An Infrastructure Supporting a Game-Based Learning System for Information Security Topics

John Jones
College of Engineering and Technology
East Carolina University

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

Abstract

Recent research shows that game-based competition motivates learners more effectively than previous methods. [1] This paper describes the design of the infrastructure and discusses the reasoning behind the decisions made in the process of to create a game-based learning system for information security topics. This paper also discusses the sophisticated virtual networking and security implementation required to tie all the parts of the gaming system together.

1. Introduction

The best way to teach the concepts of information security requires utilizing game-based competition. Game-based competition is used to motivate learners to stay engaged on a task for a period of time. [1] A game-based approach for teaching information security topics required many operating systems, such as Windows desktops, Windows Server and Linux operating systems, and needed a diverse setup and configurations with these operating systems. To reduce complexity for the learners and provide the best pedagogical outcomes, pre-setup systems needed to be at the ready. Our research covered the best infrastructure design to support a game-based learning system for information security topics.

After meeting with various faculty members in the Technology Systems department at East Carolina University, a decision was made on the best operating systems to be utilized for the learning experience. The following operating systems needed to be included, Kali Linux, Windows 10, Windows Server 2016, and Ubuntu Linux. Kali Linux served as the attacking host, while all the other listed OSes served as defenders. Once selected, the difficult task of designing the infrastructure to support the environment was next. It is instrumental to the game-based approach to host a live session where all the players would be challenged head-to-head in a competition, with a running scoreboard keeping track of all participants. Ultimately, it was decided that each participant would need to have eight defender VMs and one attacker VM, for a total of nine VMs each, and support up to twenty participants. Having approximately 200 VMs in a single environment required significant fore-thought and an equally significant computing infrastructure and setup.

This paper is structured as follows: section 2.1 covered security concerns, section 2.2 discussed the infrastructure design, section 2.3 detailed the virtual server setup, section 2.4 discusses the demilitarized zone setup, and section 3 concluded the paper.

2. Methodology

The system infrastructure was configured to support a cyber security education platform. It is an isolated environment that enabled participants to conduct cyber security activities. This approach guaranteed that all of the cyber security activities are confined within the infrastructure. It also ensured that no sensitive information could be released to the outside of this environment. Figure 1 shows the infrastructure. The infrastructure is consisted of multiple identical leaning environments and each participant owned a single learning environment. The infrastructure emulates a realistic physical network that allowed those learning environments inside of it the ability to communicate with each other.

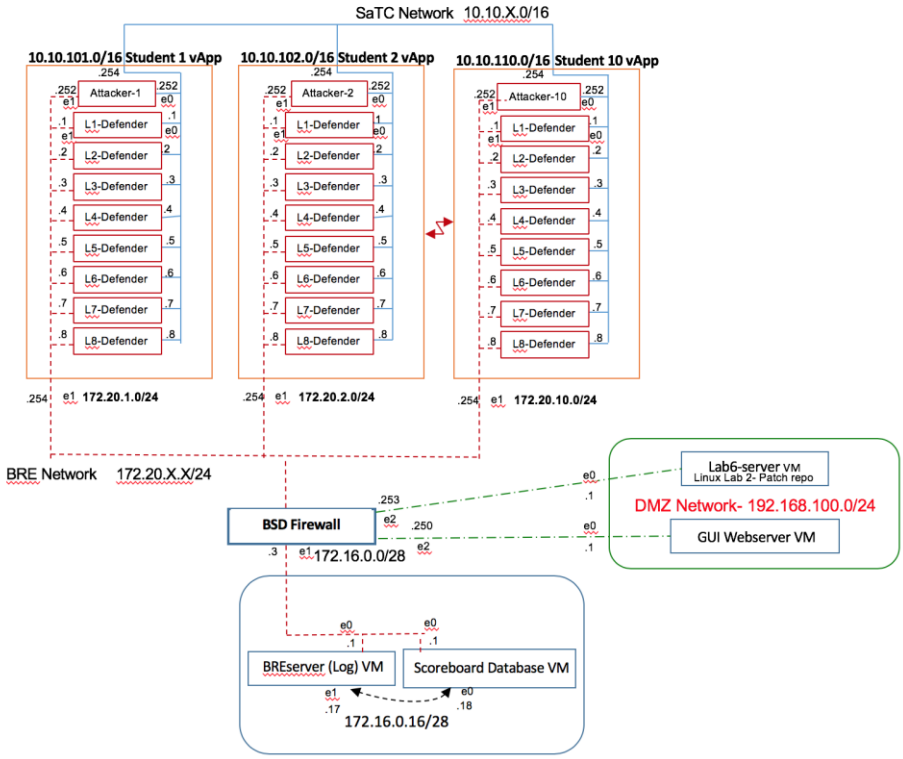

Figure 1. Network layout

In total, eight labs, listed in Table 1, were developed and each included a pair of attack and defense sub-labs. Virtualization technology was used to host multiple VMs in each participant's environment to conduct the lab activities. Each virtual application (vApp) was running VirtualBox hypervisor that contained a single Attack VM and Multiple Defense VMs (Defender 1-8).

Table 1. Labs Supported by Infrastructure

Lab Number	Name
1	Linux Lab. Secure Remote Login
2	Windows Lab. Denial of Service
3	IPv6 Lab. DHCP Starvation
4	Linux Lab. Patch Management
5	Windows Lab. SQL Injection
6	IPv6 Lab. Backdoor
7	Linux Lab. Honeypot
8	Windows Lab. Web Defacement

2.1. Security

Due to the nature of the game, with participants who are trained in security, it was determined that the environment would need to be secured. Information Security approaches are covered in many modern research papers, with a heavy emphasis on the multi-layered security approach. [2] We agreed and decided to set out to utilize multiple layers to provide the best security. The design of the network was carried out with thought toward not merely creating a working environment but creating a working environment that is also secure. The lure of winning the competition by means outside of the confines of the rules of the competition might be strong, and we had to bear in mind that all participants are well versed in both security and anti-security measures. The first layer of network security lies in providing participants with a host VM that is attached to the LAN, the BRE network as it came to be named. The VMs that house the labs were attached to a separate network, called the SaTC network. Finally, a third network was required to protect the systems that house the scoreboard, database and documentation servers. The third network was located behind a BSD-based firewall, so that it would not likely be susceptible to the same vulnerabilities as the main network VMs while adding an extra layer of security.

Figure 1 shows three network IP schemes. The SaTC network uses 10.10.X.0/16, such that student 1 has 10.10.101.0/16, and student 2 has 10.10.102.0/16, etc. All the participant's VMs were connected to the SaTC network only, while only their host has access to the BRE network, which uses the 172.20.X.0/16 IP scheme. The BRE network is the only network which could communicate with the BSD firewall and to the systems behind it. Additionally, the student host VM was not able to make a new connection to the systems behind the firewall. Students were only able to return data once a connection was requested from behind the firewall. The established and related communication was only possible with a single system behind the firewall, communication with other systems behind the firewall was not permitted.
Software was resident on all the participant systems which continuously scanned for new network configurations. If a participant attempts to spoof a network configuration, it will be reported for proper administrative action.

2.2. Infrastructure Design - Clients

Most networking in the environment only exist virtually. In other words, most networks only exist as a software construct. Every item listed in Figure 1 is a virtual machine. Even the student host machine is a virtual machine. Students connected to said host virtual machine with a zero client located in our computer lab. According to VMware, zero clients provide an extra level of security as all data remains in the datacenter with no data exposed at the endpoint. [3] The only accessible physical network was the network that connects the zero clients to the virtual infrastructure. At the time of this writing, the virtual infrastructure was based on VMware's Horizon View software. Students had limited access to most systems they used to compete, starting with the zero client. The zero clients had an embedded OS installed, providing a very minimal attack surface. The zero client connected to the host OS, which students had minimal access to. Utilizing this design, students only had elevated privileges on the VMs provided by the host, which are labeled attacker or defender in Figure 1. In addition to the security aspects, zero clients provided a way to efficiently set up a new, consistent environment for each participating group.

2.3. Infrastructure Design - Servers

At the bottom of Figure 1 is a group of virtual servers with BSD firewall displayed at the top of the group. These virtual servers provided the main website for participants, the grading server, a firewall and a database server. Combined, these components enabled the management of the environment for administrators and provided a website for each participant to utilize for instructions and documentation. Participants checked in via the website, read instructions and took quizzes to ensure everyone is prepared for the start of the competition. Additionally, participants were able to track their score via the website as the competition progresses. Similar to the student environments, these virtual servers were connected via virtual networks, which only exist in the datacenter. The firewall was hosted on a BSD-based operating system in order to artificially prevent a monoculture based on similar operating systems. According to Lala, security risks are reduced by implementing diversity which reduces the likelihood of a successful single malware vector. [4] Indeed, the virtual machine providing the firewall is the only place that BSD was utilized in the environment and it is provided by the pfSense distribution. According to Venezia, pfSense may be the best firewall available, open source or otherwise. [5] Additionally, pfSense provides a way to control traffic, impose bandwidth limits for each participant and provide quality of service components, if needed.

2.4. Demilitarized Zone (DMZ)

The DMZ housed some virtual machines that needed access to the Internet. The virtual machines housed inside it had two dedicated network interfaces, with only one capable of connecting to the Internet, and the other network interface connected to the BSD firewall. One of the virtual machines is a patch server, which allowed us to provide security patches for the systems within and behind the firewall. Applying security patches was considered highly important based on our research. Much research has been conducted on the importance of security patches, more recent research focuses on the human factor. Security must be integrated into the process and easy to maintain, or security suffers, leading to more vulnerable systems. [6] The other virtual machine

provided the main website, documentation and score board. The score board kept a running tally of scores for both participants to view and track participant progress and for administrators of the event to see how the competition was progressing.

3. Conclusions and Future Work

We researched the best approach for teaching a Cyber Security system. Through our research, we designed a game-based learning system that was based on layers of security, with heavily virtualized underpinnings. We found that the devised system was easy to set up and maintain for each group of participants. The environment was easy to keep up to date with the latest security patches. This system was also easy to clear and set up for the next group of participants who compete. Additionally, the devised system was easy to keep secured. Our research will be helpful to anyone trying to implement an infrastructure to support a game-based cyber security competition. In the future, we'd like to take additional steps to automate the following processes, applying security patches based on a schedule, cloning entire participant environments with one script or button press, implementing VM snapshots and/or backups during competition and designing a survey to capture input from participants immediately following the competition. We believe the survey feedback will help us refine all the processes and continuously improve the environment.

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] K. Kiili, "Digital game-based learning: Towards an experiential gaming model," *The Internet and Higher Education*, vol. 8, no. 1, pp. 13-24, 2005.

[2] M. Olivier, "A LAYERED SECURITY ARCHITECTURE: DESIGN ISSUES," *South African Computer Journal*, vol. 2003, no. 31, pp. 53-61, 2003.

[3] J. Chapin, "Key Considerations in Choosing a Zero Client Environment for View Virtual Desktops in VMware Horizon," 2014. [Online]. Available: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/vmware-top-five-considerations-for-choosing-a-zero-client-environment.pdf. [Accessed 08 10 2018].

[4] J. H. Lala, "IT Monoculture Security Risks and Defenses," *IEEE Security and Privacy*, vol. 7, no. 1, pp. 12-13, 2009.

[5] P. Zenezia, "InfoWorld," 22 12 2014. [Online]. Available: https://www.infoworld.com/article/2861574/network-security/you-should-be-running-pfsense-firewall.html. [Accessed 8 10 2018].

Biography

JOHN JONES is currently an Instructional Technology Consultant with the College of Engineering and Technology at East Carolina University. He received his Bachelor degree in Computer Science from Ohio University and a Master's degree in Technology Management / Information Security from East Carolina University. He teaches classes in both Computer Science and Technology Systems at East Carolina University. He has worked in the IT industry over 20 years in varied roles such as software design, IT director, IT security, infrastructure management, systems administration, Internet Services and part-time faculty.

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.