Experience of Teaching Defensive Cybersecurity in Hybrid Mode

Vamsi K. Gondi
vkgondi@bsu.edu

David M. Hua
dhua@bsu.edu

Center for Information and Communication Sciences
Ball State University
Muncie, IN 47306, USA

Abstract

COVID-19 pandemic had a major impact on how universities and schools operate. At Ball State University, due to COVID restrictions only 12 persons are allowed in computer labs and cluster even though the class strength is 24 for that semester. I chose a hybrid approach where 12 students will be in class and 12 students through online, and vice-versa in the next class. Being a defensive cybersecurity course, the students have to go through intensive labs and theoretical sessions. Setting up the labs is one of the major challenge as the students rotate and they need to have access to this lab setup in every session to complete lab assignments and projects. In this paper, I discuss how I setup these labs and how I worked with students to obtain course objective setup in the syllabus. I will also discuss the final project which is key to complete this course and how students completed it using 3 different platforms. I will also discuss major challenges students faced to complete the course. I also collaborated with my colleague who teaches offensive cybersecurity course, his students work in groups and break into the infrastructure setup up by defensive cybersecurity students.

Keywords: Defensive Cybersecurity, Hybrid Teaching, Lab Setup, Persistence Linux USB Drive, Cluster, Amazon AWS.

1. INTRODUCTION

Defensive Cybersecurity is a very intensive course involving various aspects of Computer Science and Information Technology. Students need to have a very good understanding in all the domains and also with the offensive cybersecurity concepts before they attend this course. The labs and project are difficult and very technical oriented.

Usually this course is conducted in an air gab lab setup, as some offensive tools are used to break the infrastructure, it is quite common students make some mistakes in the lab which results in failure in production network. Due to COVID and limited accessibility to the physical labs it was challenging to design lab environment suitable for the lab completions and project successfully in hybrid mode.

The remaining paper is organized as follows; section 2 describe the course, course objectives, and labs. Section 3 discuss the lab environment setup. Section 4 discuss the final project and its tasks and outcome. Section 5 describes the cluster environment and Amazon AWS setup to complete the project. Section 6 concludes the student learning outcomes and Section 7 concludes the paper.

2. DEFENSIVE CYBERSURITY COURSE

This course prepares students to defend networks and infrastructure against attacks by implementing proactive protection measures and by responding to active and potential threats. It covers multiple techniques for network defense, including firewalls, intrusion-detection systems, VPNs, encryption, and system hardening. Upon successful completion of this course, students should demonstrate proficiency in the following areas:

- Attack types and how they operate
- Firewalls
- Intrusion-detection systems
- VPNs
- Encryption
- OS hardening
- Virus attacks
- Trojan horses, spyware, and adware
- Security policies
- System security assessment
- Security standards
- Physical security
- Disaster recovery
- Techniques used by attackers
- Forensics
- Cyber terrorism

Labs

The students need to complete multiple labs to complete this course successfully.

In lab 1, students need to know how to use some of the offensive tools to use them in later labs that are involving defensive tasks; ping attacks, TCP SYNC attacks, NMAP, NESSUS, HTTP Metasploit, UDP Flooding, HTTP post dos.

In lab 2, students work on setting up the firewalls on a Linux server using UFW, iptables and use multiple tools in lab1 to break the Linux server.

In lab 3, students install and configure ConfigServer security and Firewall (CSF) (ConfigServer Security & Firewall (Csf), 2021) and webmin interface and use Lab 1 tools to test the Linux server.

In lab 4, students will be installing and configuring Snort (Intrusion Detection and Intrusion Prevention) (Snort, 2021) and openAppID, and enabling built in rules to prevent various attacks.

In Lab 5, students will be installing and configuring Kerberos server (Kerberos: The Network Authentication Protocol, 2021) and client for token based secured authentication.

3. LAB ENVIRONMENT SETUP

As the course is conducted in a hybrid mode, student doesn't have 100% access to labs. Taking this into consideration I developed the whole environment using a Linux image and USB Drive. I installed Ubuntu Desktop latest version on a USB drive of 128GB capacity using etcher (BalenaEtcher - Flash OS Images to SD Cards & USB Drives, 2021), other tools such as Rufus (Batard, 2021) can be used to accomplish this task. Later I enabled this drive as persistence drive. Later, I installed Oracle Virtualbox (Oracle VM VirtualBox, 2021) and installed three virtual machines; Ubuntu Server (Get Ubuntu Server | Download | Ubuntu, 2021), Kali OS (Kali OS, 2021), Windows Server (Windows Server 2019, 2021). For networking NAT is setup between these three servers and external networking is disabled by default. Using Linux dd imager tool, I created iso image and distributed to students through box. Students later installed this image in 128GB USB drive. They place USB drive in their own personal laptops or university lab computer and boot into it through BIOS. Server tasks, defensive tools, etc…, are installed and configured on Ubuntu server and Windows server, and Kali OS is used for offensive attacks.

4. FINAL PROJECT

Objective

Design and develop systems and security infrastructure for a financial startup company – BallFi.

BallFi: It is a startup company that has developed an application that will gather critical information on home owners and their current interest rates and provide better re-finance options. The application collects home owner's data from its users. They collect personal data, financial data and their social security numbers in their systems. Once they collect the data, they compute and identify the better options they can provide and give feedback and financing options. This application is hosted on the webserver, and browsers like firefox, chrome, or internet explorer is used to interact this server using secure.

As a consultant company you need to provide a comprehensive security architecture to secure the webserver, SQL database, SSH server and services and its systems, and thwart any intrusions or hackers to get access to BallFi systems and data.

ISSN 2473-4901
v7 n5625

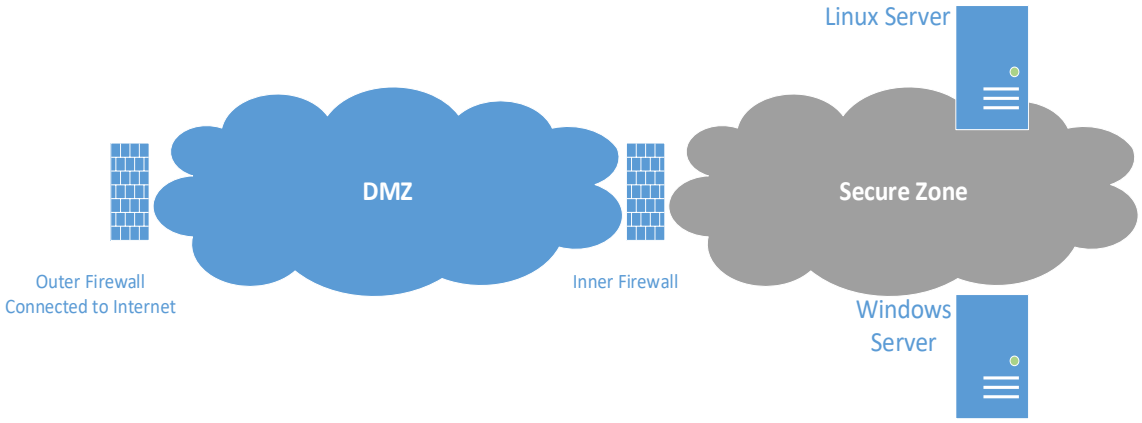

Figure 1. System Architecture

Software and Hardware
Option 1: BallFi procured 3 bare metal servers: 2 for hosting VMs and one for storage. All the software used in this project need to be open source due to financial constraints in buying the licenses and maintaining the licenses. BallFi will provide a windows server image and its key that need will be hosting webserver and SQL database.

Option 2: BallFi leases Amazon AWS services to host the entire infrastructure. Design the architecture and deploy in the AWS cluster.

Services need to render as a part of the project
Your company needed to design and develop system architecture which is robust and secure the development linux server, windows server and its services. You need to deploy multiple Linux systems with security configurations such as firewalls, proxies, NAT server, Config Server, DMZ zone, honey pots, VPN server for access to developers, IDS, IPS, Kerberos.

Tasks 1
Design a system architecture to host all the requested servers and services as shown in the above figure, draw a system diagram and provide a system design documentations of all the severs and detailing its services with the IP address that are assigned to them.

Deliverables: Word Document on the system architecture, components, systems, IP address (

Tasks 2
1. Deploy all the systems and services (inner firewall, outer firewalls, IDS, IPS, etc…) and their configurations as detailed in system architecture.
2. Deploy windows server, apply patches, close ports, configure IIS for webserver and SQL
3. Deploy Linux server for development server, apply patches, close ports, configure firewall and allow only SSH server and its connections through Kerberos
4. Test the connections and configurations
5. Deliverables: Word Document on the system configurations, patches, ports, software, and the documents should also detail the following:
   a. What firewall is used and how it is configured
   b. What IDS is in use and how it is configured
   c. What antivirus/antispyware is used
   d. Are honeypots in use
   e. Are individual machine security measures in use and what are they, etc..

Deliverables: Screenshots, Internal probing, testing applications and security services in a word document.

Tasks 3: (external group is going to try to hack and you prep your systems to block their attack)
1. External probing (tools and techniques used by hackers and documentation from your side)
Deliverables: Word document of results.

Due to time constrains and moving to AWS this tasks was optional at the completion of this project.

5. INFRASTRUCTURE SETUP USING LOCAL CLUSTER AND AMAZON AWS

At our department we have an operation cluster for student access for labs and projects. Every racks has 3 HP DL360 1u servers, 1 DL380 2u or 1 DL385 1u storage array already racked and ready for implementation. All servers are currently wired to network equipment as well as a Raritan KVM system to allow ease of administrative tasks. The servers are also connected to a monitored and switched power distribution system.

In the second option, I partnered with Amazon for its AWS access for free for the students. I designed various tutorials on how to use AWS, creating EC2 instances, route 53, RDS, etc…, and provided access to students to have a good knowledge of AWS.

Students are divided into multiple groups, and asked to choose any of these two options. And also I gave options of getting 100% access to lab if they chose cluster version and 100% remote who chose AWS option. 3 groups chose cluster option and 5 groups chose to work with AWS.

6. STUDENT LEARNING OUTCOMES

The project is very challenging, out of 8 groups only 4 groups successfully completed all the tasks assigned in the project, 2 groups successfully met the minimum criteria and 2 groups failed to reach minimum criteria.

3 groups who chose cluster successfully. Whereas out of 5 groups who chose AWS, only 1 group completed the project, 2 met minimum requirement, and other 2 groups failed to reach minimum requirements set in the tasks.

Cluster based project is very hands on where students were working with Hardware, and use networking, routing, VLANS through hardware very effectively to complete the tasks. On the other hand AWS being new to them, it was little bit different on how to setup the infrastructure even with provided tutorials. Also being 100% remote some of the student's participation was almost null, which resulted in failure of the project. These kinds of projects need very careful planning, tasks assignment among team members. Students who took the 100% virtual failed to coordinate and planning on tasks creation and assignment.

7. CONCLUSIONS

COVID or no COVID Defensive Cybersecurity course is very challenging for students as the content and breadth and depth is overwhelming to any undergrad student. With COVID, the delivery of the content, labs and project need to perform with limited access to physical labs. Using lab setup mentioned in this paper provided a successful platform to deliver the content and conducting the labs in an effective manner. The cluster based project execution was very successful where students work in groups in labs with social distancing, where AWS based project has limited success as coordination and students working in groups is limited to online and some students efforts was limited for completion of the project. Also for most of the students had limited knowledge of working in cloud environment.

While as a facilitator for this concept for whole semester was challenging with full success in one mode of delivery and limited success in the other. In the coming semester, I intent to plan little emphasis on project management, tasks creation and assignment while working online.

8. REFERENCES

ConfigServer Security & Firewall (csf). (2021). ConfigServer Services. Retrieved August 30, 2021, from https://configserver.com/cp/csf.html

Snort. (2021). Snort. Retrieved August 30, 2021, from https://www.snort.org/

Flash OS images to SD cards & USB drives. (2021). BalenaEtcher. Retrieved August 30, 2021, from https://www.balena.io/etcher/

Batard, P. (2021). Rufus - Create bootable USB drives the easy way. Rufus - The Official Website (Download, New Releases). Retrieved August 30, 2021, from https://rufus.ie/en/

Get Ubuntu Server | Download | Ubuntu. (2021). Ubuntu. Retrieved August 30, 2021, from https://ubuntu.com/download/server

Kali OS. (2021). Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. Retrieved August 30, 2021, from https://www.kali.org/

Kerberos: The Network Authentication Protocol. (2021). MIT - Massachusetts Institute of Technology. Retrieved August 30, 2021, from https://web.mit.edu/kerberos/

Oracle VM VirtualBox. (2021). Oracle VM VirtualBox. Retrieved August 30, 2021, from https://www.virtualbox.org/

Windows Server 2019. (2021). Microsoft – Cloud, Computers, Apps & Gaming. Retrieved August 30, 2021, from https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019