A Game-Based Multiplayer System for Cyber Security Training and Awareness

Te-Shun Chou

Department of Technology Systems
College of Engineering and Technology
East Carolina University
Greenville, North Carolina

Abstract

This paper discusses a set of cyber security labs to help students learn the fundamentals of cyber security. Each lab included a combination of theoretical and practical knowledge education. The theoretical learning introduced the background and techniques of cyber security while the practical learning aspect helped students gain a deeper understanding through hands-on activities. In total, eight labs were designed to help students acquire knowledge and exercise skills. Each lab included two sub-labs: attack and defense. The attack labs led students to find system vulnerabilities and model the actions of attacks. The defense labs required students to identify and fix system vulnerabilities.

A system infrastructure was designed that included a number of identical and isolated learning environments. Virtual machines (VMs) were installed in each environment and served as tasks of both attack and defense. Each student owned his/her environment. In an attack sub-lab, students exploited vulnerabilities and launched attacks against other students' VMs. In a defense sub-lab, students implemented protection mechanisms on their VMs to prepare the best defense against cyber-attacks. This paper also describes system infrastructure.

1. Introduction

A huge number of cyber-attacks occur on a daily basis in this fast-evolving technological world with cybercrime becoming the greatest threat to individuals, private industries, and government agencies. Based on the report from Statista, in the first half of 2018 there were over 22 million records exposed in the United States alone [1]. Cybersecurity Ventures predicts globally cybercrime will cost in excess of $6 trillion annually by 2021 [2].

Computer systems and networks depend on well-trained professionals working in cybersecurity roles in order to adequately protect them from attacks. Cybersecurity knowledge and cyber skills training are vital in cybersecurity education. Hence, a set of CyberSec labs was developed to illustrate important offense and defense concepts of the cyber space. Each lab included a pair of cyber-attack and defense sub-labs and involved both cyber security theoretical learning and practical training. The theoretical learning helped students become familiar with the basis of cybersecurity skills and knowledge. The practical training enabled students to gain a deeper

understanding of cyber security through hands-on activities.

A system infrastructure was developed to mimic a network for students conducting the lab activities. The system was composed of ten identical learning environments that were implemented using virtualization technology. A graphic user interface (GUI) and multiple VMs were implemented in each learning environment. In addition, the system allows interaction among learning environments, therefore making it more similar to a realistic world network.

This paper is organized as follows: Section 2 introduces cyber security labs. Section 3 describes the GUI. The system infrastructure is then illustrated in Section 4. Finally, we conclude our work in the last section.

2. CyberSec Labs

According to the September 2017 quarterly threat report from McAfee Labs, network attacks by type recorded from April to June 2017 were classified into eight categories: browser attacks (20%), brute force attacks (20%), denial of service (DoS) attacks (15%), worm attacks (13%), malware attacks (10%), web attacks (4%), scan attacks (4%), and other attacks (14%) [3]. Table 1 shows examples of the attacks in these categories.

Table 1. Cyber attack categories

Category	Examples
Browser Attacks	Man-in-the-Browser and Clickjacking
Brute Force Attacks	Password Cracking
DoS Attacks	Distributed DoS, ICMP Flood, and Ping of Death
Worm Attacks	Email Worms, Instant Message Worms, Chat Room Worms, and WannaCry Ransomware
Malware Attacks	Viruses, Spyware, Adware, Trojan Horses, Phishing, Ransomware, Backdoor, and Malvertising
Web Attacks	Cross-Site Scripting (XSS), SQL Injection (SQLI), and Path Traversal
Scan Attacks	Port Scan, Network Scan, and Vulnerability Scan
Other Attacks	Physical Attacks, Insider Attacks, and Advanced Persistent Threats

Since there are so many different types of attacks, it is impossible to introduce all of them to students. Thus, only the most popular cyber security issues are investigated in this project. In total, eight-pairs of attack/defense labs were developed and all of the cyber-attack categories are covered.

- Browser attacks and scan categories: web defacement lab
- Brute force attacks and scan categories: remote secure login lab
- DoS attacks and scan categories: FTP server DoS lab
- worm and malware attacks categories: patch management and backdoor labs
- Web attacks and scan categories: SQLI lab

- Other attacks and scan categories: honeypot and secure plain text traffic labs

Kali Linux was used as the attack host in all of the eight labs. In order to help students become familiar with different operating systems (OSs), two labs (backdoor and FTP server DoS) used Windows OS and six labs (remote secure login, SQLI, patch management, honeypot, web defacement, and secure plain text traffic) used Linux OS as defense hosts. Also, both IPv4 and IPv6 address families were included, of which backdoor lab used IPv6 address schemes and the rest of labs used IPv4 address. Table 2 shows the tools used in the labs.

Table 2. Tools used

Remote Secure Login • Attack: Metasploit framework, netdiscover, nmap, cup, and hydra • Defense: OpenSSH, ACL, and iptables
Web Defacement • Attack: nmap and XSS scripts • Defense: iptables and PHP
SQLI • Attack: nmap, dirbuster, and sqlmap • Defense: iptables and PHP
Patch Management • Attack: Metasploit framework, nmap, and OpenVAS • Defense: nmap, OpenVAS, and yum
Honeypot • Attack: nmap and SSH • Defense: nmap, SSH, and cowrie
Secure Plain Text Traffic • Attack: Wireshark • Defense: vsftpd.conf
FTP Server DoS • Attack: nmap and hping3 • Defense: Windows firewall, server manager, and Windows registry
Backdoor • Attack: Metasploit framework, and atkalive6 • Defense: Server manager

2.1. Remote Secure Login lab

Password authentication is inherently vulnerable to attack, and a weak password is easy pickings for even the most rookie attacker. Most organizations use passwords to secure services, such as FTP and SSH, and have password procedures in place to ensure these passwords are strong; however, these procedures are not often enforced. A brute force dictionary attack (BFDA) is a method used to discover passwords by guessing rapidly.

In the attack lab, students scanned the network for the target host and created a candidate password wordlist. Then, a BFDA was performed to create a second wordlist to guess roots password and login as the root user to change the root user's password. In the defense lab, students configured secure services and created ACL on firewall to limit the amount of connections and block connections from any host that goes over the defined threshold.

2.2.Web Defacement lab

Web defacement is a type of attack that changes the visual appearance of a website. It can also 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. In other instances, hackers may inject code in order to add images, popups, or text to a page that were not previously present.

In the attack lab, students used the Persistent XSS attack to post malicious codes in the comment box of a victim website to add text and change the background color of the web page. In the defense lab, Students configured the web server in order to filter unwanted packets from the network.

2.3. FTP Server DoS Lab

A DoS attack is a kind of attack that occurs when an attacker floods web applications or servers and prevents legitimate users from gaining access to targeted computer systems, devices, or other network resources. The attack overwhelms the victim resources, including servers, systems or networks by using numerous traffic to make them difficult to recover from, thus rendering them impossible for legitimate users to use.

In the attack lab, students used a large amount of packets to cripple the FTP server on a victim's Windows Server VM. In the defense lab, students practiced deactivating the anonymous user authentication as well as editing the registry of the server to activate the SYN protect key against SYN flooding attack.

2.4. Patch Management Lab

Patch management, at its core, is a system that helps administrators recognize when patches are released, confirm what systems are affected, how to test them, and finally, where and when to apply them as quickly as possible. Many zero-day attacks rely on the hope that the target is unpatched, rendering patch management one of the most powerful defenses against attacks for systems administrator [4].

In the attack lab, students scanned a CentOS Linux host for vulnerable services and exploited weaknesses in order to gain access to the computer. In the defense lab, students used a scanning tool to discover network vulnerabilities and patch outdated and vulnerable services.

2.5. Backdoor Lab

Backdoors allow attackers to establish a connection with a target system or network while evading detection. This means that an attacker can maintain an extended presence on the target network or system network, allowing them ample time and opportunity to steal data and gain better insight into how the target network systems communicate [5]. 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. Therefore, relying merely on firewalls and anti-malware solutions to mitigate backdoors is not enough to prevent these types of attacks. In order to be effective, networks must be monitored for all abnormal activity [6].

In the attack lab, students aimed to target a Windows server VM and install a persistent backdoor after exploitation. In the defense lab, configurations were properly set up to ensure protection against bypasses over server message block (SMB) file-sharing connections.

2.6. SQLI Lab

SQLI is an injection attack where the attacker injects a SQL query or malicious SQL statements in a web application's database server, also known as a relational database management system. Once the exploit of SQLI is successful, the database can be manipulated. The hacker is able to modify, insert, update and delete the database data. The SQLI is commonly applied in the PHP and ASP applications as a result of the functional interfaces.

In the attack lab, students scanned the network for possible vulnerabilities in the open ports and ran a login bypass to the host to steal information from the database. In the defense lab, students checked for vulnerabilities and set up the firewall to filter unwanted packets from the network.

2.7. Honeypot Lab

A honeypot is designed as a decoy or trap to entice and attract intruders, preventing them from accessing other parts of the network and collecting information on their actions [7]. Usually, the honeypot presents services or hosts data that appears to be a legitimate part of the network – an attractive target to attackers. Once an attacker accesses a honeypot, their actions are closely monitored, which allows their intentions to be discerned and helps to potentially prevent future attacks [8].

In the attack lab, students accessed a remote computer and determined if they have found a real machine or a honeypot. In the defense lab, students configured an open source honeypot to make it look and feel like a real CentOS server.

2.8. Secure Plain Text Traffic Lab

Packet sniffing attack captures network traffic at the ethernet frame level and analyzes the data to extract sensitive information [9]. During the extraction process, any data that are not encrypted are readable. Some of the protocols vulnerable to sniffing include HTTP (hypertext transfer

protocol), where data is sent in clear text; Telnet and Rlogin, which comprises of usernames and passwords; POP (post office protocol) and IMAP (internet message access protocol), which access email from the mail server with usernames and passwords; SMTP (simple mail transfer protocol), which uses mail servers to transfer email; and FTP (file transfer protocol), which transfers files between two hosts. Clear text protocols do not encrypt data while communicating. In order to secure clear text communication, the following should be considered.

In the attack lab, students captured network packets and used them to determine the credentials needed to access an FTP server. In the defense lab, students modified the configuration of the FTP server to only allow secure connections using SSL.

3. GUI

In order to make the labs more manageable and to maximize the effectiveness of navigational instructions, a GUI was designed, as shown in Figure 1. The GUI was composed of eight CyberSec activities and each included a pair of attack and defense buttons. Each defense button was mapped to the attack button, i.e., a defense mechanism was implemented to its corresponding attack.

Each button featured a series of actions that require students to complete their attack/defense work. The button led students through a three-stage learning process: Introduction, Quiz, and Instruction. First, an overview is displayed to introduce the attack technique (defense mechanism). Second, a quiz is shown 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 exhibited to help students conduct hands-on activities.

The learning process acted as a learning development for students to raise their level of knowledge pertaining to a certain task. By successfully completing all of the labs, students adequately advanced their skills and understanding in the field of cyber security.

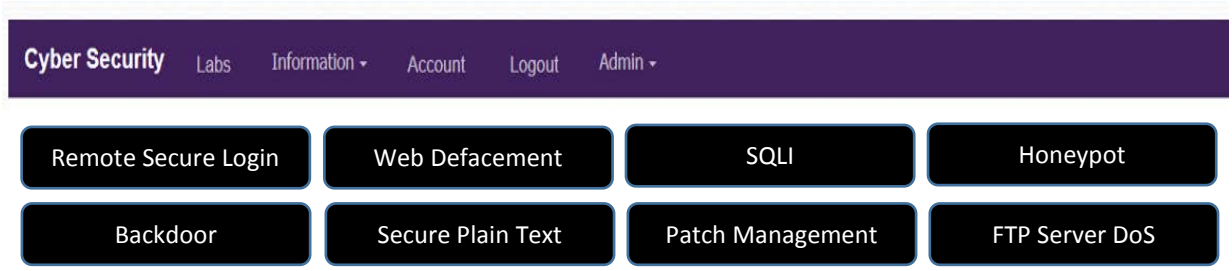

Figure. 1. GUI

4. System Infrastructure

A system infrastructure was configured to support the cyber security learning activities. It was an isolated environment that guaranteed all of the activities are confined within the infrastructure. It also ensured that no sensitive information could be released to the outside of this environment. Figure 2 shows the infrastructure.

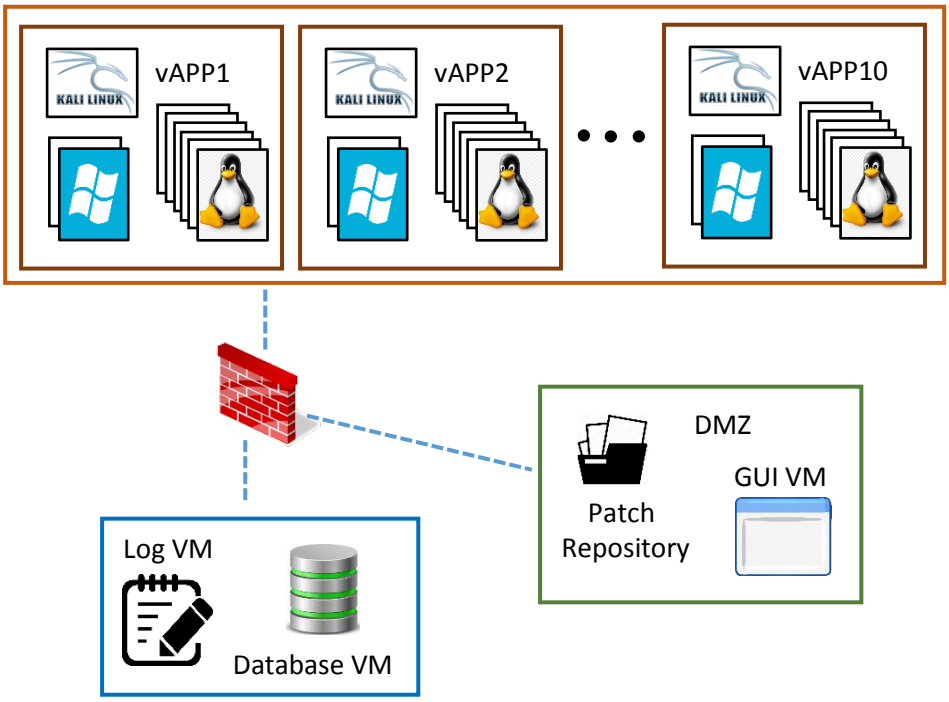

Fig. 2. System infrastructure

The infrastructure was consisted of ten identical learning environments with each student owning a single learning environment. Virtualization technology was used to host multiple VMs in each learning environment. Each virtual application (vApp) was running VirtualBox hypervisor that contained eight VMs, with one being used as the attacker and eight as the defenders. The attack VM equipped a variety of penetration testing tools for students to initiate attacks and exploit system vulnerabilities on other students' defense VMs. Each defense VM was either a Windows server or CentOS Linux that was configured specifically for its corresponding attack or defense lab.

The infrastructure emulated a realistic physical network that allowed ten students to conduct the CyberSec activities simultaneously and those learning environments were able to communicate with each other. In order to encourage students to interact with each other, a score and message board was designed to display the points students achieved. The student gained one-thousand positive points when s/he successfully attacked someone's VM or configured his/her own defense VM; on the contrary, the student got negative one-thousand points when s/he did not prevent an attack from others or failed to configure his/her own defense VM. During the competition, instant messages showing the real-time statuses of the attack/defense were displayed on the board. In addition, students gained ten points of each question when successfully passing a minimum of 80% on a quiz.

In order to display correct scores and messages on the board, the activities by students were monitored and automatically recorded to the Log VM and parsed to the Database VM for the GUI VM to display. Scripts were written to detect changes of the VMs located in each learning environment.

5. Conclusions

This paper described an interactive cyber-attack and defense system infrastructure. The infrastructure emulated a physical network that included a number of identical student learning environments. Attack and defense VMs were implemented in each student's learning environment. The interaction between attack and defense strategies was studied by allowing each student to act as both attacker and defender. From the perspective of the attacker, students were able to perform hacking activities to other class members. From the defender's point of view, students were required to identify system vulnerabilities and fix the weaknesses accordingly. Eight pairs of attack and defense labs were developed, and each used a three-stage learning process to help students transform abstract concepts into practical skills to solve real-world problems and challenges. In the future, increasingly complicated cyber security learning environments, along with more labs, could be developed.

Acknowledgments

This research is based upon work supported by the Secure &Trustworthy Cyberspace 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] Statista, "Cyber crime: Number of breaches and records exposed 2005-2018," 2018. [Online]. Available: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[2] Herjavec Group, "The 2019 official annual cybercrime report," 2020. [Online]. Available: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/?utm_source=twitter&utm_medium=social&utm_campaign=2019cybercrimereport.

[3] McAfee Labs, "Threat Report," 2017. [Online]. Available: https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-sept-2017.pdf.

[4] K. Rankin, "Sysadmin 101: Patch management," 2017. [Online]. Available: https://www.linuxjournal.com/content/sysadmin-101-patch-management

[5] Incapsula, "Backdoor attacks," 2018. [Online]. Available: https://www.incapsula.com/web-application-security/backdoor-shell-attack.html

[6] Trend Micro, "Backdoor attacks: How they work and how to protect against them," 2015. [Online]. Available: https://blog.trendmicro.com/backdoor-attacks-work-protect/

[7] E. Cole, and S. Northcutt, "Honeypots: A security manager's guide to honeypots," n.d. [Online]. Available: https://www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide.

[8] J. Riden, and C. Seifert, "A guide to different kinds of honeypots," 2008.[Online]. Available: https://www.symantec.com/connect/articles/guide-different-kinds-honeypots.

[9] E. Tetz, "Common network attack strategies: Packet sniffing," n.d. [Online]. Available: https://www.dummies.com/programming/networking/cisco/common-network-attack-strategies-packet-sniffing/

Biographical Information

TE-SHUN CHOU is an associate professor in the Department of Technology Systems at ECU. He received his bachelor's degree in Electronics Engineering at Feng Chia University and both master's degree and doctoral degree in Electrical Engineering at Florida International University. He serves as the program coordinator of the master's program in Network Technology for the Department of Technology Systems and the lead faculty of Digital Communication Systems concentration for the Consortium Universities of the PhD in Technology Management. He is also the point of contact of ECU National Centers of Academic Excellence in Cyber Defense Education. Dr. Chou teaches IT-related courses, which include network security, network intrusion detection and prevention, wireless communications, and network management. His research interests include machine learning, wireless communications, technology education, and information security, especially in the field of intrusion detection and incident response.