DEVELOPING AN ISOLATED NETWORK ENVIRONMENT FOR ETHICAL HACKING EDUCATION

Phillip Nikolov

A Capstone Project Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Master of Science

Department of Computer Science
Congdon School of Supply Chain, Business Analytics, & Information Systems

University of North Carolina Wilmington

2024

Approved by

Advisory Committee

Hosam Alamleh	Ulku Clark

Geoff Stoker, Chair

Accepted By

Dean, Graduate School

TABLE OF CONTENTS
(Insert Automatic Table of Contents)

ABSTRACT

Developing an Isolated Network Environment for Ethical Hacking Education. Nikolov, Phillip, 2024. Capstone Paper, University of North Carolina Wilmington.

This project developed an Ethical Hacking lab to support hands-on cybersecurity education, enabling students to gain practical experience with penetration testing tools and techniques. Housed in an isolated network environment, the lab integrates both physical and virtual resources, including a server, switch, and workstations managed by Proxmox VE. Key components include Kali Linux for testing and Metasploitable 2 as a vulnerable virtual machine, allowing students to practice a range of attacks and assess various vulnerabilities. The lab exercises follow the typical penetration testing workflow—reconnaissance, network scanning, vulnerability assessment, and exploitation—guiding students through structured tasks while fostering independent problem-solving skills. Additionally, Proxmox's snapshot feature enables easy resetting, ensuring a consistent testing environment across users.

Challenges included acquiring suitable hardware, adapting software for compatibility with Proxmox, and refining lab tasks based on student feedback. Initial plans to include additional workstations and a router were adjusted due to hardware limitations, though scalability was prioritized in the lab's design to support future hardware expansions and more complex network configurations. Student feedback confirmed the lab's educational value, highlighting its effectiveness in building cybersecurity skills and suggesting minor task rewording to improve clarity. This Ethical Hacking lab aligns with the NICE Cybersecurity Workforce Framework and serves as a foundational tool for cybersecurity education at UNCW. With future enhancements, the lab can evolve into a more sophisticated training environment, introducing defensive exercises and advanced network configurations to provide a comprehensive learning experience for both novice and advanced users

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Background Research

Ethical hacking has become an integral part of cybersecurity, providing a proactive approach to identifying and mitigating vulnerabilities in systems before malicious actors can exploit them. The need for practical, hands-on experience in cybersecurity education has driven the development of dedicated hacking labs, where students can safely explore the techniques used by attackers. These labs offer a controlled environment where learners can practice ethical hacking, including network scanning, vulnerability assessment, exploitation, and post-exploitation tasks.

The traditional approach to ethical hacking labs involved using physical hardware such as routers, switches, and servers to create isolated networks. However, with advancements in virtualization technologies, many institutions have shifted towards virtualized environments that offer flexibility and scalability. Virtual machines can be easily configured, cloned, and restored, making them ideal for educational settings where different scenarios need to be tested repeatedly.

Despite the advantages of virtualized labs, there remains a significant value in using real hardware. Real hardware provides a more authentic experience, mimicking the complexities and challenges of managing physical infrastructure in a real-world setting. Additionally, hybrid setups that combine both physical and virtual components can offer the best of both worlds, providing a robust platform for learning while maintaining flexibility.

Purpose

The primary purpose of this capstone project is to design and implement an ethical hacking lab that combines the use of real hardware with virtual machines to create

a realistic and isolated network environment. This lab will serve as a training ground for students, enabling them to develop and refine their penetration testing and cybersecurity skills. By providing a safe, controlled environment, the lab will allow students to explore a wide range of hacking techniques without risking the security of live systems.

This project is particularly focused on addressing the challenges and complexities involved in setting up a hacking lab using real hardware. It will explore the process of acquiring and configuring the necessary equipment, establishing a secure network, and integrating various software tools that are essential for ethical hacking. The lab will be designed to support a range of tasks, from basic network enumeration to advanced exploitation, ensuring that it can cater to learners at different skill levels.

The project will also consider the logistical aspects of setting up the lab within an academic environment, including securing space on a server rack, ensuring compliance with institutional policies, and collaborating with university IT staff. The lab will also include the ability to reset the lab to a baseline configuration, allowing for the lab to be reset between student uses. The resulting lab will not only serve as an educational resource but also as a model for future developments in cybersecurity training.

Goals

The goals of this project are both technical and educational objectives. The key goals are as follows:

1. Establish an Isolated Network Environment: The lab will be built on a standalone network, isolated from the university's main infrastructure, to ensure security and prevent any unintended consequences. This network will include both physical and virtual components, providing a realistic setting for penetration testing. The network will be hosted in room 2003 in

Congdon Hall

2. Integrate Real Hardware with Virtual Machines: The lab will utilize a combination of real hardware (such as routers, switches, and servers) and virtual machines. This hybrid approach will offer students a comprehensive understanding of both physical and virtual network environments.
3. Develop a Range of Ethical Hacking Exercises: A series of tasks and exercises will be developed, starting with basic tasks such as network enumeration and progressing to more complex activities like exploiting vulnerabilities in web and email servers. These exercises will be designed to build students' skills incrementally, ensuring a solid foundation in ethical hacking.
4. Facilitate Hands-On Learning: The lab will be designed to support hands-on learning, with students gaining practical experience in using tools such as Nmap, Wireshark, Metasploit, and Nikto. By engaging in real-world scenarios, students will develop the critical thinking and problem-solving skills necessary for cybersecurity professionals.
5. Ensure Scalability and Flexibility: The lab will be designed to be scalable, allowing for the addition of new tasks, tools, and scenarios as needed. Flexibility will be a key consideration, enabling the lab to accommodate different learning paths and levels of expertise.
6. Document the Setup and Maintenance Process: As part of the project, comprehensive documentation will be created to guide the setup, maintenance, and use of the lab. This documentation will serve as a

resource for future students and instructors, ensuring the sustainability of the lab.

By achieving these goals, the project will contribute to the development of a robust educational resource that enhances cybersecurity training and prepares students for real-world challenges in the field of ethical hacking.

CHAPTER 2: REVIEW OF LITERATURE REVIEW AND ANALYSIS

Advanced Persistent Threats (APTs) in Cybersecurity Education

The increasing sophistication and persistence of cyber threats, particularly Advanced Persistent Threats (APTs), have emerged as a significant challenge for cybersecurity professionals. APTs are characterized by their advanced technological tools, stealthy behavior, and complex attack strategies, which allow them to evade traditional security measures and remain undetected within networks for extended periods (Hu, 2022). The critical nature of these threats necessitates a comprehensive defense plan, part of which includes enhancing cybersecurity education to better prepare students for real-world scenarios.

Role of Hands-On Learning in Cybersecurity Education

Hands-on learning has been increasingly recognized as an effective educational approach to cybersecurity. It provides students with practical experience that bridges the gap between theoretical knowledge and real-world application. This method has been successfully employed in various disciplines, including nursing, web design, software engineering, and cybersecurity. For instance, in the field of nursing, hands-on learning has improved students' critical thinking and clinical judgment skills, while in computer science, it has enhanced understanding of complex systems and practical skills necessary for industry (Hu, 2022).

In the context of cybersecurity, hands-on learning is particularly valuable for understanding and mitigating APTs. Traditional classroom-based learning, which often focuses on theoretical concepts, may not sufficiently prepare students to handle the dynamic and evolving nature of APTs. Instead, incorporating practical exercises, such as ethical hacking labs, allows students to engage directly with the technologies and

strategies used in APTs, thereby gaining a deeper understanding of the threats and how to counter them (Hill, 2001).

Cybersecurity Competitions as a Learning Platform

Cybersecurity competitions, like Capture the Flag (CTF) events, offer another effective hands-on learning environment that complements formal education. These competitions simulate real-world scenarios, requiring participants to apply their knowledge and skills to solve complex cybersecurity challenges. Through these events, students not only reinforce their understanding of cybersecurity principles but also develop critical problem-solving and teamwork skills. Furthermore, cybersecurity competitions have been shown to motivate students to delve deeper into the subject matter, fostering a competitive yet collaborative learning atmosphere (Chou, 2022).

Chou's (2022) research highlights that cybersecurity competitions are particularly effective in helping students connect theoretical knowledge with practical application. By participating in these events, students are exposed to a wide range of security challenges, from basic exploits to advanced attack vectors like APTs. This exposure is crucial for preparing students to address the sophisticated nature of modern cyber threats.

Integration of Ethical Hacking Labs with APT Training

To address the emerging challenge of APTs in cybersecurity education, Hu (2022) proposed the integration of NDG ethical hacking labs into the curriculum. These labs are designed to align with the phases of the APT lifecycle, providing students with a structured learning experience that mirrors real-world APT scenarios. The NDG labs cover various aspects of ethical hacking, from initial intrusion to persistence and exfiltration, allowing students to practice and refine their skills in a controlled environment.

The adoption of ethical hacking labs not only enhances the hands-on learning experience but also ensures compliance with the NICE Cybersecurity Workforce Framework. This alignment is crucial for developing the necessary Knowledge, Skills, and Abilities (KSAs) in students, preparing them for roles in cybersecurity that require expertise in dealing with APTs (Hu, 2022).

Theoretical Foundations of Hands-On Learning Models

The educational strategies discussed above are rooted in established learning theories, such as Kolb's Experiential Learning Model. Kolb's model emphasizes the importance of experiential learning, where practical experiences are central to the learning process. According to this model, effective learning occurs when students can engage in concrete experiences, reflect on these experiences, form abstract concepts, and then apply these concepts in new situations (Kolb, 2001).

In the context of cybersecurity education, this model supports the use of hands-on learning techniques such as ethical hacking labs and cybersecurity competitions. These activities allow students to experience the full cycle of learning, from direct interaction with cybersecurity tools and scenarios to reflecting on their experiences and applying their newly acquired knowledge to more complex challenges (McFadden, 2021).

Conclusion

The literature underscores the importance of integrating hands-on learning approaches in cybersecurity education. Ethical hacking labs and cybersecurity competitions are effective tools for bridging the gap between theoretical knowledge and practical application, providing students with the necessary skills to combat sophisticated cyber threats. This paper aims to take the idea of hands-on learning and develop an

Ethical Hacking lab for students to gain real world experience in their pursuit of cybersecurity expertise.

CHAPTER 3: METHODOLOGY

Overview

The Methodology section of this paper will outline the steps involved in creating an isolated ethical hacking lab, focusing on setting up a dedicated network, configuring the required hardware and software, and designing lab challenges. This section provides a roadmap of how the lab will be constructed, emphasizing the need for a hands-on approach to learning real-world applicable ethical hacking techniques. The setup proposed is subject to change depending on the compatibility of available lab equipment and software. Any changes to software or hardware will be reflected in Chapter 4.

Hardware Setup

The lab will be hosted in room Congdon Hall Room 2003, mounted in the server racks in the back of the classroom. The rack will start with one physical server that will host a number of virtual machines for the lab. There will also be at least 2 workstations, with the ability to expand and add more. The lab will also incorporate a switch and a router to simulate an actual network environment for students. There will also be the ability to connect to the network via a student's own device if they desire.

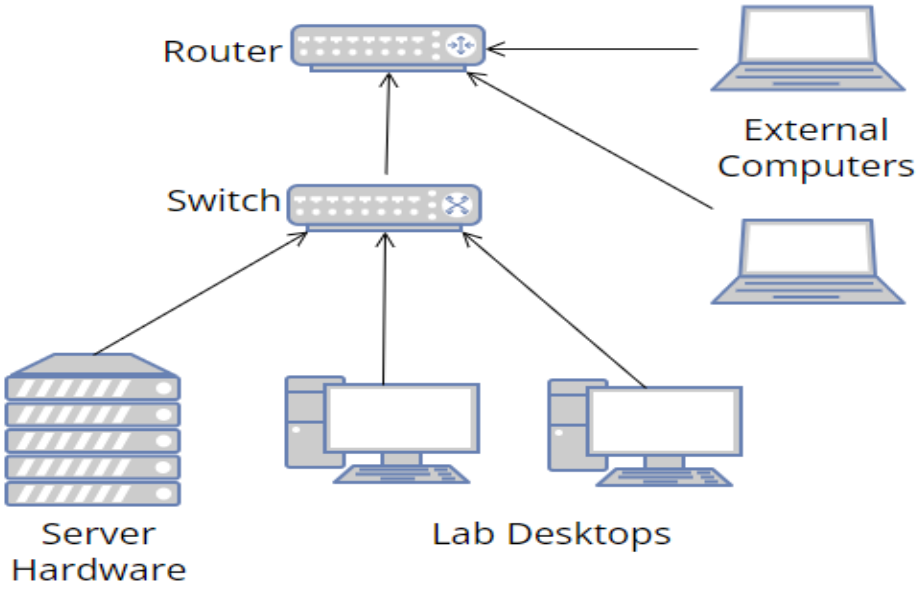


Figure 1. Hardware Lab Schematic.

Software Setup

The Server hardware will be leveraging Ubuntu/Debian to configure the different elements of the lab. Using a tool such as Proxmox VE, the lab will have a simulated virtual environment that will host A domain controller, a web server, a mail server, as well as intentionally vulnerable machines. The domain controller will be configured using domain controller tools built directly into the Proxmox software, allowing it to act as an Active Directory Domain Controller for the network. Apache software will be used to host an intentionally vulnerable web server with multiple potential angles of attack. The current proposed web server that will be used is called bWAPP, which is an intentionally vulnerable web server that is vulnerable to multiple attack vectors. The mail Server will be configured using postfix, a Mail Transfer Agent (MTA) to use SMTP protocol within the lab environment. Along with these servers, there will also be a Capture the Flag type of challenge that will be hosted through a vulnerable machine on the server. See Figure 2 for a schematic for controller and virtual machine configuration.

The network will be a completely isolated environment, with no connection to the internet. The only way to connect will be through ethernet, or a LAN connection.

The user machines will be preconfigured with Kali Linux, as Kali comes standard with many tools commonly used in ethical hacking. Tools like Nmap, Wireshark, and Nikto will be needed for many of the tasks. However, students are free to use whichever tools are available to them, as the goal of the lab is for students to think critically. These tools will be preinstalled, but the students will not be given any hints on which tools to use.

Tasks

Currently, the lab has 8 proposed tasks. These tasks attempt to start simple, and gradually increase in difficulty, aiming to challenge the students to think critically. While there are only 8 at this time, the lab will be built with scalability in mind, allowing more tasks and vulnerable machines to be added for further educational enrichment.

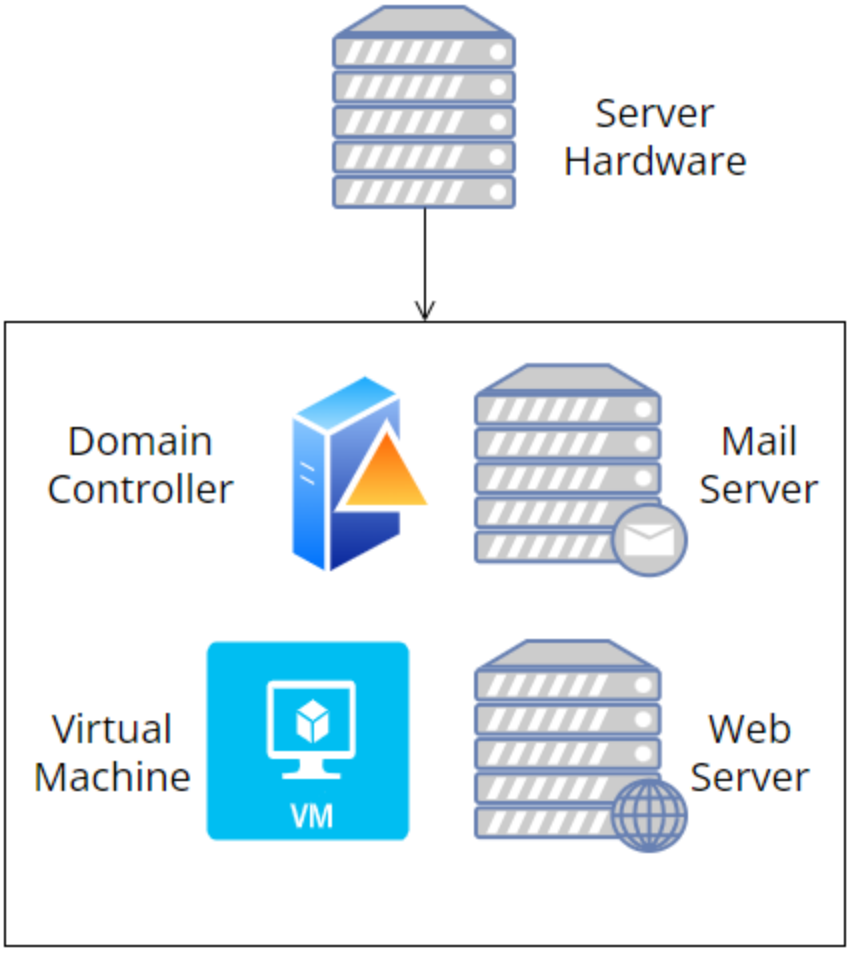


Figure 2. Hosted Software Configuration.

The tasks go as follows in order:

1. Scan the network and find all connected devices and their IP addresses.
2. Scan the network to find all ports that are in use.
3. Sniff the network traffic and identify which 2 devices are communicating the most.
4. Identify which IP addresses are the email server, and the web server.
5. Scan the email server for vulnerabilities and report what you find.
6. Scan the web server for vulnerabilities and report what you find.
7. Perform a SQL injection on the web server.
8. Complete a Capture the Flag VM Challenge (BeelZebub)

The purposeful ambiguity of the tasks allows students to be creative, with the ability to use multiple different tools to solve the same task.

Summary

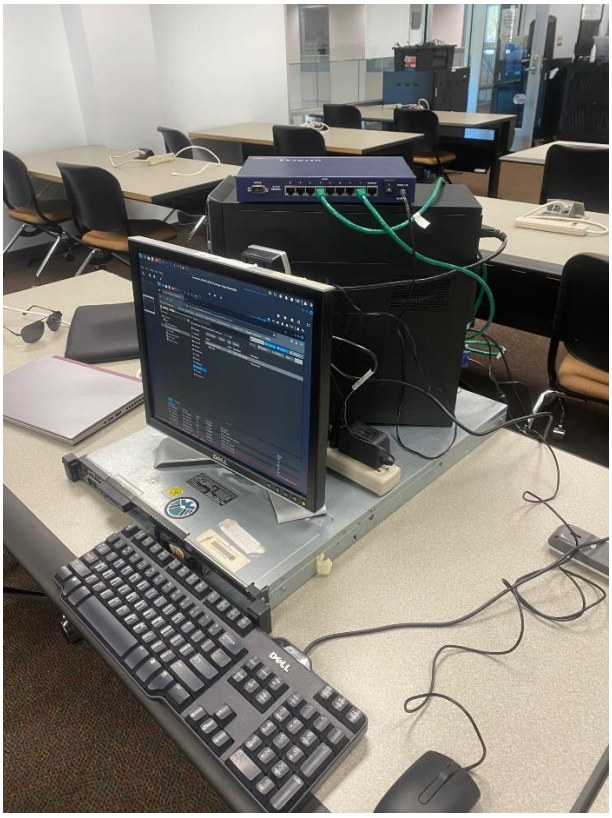
Overall, The purpose of the lab is to ensure a sustainable and educational environment for current and future students. The lab will be built with scalability in mind, allowing the expansion of the lab and more tasks to be added. There will also be extensive documentation on how the lab was set up, how to reset the lab after each student, and on how to solve the tasks for those that may need the help. Students are encouraged to come up with their own methods of completing the tasks with little assistance, as hands-on learning has been proven effective, and the lab can only enrich the learning experience of students who wish to further their cybersecurity expertise.

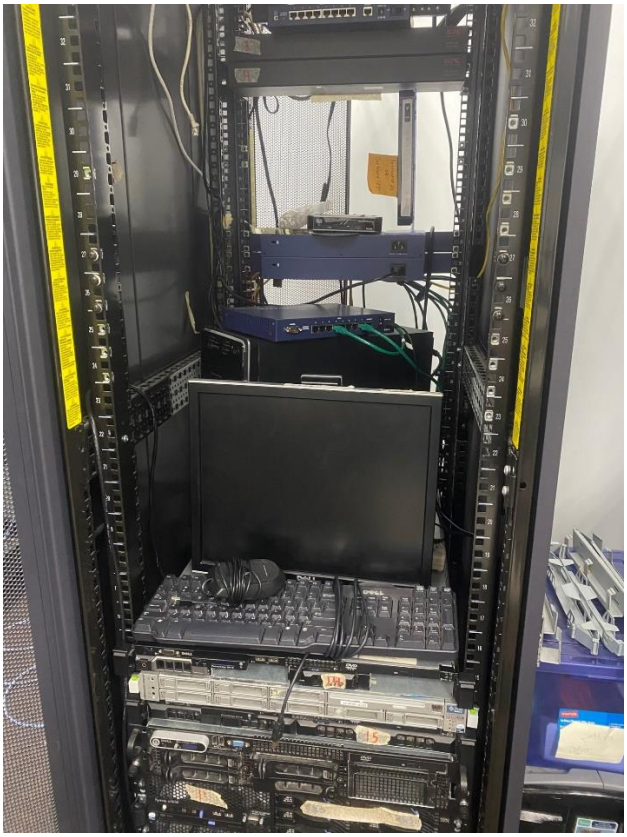
CHAPTER 4: OUTLINE OF COMPLETED THESIS OR PROJECT

During the lab's development, there were a few roadblocks that occurred that hindered development. However, the lab is still able to serve as a quality tool for ethical hacking education.

Results

The first step before a lab can be configured was to gather physical hardware equipment, and to connect with the Cyber Defense club about the use of their server racks. With approval from the club, the lab was allocated a physical server, a switch, and a workstation. Next, new storage drives were acquired. One to host the Proxmox virtual environment, and one for the existing workstation. A router was originally planned to be acquired, however as project development started, at this point in development, a router had not been secured yet. See Figure 3 for a picture of the hardware setup.





Figures 3 & 4. Hardware Visual.

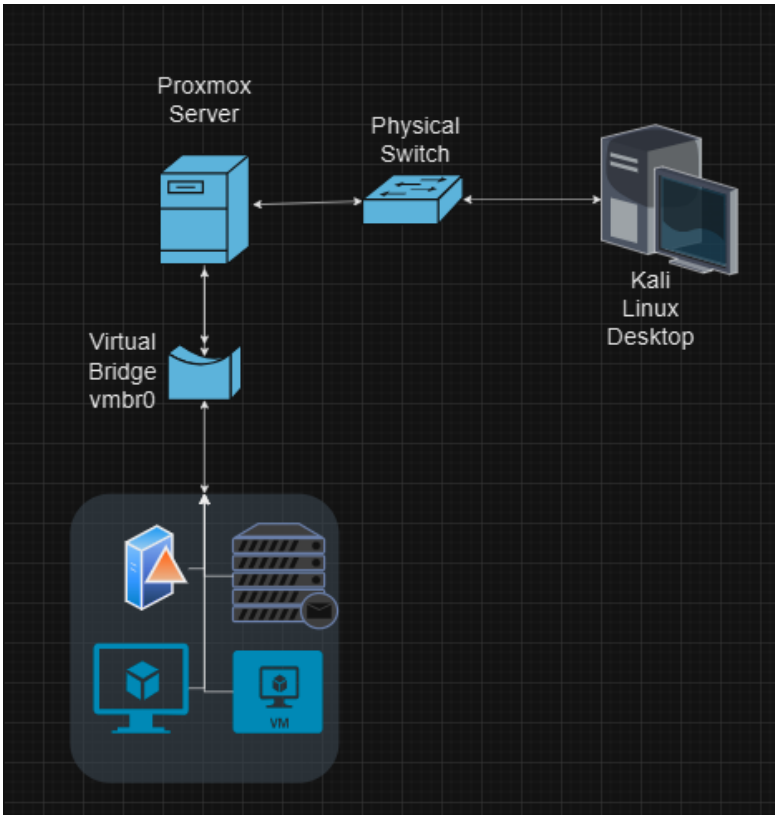


Figure 5. Network Diagram.

Once the hardware had been collected and assembled, the development of the software in the lab was to begin. While creating the lab software, it was discovered that Proxmox has a built-in domain controller, which was used to configure the network for the lab, meaning that setting up a domain controller for the LAN through a router was no longer necessary to create the network. The mail server was then configured inside a virtual machine in Proxmox. The local mail server was configured with Postfix as a mail transfer agent that uses SMTP protocol to send and receive emails within the local domain. Next came the configuration of the vulnerable machine. Initially, it was planned to use bWAPP as the vulnerable web server, however, that premade vulnerable machine was not compatible with the Proxmox system, so changes had to be made. Instead of using bWAPP, the Virtual machine would be created using Metasploitable 2, an

intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common web server vulnerabilities. The user machine was configured with Kali Linux and has all the tools required to complete the given lab tasks.

A large concern of the lab was also the ability to revert to an “original state” in which the lab can be reset to between users. This functionality is built into Proxmox Virtual Environment as a “snapshot” of a virtual machine. To set this up, the admin of the Proxmox server must take a snapshot of a virtual machine (which has already been done). Once a user is complete with their testing, the admin can go into the Proxmox manager, and reset each virtual machine to their original state prior to testing. This is done by clicking the “rollback” command on the same page.

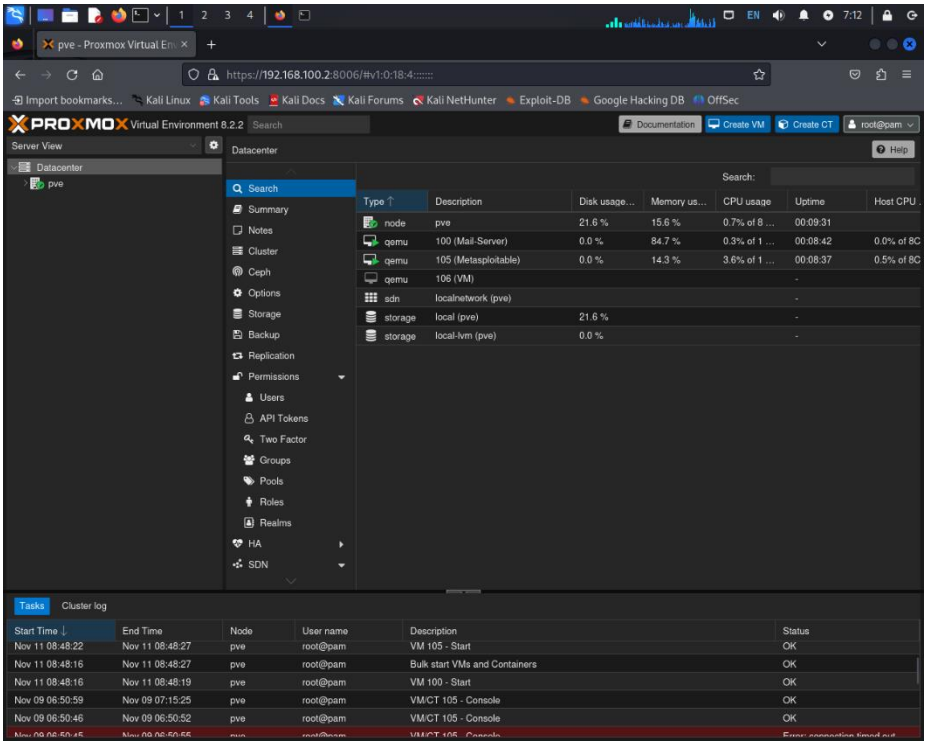


Figure 6. Proxmox VE Management Console Interface

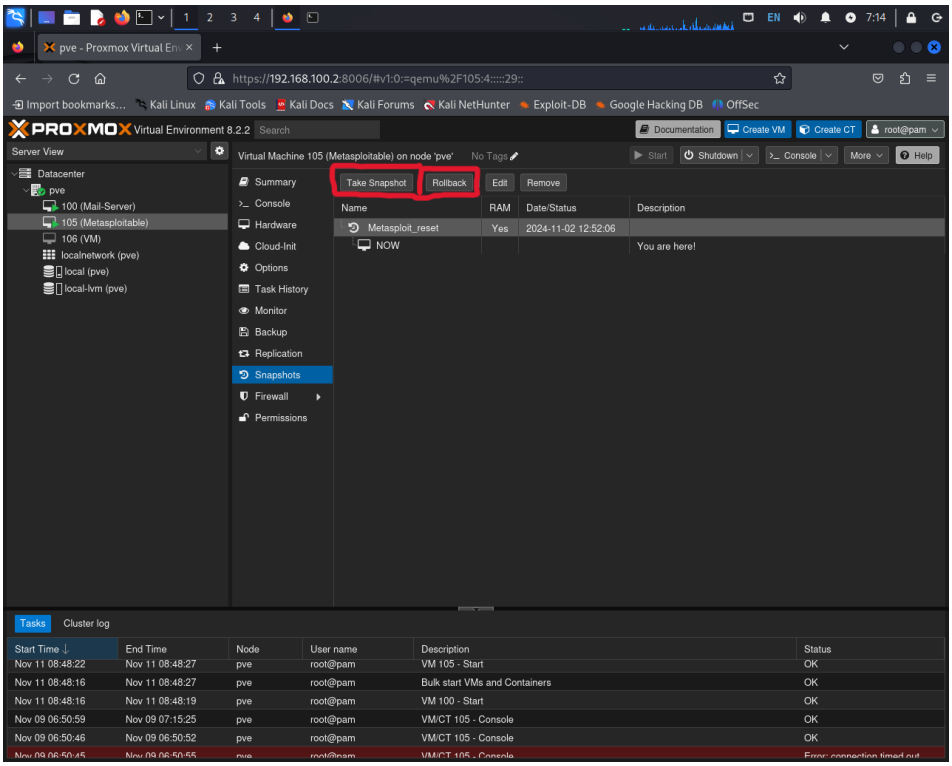


Figure 7. Proxmox Snapshot and Rollback Features

Once the base software was constructed and functional, the next thing to refine were the proposed tasks based. The new tasks developed were a combination of previous tasks modified to fit the Metasploitable framework. Then they were refined with feedback from 4 student testers to be more user friendly. The final number of tasks for the lab is 10, with the tasks themselves to be performed in the following order below:

1. Find the IP address of your Kali Linux machine.
2. Enumerate the Network: Find IP addresses of other devices on your network.
3. Identify the IP addresses and what each service is.
4. Open a packet sniffing tool of your choice and begin capturing. Type the IP address of the web server into a browser and poke around the website. What happens on the packet sniffer when you interact with the website.
5. Scan for open ports on the email server. Do you see any vulnerable ports?

6. Scan for open ports on the web server. Do you see any vulnerable ports? (List 3)
7. Perform a port exploitation on the http port of the web server.
8. How would a network admin secure this port?
9. Perform a SQL Injection attack within the web server (Hint, go to this page: Mutillidae > OWASP Top 10 > A1–Injection > SQLi – Extract Data > User info).
10. How would a web designer secure this application against similar SQL injection attacks?

Challenges

There were several challenges when creating the lab. The most notable being gathering hardware and setting up bWAPP. Initially the lab design included 2 user workstations, however, a second desktop was not able to be acquired within the timeline of the project. Even without this second user workstation however, the lab is still able to serve its purpose as a more hardware focused Ethical Hacking environment for student enrichment. A router was also planned to be part of the solution, but as the project neared its deadline. A router had not been secured, and thus Proxmox was used as an active directory to assign IP addresses to its devices and virtual machines.

The other main challenge of the lab was the configuration of bWAPP. During software setup, it was discovered that the format of the virtual machine was not compatible with the system of Proxmox. The is due to incompatible file types. bWAPP uses the .VMXF file type for its virtual machine, and Proxmox does not support this file type as a VM template. Due to this, the web app had to substituted for a file type that Proxmox would support. One of these supported file types is .VMDK, which happens to be the file type of the Metasploitable 2 vulnerable machine. Thus, Metasploitable 2 was used instead as the web application within the lab.

Discussion

Next came the creation of tasks. Many of the tasks originally proposed were adapted to fit this version of the lab and follow a similar nature to the originals. The nature and order of tasks intends to mimic the actual process of penetration testing in which a tester will perform reconnaissance on a target system before scanning the system and identifying vulnerabilities to exploit. This also allows the tester to flow naturally from easier to more challenging tasks as they progress, pushing the boundaries of what the student knows and does not. The wording of the tasks is also ambiguous and does not guide the user through the process. The idea behind this is to allow students to think critically about their actions and how to progress through the lab, as well as allowing them the opportunity to solve tasks using several methods. In conclusion, the development of the tasks aims to get users to think critically and allows them the opportunity to test multiple tools during the completion of the tasks.

After development was completed lab testing occurred with 4 students of varying experience with ethical hacking, with a survey that was completed by students at the end. The lab is mainly targeted towards beginners in the cybersecurity space but is intended to provide value to more experienced users as well. 2 Students were taken from the Introduction to Ethical Hacking Course, and 2 more students from the UNCW Cyber Defense Club, and all of them were required to submit a survey that contained 8 questions about the lab. The first 5 questions were Likert Scale style. These questions were:

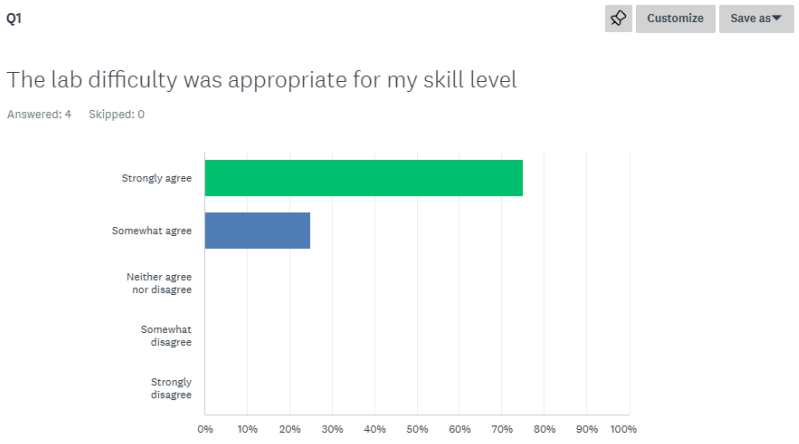
- The lab difficulty was appropriate for my skill level.
- The instructions were clear on what the tasks were asking.
- The lab helped me gain a better understanding of ethical hacking concepts.

- The tools provided were sufficient for completing the lab.
- Do you agree this would be beneficial to a student's Cybersecurity education?

The responses for these questions were very positive, with no disagreement. However, the next 3 questions were more open ended, and provided good feedback. These questions were:

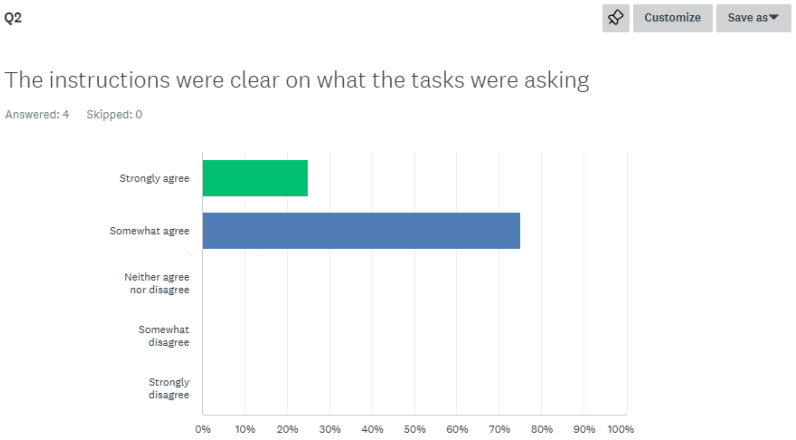
- Would you change anything about the lab tasks?
- Do you have any suggestions for improving lab equipment or tools?
- Any other comments?

The results of these survey questions yielded satisfactory feedback which related to the wording of the questions. Specifically, some of the questions about later tasks were confusing to some of the students as to what the tasks was asking. Question 7 and 9 were confusing, as they had originally been too open ended, and thus have been reworded to provide more guidance to the user about where to start the tasks.



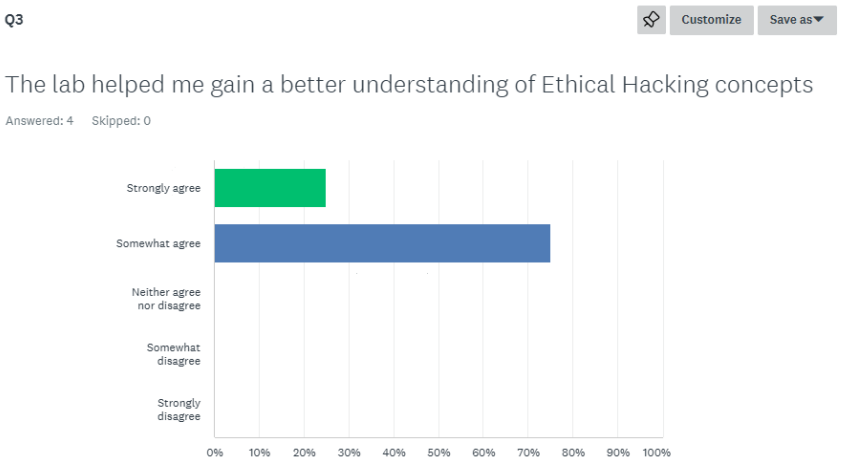
ANSWER CHOICES	RESPONSES	
Strongly agree	75.00%	3
Somewhat agree	25.00%	1
Neither agree nor disagree	0.00%	0
Somewhat disagree	0.00%	0
Strongly disagree	0.00%	0
TOTAL		4

Figure 8. Survey Question 1



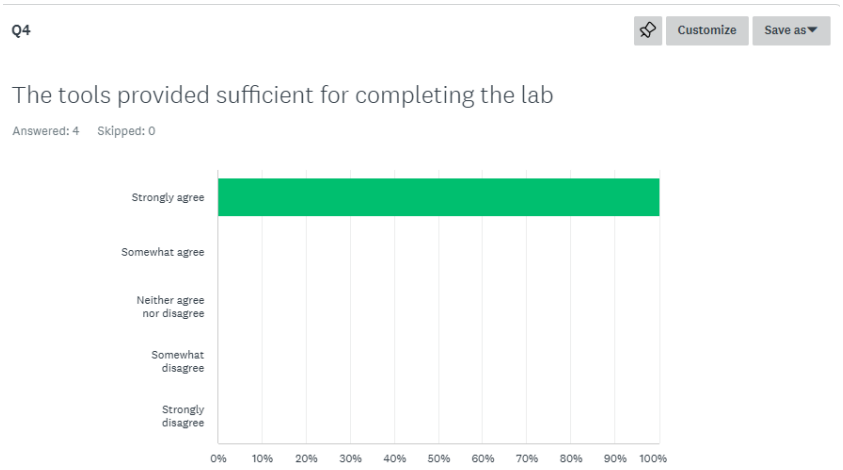
ANSWER CHOICES	RESPONSES	
Strongly agree	25.00%	1
Somewhat agree	75.00%	3
Neither agree nor disagree	0.00%	0
Somewhat disagree	0.00%	0
Strongly disagree	0.00%	0
TOTAL		4

Figure 9. Survey Question 2



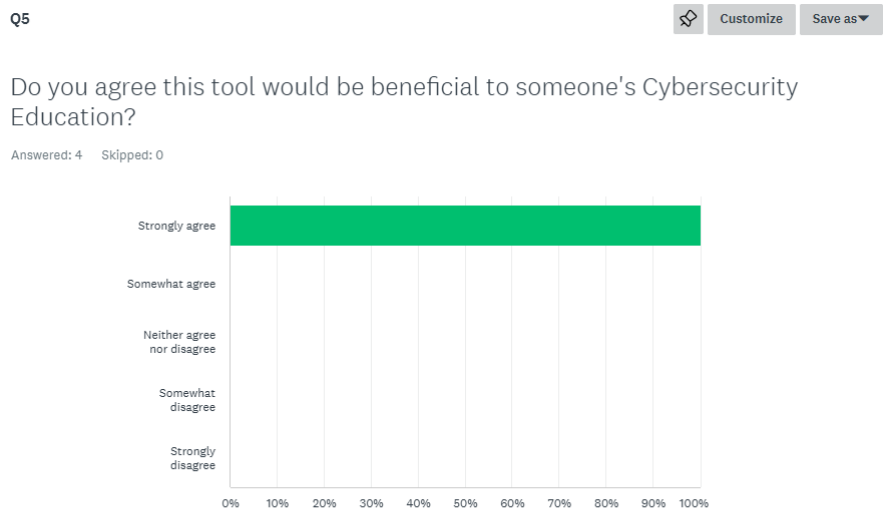
ANSWER CHOICES	RESPONSES	
Strongly agree	25.00%	1
Somewhat agree	75.00%	3
Neither agree nor disagree	0.00%	0
Somewhat disagree	0.00%	0
Strongly disagree	0.00%	0
TOTAL		4

Figure 10. Survey Question 3



ANSWER CHOICES	RESPONSES	
Strongly agree	100.00%	4
Somewhat agree	0.00%	0
Neither agree nor disagree	0.00%	0
Somewhat disagree	0.00%	0
Strongly disagree	0.00%	0
TOTAL		4

Figure 11. Survey Question 4



ANSWER CHOICES	RESPONSES	
Strongly agree	100.00%	4
Somewhat agree	0.00%	0
Neither agree nor disagree	0.00%	0
Somewhat disagree	0.00%	0
Strongly disagree	0.00%	0
TOTAL		4

Figure 12. Survey Question 5

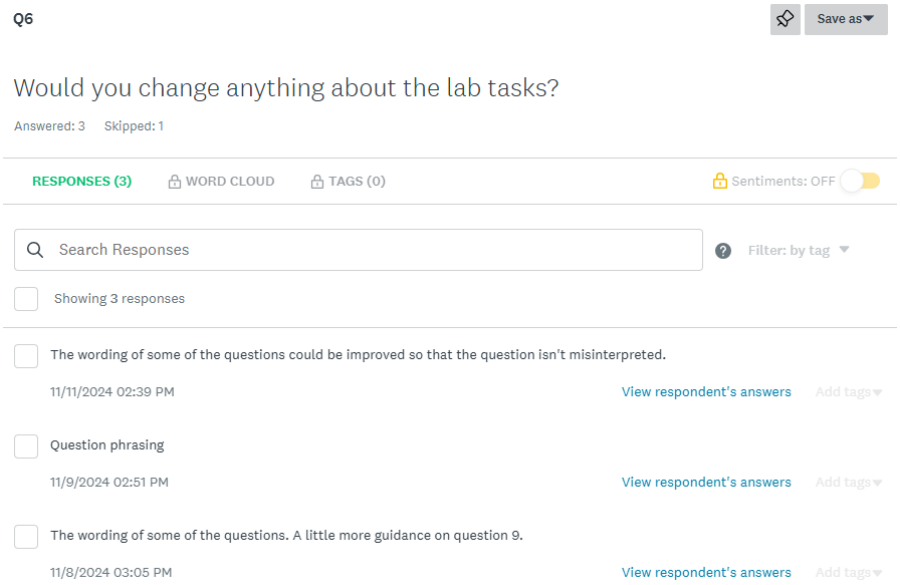


Figure 13. Survey Question 6

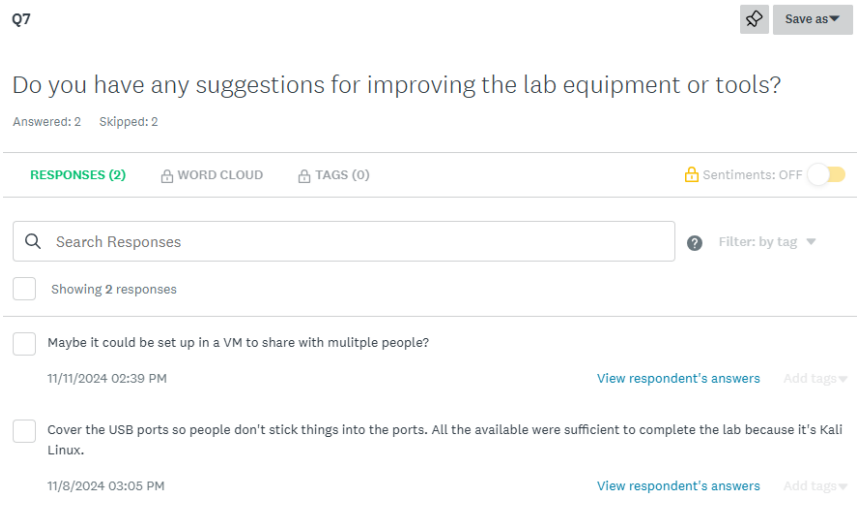


Figure 14. Survey Question 7

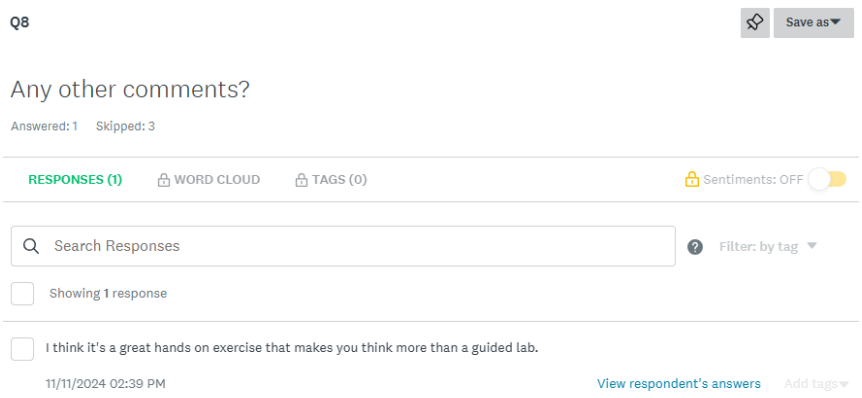


Figure 15. Survey Question 8

Lastly, the lab was built with scalability in mind. The design allows for more virtual machines to be added to the lab, allowing users to expand the lab in the future, both through virtual machine management in Proxmox, and through physical hardware with the usage of a switch to connect devices to the network via ethernet.

CHAPTER 5: CONCLUSIONS AND FUTURE WORK

The completion of this Ethical Hacking environment will enable students to supplement their classroom learning with hands on experience in penetration testing techniques and tools. The Metasploitable 2 framework that is provided inside a virtual machine allows students to test several different avenues and vulnerabilities to test with beyond the given tasks, and Kali Linux provides one of the best toolsets needed to complete those tasks. The tasks are a guide to the methods of penetration testing, but the students have unlimited possibilities to play around with inside this environment, especially with the ability to expand the lab in the future.

Suggestions For Improvement and Future Work

In the short-term future, there are a number of improvements that can be made to allow students a more immersive environment. While the current setup with virtualized machines acting like hardware is a step up from using VMware on a laptop, it can still be improved. The main improvement is to add another desktop computer that can act as a "worker machine" that can be attacked. This would allow users to get even more experience with testing hardware rather than virtualizing machines with Proxmox.

Another potential improvement to the hardware is to add a router and configure DHCP for the local network. This change can create a more realistic network environment that more closely mimics a real-world system. The overall goal of the lab is to mimic what a network may look like out in the real world, and having the full hardware setup to include a router is conducive to the Ethical Hacking lab environment.

The final improvement that could be made is the addition of "blue" or "good guy" hacking exercises. Currently, the tasks that fall under this category are more theoretical and ask the student about how they would do it but does not actually ask them to

implement those changes. The reasoning behind adding these tasks is to encourage students to understand penetration testing, and how to secure the system as well.

Due to the scalability of the lab, there are endless possibilities to add onto the given materials in the future. This can be done in several ways. The first of which is to import virtual machine templates into Proxmox and configuring the machine with the "Snapshot" feature to ensure that it can be rolled back to before a user began testing. This can be expanded for as much as the hardware can handle, with the main limiting factor being RAM, with the server currently only having 24 GB.

While the single server likely can get overwhelmed if lots of virtual machines are imported, the lab also can expand through its hardware as well. Due to the construction of the lab and the focus on hardware components, more hardware can be introduced to the system if desired. The switch allows both the ability to add more servers, more user desktops, and the addition of a router to create a wireless local area network.

Conclusion

Keeping in mind the 6 goals set at the beginning of this project, the completion of the lab environment can be considered successful. To reiterate, the original goals were: Establish an Isolated Network Environment, Integrate Real Hardware with Virtual Machines, develop a Range of Ethical Hacking Exercises, Facilitate Hands-On Learning, Ensure Scalability and Flexibility, and to Document the Setup and Maintenance Process. With these goals in mind, the lab was created to serve the UNCW Cybersecurity community in providing educational value to all levels of students with multiple tasks, allowing students to investigate and answer them using a variety of tools. The lab was built with maintenance and scalability in mind for the lab to be supported for as long as there is a use for it.

REFERENCES

Afamugat, Nart. *Building an Ethical Hacking Environment*, www.theseus.fi/bitstream/handle/10024/752409/Afamugat_Nart.pdf?sequence=2.

Pearson, Martin. "Build a Home Lab: Equipment, Tools, and Tips." *Black Hills Information Security*, 31 May. 2024, www.blackhillsinfosec.com/build-a-home-lab-equipment-tools-and-tips/.

Chou, Te-shun. *The Role of Ethical Hacking and Penetration Testing in Cybersecurity Education*, peer.asee.org/the-role-of-ethical-hacking-and-penetration-testing-in-cybersecurity-education.pdf.

Hill, John. *Using an Isolated Network Laboratory to Teach Advanced Networks and Security*, www.researchgate.net/publication/2485860_Using_an_Isolated_Network_Laboratory_to_Teach_Advanced_Networks_and_Security.

Hu, Yen-Huang. *View of Providing A Hands-on Advanced Persistent Threat Learning Experience Through Ethical Hacking Labs | Journal of The Colloquium for Information Systems Security Education*, cisse.info/journal/index.php/cisse/article/view/153/153.

Kolb, D. A., Boyatzis, R. E., & Mainemelis, C. (2001). Experiential learning theory: Previous research and new directions. Perspectives on thinking, learning, and cognitive styles, 1(8), 227-247.

McFadden, Matthew L. "Cybersecurity Experiential Leadership Learning." *Northeastern University Library*, 2021, library.northeastern.edu/.

"NICE Framework: Current Versions." *NIST*, 9 Oct. 2024, www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions.

"Proxmox VE: Installation and Configuration." *Proxmox Support Forum*, forum.proxmox.com/forums/proxmox-ve-installation-and-configuration.16/.

"Workforce Framework for Cybersecurity (NICE Framework)." *National Initiative for Cybersecurity Careers and Studies*, niccs.cisa.gov/workforce-development/nice-framework.

Van Hoose, Ryan. "Pentesting, Threat Hunting, and SOC: An Overview." *Black Hills Information Security*, 31 Oct. 2024, www.blackhillsinfosec.com/pentesting-threat-hunting-and-soc-an-overview/.