu, & Fitzgibbons, 2012, p. 82). Virtual labs provide flexible options for installations and configurations of operating systems and application software for sharing. Unlike physical labs with fixed locations and hardware facilities, a virtual lab may allow user access from various locations. Therefore, a virtual lab with Internet access is often the best option for testing, hands-on practice, and training for corporations and educational institutions with employees and students distributed in various physical locations. There is a fast-growing demand for qualified cybersecurity workforce, and effective education and training are the solutions to meet the demand. Therefore, this paper will focus on sharing the success of simulation tests for vulnerability analysis in an effective large-scale virtualization environment for cybersecurity training.

This paper will demonstrate the effectiveness of cybersecurity vulnerability testing and analysis using a distributed virtual lab environment. The vulnerability test simulates scanning, probing, and information gathering in the reconnaissance phase of cyberattacks in a contained virtual lab environment. The following sections of the paper will explain the focus of the research, research methodology, the virtual lab environment, and present and discuss the vulnerability test findings. The paper also discusses important implications for cybersecurity workforce training.

RESEARCH FOCUS

This paper focuses on the identification and analysis of cybersecurity vulnerabilities in a virtualized testing environment that can be effectively for cybersecurity workforce training. A security vulnerability is a weakness of an information system that could be exploited by a security threat leading to infections and consequential damage and losses to users and organizations. For example, the recent WannaCry ransomeware attack targeted and exploited a critical Windows Server Message Block (SMB) vulnerability and caused infections of tens of thousands of various Windows systems with various organizations in more than 150 countries including the United States, and the impact of the ransomeware includes loss of sensitive information, disruption of service availability, and financial losses (US-CERT, 2017). Microsoft had to scramble to release emergency patches, including for the legacy Windows XP systems, to address the vulnerability after the ransomeware attacks. Therefore, it is critical to identify and analyze system vulnerabilities in order to prevent and respond to such exploitations.

Penetration testing (or pen testing) is primarily used to validate and verify information system vulnerabilities, and identifying vulnerabilities is a critical initial phase of pen testing (Cardwell, 2014). The vulnerability tests use scans to footprint or gather target information and identify and classify system and network security weaknesses and flaws, such as security holes from bad coding, absence of security patches, poor configurations or weak authentication; the scans and tests may include port scans, network mapping, networking sniffing, and more advanced pen testing techniques such as session highjacking, MAC flooding, DNS poisoning, and planting spyware and Trojans (Gupta & Kaur, 2013). The pen testing activities may lead to disruptions and cause security risks to live production systems. Thus, virtualization technology is useful for providing a safe environment simulating the real systems for penetration testing.

There are various options of virtualization vendors and products available with varied levels of cost and service support. The important common benefits of virtualization for cybersecurity workforce training and education include elimination of expensive hardware and facilities for physical labs, enabling active hands-on learning and virtual team collaboration activities through virtual labs (Wu, Fulmer, & Johnson, 2014). This paper focuses on and uses the examples of virtualized vulnerability scanning and pen testing in an educational environment because of the fairly new and fast-growing demand for cybersecurity training and education to produce qualified cyber workforce. Even though virtualization technology is not new, experience and examples of innovative and effective use of virtualized lab environment are still valuable and needed in order to share with and inform the cybersecurity education and training community, which is the goal and main contribution of this paper.

RESEARCH METHODOLOGY

This study simulates port scanning and system probing activities, which are often the first step of foot printing or information gathering in real cyber-attacks. The goal of the simulation is to identify and analyze vulnerabilities that exist with the systems and networks. Scanning tools are often used by hackers to probe potential target networks and systems to find open and available ports and services and determine their vulnerabilities before launching an attack. The tools used in the simulation are Nmap (Network Mapper) and Nessus, and both of them are freely available to hackers and network security professionals. Both Nmap and Nessus can scan a range of host addresses or a network address range entered at the command line. A hacker may use Nmap and Nessus offensively to probe for vulnerabilities to exploit. On the other hand, they can be used defensively by a cybersecurity professional to identify system and network weaknesses that need to be addressed.

Nessus and Nmap are separate tools. Nmap is an open-source fingerprinting scanner that is used for port scanning, network mapping, and vulnerability scanning (Rashid, 2016). Fingerprinting is the process of trying to identify the operating system running on a system by analyzing different packets, ports, and services running on the system (Yek, 2005). Nmap is a port scanner whereas Nessus is a vulnerability assessment tool that can potentially be used to assess vulnerabilities based on a basic knowledge of the tool. Nessus was created by Tenable Network Security and is open-source software. It was developed in an attempt to detect known security vulnerabilities in a system or network, such as flawed configurations, code errors, and other vulnerabilities. Since its creation, Nessus has evolved into a suite of even more powerful abilities that allow for functions such as malware detection and patch management ("Tenable Network", n.d.). Nessus uses built-in lists, or databases of vulnerability information, to compare its scan results. Plugins are also used in Nessus to identify any vulnerabilities within a system or network.

On the other hand, Nmap was developed in an attempt to scan networks for open or closed ports, services, or operating systems. Nmap is able to discover system information, such as a host operating system based on scanning through different packets. However, Nmap's primary functionality is that of port scanning and discovery as well as mapping a network. Contrary to Nessus that is installed on a server and runs as a web-based application, Nmap code can be installed on Windows, Linux/Unix, or Mac OS's and has a command line based and a GUI-based (Zenmap) interface (Cobb, 2006). Other key differences between the Nmap and Nesseus are the stark differences in report generation and customization, costs (Nessus is no longer free but Nmap is), and their capabilities. While each tool holds value and can greatly increase overall security, it may be beneficial to include both in a security posture so as to get the best possible implementation and ensure maximum effectiveness of all security mechanisms.

The virtual lab network used for the simulation for this study is hosted by a VMware vSphere server on a university network with secured online access using VPN (virtual private network). Users from around the world may use their VPN accounts to log into the virtual lab and create their virtual machines to conduct testing and capture data from the virtual network. The virtual hosts are on a 192.168.100.x subnet. The great benefits for using the virtual lab network include flexible anytime access without time constraints and freedom from worrying about breaking or damaging any facilities in conducting the security scans and tests. This network is also scalable and supports thousands of users physically located around the world. The following section presents the findings of the security tests using Nmap and Nessus in the virtual network environment.

FINDINGS AND DISCUSSIONS

The Nmap test scan shows that each host had a different set of services running. For example, Host 1 (192.168.100.103) had the following services running: File Transfer Protocol (FTP), Network Virtual Terminal Protocol (TELNET), HyperText Transfer Protocol (HTTP), Microsoft Remote Procedure Protocol (MSRPC), Network Basic Input/Output System (NetBIOS), secure HTTP (HTTPS), Microsoft Directory Services, Structured Query Language (MySQL), Microsoft Remote Desktop Protocol (RDP), and Virtual Network Computing (VNC). All ports were easily identified, labeled, and the operating system (OS) was easily discovered by the Nmap scan. However, Host 2 (192.168.100.105) was not as cooperative and many ports were not identified by the scan. These ports and services discovered would provide specific target areas for hackers to search for and plot against vulnerabilities. For pen testers and other cybersecurity professionals, the scan results serve as alerts to possible security holes that need to be patched and addressed. The scan results also indicate that the pen testing scans are limited momentary snapshots valid during the time period for the scan (Gupta & Kaur, 2013).

Figure 1 below shows a different host (192.168.100.105), which required multiple scan attempts in order to retrieve the desired information. The use of a *slow comprehensive scan* allowed for the acquisition of the desired information. The important OS information was not obtained through an Nmap scan but was found by using a special feature of the tool. Nmap has a command line feature that can be used to guess the OS of the host. It includes several command-line options to configure the OS detection engine. To limit OS detection of targets with at least one open port and one closed port, the --*osscan*- limit command-line option can be used to increase the chances of a successful identification. To make Nmap guess more aggressively, the --osscan-guess command-line option can be used. Figure 2 below shows that the operating system of host 192.168.100.105 is found as Linux.

Figure 2 depicts the services running on Host 2: Secure Shell (SSH), VNC, Session Initiation Protocol (SIP), Domain Naming Service (DNS) based service directory (MDNS), and 9 unidentified, filtered, but open ports. Similarly, Host 3 (192.168.100.106) acted in the same way as Host 2. Host 3 presented some of the same challenges as Host 2 in that it required a more comprehensive Nmap scan to divulge the information needed. The following services were found running on Host 3: SSH, DNS, MDNS, SIP, Internet Printing Protocol (IPP), SYSCOMLAN, and 8 unidentified, filtered, but open ports.

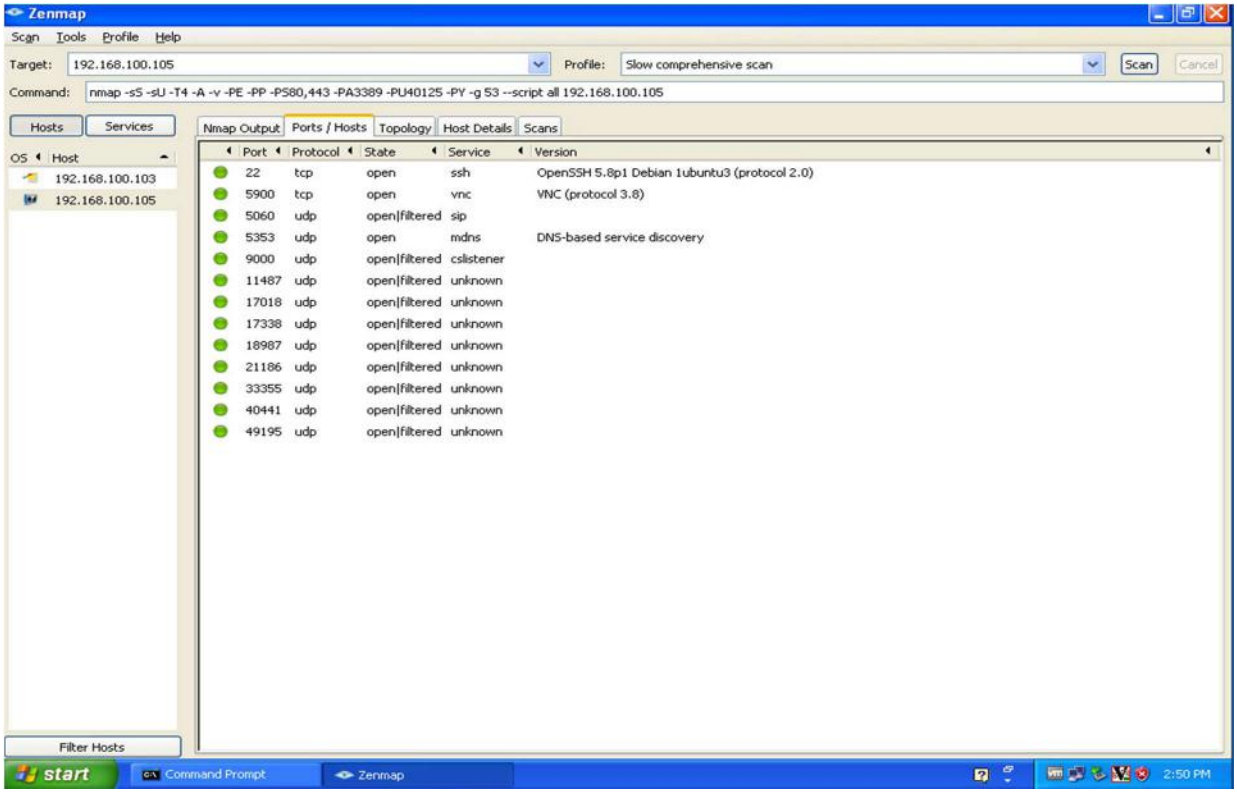

Figure 1. Nmap host scan results

It is still quite challenging to determine which host is the most secured based on the Nmap port scan results. However, the least secured host was Host 1 (192.168.100.103). This host was scanned with a somewhat passive scan and it revealed enough information for an attacker to begin enumerating the network. Further, this host did not follow the simple principle of disabling all ports that are not necessary for functionality. With services such as FTP, TELNET, and HTTP running, it allows a threat actor to intercept any transmissions that are sent in plaintext, which poses a great security risk to organizations (Cobb, 2005). Also, MySQL would allow for malicious text strings to be added into value fields, which could allow web page or database manipulation.

While Host 1 was a standout for the least secured host, it is difficult to determine the most secured host. The three hosts have a total of 14 open ports, but on an initial review Host 2 has 9 open ports compared to Host 3's 8 open ports. This would lead an analyst to determine Host 3 was the most secured. However, further reviews of which ports are actually open may lead to a different determination. Host 2 has the VNC port open, which can allow an attacker to bypass RDP security mechanisms and remote access to a victim's machine. However, Host 3 has its DNS and MDNS ports active, both of which could allow an attacker to manipulate user-browsing habits and infect the network as a whole. All things considered, this lab concludes that Host 3 is the most secured due to the fact that there isn't enough information about other configurations and security mechanisms to determine otherwise.

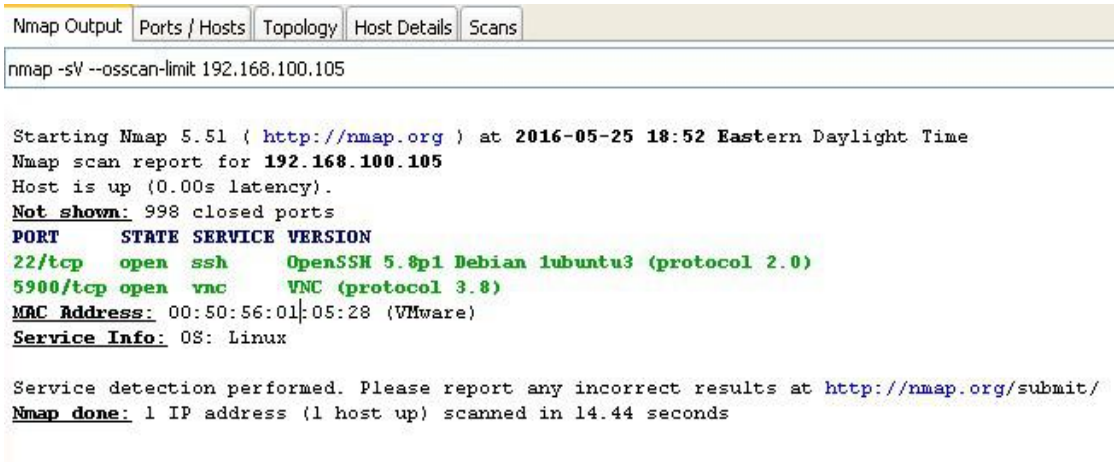

Figure 2. Nmap OS scan results

Nessus offers a wide array of services, but mainly provides its users with the ability to scan a network for vulnerabilities. It also has built-in configurations to ensure compliance and conduct audits, and Nessus can detect the presence of malware. Vulnerability assessments are cornerstones of any security posture as they allow for the active monitoring of networks and hosts, allow maximum efficiency in security mechanisms, and enable administrators to remain proactive in their attempts to prevent future attacks. With Tenable's new Nessus release, customers are now given even more functionality and convenience. Nessus 5.2 allows all vulnerability scans to come with attachments, post scan plugins, and it offers compatibility with more OS versions and has an updated user interface ("Tenable Network", n.d.).

The compliance audits and reporting features offered by Nesseus are especialy valuable, which can help network administrators to ensure that they are abiding by regulatory mandates. These reports should be generated on a routine basis and provided to senior management for review. This will ensure that all policies, processes, and procedures are in compliance with the rules set by the industry regulatory body that oversees the organizations and businesses. For example, Nessus offers auditing capabilities for National Institute of Standards and Technology Federal Desktop Core Configuration (NIST FDCC), the Security Content Automation Protocol (SCAP), the Defense Information Systems Agency's Database Security Technical Implementation Guide (DISA STIG), the Center for Internet Security (CIS), and the Payment Card Industry (PCI) (Stephenson, 2010). All reports are customizable and should be curtailed to their target audience for proper understanding. Nessus also offers its users the ability to save reports in a variety of formats.

Nessus goes one step further than what antivirus tools can do in terms of malware detection. Traditionally, some viruses, such as polymorphic viruses, can bypass some antivirus software tools because these tools do not scan the virus sample as a whole (Asadoorian, 2012). Nessus does better than that and compares the sample to lists of known malicious code and can even audit the antivirus software that is installed on the network. Nessus will check to see if the antivirus software has any configuration vulnerabilities and if any aspect of the software is out of date. It will then alert the administrator and provide suggestions as to how to strengthen security.

Based on the Nessus scan results on host vulnerabilities, the host with the most vulnerabilities was Host 192.168.100.103 with 78 vulnerabilities. The Hosts with the least vulnerabilities was a tie between Host 192.168.100.105 and Host 192.168.100.106. Figure 3 below presents the results on all three hosts with their respective number of vulnerabilities and the severity levels and open ports.

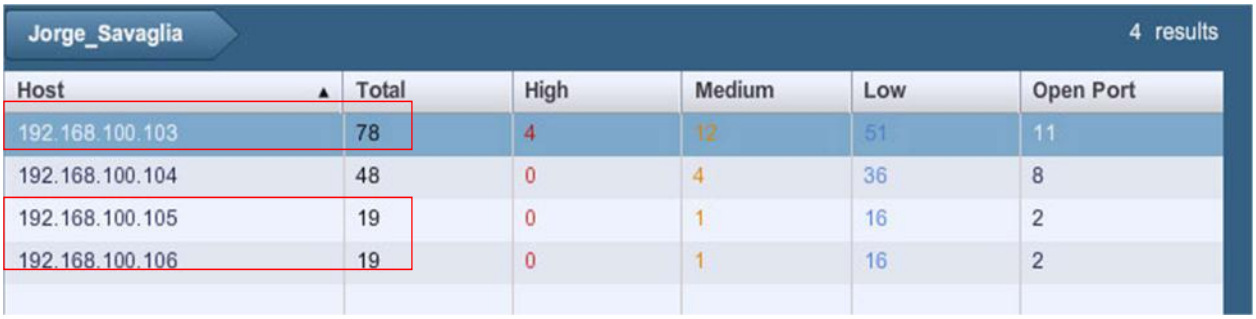

Figure 3. Nessus scan results on host vulnerabilities

A special Nessus feature that is worthy discussion is its auditing feature, which is a very important aspect to any organization. As mentioned above, regulatory compliance is built into Nessus and can allow administrators to ensure that processes that store and transmit sensitive information are doing so in a secured manner. Further, it allows for filtering and organizing sensitive information based on different criteria, which are determined through the use of plugins. This would be exceptionally helpful to an organization that falls under two separate regulatory bodies such as PCI and Sarbanes-Oxley (SOX). It is extremely beneficial to the security of information assets to separate credit card based information from accounting information and isolate services that facilitate the transmission and storage of each type of data. One of the major tenants of PCI compliance is protecting consumer information. During this lab, a PCI audit was conducted to ensure compliance. Among all of the vulnerabilities found, one that stuck out was that port 3389 (RDP) was active on Host 192.168.100.103. Failure to secure this port could allow a remote host to act as a local host and gain unauthorized access to areas of the network or database information as seen in Figure 4.

Figure 4. Results from Nessus auditing feature

CONCLUSIONS

This paper explains the importance of penetration testing for identifying and analyzing computer and network vulnerabilities and focuses on the benefits of using an effective virtual lab simulation for conducting cybersecurity vulnerability testing. The study presents a virtual lab simulation uses Nmap and Nessus tools for system and network vulnerability scanning and probing. The lab results show that the virtual lab network can be effectively manipulated

and scanned for vulnerabilities without interruption of normal production or service or security risks and damage to live productions systems and networks. The educational setting for the sample virtual lab in the study also shows the benefits of cost-effectiveness of using virtualization as well as flexible distributed access compared with physical labs.

The use of virtual lab simulations has valuable implications for cybersecurity training and workforce preparation. There is a large and increasing demand for qualified cybersecurity professionals. According to the U.S. Department of Labor Bureau of Labor Statistics (BLS), employment of information security analysts is projected to grow 18% from 2014 to 2024, much faster than the average growth rates of 7% for all occupations and 12% for all computer related occupations (U.S. Department of Labor, 2015). To train and prepare qualified workers for cybersecurity, hands-on labs using a virtual lab environment would be ideal for working professionals and military service members located around the world to participate at their own times of convenience. The sample virtual lab environment from this study provides a good example in this respect.

It should be pointed out that penetration testing is momentary snapshots and not able to identify all security vulnerabilities, whether in a real or simulated lab environment. Vulnerability assessments with careful monitoring and diagnostic reviews of all network services and devices will complement penetration testing in finding information system vulnerabilities (Gupta & Kaur, 2013). Therefore, virtualization of the test environment will not overcome the limitations of penetration testing itself.

This study is preliminary on a sample virtual lab environment for the initial phase of footprinting in penetration testing. Future studies may focus on more advanced simulations of cyber defense and offense activities, such as conducting session hijacking, MAC flooding, and DNS poisoning to determine the level of vulnerabilities and resilience of a target system or network. Another area for further research could be focus on assessing cybersecurity learning or training effectiveness of using a virtual lab environment, such as evaluating the effectiveness of team activities in a distributed virtual environment to determine how students can better participate in online learning using a virtual lab environment. Given the fast-growing cloud computing environment, another possible follow-up research topic would be on evaluating and comparing the strengths and limitations of using virtualization for cybersecurity hands-on work in different cloud environment.

REFERENCES

Ali, A. (2016). Selecting contents for a new virtualization course in information technology (IT) track. *Issues in Information Systems, 17*(1), 47-57.

Asadoorian., P. (2012). Detecting Known Malware Processes Using Nessus. Retrieved from https://www.tenable.com/blog/detecting-known-malware-processes-using-nessus

Cardwell, K. (2014). B*uilding virtual pentesting labs for advanced penetration testing.* Birmingham – Mumbai: Packt Publishing.

Ciampa, M. (2015). Security+ guide to network security fundamentals (5th ed.). Cengage Learning.

Cobb, M. (2005). The future of Telnet and FTP. Retrieved February 6, 2017, from http://searchsecurity.techtarget.com/answer/The-future-of-Telnet-and-FTP

Gregg, M. (2015). The network security test lab: A step-by-step guide. Indianapolis, IN: John Wiley & Sons, Inc.

Gupta, A., & Kaur, K. (2013). Vulnerability assessment and penetration testing. *International Journal of Engineering Trends and Technology, 4*(3), 328-333.

Nessus Compliance Checks. (2017). Retrieved February 11, 2017, from https://support.tenable.com/support-center/nessus_compliance_checks.pdf

Port Scanning Techniques. (n.d.). Retrieved February 9, 2017, from https://Nmap.org/book/man-port-scanning-techniques.html

Rashid, F. Y. (2016). Nmap security scanner gets new scripts, performance boosts. *CIO (13284045)*, Retrieved from http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=120389220&site=eds-live&scope=site

Shakeel, I. (2016). Nmap from beginner to advanced. Retrieved from http://resources.infosecinstitute.com/Nmap/#gref

Son, J., Irrechukwu, C., & Fitzgibbons, P. (2012). A comparison of virtual lab solutions for online cyber security education. *Communications of IIMA, 12*(4), 81-96.

Stephenson, P. (2010). Group Test: Vulnerability assessment. *SC Magazine: For IT Security Professionals (15476693)*, *21*(2), 42-49. Retrieved February 10, 2017, from http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=51372468&site=eds-live&scope=site

Tenable Network Security, I. (4). Tenable Network Security Announces Nessus 5.2 Vulnerability Scanner. *Business Wire (English).* Retrieved February 10, 2017, from http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=bizwire.c48181924&site=eds-live&scope=site

US-CERT. (2017, May). Alert (TA17-132A): Indicators associated with WannaCry ransomware. Retrieved from https://www.us-cert.gov/ncas/alerts/TA17-132A

U. S. Department of Labor. (2015, December). Occupational outlook handbook. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

Valladares, C. (2014). Vulnerability Management: Just Turn It Off! Part III. Retrieved February 9, 2017, from https://www.tripwire.com/state-of-security/vulnerability-management/vulnerability-management-just-turn-it-off-part-iii/

Whitman, M. E., & Mattord, H. J. (2015). Principles of information security (5th ed.). Cengage Learning.

Wu, D., Fulmer, J., & Johnson, S. (2014). Teaching information security with virtual laboratories. In J. M. Carroll (Ed.), *Innovative Practices in Teaching Information Sciences and Technology* (pp. 179-192). Switzerland: Springer International Publishing. doi: 10.1007/978-3-319-03656-4_16,

Yek, S. (2005). Blackhat fingerprinting of the wired and wireless honeynet. Retrieved from http://ezproxy.umuc.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.ftedithcowan.oai.ro.ecu.edu.au.ecuworks.3825&site=eds-live&scope=site