An Interactive Learning System for Cyber Security Education

Te-Shun Chou
Department of Technology Systems
College of Engineering and Technology
East Carolina University

Abstract

This paper describes a learning system that uses virtualization technology to build a multiplayer cyber-attack and defense learning system infrastructure. The infrastructure emulated a realistic network that included numerous student network environments. Virtual machines were implemented in each student's network environment and they served as both attack and defense. In addition, the system infrastructure allowed interaction among students' network environments, therefore making it more similar to a realistic world network.

The learning system functioned as a competition environment to encourage students to interact with each other. Each student acted as both attacker and defender. From the perspective of the attacker, students were able to perform hacking activities to other class members. Students were required to identify other students' system vulnerabilities and model the actions of the attacks. From the defender's point of view, students needed to apply a certain technique to prevent the corresponding attacks. The system allowed students access to the infrastructure anytime and anywhere. The system provided students with opportunities to learn cyberattack and prevention techniques in a simulation environment.

1. Introduction

The innovation of technology continues to proceed with a fast pace over the past years. Meanwhile, the scale and sophistication of cyber-attacks are also advancing at a worrisome pace against individuals, governments, and companies. According to the report from the Council of Economic Advisers in White House, malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 [1]. Hence, America needs well-trained professionals working in cyber security roles to protect critical infrastructures from attacks, thus making cyber security education increasingly important and urgent.

Cyber security education is responsible for delivering the theoretical knowledge across different topics as well as preparing students with practical skills to apply what they have learnt in the real world. In general, lecture is the most effective method to convey fundamentals, theories, and technologies to students. To tackle the second goal, a network environment is usually prepared that allows students to practice what they have learnt in classes [2-4]. With the usage of those learning environments, students are able to apply their knowledge and skills to real world cyber security problems, however, most of the cyber security lab environments are designed for learning either defense mechanism or attack techniques. Also, the majority of lab environments limit students' activities in their own environments, which lack interactions with each other.

Hence, we built an interactive cyber-attack and defense competition infrastructure. In order to facilitate students' learning of theoretical knowledge and practice of hands-on activities, eight pairs of attack/defense labs are developed. During the competition, each student is given an identical lab environment that includes both attack and defense VMs. The attack VM is equipped with a variety of penetration testing tools for students to initiate attacks and exploit system vulnerabilities on other students' defense VMs. In order to defend against the attacks, students are required to identify and patch vulnerabilities to protect their own defense VMs.

This paper is organized as follows: Section 2 discusses cyber security competitions. Section 3 illustrates the methodology. We then demonstrate the labs in Section 4 and automated score and message board in Section 5. Finally, we conclude our work in the last section.

2. Cyber Security Competitions

Cyber security competition is a popular way to train and inspire future cyber security professionals. Through a series of cyber security activities, interest in cyber security in young individuals could be promoted. There are many local, state, regional, national, and international competitions today and the format of the competitions is either face-to-face, virtual, or a combination of both. In general, the competitions can be classified into four categories: network defense competitions, computer forensics competitions, penetration testing competitions, and capture the flag (CTF) competitions.

Network defense competition is focused on operational tasks and administrative duties for an existing commercial network. Teams are assessed based on their ability to detect and respond to outside threats, maintain availability of existing services, such as mail servers and web servers. Other tasks also include business request responses, such as the addition or removal of services, and balance security needs against business needs. National Collegiate Cyber Defense Competition [5] and AFA CyberPatriot [6] are examples of this type of competition.

Computer forensics competition requires teams to identify and analyze electronic evidence in order to recognize how many of cyber-crimes have taken place. The challenges tests include stenography, data carving, data recovery, malicious software detection, network analysis, mobile forensics, live system forensics, steganography, file carving. Examples of such competition are Digital Forensics & Incident Response Challenge [7] and RED [8].

Penetration testing competition needs participating teams to use their technical knowledge and skills to identify weaknesses of computer systems. In addition, the competition asks teams to present their findings and offer suggestions for mitigating risks in critical security vulnerabilities. Examples are Collegiate Penetration Testing Competition [9] and Global CyberLympics Security Competition [10].

There are two major types of CTF competitions: jeopardy and attack-defense. In a jeopardy CTF, teams get points according to the number of cyber security challenges completed. The challenges typically include web, forensic, crypto, binary, reverse engineering, mobile security, internet of thing, secure programming. DEF CON CTF Qualifier [11] is this type of CTF

competition. In an attack-defense CTF competition, every team has its own servers with vulnerable services. To get attack points, teams must hack other teams' services. In the meantime, teams keep their services up and running in order to get defense points. The example of such CTF competitions is DEF CON CTF [12].

3. Methodology

Cyber security competitions have become a popular way to promote education in cyber security and to inspire future cyber security professionals. However, three major problems might arise in current cyber security competitions. First, individuals/teams are assessed based on their existing technical knowledge and skills, but competitions do not provide any training to those participants. Second, most of the competitions only allow participants to conduct activities in their own environments, which lack interaction with other participants. Lastly, most of the competitions are limited to either cyber-attack or cyber defense activities.

However, cyber security education should not only be limited to either implementing defense mechanisms or practicing attack techniques; and both defense and offense are equally important. With the understanding of attackers' behavior, a good defense strategy can therefore be deployed. Twenty-five hundred years ago, Sun Tzu stated the same principle in The Art of War: "Know the enemy and know yourself; in a hundred battles you will never be in peril." Therefore, we created a system infrastructure, Figure 1, that allows students to act not only as a defender but also as an attacker. From the perspective of an attacker, students are able to identify other students' system vulnerabilities and model the actions of the attacks. From the defender's point of view, students need to evaluate potential risks to the system's security, discover the weak points, and then fix the vulnerabilities accordingly.

3.1.System Infrastructure

The system infrastructure is a cyber security education platform. It is an isolated environment that enables students to conduct cyber security activities. This approach guarantees that all of the cyber security activities are confined within the infrastructure. It also ensures that no sensitive information can be released to the outside of this environment. The infrastructure is open to students 24/7. The student may access the system multiple times and perform cyber security activities at his or her own pace. The system is secure and available over the Internet. This personalized learning experience is a student-centric approach which allows the student to be an active participant in the learning process, instead of passively absorbing information from lectures. This self-guided approach makes learning enjoyable and is effective in improving student learning and understanding [13,14].

The infrastructure is consisted of multiple identical leaning environments and each student owns a learning environment. The infrastructure emulates a realistic physical network that allows those learning environments inside of it the ability to communicate with each other. Virtualization technology is used to host multiple VMs in each student's environment to practice cyber-attack and defense skills. 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.

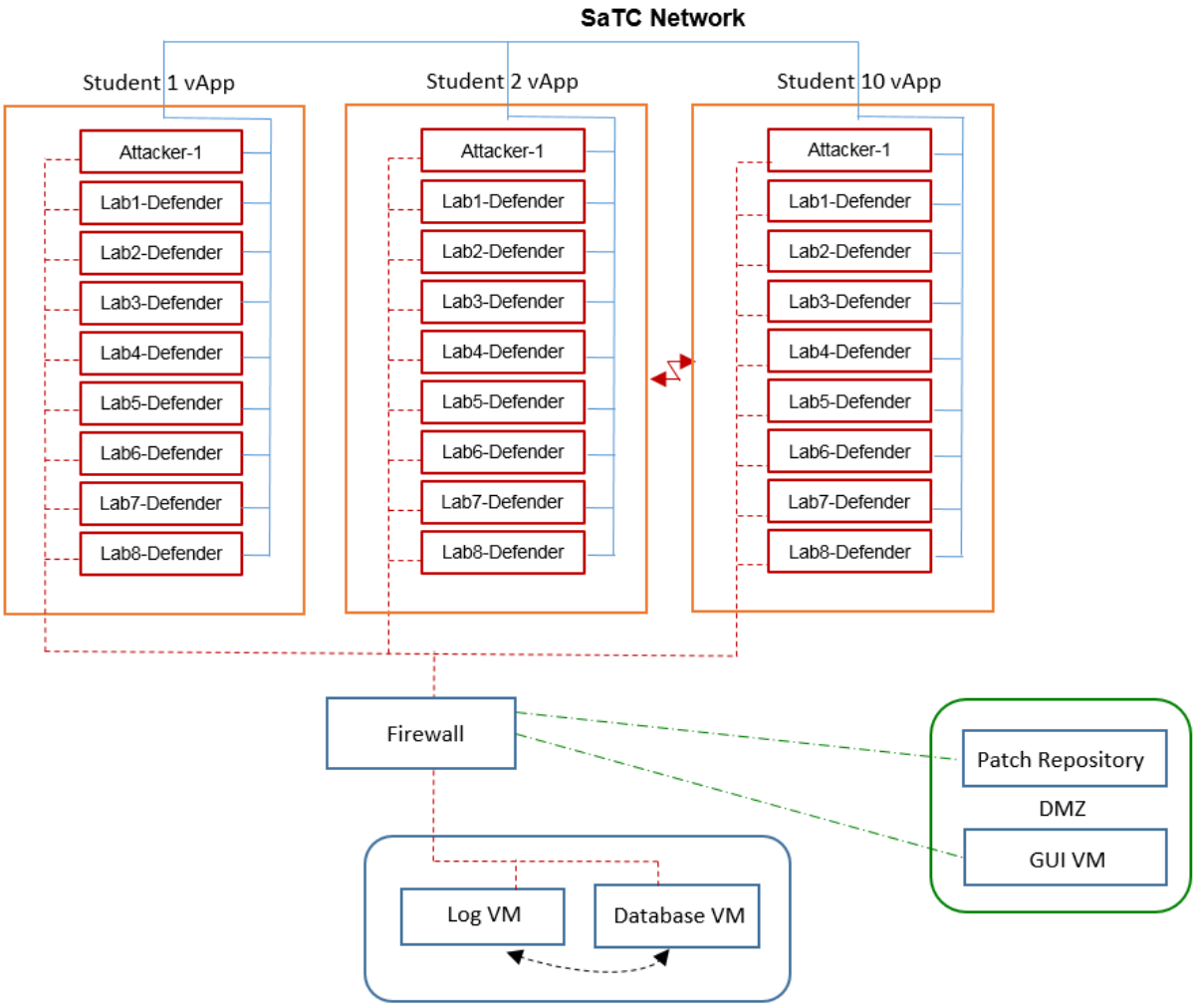

Figure 1. System infrastructure

3.2. Automatic Score and Message Board

In order to encourage students to actively interact with each other, a Score and Message Board, Figure 2, is under development to display the results of the competition amongst the students. The student who successfully launches an attack will gain ten-points; on the contrary, the student who does not successfully implement a mechanism to prevent the corresponding attack will lose ten-points. The total points students obtain will be displayed on students' Boards.

A set of scripts is installed within defense VMs. The scripts continuously check for current configurations of defense VMs and store them into log VM in order to determine if the defense VM has been compromised or properly configured. During the competition, GUI VM retrieves log data and then displays messages on Score and Message Board. The message shows whether

the attack and prevention were successful or not. Proper action should be immediately taken when the message shows an attack is happening. The student should implement the defense mechanism against that attack at once because s/he will keep losing points if other students launch the same attacks.

Name	Score	Message
Lisa	+90	You have successfully cracked the root password of 10.0.2.15.
Alexander	+50	You have successfully configured your DHCP server.
David	+10	You have successfully inject malicious code to home page of 10.0.2.10.
Michael	-30	Your Web server is under attack.
Nicholas	-50	Your FTP server has been compromised.

Figure 2. Score and Message Board

3.3. Graphic user interface (GUI)

A graphic user interface (GUI) application is designed for each student to log into his/her learning environment. The main menu of the application includes a set of InfoSec activities and each includes two labs: attack and defense. Each lab features a series of actions that require students to complete their attack (defense) task. Each defense lab in an InfoSec activity is mapped to one attack lab, i.e., a defense mechanism should be implemented to its corresponding attack. The application provides links to help students perform the necessary lab activities. Figure 3 shows the GUI application.

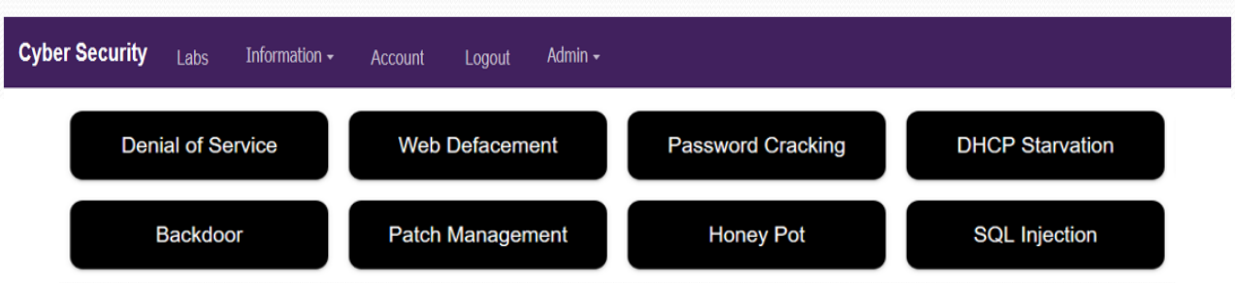

Figure 3. GUI application

3.4. InfoSec Activities

Cyber-attacks are becoming increasingly widespread and occur every single day worldwide. There are several types of attacks, such as denial of service (DoS) attacks, probe attacks, information gathering, system vulnerability assessment and exploitation, privilege escalation, and data stealing. The McAfee Labs report of 2017 Quarterly Threat recorded that the top eight network attacks by type from April to June 2017 were 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%) **Error! Reference source not found.**.

Based on the complex nature of these attacks, it would be unrealistic to fully cover each of these attacks in a short period of time. In order to give students a comprehensive basis of cyber-attacks in general, only the most relevant and current cyber security attacks are discussed in this project. In total, eight InfoSec activities are developed and each includes a pair of attack and defense labs. Table 1 shows the activities. During each lab, students are required to learn theoretical knowledge as well as apply their knowledge to hands-on experiments, which include attack generation, exploit mitigation, and protection implementation.

Table 1. InfoSec Activities

Remote Secure Login
• IP address: IPv4
• Attacker
  o Host: Kali Linux
  o Goal: Perform brute force attack and log in to change the password
  o Tools: Metasploit framework, netdiscover, nmap, cup, and hydra
• Defender
  o Goal: Secure the host and the OpenSSH service
  o Host: CentOS Linux
  o Tools: OpenSSH, ACL, and iptables

SQL Injection
• IP address: IPv4
• Attacker
  o Host: Kali Linux
  o Goal: Modify and delete the existing information throughout the website
  o Tools: nmap, dirbuster, and sqlmap
• Defender
  o Goal: Implement protection mechanisms on the MariaDB Server
  o Host: CentOS Linux
  o Tools: iptables and PHP

Web Defacement
• IP address: IPv4
• Attacker
  o Host: Kali Linux
  o Goal: Use cross site scripting attack to inject malicious codes into the comment box to deface the webpage
  o Tools: nmap and XSS scripts
• Defender
  o Goal: Set up appropriate defense mechanisms on the Linux MariaDB Server
  o Host: CentOS Linux
  o Tools: iptables and PHP

Patch Management • IP address: IPv4 • Attacker   o Host: Kali Linux

- Goal: Scan the host to find vulnerable services
- Tools: Metasploit framework, nmap, and OpenVAS

- Defender
  - Goal: Patch outdated and vulnerable services
  - Host: CentOS Linux
  - Tools: nmap, OpenVAS, and yum

Honeypot

- IP address: IPv4
- Attacker
  - Host: Kali Linux
  - Goal: Change the honeypot architecture information
  - Tools: nmap and SSH
- Defender
  - Goal: Configure the honeypot and install packages needed for the honeypot
  - Host: CentOS Linux
  - Tools: nmap, SSH, and cowrie

FTP Server DoS Attack

- IP address: IPv4
- Attacker
  - Host: Kali Linux
  - Goal: Flood the FTP Server and prevent legitimate users from gaining access to it
  - Tools: nmap and hping3
- Defender
  - Goal: Configure firewall and other parameters to protect against the attack
  - Host: Windows Server
  - Tools: Windows Firewall, Server Manager, and Windows Registry

DHCP Starvation

- IP address: IPv6
- Attacker
  - Host: Kali Linux
  - Goal: Send Neighbor Solicitation packets to starve the address pool of the DHCP Server
  - Tools: nmap, atkalive6, and atk-flood_dhcp6
- Defender
  - Goal: Use the Server Manager tool to analyze the CPU usage and write rules to prohibit illegitimate incoming traffic
  - Host: Windows Server
  - Tools: Server Manager and Wireshark

Backdoor

- IP address: IPv6
- Attacker
  - Host: Kali Linux
  - Goal: Install a persistent backdoor and retrieve files from the victim
  - Tools: Metasploit framework, and atkalive6

- Defender
  - Goal: Ensure protection of Server Message Block (SMB) file-sharing connections
  - Host: Windows Server
  - Tools: Server Manager

3.5. Three-Sage Learning Process

The attack lab will lead students through an attack process. A three-stage learning process is designed to lead students through a certain type of attack process. Students are required to read an introduction of the attack, pass a quiz, and then move on to the attack instruction. The introduction includes all the background information of the cyber-attack in order to help students acquire enough knowledge of the attack. After reading the introduction, students will need to successfully pass a five-question quiz in order to move on to next stage. The introduction and quiz must be followed through in that order. The quiz is used to verify the level of student comprehension of the material. Having successfully passed the quiz, detailed instructions will be available to guide students through the necessary procedures for launching the attack. The three-stage learning process is also applied to the defense lab. Students are required to successfully pass the quiz and then proceed to the instruction of mitigating the corresponding attack.

4. Conclusions

This research focuses on building an interactive cyber-attack and defense learning infrastructure. The infrastructure emulates a physical network that includes numerous student network environments. Attack and defense VMs are implemented in each student's network environment. The interaction between attack and defense strategies is studied. Each student is allowed to act as both attacker and defender. From the perspective of the attacker, students are able to perform hacking activities to other class members. From the defender's point of view, students need to identify system vulnerabilities and fix the weaknesses accordingly. Eight pair of attack and defense labs are developed and each uses a three-stage learning process to help students turn abstract concepts into actual skills to solve real-world problems and challenges. In the future, increasingly complicated environments, along with more labs could be developed.

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. The Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
2. Thompson, M. F. and Irvine, C. E. 2018. Individualizing Cybersecurity Lab Exercises with Labtainers. IEEE Security & Privacy, 16(2), 91-95.
3. Mahadev, N. 2017. Building a Secure Hacking Lab in a Small University. Proceedings of the 2017 ACM Conference on Innovation and Technology in Computer Science Education, Bologna, Italy.
4. Han, D., Yang, J., and Wayne S. 2017. Inject Stenography into Cybersecurity Education. 2017 31st International Conference on Advanced Information Networking and Applications Workshops, Taipei, Taiwan.
5. National Collegiate Cyber Defense Competition. Retrieved from https://www.nationalccdc.org/
6. AFA CyberPatriot. Retrieved from https://www.uscyberpatriot.org/
7. Digital Forensics & Incident Response Challenge. Retrieved from https://digital-forensics.sans.org/community/challenges
8. RED. Retrieved from https://csaw.engineering.nyu.edu/RED
9. Collegiate Penetration Testing Competition. Retrieved from https://nationalcptc.org/
10. Global CyberLympics Security Competition. Retrieved from https://www.cyberlympics.org/
11. DEF CON CTF Qualifier. Retrieved from https://ctftime.org/ctf/1
12. DEF CON CTF. Retrieved from https://ctftime.org/ctf/2/
13. Hightower, A. M., Delgado, R. C., Lloyd, S. C., Wittenstein, R., Sellers, K., and Swanson, C. B. 2011. Improving Student Learning by Supporting Quality Teaching: Key Issues, Effective Strategies. Editorial Projects in Education Inc. Retrieved from http://www.edweek.org/media/eperc_qualityteaching_12.11.pdf
14. Froyd, J. and Simpson, N. 2008. Student-centered learning addressing faculty questions about student centered learning. Course, Curriculum, Labor, and Improvement Conference, Washington DC,

Biography

TE-SHUN CHOU is an Associate Professor in the Department of Technology Systems at East Carolina University. He received his Bachelor 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 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 Ph.D. in Technology Management. He is also the point of contact of ECU National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE). 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.