A Three-Stage Process to Learn Cyber Security

Te-Shun Chou
Department of Technology Systems
East Carolina University
Greenville, NC, USA
chout@ecu.edu

Tolulope Awojana
Department of Technology Systems
East Carolina University
Greenville, NC, USA
awojanat17@students.ecu.edu

ABSTRACT

This paper discusses labs and a three-stage learning process to help students learn the contents of cyber security. A system infrastructure that includes a number of identical, secure, and isolated learning environments is developed. Each learning environment includes a set of cyber security labs with each lab consisting of two sub-labs: attack and defense. These labs facilitate students learning of theoretical knowledge and allow them to practice hands-on activity of attack and defense. Each lab involves a three-stage learning process: learning, assessment, and engagement. The learning environments are implemented by using virtualization technology. Multiple virtual machines (VMs) are implemented in each learning environment and those machines serve tasks of attack and defense. In addition, the system infrastructure allows interaction among learning environments, therefore making it more similar to a realistic world network.

KEYWORDS

Virtualization technology; cyber attacks; cyber security

1 Introduction

A cyber attack is an illegal attempt by hackers to damage systems or gain access to the systems. For example, hackers can use code inject technique, such as SQL injection or cross-site scripting (XSS), to attack web applications and retrieve sensitive information from databases retained on the web server, redirect the victim to web controlled by the attacker, or perform malicious operations on the user's machine. The attacks can also affect computer systems. For example, denial of service (DoS) attacks can be used to send a large amount of traffic to a targeted computer system in order to make it difficult or impossible for legitimate users to access it. From the statistic reported to the Internet Crime Complaint Center (IC3) from 2001 to 2017, the amount of damage caused by cyber crime has dramatically increased from 17.8 million to 1.42 billion [1].

The trend of annual loss is increasing and the most costly cyber attack consequences for companies were suffered through business disruption and information loss. For example, the biggest known breach of a company's computer network occurred in August 2013 when Yahoo's 3 billion user accounts were hacked [2]. The information accessed included users' name, email address, hashed passwords, birthdays, phone numbers, and, in some cases, encrypted or unencrypted security questions and answers. An example can also be seen from 110 million Target credit/debit card information that was stolen in December 2013. This data breach incident caused the company to lose $162 million [2]. Uber also suffered from a massive data breach in 2016 when Uber's 57 million rider and driver accounts were stolen. As a result, Uber paid the hackers $100,000 to delete the information and to keep quiet [2]. Because of the incident, the Japanese company, Softbank, bought Uber shares at a nearly 30% discount compared to its initial offer. The latest data breach event happened to Facebook [3]. Eighty-seven million Facebook users' information was misused by Cambridge Analytica. The scandal was exposed on March 18, 2018 and the stock value of Facebook dropped 6% the next day.

The data breach could happen not only in private sectors but also in government agencies. Personal information of 22 million federal employees, contractors, and their families and friends in the US Office of Personnel Management was hacked in 2014 [4]. The personnel information included Social Security numbers, job assignments, and performance evaluations. Recently, ransomware has become a popular technique used to lock a victim's computer screen or encrypt the victim's files. Two examples below illustrated that hackers used ransomware to attack government agencies and threaten to publish their data unless a ransom is paid. The first ransomware example happened in the most populated county in North Carolina: Mecklenburg County [5]. The county's tax assessor's office, Social Services Department and the Department of Parks and Recreation were hacked in December 2017. Hackers seized control of several government computer systems and asked for a $23,000 ransom. The office refused to pay because they had a backup system and were confident in their ability to recover the stolen information. Another example happened in Montgomery County, Alabama in September 2017 [6]. The county's computer systems were hit by ransomware and the hackers gave local officials a week to pay the ransom, otherwise threatening to erase the data. The government paid nine bitcoins, amounting to between $40,000 and $50,000, to hackers in order to recover between 60 and 70 terabytes of data.

Computer systems of both private industries and governments depend on well-trained professionals to protect from attacks. Hence, cyber security education has become the first priority to foster security specialists in securing the Nation's critical hardware, software, information, and services from attack, damage, or unauthorized access.

In this project, we build a system infrastructure that includes a set of learning environments. In order to assist students learning of theoretical knowledge and practice of hands-on activities, a set of cyber security labs are developed. The labs are implemented in each learning environment and each student is given an identical

learning environment that includes multiple VMs. Students are able to use attack VM to initiate attacks and exploit system vulnerabilities on other students' defense VMs. In the meantime, students are also required to identify and patch vulnerabilities to protect their own defense VMs.

For each lab, a three-stage step-by-step process is designed to help students turn abstract concepts into actual skills to solve real-world problems and challenges. First, an overview is developed to introduce the attack technique (defense mechanism). Second, a quiz is developed at the end of each introduction. Students must demonstrate mastery of relevant attack (defense) knowledge by successfully scoring a minimum of 80% on a pseudo-adaptive quiz. Lastly, a detailed walkthrough of attack (defense) is developed to help students conduct hands-on activities.

This paper is organized as follows: Section 2 illustrates system infrastructure. Section 3 demonstrates the labs. We then discuss the three-stage learning process in Section 4. Finally, we conclude our work in the last section.

2 System Infrastructure

A virtual network infrastructure is configured as shown in Figure 1. It includes a set of identical students' learning environments and each provides the student with realistic experiences in an isolated environment for conducting cyber security experiments. This approach guarantees that all of the crafted malicious activities are confined inside the network. It also provides an isolation environment so no sensitive information can be released outside of this environment.

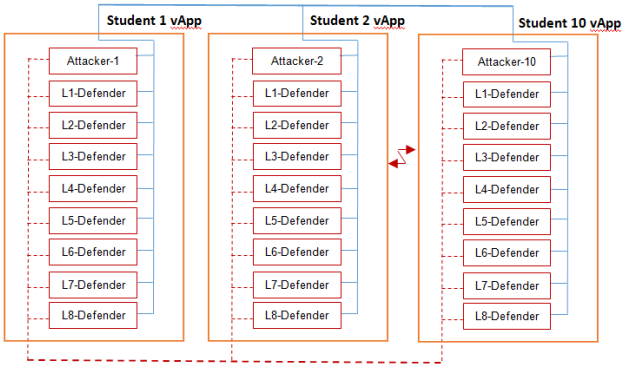

Figure 1: System Infrastructure

Virtualization technology is used to host multiple VMs in each student's learning environment. Each virtual application (vApp) is running VirtualBox hypervisor that contains a single Attack VM and Multiple Defense VMs (Defender 1-8). The Attack VM is the Kali Linux that equips students with a variety of penetration testing tools to initiate attacks and exploit system vulnerabilities on other students' defense VMs. Each defender is either a Windows Server or Linux machine that is configured specifically for its corresponding attack or defense lab.

3 Labs

Cyber attacks are launched every second every day worldwide. These attacks cover a broad spectrum of topics, such as DoS attacks, probe attacks, information gathering, system vulnerability assessment and exploitation, privilege escalation, and data stealing. According to the McAfee Labs report of 2017 Quarterly Threat, the top eight network attacks by type recorded from April to June 2017 are Browser Attacks (20%), Brute Force Attacks (20%), DoS Attacks (15%), Worm Attacks (13%), Malware Attacks (10%), Web Attacks (4%), Scan Attacks (4%), and Other Attacks (14%) [7].

It is impossible to introduce all of these cyber threats to students in a short period of time. Therefore, only the most important and current cyber security issues are discussed in this project. In total, eight-pair of attack/defense labs are developed. The labs include Remote Secure Login, DoS, SQL Injection, Patch Management, Honeypot, DHCP Starvation, Backdoor, and Web Defacement. For each lab, students will learn both theoretical knowledge as well as practice hands-on experiments that include the attack launch, exploit mitigation, and protection implementation.

3.1 Password Guessing Attacks

Password guessing attacks are at the top of the list of McAfee Labs Threat Report [7]. Password guessing (also known as password cracking) is a type of network attack in which an attacker attempts to recover user credentials through the process of attempting to log in repeatedly. The purpose of password guessing might be to help a user recover a forgotten password, to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily guessed passwords. There are various methods used to break into a password-protected system, such as brute force attack, dictionary attack, rainbow table attack, phishing, malware, offline cracking, shoulder surfing, and guessing. Once attackers have gained access to your website, they can use its files and the web host server to cause a wide variety of damage through malicious behavior, including: defacement, malware distribution, spamvertising, redirection, and stealing system resources.

In the attack lab, students use Nmap to scan the network to find potential attack targets (Linux VMs) and create a candidate password wordlist using Cupp. The student then performs a brute force dictionary attack using Hydra and retrieves sensitive information to create a second wordlist for guessing the root password. With the help of Metasploit framework and the previously created wordlist, the student is able to guess user's root password of the system, log in as the root user, and change the password. At the end of the lab, students would be able to achieve the following objectives:

- Use security scanner to enumerate target host and identify the listening Secure Socket Shell (SSH) service port on target host
- Use password profiler to generate a wordlist of candidate passwords
- Perform brute force attack to discover the root password on a target host and then login to change the password

The defense lab involves securing the Linux host and the OpenSSH service. The following objectives are expected to be achieved at the end of the lab.

- Edit the openSSH configuration file to restrict root user from logging in via SSH
- Add rules to the host iptables firewall, limit the amount of connections to the SSH service over a period of time, and temporarily block connections from any host that goes over the defined limit
- Create an Access Control List (ACL) for SSH using host firewall iptables

3.2 DoS Attacks

DoS attacks are third on the list of McAfee Labs Threat Report [7]. The attacks focus on disrupting services to prevent some or all legitimate requests from being fulfilled. Basically, DoS attacks are divided into two major categories: volume-based attacks and protocol-based attacks. Volume-based attacks send a large volume of traffic to saturate the bandwidth of the target in order to ensure the target becomes overloaded and ultimately, no longer able to respond to legitimate requests. The techniques include UDP floods, ICMP floods, and other spoofed-packet floods. Protocol-based attacks disrupt service by consuming all of the processing capacity of the target server or intermediate critical resources. The techniques include SYN floods, fragmented packet attacks, and Ping of Death. For example, on September 30, 2017, the UK National Lottery was attacked by DDoS [8]. The attack knocked the Lottery's website and its mobile app offline, which prevented many UK citizens from playing the Lottery.

Two labs have been developed to help students understand DoS attack. One is volume-based DoS attack to FTP server and the other is protocol-based DHCP starvation attack.

3.2.1 FTP Server DoS Attack

This attack involves sending a large amount of SYN packets to flood a File Transfer Protocol (FTP) server on a Windows Server and prevents legitimate users from gaining access to it. Hping3 in Kali Linux is used to launch the attack. The main objectives of this lab are:

- Scan the target network for possible vulnerabilities in the open ports
- Access the FTP server through an anonymous user account
- Bring down the FTP server after sending SYN flood packets

In the defense lab, specific measurements are needed to be set up in order to protect against the attack on the FTP server. Upon completion, the following objectives would be achieved:

- Configure Windows Server to turn on the firewall and change the default value on maximum connections to the FTP data
- Deactivate the anonymous user authentication to prevent unwanted access into the network
- Edit the Windows Server's registry to activate the SYN protect key against the SYN flooding attack

3.2.2 DHCP Starvation Attack

A DHCP starvation attack occurs when an attacker broadcasts a large number of Neighbor Solicitation packets with spoofed source MAC addresses to a DHCP server. When the legitimate DHCP server in the network starts responding to all these bogus DHCP request messages, available IP Addresses in the DHCP server scope will be depleted within a very short span of time.

In order to help students get familiar with IPv6, all of the IP addresses used in this lab employ IPv6 scheme. In the attack lab, atk-alive6 utility tool is used to send a flood of Neighbor Solicitation packets with spoofed MAC addresses to the DHCP server, bringing the Server down and denying legitimate access to the Server. The main objectives of the lab are:

- Use IPv6 Toolkit to check which hosts are live on the network
- Use network scanner to check the state of the ports
- Send Neighbor Solicitation packets to starve the address pool of the DHCP Server

In the defense lab, the native performance counter, Windows firewall with advanced security, and Wireshark are used to find a suitable disaster recovery solution to prevent the DHCP starvation attack. At the end of the lab, the following objectives would have been achieved:

- Use the Server Manager tool to analyze the CPU usage in the last 24 hours
- Use network analyzer to examine the source and destination addresses
- Write proper rules to prohibit illegitimate incoming IPv6 traffic

3.3 Web-Based Application Attacks

Web-based applications provide dynamic web pages for Internet users to access application servers via a web browser. The applications can be as simple as an email system or as complicated as an online banking system. In order to gain access to private information or system resources, hackers have used different techniques to breach the system's protection mechanisms, which include XSS, injection flaws, information leakage and improper error handling, broken authentication and session management, failure to restrict URL access, improper data validation, insecure communications, and malicious file execution [9]. Among them, XSS attacks and SQL injection attacks are the two most common forms, 39.1% and 24.9% of all attacks, respectively [7]. Therefore, labs are developed for those two types of attacks.

3.3.1 XXS Attack

Web defacement is a type of attack that changes the visual appearance of a website. The attack can be referred to as any unauthorized changes made to the appearance of either a single webpage, or an entire site. Sometimes, a website is completely taken down and replaced by something new. Hackers may inject code in order to add images, popups, or text to a page that were not previously present. For example, Taiwan's government websites were hit with over 20 million cyber attacks a month in 2017, 360 of which were successful and most involving a change of website [10].

XSS attacks are a type of injection, in which malicious scripts are injected into trusted websites. In the attack lab, the Persistent (Stored) XSS attack is used to post malicious codes in the comment box of a victim's website. Students are asked to add

"the website has been hacked" and to change the background color of the web page. At the end of the lab, students should be able to:

- Create a new user's account on a web page and inject malicious codes into the comment box
- Deface the webpage

The task of the defense lab is to set up appropriate defense mechanisms on the Linux MariaDB Server in order to prevent the XSS attack launched from the Kali Linux. Student should be able to achieve the objectives shown below upon completion of the lab:

- Set up the firewall iptables to filter unwanted packets from the network
- Sanitize the strings by filtering the input on the PHP login page
- Run malicious codes on the sanitized webpage to identify possible vulnerabilities

3.3.2 SQL Injection

SQL injection is an injection attack wherein the attackers inject a SQL query or malicious SQL statements into a web application's database server, which is also known as a Relational Database Management system. Once the exploitation is successful, the database data can be manipulated. For example, three hackers from the Surabaya Black Hat (SBH) group, were arrested by police in Surabaya, East Java in March 2018, because they hacked over 600 websites spread across 44 countries by using SQL injection method to destroy databases [11].

The attack lab exploits the MariaDB Server on a CentOS Linux, using the Kali Linux to modify and delete the existing information throughout the website. The main objectives of the lab are:

- Scan the network for possible vulnerabilities on the open ports
- Run a login bypass on the victim's web address
- Use SQL injection and database takeover tool to discover vulnerabilities and steal information from the database, e.g., passwords
- Use a syntax to replace the old password stolen from the database with a new password

The mission of the defense lab is to implement protection mechanisms on the MariaDB Server. In the end, students should be able to achieve the following objectives:

- Set up firewall iptables to filter unwanted packets from the network
- Sanitize the strings by filtering the input on the PHP login page
- Run a login bypass and check for potential weaknesses

3.4 Patch Management

Vulnerable services running on an Internet-connected host can present an attacker with a way inside the network. Automated tools known as vulnerability scanners are designed to discover open ports and scan for vulnerable services on network hosts. The attack task involves using the scanner OpenVAS to scan a Linux host to find any vulnerable services that could be used to gain access to the system. At the end of this lab, the following objectives are expected to be achieved:

- Use network mapper to discover running network services
- Use open vulnerability assessment system to scan for network vulnerabilities on a target computer
- Exploit a vulnerable service on the target computer to gain access and modify files

Patch management acquires, tests, and installs patches. Patches are used to fix the bugs of the software after the initial release, with many relating to security issues. These security flaws leave systems open to compromise and therefore, creating the possibility to be exploited. Other patches may address new security vulnerabilities, resolve software stability issues, or upgrade the software. In order to protect the system against attacks, the tasks of the defense lab include scanning a Linux host for vulnerable services and then patching found vulnerabilities. At the end of the lab, students should be able to achieve the following objectives:

- Use network mapper to discover running network services
- Use open vulnerability assessment system to scan for network vulnerabilities on the target computer
- Patch outdated and vulnerable services

3.5 Backdoor

The purpose of a backdoor is to access a system by negating normal authentication procedures. It allows attackers to establish a connection with the target system or network while evading detection. This means that the attacker can maintain an extended presence on the target or system network, allowing them ample time and opportunity to steal data and gain better insight into how the target communicates.

There are various techniques used by backdoors to enable attackers to gain command and control (C&C) of the target system or network, e.g., port binding: connect-back, connect availability use, legitimate platform abuse, common services protocol or file header abuse, protocol/port listening, custom DNS lookup use, and port reuse. These types of attacks are often directed against networks from multiple entry points. Sophisticated attackers can figure out how to bypass standard security measures and intrusion detection capabilities, so relying merely on firewalls and anti-malware solutions to mitigate backdoors is not enough **Error! Reference source not found.**. Understanding these techniques is vital for administrators to detect and mitigate backdoor attacks.

Labs are developed to help students understand the behavior of backdoor attacks. All of the activities are conducted using IPv6 addresses. The attack lab aims to install a persistent backdoor on a Windows Server using Metasploit Framework. The objectives of the lab are:

- Discover all live hosts on the network
- Use penetration testing tools to run a port scan and exploit the IPv6 auxiliary modules
- Create a persistent backdoor on a target host
- Retrieve files from the victim

In the defense lab, configurations are set up to ensure protection against EternalRomance exploit, which bypasses security over Server Message Block (SMB) file-sharing connections and then remotely executes instructions on Windows Operating Systems. At the end of the lab, students are expected to achieve the following objectives:

- Close unnecessary ports
- Set up firewall to block traffic on SMB over IP port

3.6 Honeypot

A honeypot can best be described as a decoy or trap designed to entice and attract intruders, keeping them from attempting to access other parts of the network and collecting information on their actions. Usually, the honeypot presents services or hosts data that appears to be a legitimate part of the network. Once the attackers access a honeypot, their actions are closely monitored to help the prevention of future attacks. In general, honeypots fall into one of three categories based on their characteristics: low Interaction honeypots, medium Interaction honeypots, and high Interaction honeypots. Low Interaction honeypots simulate services/vulnerabilities to collect information of attackers' activities but does not provide a usable system for attackers. Medium Interaction honeypots imitate a service and provides a controlled environment for the attacker to interact with. High Interaction honeypots simulate a production service or system and allow attackers free reign over the entire simulated system.

In the attack lab, a Cowrie Honeypot is configured; it looks and feels like an actual Linux Server in order to trick attackers. Cowrie is an open source honeypot that is designed as a medium interaction SSH and Telnet Honeypot. The major feature of the Cowrie Honeypot is that it is able to log the username/password information when login attempts are made. In the lab, Cowrie has been installed to be simply operational, which means no configurations have been changed. The major objectives include:

- Change the honeypot architecture information
- Customize honeypot files
- Create replica files in the honeypot file system

The defense lab builds the Cowrie Honeypot to log SSH connection attempts and record authenticated users' activities and commands. The following objectives would be achieved at the end of the lab:

- Install the prerequisite packages needed for the honeypot
- Install required python packages
- Move the listening port before creating the honeyport
- Configure the honeypot

4 Three-Stage Learning Process

Studies have suggested that cyber security curriculum in academic programs should be taught in an integrated fashion, which addresses both technical and theoretical issues [13][14]. Hence, each attack (defense) lab features a three-stage process (learning, assessment, and engagement) that not only delivers the principles and theory of cyber security, but also equips students with practical skills so they are able to apply their theoretical knowledge to real-world problems and challenges. The three-stage process is depicted in Figure 2. It outlines the logical links among three major stages when conducting a lab activity.

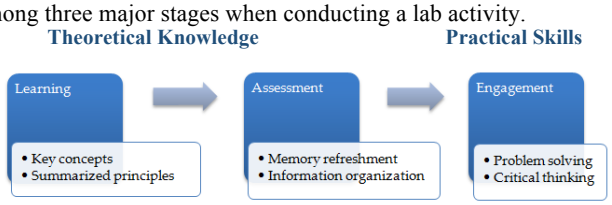

Figure 2: Three-stage learning process

The attack lab will lead students through an attack process. The relevant learning resources of a cyber threat are identified and described in detail in the first stage. This stage involves introducing students to the fundamental concepts, theories, and skills regarding a specific type of cyber attack and system vulnerability. Examples are presented to help students quickly acquire subject knowledge. For example, the introduction of DoS attacks includes the following questions with corresponding answers: What are DoS attacks? Is there a three-way handshake that establishes a connection between the attack host and target machine's destination port in the beginning of the attack? What are the attack techniques to launch DoS attacks and any countermeasures to the attacks? A section on port scanning attacks could include the following questions with answers: What are probing attacks? What is port scanning? What are the different types of port scanning? What are the legal implications? Figure 3 shows a partial introduction of the SQL injection attack lab.

SQL injection attack

SQL injection (SQLi) is an injection attack where the attackers injects a SQL query or malicious SQL statements in a web application's database server which is also known as a Relational Database Management system. Once the exploit of SQL injection is successful, the database can be manipulated. The hacker can modify, insert, update and delete the database data. The SQL injection is commonly applied in the PHP and ASP applications as a result of the functional interfaces. In a recent survey carried out on the 1599 WordPress plugin vulnerabilities in 2017, SQL injection attack was recorded to have 18.01% amongst the other vulnerabilities recorded hence making it the second most common vulnerability found in Word Press. (Wordfence, 2017). SQL Injection vulnerability could occur if the web application trusts the user's input without parameterizing it and using prepared statements. This is done by instructing the database that a certain part of the query should be executed while the rest is to be treated as the user's input. (Firewall, n.d.)

There are three ways in which SQL injection can be classified into and they are listed as follows:

In-band SQL Injection: This form of attack also known as the classic SQLi is one of the most commonly used SQL injection attack. The same transmission medium is used by the attacker to launch the attack and accumulate results (Muscat, 2017). The Inband class is used for data retrieval using the current communication channel between the target and the attackers. (Stampar, 2016). There are various types of In-band SQL injection, the most common types includes:

(i) **Error-Based SQLi**: This is a type of in-band SQL injection technique that depends on the error messages reported by the database server to collect information about the structure of the database. Whatever error message reported by the victim database server would be used to determine the structure of the database. "While errors are very useful during the development phase of a web application, they should be disabled on a live site, or logged to a file with restricted access instead". (Acunetix, n.d.). Examples of this form of attack includes using the following syntax:

Figure 3: Example of the first stage in the learning process

After reading the introduction, students move to the second stage where they must successfully pass a multi-question quiz in order to move on to next stage. The quiz is used to assess student learning with questions that are designed to reinforce important topics. The quiz will force students to refresh their memory and organize information that they have learned [15]. Figure 4 shows three questions of the password guessing defense lab.

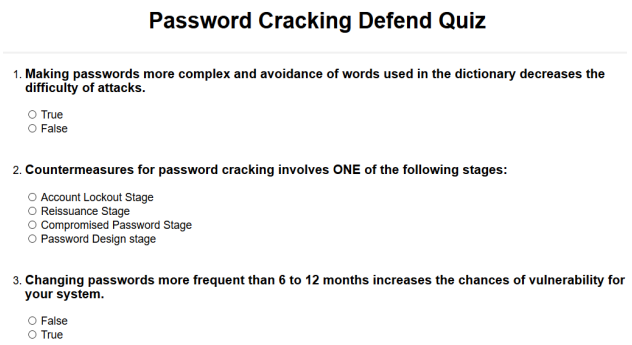

Figure 4: Example of the second stage in the learning process

Students are required to successfully pass the quiz with 80% or higher and then proceed to the exercise of launching the attack in the third stage. Detailed guidance in attacking is provided in this stage. Instructions are illustrated to show how to carry out the attack activities in a logical, step-by-step fashion. This practice will enable a deeper understanding of the subject and help students to develop broader experimental and problem solving skills [16]. Figure 5 shows the walkthrough of the password guessing defense lab.

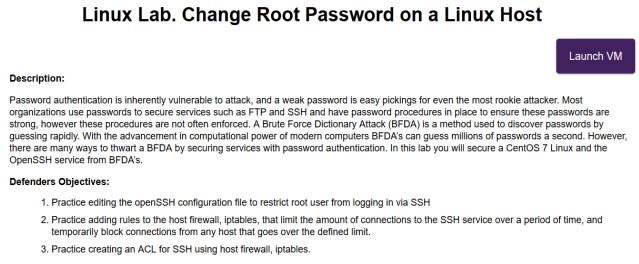

Figure 5: Example of the third stage in the learning process

The defense labs have a similar introduction and quiz components before starting the defense actions. Students are also required to successfully pass the quiz before proceeding to the instruction of mitigating the corresponding attack in the third stage. In this stage, students are required to implement proper security mechanisms to protect their systems.

5 Conclusions

This paper focuses on the discussion of eight labs that have been developed, which are Remote Secure Login, DoS, SQL Injection, Patch Management, Honeypot, DHCP Starvation, Backdoor, and Web Defacement. In order to help students get familiar with different operating systems, some of the labs are developed on Windows hosts and others are developed on Linux hosts. Also, both IPv4 and IPv6 address families are included in the labs. A three-stage, logical, step-by-step, process is designed to help students master lab contents. Each lab helps students become proficient in dealing with a certain cyber attack. With successful completion of all of the labs, students are able to advance their skills and understanding in the field of cyber security.

ACKNOWLEDGEMENTS

This research is based upon work supported by the Secure &Trustworthy Cyberspace (SaTC) Program of the National Science Foundation under Grant Number 1723650. The authors are grateful to the support of Department of Technology Systems in the College of Engineering and Technology at East Carolina University.

REFERENCES

[1] Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2017 (in million U.S. dollars). Retrieved from https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

[2] Armerding, T. 2018. The 17 biggest data breaches of the 21st century. Retrieved from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

[3] Fontana, F. 2018. Facebook Now Estimates 87 Million Users Could Have Had Data Improperly Shared. Retrieved from https://www.thestreet.com/story/14545679/1/facebook-87-million-users-had-data-improperly-shared.html

[4] Yoder, E. 2017. Federal court denies cash awards to 22 million OPM data theft victims. Retrieved from https://www.washingtonpost.com/news/powerpost/wp/2017/09/20/federal-court-denies-cash-awards-to-22-million-opm-data-theft-victims/?utm_term=.978916738452

[5] The New York Times. 2017. North Carolina County Refuses to Pay $23,000 Ransom to Hackers. Retrieved from https://www.nytimes.com/2017/12/06/us/mecklenburg-county-hackers.html

[6] Chalfant, M. 2017. Alabama county officials paid ransom for stolen data. Retrieved from http://thehill.com/policy/cybersecurity/352302-alabama-county-officials-pay-ransom-for-stolen-data-reports

[7] McAfee Labs. 2017. McAfee Labs Threat Report. Retrieved from https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-sept-2017.pdf

[8] Bisson, D. 2017. 5 Notable DDoS Attacks of 2017. Retrieved from https://www.tripwire.com/state-of-security/featured/5-notable-ddos-attacks-2017/

[9] Ramgonda, P. P. and Mudholkar, R. R. 2012. Cloud Market Cogitation and Techniques to Averting SQL Injection for University Cloud. International Journal of Computer Technology and Applications, 3(3), 1217-1224.

[10] Huang, T. T. 2018. Taiwan government websites hit with over 20 million cyber attacks a month, mostly from China, Taiwan News. Retrieved from https://www.taiwannews.com.tw/en/news/3398654

[11] Arresting Three Hackers, Police Trace Members of Surabaya Black Hat Hacker Group. 2018. Retrieved from http://www.en.netralnews.com/news/currentnews/read/19450/arresting.three.hackers..police.trace.members.of.surabaya.black.hat.hacker.group

[12] Trend Micro.2015. Backdoor attacks: How they work and how to protect against them. Retrieved from https://blog.trendmicro.com/backdoor-attacks-work-protect/

[13] Jarvis, D. 2013. Cybersecurity education for the next generation. IBM Center for Applied Insights.

[14] Report on EU practice for cybersecurity education. 2013. European Commission Tempus Project.

[15] Tewksbury, B. J. and Macdonald, R. H. Assessing Student Learning, Course Design Tutorial. Retrieved from http://serc.carleton.edu/NAGTWorkshops/coursedesign/tutorial/assessment.html (assessed June 2016)

[16] Redish, E. F. 2003. Teaching Physics with the Physics Suite, John Wiley & Sons, Inc.