

Tunisian Republic
Ministry of Higher Education
and Scientific Research

University of Sfax

National school of electronics
and telecommunications of Sfax



Departments :
Electronics and communication engineering
Telecommunications engineering

N° d'ordre : GEC-aaa-0-00-00
N° d'ordre : GT-aaa-0-00-00

End of year project thesis

presented at :

**The National School of Electronics
and Telecommunications of Sfax**

Elaborated by :

**Alaa Eddine Ayedi
Ranim Hassine**

**Cybersecurity test and practice environment
With a portable pentesting Lab**

Presented on the 24/04/2024, to the esteemed jury :

M. Achraf Makhlouf
M. Tarek Abbes

Examinator
Supervisor

2023-2024



DEDICATION

Dedicated to those who have been the cornerstone of our journey,

To our esteemed supervisor, whose guidance has illuminated our path with wisdom and insight, we dedicate this work. Your unwavering support and encouragement have been invaluable throughout this academic endeavor.

To our cherished friends, whose laughter and camaraderie have lightened even the heaviest of academic burdens, we offer our heartfelt appreciation. Your companionship has enriched our experience immeasurably.

And to our beloved families, whose endless love, patience, and understanding have sustained us through the challenges and triumphs of this academic pursuit, we dedicate this achievement.

Your unwavering belief in us has been our greatest source of strength.

This thesis stands as a testament to the collective support, encouragement, and love that have shaped our journey. With deepest gratitude, we dedicate this work to you.

For you all,

We dedicated this work.

Alaa Eddine Ayedi AND RANIM HASSINE



REGARDS

Additionally, we extend our sincere regards to all those who have contributed to our academic journey, whether through insightful discussions, constructive feedback, or simply lending an empathetic ear during moments of doubt. Your contributions, no matter how small, have left an indelible mark on our work and our hearts. We express our utmost appreciation for your involvement and support throughout this endeavor.

Furthermore, we offer a special acknowledgment to ourselves, for persevering through the challenges and uncertainties that inevitably arose along this arduous path. It is through our resilience, determination, and unwavering commitment that we stand here today, poised to present this culmination of our efforts. Let us take a moment to commend ourselves for the courage to push forward, even when the journey seemed daunting. Our steadfast dedication has brought us to this moment of achievement, and for that, we offer ourselves heartfelt thanks.



TABLE OF CONTENT

LIST OF FIGURES	vi
LISTE DES ABRÉVIATIONS	vii
CONCLUSION GÉNÉRALE	x
1 Addressing the project	2
1.1 Introduction	3
1.2 Building Your Cybersecurity Skills : A Home Lab Approach	3
1.2.1 Demystifying Cybersecurity	3
1.2.2 Building Your Skills : The Home Lab Advantage	3
1.2.2.1 A Simulated Playground for Learning	3
1.2.2.2 Flexibility and Personalized Learning	4
1.2.2.3 Developing In-Demand Skills	4
1.3 Understanding the Security Spectrum : Blue vs. Red	5
1.3.1 Blue Team : Guardians of the Digital Fortress	5
1.3.2 Red Team : Ethical Hackers on the Attack	6
1.3.3 Blue vs. Red : A Collaborative Ecosystem	6
1.4 Core Concepts : Penetration Testing and Beyond	7
1.4.1 Penetration Testing : Simulating the Attacker	7
1.4.2 Beyond Penetration Testing : A World of Cybersecurity Expertise	8
1.5 Context of the project	8
1.5.1 Motivation	8
1.5.2 Problem Statement	9
1.5.3 State of the Art	9
1.6 Bridging the Gap	9
1.7 Proposed solution	9
1.8 Conceptual Foundation	10
1.8.1 Advantages of Virtual Security Labs	10

1.8.2	Design Considerations for a Secure and Effective Virtual Lab	11
1.9	Unveiling the Virtual Security Lab : Training Grounds	12
1.10	Blue Team Lab	13
1.10.1	Overview and Functionalities	13
1.10.2	Hardware and Software Considerations	14
1.11	Red Team Lab	16
1.11.1	Overview and Functionalities	16
1.11.2	Hardware and Software Considerations	18
1.11.3	Network Topology Design	21
1.12	Conclusion	24
2	TITRE DE CHAPITRE 2	25
2.1	Introduction	26
2.2	Firewall Rule Management with pfSense	27
2.2.1	Introduction to pfSense	27
2.2.2	Functionality of pfSense in the Virtual Security Lab	27
2.2.3	pfSense Management Interface	27
2.2.4	Firewall Rules in the Virtual Security Lab	28
2.2.4.1	Understanding Firewall Rules :	28
2.2.4.2	Rules Applied within the Virtual Security Lab	28
2.3	Cyber Range : Vulnerable Machines for Security Training	29
2.3.1	A Controlled Environment for Security Training :	29
2.3.2	Preloaded Vulnerable Machines :	30
2.3.3	Benefits of Utilizing Vulnerable Machines :	30
2.4	Active Directory Lab	31
2.4.1	Simulating a Corporate Network for Security Training	31
2.4.2	Technical Components :	31
2.4.3	Isolation and Security :	32
2.5	Malware Analysis Sandboxes	33
2.5.1	Safe Detonation and Analysis of Malicious Software :	33
2.5.2	Key Components of the Malware Analysis Lab :	33
2.6	Security Oriented Subnet	35
2.6.1	Centralized Monitoring and Forensics :	35
2.6.2	Benefits of the Security Subnet :	36
2.7	Pentesting Lab : Crafting C1PH3RCR4FT	37
2.7.1	Functionalities of C1PH3RCR4FT in the Virtual Security Lab	37

TABLE OF CONTENT

2.7.2	Main Features of C1PH3RCR4FT	37
2.8	Conclusion	38
	GENERAL CONCLUSION	40
	BIBLIOGRAPHY	40
	ATTACHEMENTS	43
A.1	New forrest deployment	43
A.2	DNS Installation	44
A.3	THE PENTESTER FRAMEWORK	44
A.4	OWASP ZAP	46
A.5	OWASP Netrunner	46



LIST OF FIGURES

1.1	Hypervisor and OS	14
1.2	Raspberry pi 4	17
1.3	Ubuntu logo	18
1.4	VirtualBox Logo	19
1.5	Putty logo	19
1.6	Some Pentesting Framework	20
1.7	Python Logo	20
1.8	Network Topology Design	22
2.1	Applied Firewall Rules	28
A.1	The "Server Roles" page	43
A.2	The "Server Roles" page	44
A.3	Welcome interface of ptf	45
A.4	ZAP attacking interface	46
A.5	OWASP nettacker logo	47



LIST OF ACRONYMS

ACK Acknowledgement

AD Active Directory

ADCS Active Directory Certificate Services

ADUC Active Directory Users and Computers

CA Certificate Authority

CEH Certified Ethical Hacker

CLI Command Line Interface

CPU Central Processing Unit

CVE Common Vulnerabilities and Exposures

DC Domain Controller

DFIR Digital Forensics and Incident Response

DHCP Dynamic Host Configuration Protocol

DMZ Demilitarized Zone

DNS Domain Name System

DNSSEC Domain Name System Security Extensions

FTP File Transfer Protocol

GCC GNU Compiler Collection

GNU

GPMC Group Policy Management Console

GPO Group Policy Object

GUI Graphical User Interface

HTTP Hypertext Transfer Protocol

HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDA	Interactive Disassembler
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPv4	Internet Protocol Version 4
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
OPT	Optional
OSCP	Offensive Security Certified Professional
OWASP	Open Web Application Security Project
PTES	Penetration Testing Execution Standard
PTF	The Pentester Framework
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RFC1918	Request for Comments 1918
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protocol
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSP	System Security Plan
SYN	Synchronize

LIST OF ACRONYMS

TCP Transmission Control Protocol

URL Uniform Resource Locator

VDI Virtual Disk Image

VM Virtual Machine

WAN Wide Area Network

WinRM Windows Remote Management

ZAP OWASP Zed Attack Proxy



GENERAL CONCLUSION

The development and implementation of a portable pentesting lab for cybersecurity testing and practice environments represent a significant step forward in enhancing the practical skills and knowledge of cybersecurity professionals. Throughout this project, we have meticulously outlined the necessary tools, configurations, and methodologies required to construct and utilize such a lab effectively.

By providing a comprehensive guide on building the portable pentesting lab, including configuring machines, setting up pfSense rules, and customizing the distribution, we have empowered cybersecurity enthusiasts and professionals alike to create their own immersive learning environments. This lab serves as a versatile platform for hands-on practice, allowing individuals to hone their skills in various cybersecurity domains, including network security, penetration testing, and incident response.

The portable nature of this lab ensures flexibility and accessibility, enabling users to conduct cybersecurity testing and practice sessions anytime, anywhere. Whether it's exploring new tools and techniques, simulating real-world cyberattacks, or testing defense strategies, the pentesting lab offers a safe and controlled environment for experimentation and learning.

Moreover, the emphasis on highlighting the importance of each step in the setup process, from initial configuration to rule customization, underscores the significance of attention to detail in cybersecurity practices. By understanding the intricacies of building and securing the lab environment, users gain valuable insights into the complexities of cybersecurity operations and the importance of robust security measures.

In conclusion, the creation of a portable pentesting lab serves as a valuable resource for cybersecurity professionals, students, and enthusiasts seeking to enhance their practical skills

and knowledge in cybersecurity. By providing a hands-on learning environment and a comprehensive guide to its setup and utilization, this project contributes to the continuous development and improvement of cybersecurity practices in an ever-evolving threat landscape.

Addressing the project

Sommaire

1.1	Introduction	3
1.2	Building Your Cybersecurity Skills : A Home Lab Approach	3
1.2.1	Demystifying Cybersecurity	3
1.2.2	Building Your Skills : The Home Lab Advantage	3
1.3	Understanding the Security Spectrum : Blue vs. Red	5
1.3.1	Blue Team : Guardians of the Digital Fortress	5
1.3.2	Red Team : Ethical Hackers on the Attack	6
1.3.3	Blue vs. Red : A Collaborative Ecosystem	6
1.4	Core Concepts : Penetration Testing and Beyond	7
1.4.1	Penetration Testing : Simulating the Attacker	7
1.4.2	Beyond Penetration Testing : A World of Cybersecurity Expertise	8
1.5	Context of the project	8
1.5.1	Motivation	8
1.5.2	Problem Statement	9
1.5.3	State of the Art	9
1.6	Bridging the Gap	9
1.7	Proposed solution	9
1.8	Conceptual Foundation	10
1.8.1	Advantages of Virtual Security Labs	10
1.8.2	Design Considerations for a Secure and Effective Virtual Lab	11
1.9	Unveiling the Virtual Security Lab : Training Grounds	12
1.10	Blue Team Lab	13
1.10.1	Overview and Functionalities	13
1.10.2	Hardware and Software Considerations	14
1.11	Red Team Lab	16
1.11.1	Overview and Functionalities	16
1.11.2	Hardware and Software Considerations	18
1.11.3	Network Topology Design	21
1.12	Conclusion	24

1.1 Introduction

1.2 Building Your Cybersecurity Skills : A Home Lab Approach

This chapter introduces the exciting world of cybersecurity and how you can leverage a home lab to develop in-demand skills.

1.2.1 Demystifying Cybersecurity

The digital age has transformed our world, making cybersecurity a paramount concern. In essence, cybersecurity is the practice of safeguarding computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction. This protection is crucial for individuals, organizations, and critical infrastructure alike. From personal data and financial information to healthcare records and national security secrets, a robust cybersecurity posture is essential in the face of ever-evolving cyber threats.

1.2.2 Building Your Skills : The Home Lab Advantage

The ever-evolving field of cybersecurity demands a workforce equipped with practical skills and the ability to adapt to new threats. Traditional training methods, while valuable, can often be cost-prohibitive and lack a hands-on learning approach. Here's where the concept of a home lab shines as a powerful tool for developing in-demand cybersecurity skills.

1.2.2.1 A Simulated Playground for Learning

A home lab is a simulated IT environment you can create on your own computer. Imagine a virtual playground where you can build networks, configure security tools, and experiment with various technologies. Unlike traditional labs with limited access or expensive equipment, a home lab offers :

- **Cost-Effectiveness :** Compared to expensive bootcamps or specialized training programs, a home lab offers a significantly more affordable way to develop your skills. You can leverage open-source software and readily available resources to set up your lab, minimizing financial barriers.
- **Hands-on Practice :** Learning by doing is paramount in cybersecurity. Home labs provide a safe and controlled environment to experiment with security tools, practice vulnerability scanning, simulate security incidents, and test your skills without risk to real systems. This practical experience allows you to solidify theoretical knowledge and gain valuable hands-on experience.

1.2.2.2 Flexibility and Personalized Learning

Home labs cater to individualized learning styles and schedules. You can :

- **Set Your Own Pace :** Learn at your own convenience, mastering concepts before moving on. No fixed schedules or deadlines restrict your progress.
- **Focus on Specific Areas :** Tailor your learning experience by focusing on specific areas of cybersecurity that interest you. Experiment with different security tools and techniques relevant to your career goals.
- **Make Mistakes Without Consequences :** The beauty of a home lab lies in its controlled environment. You can experiment freely, make mistakes, and learn from them without causing damage to real systems or data. This iterative learning process allows you to test your skills and troubleshoot challenges independently.

1.2.2.3 Developing In-Demand Skills

By engaging with your home lab, you can build a strong foundation of technical skills highly sought after in the cybersecurity industry. These skills include :

- **Security Tool Proficiency :** Gain experience using industry-standard security tools for vulnerability scanning, intrusion detection, and security information and event management (SIEM).

- **Network Security Fundamentals** : Learn how to configure firewalls, manage network traffic, and implement security best practices within your simulated network environment.
- **Problem-solving and Troubleshooting** : As you experiment and encounter challenges in your home lab, you'll develop critical problem-solving skills and the ability to troubleshoot security issues effectively.

A home lab is an invaluable investment for aspiring cybersecurity professionals. It empowers you to develop hands-on skills, experiment with various technologies, and gain practical experience at your own pace. As you delve deeper into the world of cybersecurity, your home lab will serve as a springboard for continuous learning and professional development.

1.3 Understanding the Security Spectrum : Blue vs. Red

The world of cybersecurity encompasses two major approaches, each playing a crucial role in safeguarding digital assets : defensive security (Blue Team) and offensive security (Red Team). Understanding these distinct perspectives provides a foundational view of the cybersecurity landscape.

1.3.1 Blue Team : Guardians of the Digital Fortress

Imagine a dedicated team working tirelessly behind the scenes to protect an organization's IT infrastructure from cyberattacks. That's the essence of a Blue Team. Blue Teams act as the guardians of an organization's digital assets, constantly monitoring systems and networks for suspicious activity that might indicate a potential attack.

Their primary focus lies in proactive defense activities, including :

- **Security Monitoring** : Blue Teams employ various security tools to continuously monitor networks and systems for anomalies, potential threats, or unauthorized access attempts.
- **Incident Response** : When an attack occurs, Blue Teams are the first responders, responsible for containing the incident, mitigating damage, and restoring affected systems. This involves

tasks such as isolating compromised systems, eradicating malware, and analyzing the attack to prevent future occurrences.

- **Vulnerability Management** : Proactive Blue Teams actively identify and address vulnerabilities in systems and software. This includes tasks like vulnerability scanning, patching systems, and implementing security best practices to harden defenses.

1.3.2 Red Team : Ethical Hackers on the Attack

While Blue Teams strive to protect, Red Teams take on the role of ethical hackers, simulating cyberattacks to identify weaknesses in an organization's security posture. Think of Red Teams as the internal adversaries, pushing the boundaries of an organization's defenses to uncover potential vulnerabilities that Blue Teams might miss.

Their primary activities include :

- **Penetration Testing** : Red Teams conduct authorized simulated cyberattacks against an organization's systems, networks, or applications to identify exploitable vulnerabilities. They employ various hacking techniques similar to those used by real attackers, but with the goal of improving an organization's security instead of causing harm.
- **Social Engineering** : Beyond technical exploits, Red Teams may also employ social engineering techniques to test the awareness and susceptibility of employees to phishing attacks or other social manipulation tactics.
- **Security Assessments** : Through simulations and analyses, Red Teams conduct comprehensive security assessments of an organization's defenses, identifying vulnerabilities and recommending improvements to strengthen the overall security posture.

1.3.3 Blue vs. Red : A Collaborative Ecosystem

The efforts of Blue Teams and Red Teams are not mutually exclusive; they work together to create a robust cybersecurity ecosystem. By simulating attacks, Red Teams provide the Blue Team with valuable insights into potential weaknesses, allowing them to patch vulnerabilities

and tighten defenses.

This constant testing and adaptation between defense and offense ensures a more secure environment for organizations in the face of ever-evolving cyber threats.

1.4 Core Concepts : Penetration Testing and Beyond

Building a strong foundation in cybersecurity requires understanding essential concepts like penetration testing. This section will delve into this core concept and briefly explore the diverse career paths within the cybersecurity field.

1.4.1 Penetration Testing : Simulating the Attacker

Penetration testing (pentesting), a cornerstone of Red Team activities, plays a critical role in identifying vulnerabilities within a system's defenses. During a pentest, authorized testers act as ethical hackers, employing various techniques and tools to exploit vulnerabilities in a system, network, or application. These simulated attacks mimic tactics used by real attackers, but with a crucial difference : the goal is to uncover weaknesses and report them to the Blue Team so they can be addressed before a real attack occurs.

Benefits of Penetration Testing :

- **Vulnerability Identification** : Pentesting helps identify exploitable weaknesses in systems and applications that might otherwise go unnoticed.
- **Proactive Defense** : By uncovering vulnerabilities, pentesting empowers Blue Teams to prioritize and patch them, strengthening their defenses before a real attacker exploits them.
- **Improved Security Posture** : Regular penetration testing allows organizations to continuously assess and improve their overall security posture, making it more difficult for attackers to gain a foothold.

1.4.2 Beyond Penetration Testing : A World of Cybersecurity Expertise

The cybersecurity landscape offers a diverse range of career paths beyond the Blue and Red Team specializations. Here's a glimpse into some additional areas where cybersecurity professionals can contribute :

- **Security Analysts** : As the detectives of the cybersecurity world, security analysts investigate security incidents, analyze security data to identify threats, and collaborate with other teams to mitigate risks.
- **Incident Responders** : During a security incident, incident responders take charge of containing the attack, eradicating malware, restoring affected systems, and ensuring business continuity. They often possess a strong understanding of forensics and incident response methodologies.
- **Security Architects** : Security architects play a strategic role in designing and implementing security solutions to protect an organization's IT infrastructure. They assess security needs, select appropriate security tools and technologies, and ensure their seamless integration within the existing IT environment.

Penetration testing serves as a crucial element in a comprehensive cybersecurity strategy. As you delve deeper into the world of cybersecurity, you'll discover a vast array of career paths where your skills and knowledge can be applied to safeguard digital assets and combat cyber threats.

1.5 Context of the project

1.5.1 Motivation

The ever-evolving threat landscape necessitates a skilled cybersecurity workforce capable of defending against increasingly sophisticated cyberattacks. However, traditional learning methods

often limit opportunities for hands-on experience due to the risks associated with practicing on real-world systems.

1.5.2 Problem Statement

Current cybersecurity labs often lack the ability to be customized to specific learning goals and struggle to replicate the complexities of real-world attack scenarios. This static learning environment leaves trainees unprepared for the dynamic and ever-changing nature of the cybersecurity field.

1.5.3 State of the Art

While existing resources like physical labs and online platforms offer some level of training, they may come with limitations in accessibility, cost-effectiveness, or the ability to simulate real-world scenarios effectively.

1.6 Bridging the Gap

The limitations of traditional cybersecurity training methods demand innovative approaches that prioritize accessibility, customization, and the ability to simulate real-world scenarios. This is precisely where the concept of a virtual security lab comes into play.

1.7 Proposed solution

To bridge the gap in current cybersecurity training methods, this project proposes the development of a customizable virtual security lab. This cost-effective and accessible solution empowers aspiring cybersecurity professionals to :

- **Build and Configure Blue Team and Red Team Environments :** The virtual lab allows users to build and configure dedicated Blue Team and Red Team workspaces, fostering a comprehensive understanding of both defensive and offensive security strategies. Users

can experiment with industry-standard security tools, including vulnerability scanners, intrusion detection systems (IDS), Security Information and Event Management (SIEM) tools for Blue Team activities, and penetration testing tools for Red Team exercises.

- **Practice Hands-on with Security Tools and Methodologies :** The safe and controlled environment of the virtual lab allows users to test and experiment with various security tools and methodologies without risk to real systems. This hands-on experience is crucial for solidifying theoretical knowledge and developing practical skills.
- **Design and Deploy Custom Security Solutions :** Moving beyond basic configuration, the lab empowers users to design and deploy custom security solutions tailored to specific scenarios. This could involve deploying firewalls, implementing IDS/IPS systems, or configuring security policies to harden their virtual network defenses.
- **Replicate Real-world Security Scenarios with Control and Complexity :** The virtual lab goes beyond static training environments by simulating complex and dynamic attack vectors encountered in real-world scenarios. This controlled environment allows users to experiment and learn from their mistakes without causing damage to real systems, while still experiencing the challenge and complexity of real-world threats.

1.8 Conceptual Foundation

This section establishes a strong foundation for our virtual security lab. We'll explore the key advantages of utilizing a virtual environment for cybersecurity training compared to traditional methods. Following that, we'll delve into essential design considerations that ensure your virtual lab is both secure and effective for learning.

1.8.1 Advantages of Virtual Security Labs

Virtual labs offer a unique and practical approach to cybersecurity training, particularly when building a home lab. Here's how they compare to traditional physical setups :

- **Resource Optimization :** Virtual labs eliminate the need for expensive hardware, reducing setup costs and resource requirements.
- **Scalability and Flexibility :** You can easily scale your virtual lab environment to include additional systems or functionalities within software limitations.
- **Accessibility and Remote Learning :** Virtual labs allow for remote access, enabling flexible training schedules and learning opportunities regardless of location.

Beyond the practical benefits, virtual home labs provide a safe and controlled environment to develop essential cybersecurity skills :

- **Hands-on Practice :** You can experiment with security tools, simulate real-world scenarios, and practice incident response procedures without jeopardizing a production network.
- **Targeted Skill Development :** Focus on specific areas like vulnerability scanning, security information and event management (SIEM), or penetration testing techniques relevant to your chosen security path.
- **Staying Current :** Virtual labs allow you to easily install and test new security tools, helping you stay up-to-date with evolving threats and defensive strategies.

1.8.2 Design Considerations for a Secure and Effective Virtual Lab

To leverage the benefits of virtualization effectively, we need to consider some key design principles :

- **Virtualization Platform Selection :** Choosing the right platform is crucial. Popular options include VirtualBox (free and open-source), VMware Workstation Player (free for personal use), and VMware Workstation Pro (paid, with more advanced features). Consider factors like ease of use, resource requirements (CPU, RAM), and compatibility with your chosen security tools.
- **Balancing Hardware and Complexity :** While virtual environments offer advantages, they still require sufficient hardware resources from the host machine. Carefully balance the complexity of your virtual lab (number and type of VMs) with the capabilities of your host system to ensure smooth operation.

- **Virtual Machine (VM) Planning :** Plan the number and functionalities of your VMs. This might include separate VMs for a target system, a bastion host for launching attacks, and dedicated management VMs. Consider replicating real-world network structures for a more realistic learning experience.
- **Network Segmentation :** Implement network segmentation within your virtual environment to mimic real-world network structures. This could involve separate networks for security zones (e.g., DMZ, internal network), a dedicated attacker VM network, and a management network for example. Network segmentation helps isolate potential security incidents during training exercises.
- **Security Within the Virtual Environment :** Don't neglect security within your virtual network. Use secure communication protocols (e.g., HTTPS), implement access controls for VMs to restrict unauthorized access, and consider snapshotting capabilities for easy rollback in case of security incidents during training exercises.

By carefully considering these design principles, you can create a virtual security lab that is both effective for learning and secure to use. This strong foundation allows you to focus on developing your cybersecurity skills with confidence.

1.9 Unveiling the Virtual Security Lab : Training Grounds

Building on the advantages and design principles discussed earlier, let's delve deeper into the virtual security lab itself. This section will explore its functionalities and configurations specifically tailored to security training objectives. We'll focus on two key configurations :

- **Blue Team Lab :** This section will explore the functionalities of the Blue Team Lab environment, designed to equip users with the skills and knowledge to defend against cyberattacks. We'll discuss the chosen security tools, network segmentation strategies, and training scenarios facilitated by the Blue Team Lab setup.
- **Red Team Lab :** Here, we'll delve into the Red Team Lab environment, focusing on functionalities specific to offensive security training. This includes tools used for penetration testing and how the network design facilitates simulating attacker behavior.

By dissecting these configurations, we will gain a clear understanding of how a virtual security lab can be tailored to develop essential cybersecurity skills for both defensive and offensive security professionals, ultimately preparing them for the ever-evolving threat landscape.

1.10 Blue Team Lab

The Blue Team Lab forms the core of our defensive training. Here, users can simulate real-world security operations, equipping them with the tools and knowledge to become proficient cyber defenders. This immersive environment fosters essential skills like threat detection, analysis, and response, preparing users for the challenges of the modern security landscape.

1.10.1 Overview and Functionalities

Building on the core functionalities mentioned earlier, the Blue Team Lab leverages a comprehensive suite of tools to provide a well-rounded security training experience :

- **Traffic Management and Security Rules** : pfSense, our chosen gateway and firewall, allows users to configure security rules and practice proper traffic management and control, mimicking real-world network security practices.
- **Security Driven Virtual Machines** : Dedicated virtual machines equipped with a variety of tools and softwares provide a platform for users to perform multiple tasks, including collecting logs from various virtual environment sources, identifying security incidents through log analysis and correlation, and so on.
- **Vulnerability Management** : The lab offers a realistic environment to practice vulnerability scanning and remediation processes. Users can deploy vulnerability scanners to identify vulnerabilities within simulated network systems and learn how to prioritize and remediate them before attackers exploit them.



(a) VirtualBox Logo



(b) Kali Linux Logo

FIGURE 1.1 – Hypervisor and OS

- **Malware Analysis :** A dedicated Malware Analysis Lab provides a safe and controlled space to analyze suspicious files and malware samples. Users can leverage pre-installed security tools like sandboxing environments and network traffic analysis tools to investigate malicious code behavior and understand attack vectors.
- **Security Tool Exploration :** The Blue Team Lab environment provides a platform to experiment with various security tools commonly used by professionals. This allows users to explore the functionalities of the security tools we've implemented and experiment with additional tools in a controlled setting, fostering a deeper understanding of the security landscape.

1.10.2 Hardware and Software Considerations

- **Hardware Considerations :** While virtualized, the Blue Team Lab requires sufficient hardware resources from the host machine to function effectively. Users can find online resources to determine if their hardware meets recommended specifications for running virtual security labs. This includes adequate CPU, RAM, and storage space to accommodate various security tools and multiple virtual machines.
- **Software Considerations :** Our Blue Team Lab software stack consists of several key components :

- **Virtualization Platform** : We've chosen VirtualBox as our virtualization platform due to its user-friendliness and suitability for building virtual security labs.
- **Operating Systems** : The lab utilizes a mix of operating systems, such as Linux and Windows, depending on the machine's purpose. This variety reflects real-world scenarios and allows for comprehensive security training.
- **Security Tools** : The core functionality of the Blue Team Lab relies on several security tools :
 - Network firewall and traffic management tools.
 - Security information and event management (SIEM) software for real-time monitoring and log analysis.
 - Additional tools for specific training objectives, such as vulnerability scanners or endpoint detection and response solutions.

The beauty of a virtual security lab lies in its flexibility. Depending on your resources, training goals, and desired complexity, you can tailor the lab's services and deployment.

1.11 Red Team Lab

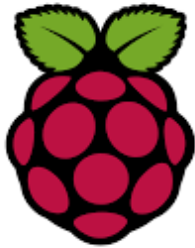
the Red Team Lab was crafted to be the core of our offensive cybersecurity training grounds. This lab is tailored to equip users with the vital tactics and expertise required to launch simulated cyberattacks. In this environment, individuals can practice real-life attack scenarios, sharpen their penetration testing skills, and master the use of critical offensive security tools.

1.11.1 Overview and Functionalities

Envision a sophisticated tool designed for the contemporary cybersecurity professional : a specialized Linux distribution, meticulously crafted for penetration testing and installed on a 64 GB SD card. This system is seamlessly integrated with a Raspberry Pi 4, which boasts 4GB of RAM, creating a compact yet potent pentesting laboratory. This innovative setup transcends traditional limitations, offering a level of portability that revolutionizes the field of cybersecurity. It enables experts to conduct thorough security assessments with unparalleled precision and efficiency. The Raspberry Pi's small size, combined with its computational power, allows this portable lab to serve as a gateway to exhaustive exploration and analysis, unbound by physical constraints. Each command executed, each vulnerability assessed, stands as a tribute to the advancement of technology and the ingenuity inherent in the evolution of cybersecurity practices. This portable pentesting lab not only exemplifies adaptability but also redefines the parameters of cybersecurity assessment. The functionalities of this portable penetration testing lab include :

- **Penetration Testing** : The lab provides a safe environment to practice exploiting vulnerabilities using tools like Metasploit and Burp Suite.
- **Social Engineering** : Users can simulate phishing attacks and other social engineering tactics to understand how attackers manipulate human psychology.
- **Exploit Development** : For those interested in delving deeper, the lab offers the means to research and develop new exploits.
- **Attack Simulation** : The lab's network is designed to mimic a corporate environment, providing a realistic backdrop for testing attack strategies.

- **Portability** : The small size of the Raspberry Pi 4 and the SD card makes it easy to carry around, allowing security professionals to conduct tests anywhere.



(a) Raspberry Pi logo



(b) Raspberry Pi4 4GB RAM

FIGURE 1.2 – Raspberry pi 4

- **Custom Linux Distro** : A specialized Linux distribution designed for penetration testing means that it comes with tools and software specifically for security testing.
- **Large Storage Capacity** : A 64 GB SD card provides ample space for storing tools, scripts, results, and other data.
- **Versatility** : This setup is adaptable to different environments and scenarios, suitable for a wide range of security tasks.
- **Precision Testing** : Tailored for detailed and precise security assessments, allowing for thorough exploration of vulnerabilities.
- **Innovation** : Represents a step forward in cybersecurity tools, offering new ways to approach security assessments.

This lab setup allows security experts to perform comprehensive security tests with the freedom to move beyond the confines of a traditional office or lab setting.

1.11.2 Hardware and Software Considerations

When constructing the Red Team Lab, we must carefully select hardware and software that can support a wide range of penetration testing activities. Our primary device, the Raspberry Pi 4, is not only portable but also powerful enough to run complex tasks. Here are some considerations :

- **Hardware Specs** : The Raspberry Pi 4 with 4GB RAM is our chosen hardware for its balance between performance and portability. It's essential to ensure that the SD card has a high read/write speed to handle the data-intensive operations typical in penetration testing
- **Portability** : The small size of the Raspberry Pi 4 and the SD card makes it easy to carry around, allowing security professionals to conduct tests anywhere.
- **Powerful Hardware** : With 4GB of RAM, the Raspberry Pi 4 can handle various tasks efficiently, making the testing process smoother.
- **Operating System** : Ubuntu is a great choice for its ease of use and support for security tools.



FIGURE 1.3 – Ubuntu logo

- **Virtualization Software** : VirtualBox is the workstation we used because it allows you to create and manage multiple virtual machines (VMs), each with different settings and tools with large flexibility.



FIGURE 1.4 – VirtualBox Logo

- **Remote access** : When managing a Red Team Lab, especially one that includes devices like the Raspberry Pi, remote access is a critical component. PuTTY, a free and open-source terminal emulator, serial console, and network file transfer application, is a key tool for this purpose. It supports several network protocols, including SSH, Telnet, and SCP, to provide secure remote access to network devices and servers

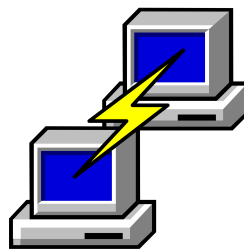


FIGURE 1.5 – Putty logo

- **Pentesting Frameworks :**

- Metasploit : For exploiting vulnerabilities.
- Nmap : For network scanning.
- Wireshark : For analyzing network traffic.
- Burp Suite : For web application security testing.
- PTF : The pentester Framework

images/python.jpg



(a) Nmap Logo



(b) Wireshark Logo



(c) Burpsuite Logo

FIGURE 1.6 – Some Pentesting Framework

Development Tools :

- Python : A programming language that's often used for scripting custom tools and exploits.



FIGURE 1.7 – Python Logo

[label=•]

Additional Security Tools :

- John the Ripper : For password cracking.
- Aircrack-ng : For Wi-Fi network security testing.
- SQLmap : For automated SQL injection and database takeover

Integrating these software elements into the Red Team Lab enriches the learning experience. It allows for a blend of standard industry practices with innovative approaches, fostering a creative and effective environment for mastering offensive cybersecurity skills.

1.11.3 Network Topology Design

This section details the virtual machines (VMs) utilized within the Lab environment and their assigned network configurations.

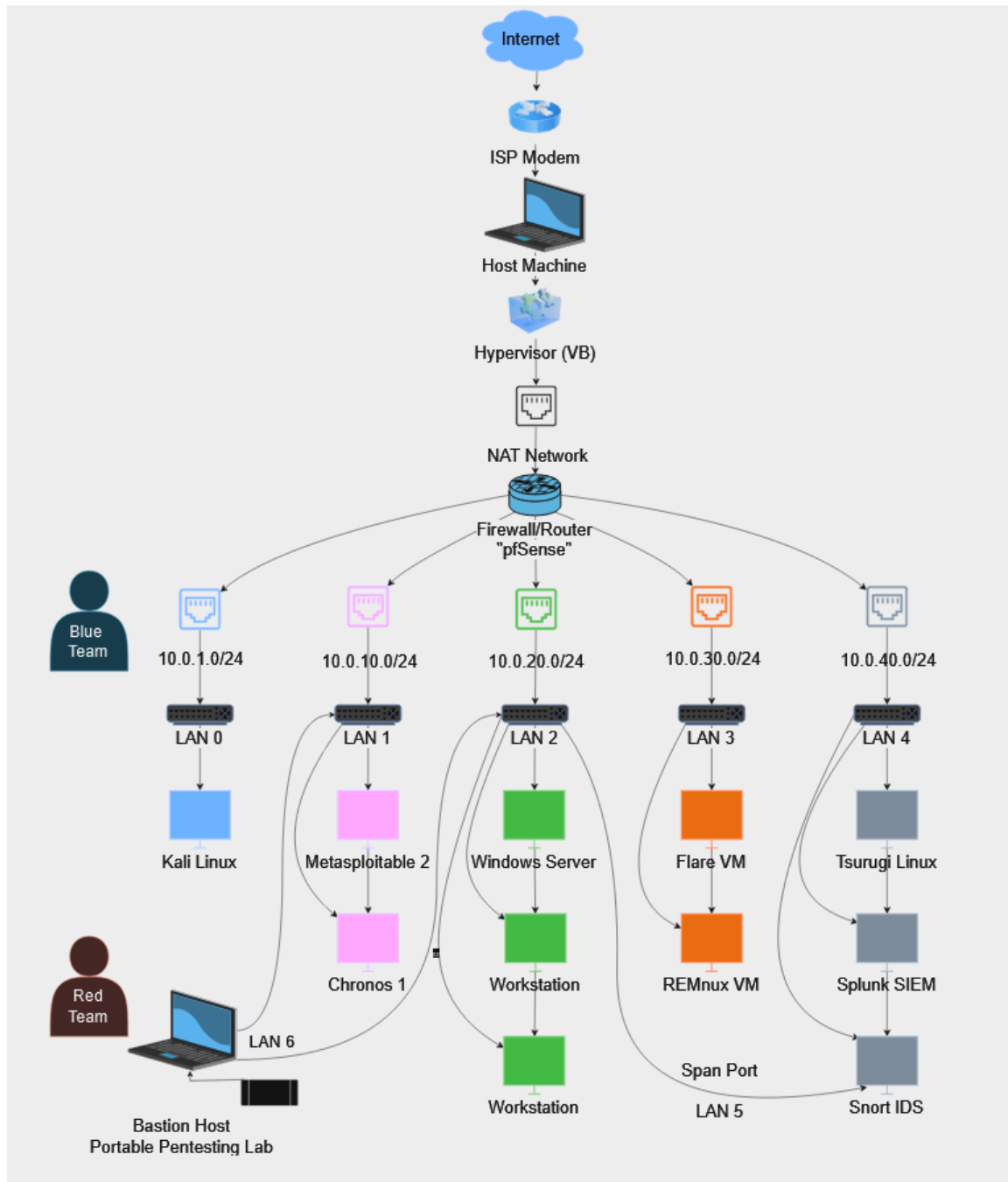


FIGURE 1.8 – Network Topology Design

The Lab network implements a segmented approach to enhance security, mimic real-world network structures, and provide a safe environment for practicing security procedures. Here's a breakdown of the network segments :

- **Management Network (LAN 0) :** Dedicated for managing the virtual lab environment. It provides secure access for lab administrators to configure VMs and deploy security tools. This segment should only be accessible from authorized devices.
(IP Range : 10.0.1.0/24)
- **Cyber Range Network (LAN 1) :** This network segment houses intentionally vulnerable machines for users to practice exploit mitigation and security hardening techniques. Strict access controls will be implemented to prevent unauthorized access and isolate potential compromises within this segment.
(IP Range : 10.0.10.0/24)
- **Corporate Network (LAN 2) :** Represents the simulated production network segment. It houses critical systems like Windows 10 workstations (WORKSTATION) and a Windows Server Active Directory (AD) domain controller. This segment will have traffic restrictions as it is for controlled testing purposes.
(IP Range : 10.0.20.0/24)
- **Malware Analysis Network (LAN 3) :** A dedicated, isolated network segment specifically designed for safe malware analysis. It houses VMs for static and dynamic analysis, preventing potential malware from infecting other segments or your physical machine.
(IP Range : 10.0.30.0/24)
- **Security Team Network (LAN 4) :** Simulates a dedicated network for security personnel. This segment provides VMs for DFIR, OSINT, and other security tools. It has controlled access to the Corporate Network (LAN 2) for retrieving logs, files, and emails necessary for investigations. Additionally, it has unrestricted access to the real internet for utilizing online resources and software updates.
(IP Range : 10.0.40.0/24)

- **Traffic Mirroring Network (LAN 5) :** This segment utilizes a dedicated network interface with an SPAN port to mirror traffic when simulating attacks on the targets, for intrusion detection purposes. Snort, an Intrusion Detection System (IDS) will be deployed within this segment to analyze the mirrored traffic for potential malicious activity. The SPAN port itself will not be assigned an IP address, as it functions to passively replicate network traffic.
- **Bastion Host Network (LAN 6) :** This segment will include a customized portable penetration testing lab which will simulate a malicious device coming from outside. Plus, it will have access only to corporate LAN 1 and 2, meaning it is unable to reach the real Internet or the host machine, to prevent pushing some malicious script/software by accident to external sources.

1.12 Conclusion

In conclusion, the landscape of cybersecurity education highlights the need for accessible and comprehensive training methodologies. Traditional methods often lack practical experience due to constraints like cost and accessibility.

However, with the increasing demand for skilled professionals, innovative solutions are essential. By acknowledging the limitations of current approaches and leveraging advanced technologies, we can bridge the gap between theory and practice.

Moving forward, prioritizing the creation of realistic and safe practice environments will empower learners to tackle real-world cybersecurity challenges effectively. Embracing innovation and collaboration is key to navigating the complexities of the cybersecurity landscape with confidence.

TITRE DE CHAPITRE 2

Sommaire

2.1	Introduction	26
2.2	Firewall Rule Management with pfSense	27
2.2.1	Introduction to pfSense	27
2.2.2	Functionality of pfSense in the Virtual Security Lab	27
2.2.3	pfSense Management Interface	27
2.2.4	Firewall Rules in the Virtual Security Lab	28
2.3	Cyber Range : Vulnerable Machines for Security Training . .	29
2.3.1	A Controlled Environment for Security Training :	29
2.3.2	Preloaded Vulnerable Machines :	30
2.3.3	Benefits of Utilizing Vulnerable Machines :	30
2.4	Active Directory Lab	31
2.4.1	Simulating a Corporate Network for Security Training	31
2.4.2	Technical Components :	31
2.4.3	Isolation and Security :	32
2.5	Malware Analysis Sandboxes	33
2.5.1	Safe Detonation and Analysis of Malicious Software :	33
2.5.2	Key Components of the Malware Analysis Lab :	33
2.6	Security Oriented Subnet	35
2.6.1	Centralized Monitoring and Forensics :	35
2.6.2	Benefits of the Security Subnet :	36
2.7	Pentesting Lab : Crafting C1PH3RCR4FT	37
2.7.1	Functionalities of C1PH3RCR4FT in the Virtual Security Lab .	37
2.7.2	Main Features of C1PH3RCR4FT	37
2.8	Conclusion	38

2.1 Introduction

This chapter serves as the practical cornerstone of this thesis, guiding users through the functionalities and applications of the established Virtual Security Lab environment. Designed to cater to a broad spectrum of cybersecurity enthusiasts and aspiring professionals, this chapter offers a structured learning experience that transcends the limitations of traditional theoretical approaches.

The primary objective of this chapter is to equip users with the necessary knowledge and practical experience to effectively navigate the Virtual Security Lab. This is achieved through a multi-faceted approach that encompasses the following key elements :

- **Network Segmentation Fundamentals :** Users will gain a comprehensive understanding of the lab's network segmentation strategy, delving into the rationale behind the compartmentalization and its significance in maintaining a secure environment.
- **Security Tool Exploration :** The chapter dives into the functionalities and core features of the pre-installed security tools within the lab's virtual machines (VMs). This exploration empowers users to leverage these tools effectively for various security tasks.
- **Scenario-Based Learning :** To solidify theoretical knowledge and cultivate problem-solving skills, users will engage in scenario-based tutorials that mirror real-world security challenges. These interactive exercises provide a practical application of the learned security tools within the context of simulated security incidents.

By fostering a hands-on learning environment, this chapter aims to bridge the gap between theoretical knowledge and practical application within the cybersecurity domain. It empowers users not only to navigate the Virtual Security Lab effectively, but also to lay the foundation for replicating the environment for further independent exploration and skill development. Following the completion of this chapter, users will possess the foundational skill set necessary to embark on their cybersecurity learning journey with confidence.

2.2 Firewall Rule Management with pfSense

2.2.1 Introduction to pfSense

The Virtual Security Lab environment leverages pfSense, a free and open-source firewall/router operating system, as its primary firewall solution. pfSense is widely recognized for its robust security features, ease of management, and extensive community support.

2.2.2 Functionality of pfSense in the Virtual Security Lab

PfSense plays a critical role in managing network traffic within the Virtual Security Lab environment. It accomplishes this through two key functionalities :

- **Traffic Restriction** : pfSense enforces the network segmentation strategy by employing firewall rules. These rules define which traffic is allowed or denied to flow between different subnets, ensuring controlled communication and mitigating potential security risks. We'll delve deeper into firewall rules in a later section.
- **Traffic Routing** : pfSense acts as the central router, directing network traffic between the various subnets within the lab environment and, potentially, towards the internet (depending on the lab's configuration). This ensures efficient data flow and communication between different lab components.

2.2.3 pfSense Management Interface

PfSense offers a user-friendly web-based management interface that simplifies firewall rule configuration, network activity monitoring, and management of other security settings. This centralized interface empowers users to efficiently oversee the lab's network security.

2.2.4 Firewall Rules in the Virtual Security Lab

Firewall rules are the cornerstone of enforcing the network segmentation strategy within the Virtual Security Lab. These rules dictate which traffic is allowed or denied flowing between different subnets, ensuring controlled communication and mitigating potential security risks.

2.2.4.1 Understanding Firewall Rules :

- **Rules Types** : Allow or deny specific traffic based on pre-defined criteria.
- **Traffic Direction** : Inbound (entering a subnet) or outbound (leaving a subnet).
- **Ports and Protocols** : Specify the communication channels (ports) and protocols (e.g., TCP, UDP) for allowed or denied traffic.
- **Source and Destination Networks** : Identify the subnets involved in the communication.

2.2.4.2 Rules Applied within the Virtual Security Lab

The following table summarizes the core elements of the firewall rules implemented within the Virtual Security Lab. By reviewing this table, you can gain a clear understanding of the permitted and restricted traffic flow between different subnets, ultimately contributing to a secure and controlled lab environment.

Rule Type	Traffic Direction	Ports/Protocols	Source Network	Destination Network
Deny	Outbound	Any	LAN Subnets	WAN Subnets
Allow	Internal	Any	CYBER_RANGE subnets	CYBER_RANGE address
Allow	Internal	Any	CYBER_RANGE subnets	10.0.1.2
Allow	Outbound	Any	CYBER_RANGE subnets	RFC1918 (Inverted match)
Deny	Outbound	Any	CYBER_RANGE subnets	Any
Deny	Outbound	Any	AD_LAB subnets	WAN subnets
Deny	Outbound	Any	AD_LAB subnets	CYBER_RANGE subnets
Allow	Outbound	Any	AD_LAB subnets	Any (except WAN & CYBER_RANGE)
Deny	Outbound	Any	SECURITY subnets	WAN subnets
Deny	Outbound	Any	SECURITY subnets	LAN subnets
Allow	Outbound	Any	SECURITY subnets	Any (except LAN & WAN)

FIGURE 2.1 – Applied Firewall Rules

Explanation : These rules control how devices in each Virtual Security Lab subnet can communicate :

- **LAN :** Restricted access to the internet (security measure).
- **Cyber Range :** Devices can talk freely within the range and to a specific device (likely Kali Linux VM) for security exercises. It can also access the internet for simulations.
- **AD Lab :** Isolated from the internet and the Cyber Range to protect the Active Directory domain environment. It can communicate with other internal lab subnets.
- **Isolated Subnet (Malware Analysis) :** Completely locked down to prevent malware from spreading to other parts of the lab.
- **Security Subnet :** Restricted from accessing the internet and the LAN to secure security monitoring tools. It can communicate with other internal lab subnets (except LAN) for analysis purposes.

As demonstrated in the table, pfSense enforces network segmentation within the Virtual Security Lab environment using the set of rules above. The detailed pfSense configuration steps can be found in Appendix X for reference.

2.3 Cyber Range : Vulnerable Machines for Security Training

2.3.1 A Controlled Environment for Security Training :

The Cyber Range subnet within the Virtual Security Lab serves as a dedicated network environment designed for safe and controlled security training. It provides students with a realistic yet isolated space to :

- **Practice Ethical Hacking Techniques :** Lab users can experiment with penetration testing tools and exploit vulnerabilities within preloaded vulnerable machines, gaining valuable hands-on experience.
- **Develop Offensive Security Skills :** By attempting to exploit controlled vulnerabilities, end users learn to identify weaknesses in systems and develop skills to ethically exploit them for security assessments.

- **Test Security Measures :** The Cyber Range allows users to create custom scenarios to test the effectiveness of security controls implemented within the vulnerable machines.

2.3.2 Preloaded Vulnerable Machines :

The Cyber Range utilizes pre-configured virtual machines known for containing exploitable vulnerabilities. Two commonly used examples are :

- **Metasploitable 2 :**
 - This popular virtual machine comes preloaded with a variety of vulnerable operating systems and applications.
 - It serves as a target system for students to experiment with penetration testing tools and exploit known vulnerabilities in a safe environment.
- **Chronos 1 :**
 - Similar to Metasploitable 2, Chronos 1 is another virtual machine platform designed for security training.
 - Chronos versions, like Chronos 1, likely come pre-configured with vulnerable software or operating systems. This allows students to practice vulnerability assessments, penetration testing methodologies, and security hardening techniques in a controlled lab setting.

2.3.3 Benefits of Utilizing Vulnerable Machines :

- **Safe Practice Environment :** The Cyber Range with preloaded vulnerable machines offers a safe space for users to experiment with hacking techniques without risking damage to production systems.
- **Hands-on Learning :** By exploiting vulnerabilities within these controlled environments, users gain practical experience in identifying weaknesses and applying penetration testing tools.

- **Improved Security Skills :** Through these exercises, students develop their offensive security skills, which can be valuable for future careers in cybersecurity or ethical hacking.

The specific vulnerable services and configurations of the preloaded virtual machines within the Cyber Range subnet can be found in Appendix X for reference.

2.4 Active Directory Lab

2.4.1 Simulating a Corporate Network for Security Training

The AD Lab within the Virtual Security Lab replicates a small-scale corporate Local Area Network (LAN) environment built on Active Directory. This controlled environment allows students to :

- **Identify Security Weaknesses :** By working with a pre-configured setup that deliberately disables essential security features and enables commonly exploited services, Lab users can learn to identify potential vulnerabilities in real-world Active Directory environments.
- **Practice Security Assessments and Mitigation :** Users can leverage their understanding of Active Directory to analyze the security posture of the lab, explore potential attack vectors through the enabled vulnerable services, and develop strategies to mitigate these weaknesses.
- **Gain Practical Experience :** The lab also allows students to practice Active Directory administration tasks like managing user accounts, configuring security groups, and implementing domain policies in a safe setting.

2.4.2 Technical Components :

- **Windows Server Domain Controller :** The AD Lab utilizes a single Windows 2019 Server as the domain controller.

- **Security Features Disabled :** To enhance the learning experience related to security vulnerabilities, some security features within the domain controller are intentionally disabled.
- **Client Workstations :** Two workstations running Windows 10 join the Active Directory domain, simulating user workstations within a corporate LAN. This allows users to observe how Active Directory manages user authentication, group memberships, and policy application on these client machines.
- **Common Services :** The domain controller provides essential network services like file sharing, Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP) for a realistic representation of a corporate network environment.
- **Vulnerable Services Enabled :** Specific services on the domain controller and potentially the client machines are configured to be accessible, mimicking real-world scenarios where these services might be exploited by attackers. Some examples of commonly exploited services include Remote Desktop Protocol (RDP), Remote Procedure Call (RPC), and Remote Management (RM).

2.4.3 Isolation and Security :

The AD Lab network is isolated from other subnets within the Virtual Security Lab as defined in the firewall rules early in this project. This isolation ensures that user experimentation with the vulnerable AD environment doesn't pose a risk to other lab components.

The detailed configuration steps for setting up the AD Lab domain controller, client machines, and common services can be found in Appendix X for reference.

2.5 Malware Analysis Sandboxes

2.5.1 Safe Detonation and Analysis of Malicious Software :

The Malware Analysis Subnet within the Virtual Security Lab serves as a dedicated and isolated network environment specifically designed for the safe analysis of suspicious software, commonly referred to as malware. This controlled space allows security researchers and students to :

- **Safely Detonate Malware :** Potentially malicious files or URLs can be detonated within the sandboxed environment, observing their behavior and potential impact without risking damage to production systems. This controlled detonation allows for a risk-free analysis of the malware's capabilities.
- **Analyze Malware Functionality :** By leveraging pre-configured sandbox tools available within the subnet, users can delve deeper into the behavior of the malware. This analysis might involve studying network communication attempts to identify exfiltration or command-and-control (C2) servers, file system modifications to understand potential data manipulation, and registry manipulations that could indicate persistence mechanisms.
- **Develop Threat Detection Techniques :** The isolated environment fosters experimentation with different malware analysis techniques and tools. Researchers can test and refine their approaches, potentially contributing to the development of new methods for identifying and mitigating future threats.

2.5.2 Key Components of the Malware Analysis Lab :

Sandbox Solutions :

- **Flare VM :** The Malware Analysis Subnet utilizes Flare VM, a popular Windows sandbox environment specifically designed for malware analysis. Flare VM offers functionalities such as :

- **Network Traffic Capture** : Capture and analyze network traffic generated by the detonated malware, providing insights into potential communication attempts and data exfiltration.
- **Process Monitoring** : Monitor the processes spawned by the malware, understanding its execution flow and potential interactions with the system.
- **System Snapshotting** : Create snapshots of the system before and after detonation, allowing researchers to analyze changes made by the malware and revert to a clean state if necessary.
- **REMnux** : Is another crucial component of the Malware Analysis Subnet. It's a Linux distribution specifically tailored for security professionals and penetration testing, making it ideal for malware analysis within the Linux environment. REMnux comes pre-installed with a variety of security and analysis tools, such as :
 - **Static Analysis Tools** : Analyze the code of the malware sample to identify potential vulnerabilities or malicious functionalities without actually executing the code.
 - **Dynamic Analysis Tools** : Analyze the behavior of the malware during execution within the sandbox environment, providing real-time insights into its actions.
 - **Debuggers** : Step through the code execution of the malware, allowing for a granular understanding of its operations.

Isolation and Security Measures :

- The Malware Analysis Subnet is meticulously isolated from other subnets within the Virtual Security Lab. This isolation ensures that any potential malware outbreak within the sandbox environment doesn't pose a risk to other lab components or the host machine.
- Additional security measures, such as host-based intrusion detection systems or network traffic monitoring tools, might be implemented to further enhance the security posture of the sandbox environment. These tools can provide real-time alerts and logs, aiding in the detection of suspicious activity within the sandbox.

Benefits of Utilizing Sandboxes :

- **Enhanced Security** : Sandboxes eliminate the risk of infecting real-world systems with potentially destructive malware. Researchers can safely detonate and analyze suspicious samples without jeopardizing critical systems.
- **Improved Efficiency** : Sandboxes allow for quick analysis and containment of threats. By detonating malware within the isolated environment, researchers can swiftly identify its behavior and potential impact, minimizing potential damage and downtime.
- **Effective Threat Research** : The isolated and controlled environment fosters experimentation with different malware analysis techniques and tools. This allows researchers to develop and refine their methodologies, contributing to the advancement of threat detection and mitigation strategies.

The Malware Analysis Lab provides a critical resource for safe malware detonation and analysis, promoting secure threat research within the Virtual Security Lab. Set up details could be found in Appendix X.

2.6 Security Oriented Subnet

2.6.1 Centralized Monitoring and Forensics :

The Virtual Security Lab's Security Subnet plays a crucial role in centralized security monitoring and forensics capabilities. This subnet provides tools and resources for :

- **Real-time Security Monitoring** : Security Information and Event Management (SIEM) software, such as Splunk, is deployed to collect and analyze logs from various security components within the Virtual Security Lab. This allows for real-time monitoring of security events and potential threats.
- **Intrusion Detection and Alerting** : An Intrusion Detection System (IDS) is implemented within the Security Subnet. The IDS actively monitors network traffic for suspicious activities based on predefined rules. Upon detecting anomalies, the IDS logs these events

and forwards the logs to Splunk for centralized analysis and alert generation. This allows security personnel to quickly identify and respond to potential security incidents.

- **Digital Forensics and Incident Response (DFIR) :** The Security Subnet utilizes a dedicated Digital Forensics and Incident Response (DFIR) Virtual Machine (VM), such as Tsurugi Linux. Tsurugi Linux comes pre-installed with a variety of forensic tools and pre-defined rules, enabling efficient investigation of security incidents. Security personnel can use this VM to download suspicious files (like malware) and transfer it to the Malware Analysis Lab, or to analyze files forensically to determine the scope and impact of the incident.

2.6.2 Benefits of the Security Subnet :

- **Enhanced Security Visibility :** Centralized log collection and analysis through Splunk allows for a comprehensive view of security events across the Virtual Security Lab, improving overall security posture.
- **Proactive Threat Detection :** The IDS actively identifies suspicious network activity, enabling early detection of potential intrusions and minimizing potential damage.
- **Efficient Incident Response :** The dedicated DFIR VM equipped with pre-installed tools facilitates efficient investigation and analysis of security incidents, expediting response times and minimizing downtime.

The Security Subnet serves as the central nervous system for security monitoring and incident response within the Virtual Security Lab. By leveraging tools like Splunk, Snort IDS, and Tsurugi Linux, the Security Subnet empowers security personnel to maintain comprehensive security visibility, proactively detect threats, and efficiently respond to security incidents.

The detailed configuration steps for setting up the Security Subnet, including Splunk, Snort IDS, and Tsurugi Linux, can be found in Appendix X for reference.

2.7 Pentesting Lab : Crafting C1PH3RCR4FT

In an age where digital threats loom large, safeguarding data is paramount.

That's where "C1PH3RCR4FT" steps in a portable pentesting lab designed to elevate both professionals and novices in the art of cybersecurity. By democratizing access to essential skills and knowledge, it fosters a community of adept defenders equipped to navigate the complexities of the digital realm with confidence and efficacy. With its innovative design and comprehensive resources, C1PH3RCR4FT heralds a new era of empowerment, where cybersecurity becomes more than just a task ,it's a collective mission to secure our digital future.

2.7.1 Functionalities of C1PH3RCR4FT in the Virtual Security Lab

- **Simulation Environment** : CIPH3RCR4FT provides a realistic simulation environment where users can replicate various network configurations and security setups, allowing for comprehensive testing without real-world consequences.
- **Vulnerability Assessment** : Users can conduct thorough vulnerability assessments, identifying potential weaknesses in systems and networks, and strategizing mitigation tactics.
- **Penetration Testing Tools** : The lab is equipped with a comprehensive suite of penetration testing tools, ranging from network scanners to exploit frameworks, empowering users to assess and exploit vulnerabilities effectively.
- **Learning Resources** : CIPH3RCR4FT offers extensive learning resources, including tutorials, documentation, and interactive exercises, enabling users to deepen their understanding of cybersecurity concepts and techniques.

2.7.2 Main Features of C1PH3RCR4FT

- **Simplicity** : C1PH3RCR4FT boasts a user-friendly interface and intuitive design, ensuring that users encounter minimal complications while maximizing their productivity.

- **Ubuntu Base** : Built upon the reliable foundation of Ubuntu, C1PH3RCR4FT offers stability and familiarity, providing a seamless experience for users accustomed to the Ubuntu ecosystem.
- **Pentester Framework** : Leveraging the Pentester Framework, users can swiftly install a vast array of tools, streamlining the setup process and empowering them to customize their toolkit efficiently.
- **Automated Pentesting Tools** : Integrated with automated pentesting tools like ZAP OWASP and OWASP Netrunner, C1PH3RCR4FT caters to users across the expertise spectrum, from seasoned experts to aspiring beginners, facilitating comprehensive pentesting with ease and efficiency.
- **Portability** : Designed for convenience, C1PH3RCR4FT's portability is unmatched. With a simple plug-and-play setup, powered by the Raspberry Pi, users can effortlessly deploy and utilize the pentesting lab wherever they go, making it an indispensable asset for on-the-go professionals and enthusiasts alike.

2.8 Conclusion

In conclusion, the homelab and test environment presented in this chapter offer a comprehensive platform for cybersecurity enthusiasts and professionals to enhance their skills, explore new techniques, and simulate real-world scenarios in a controlled setting. By dividing the infrastructure into six distinct sections, covering offensive and defensive operations as well as specialized areas like Active Directory management and malware analysis, users have the opportunity to delve deep into various cybersecurity domains.

The setup process, user guides, and benefits outlined for each section provide a clear roadmap for users to get started and make the most of their homelab experience. Whether you're setting up Kali Linux for penetration testing, deploying vulnerable machines for cyber range exercises, or analyzing malware samples for forensic investigation, the homelab offers a flexible and customizable environment to meet your learning objectives.

Moreover, the portability of the homelab, especially with the integration of a Raspberry Pi for easy access, enhances its accessibility and usability. Users can simply plug in the Raspberry Pi and access their homelab remotely, eliminating the need for complex setup procedures and hardware requirements.

Overall, this homelab and test environment serve as a valuable resource for cybersecurity education, training, and research, empowering users to develop their skills, stay updated with the latest trends and techniques, and ultimately contribute to a more secure digital ecosystem. Whether you're a beginner or an experienced professional, the homelab offers endless possibilities for learning, experimentation, and growth in the field of cybersecurity.



GENERAL CONCLUSION

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed non risus. Suspendisse lectus tortor, dignissim sit amet, adipiscing nec, ultricies sed, dolor. Cras elementum ultrices diam. Maecenas ligula massa, varius a, semper congue, euismod non, mi. Proin porttitor, orci nec nonummy molestie, enim est eleifend mi, non fermentum diam nisl sit amet erat. Duis semper. Duis arcu massa, scelerisque vitae, consequat in, pretium a, enim. Pellentesque congue. Ut in risus volutpat libero pharetra tempor. Cras vestibulum bibendum augue. Praesent egestas leo in pede. Praesent blandit odio eu enim. Pellentesque sed dui ut augue blandit sodales. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam nibh. Mauris ac mauris sed pede pellentesque fermentum. Maecenas adipiscing ante non diam sodales hendrerit.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed non risus. Suspendisse lectus tortor, dignissim sit amet, adipiscing nec, ultricies sed, dolor. Cras elementum ultrices diam. Maecenas ligula massa, varius a, semper congue, euismod non, mi. Proin porttitor, orci nec nonummy molestie, enim est eleifend mi, non fermentum diam nisl sit amet erat. Duis semper. Duis arcu massa, scelerisque vitae, consequat in, pretium a, enim. Pellentesque congue. Ut in risus volutpat libero pharetra tempor. Cras vestibulum bibendum augue. Praesent egestas leo in pede. Praesent blandit odio eu enim. Pellentesque sed dui ut augue blandit sodales. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Aliquam nibh. Mauris ac mauris sed pede pellentesque fermentum. Maecenas adipiscing ante non diam sodales hendrerit.



BIBLIOGRAPHY

- [1] **cyberwoxacademy**. Building a Cybersecurity Homelab for Detection Monitoring [Online]. Available on :
<https://cyberwoxacademy.com/building-a-cybersecurity-homelab-for-detection-monitoring/>
- [2] **TheCyberChef**. MONITORING AND DETECTION LAB [Online]. Available on :
<https://medium.com/@cyberchef1/monitoring-and-detection-lab-part-one-cd1c6df25228>
- [3] **0xBEN**. Building a Security Lab in VirtualBox [Online]. Available on :
<https://benheater.com/building-a-security-lab-in-virtualbox/>
- [4] **facyber**. Building Blue Team Home Lab.[Online].Available on :
<https://facyber.me/posts/blue-team-lab-guide-part-1/>
- [5] **darkcybe**. Building a Cybersecurity Home Lab.[Online]. Available on :
<https://darkcybe.gitbook.io/darkcybe/guides/security-engineering/building-a-cybersecurity-home-lab>
- [6] **igorsec on medium**. Snort :Installing, Configuring and Exploring Snort. [online].
Available on :
<https://medium.com/@huglertomgaw/snorting-installing-configuring-exploring-snort-4820c4696e30>
- [7] **CloudzenixIn on medium**. Starting with Splunk : A Comprehensive Guide for Beginners.
[online]. Available on :
<https://medium.com/@cloudzenix.in2023/starting-with-splunk-a-comprehensive-guide-for-beginners-ddf>
- [8] **Active Directory Pro** . How Does Active Directory Work.[Online]. Available on :
<https://activedirectorypro.com/what-is-active-directory/lesson1>

- [9] **CAROLINE on medium** .Building an Active Directory Home Lab.[**Online**]. Available on :
<https://medium.com/@gwenilorac/empowering-your-learning-journey-building-an-active-directory-home-lab-807c436a7f04>
- [10] **GoFetchAD on github** .Automated AD pentesting tool repository .[**Online**]. Available on :
<https://github.com/GoFetchAD/GoFetch>
- [11] **Aleksa Zatezalo on medium**.Exploiting Microsoft's Active Directory .[**Online**]. Available on :
<https://medium.com/offensive-security-walk-throughs/exploiting-microsofts-active-directory-47aa5eb4b4>
- [12] **Tom's Hardware** .How to Set Up a Raspberry Pi for the First Time .[**Online**]. Available on :
<https://www.tomshardware.com/how-to/set-up-raspberry-pi>
- [13] **Trustedsec on github** .The pentester framework repository.[**Online**]. Available on :
<https://github.com/trustedsec/ptf>
- [14] **OWASP nettacker on github** .Automated pentester repository .[**Online**]. Available on :
<https://github.com/OWASP/Nettacker?tab=readme-ov-file>
- [15] **ZAP** .Automated Web repository .[**Online**]. Available on :
www.zaproxy.org/



ATTACHEMENTS

A.1 New forrest deployment

Having established a Windows Server 2019 environment with a designated hostname and static IP address, we can now take the critical step of promoting this server to a Domain Controller (DC) for our Active Directory lab. This process involves installing the necessary roles using Server Manager. We successfully achieved this by launching the "Add Roles and Features Wizard" and selecting "Active Directory Domain Services" for core DC functionality. Additionally, "DNS Server" was chosen to facilitate hostname resolution within the network. The wizard prompted for additional features required by Active Directory, which were confirmed for installation. Following a final confirmation step, the installation process for both roles commenced. Upon completion, we exited the wizard, ready to proceed with the Active Directory domain configuration. On the "Deployment Configuration" page, we opted for "Add a new forest" since we're establishing the first domain in this lab environment, laying the foundation for our Active Directory infrastructure.

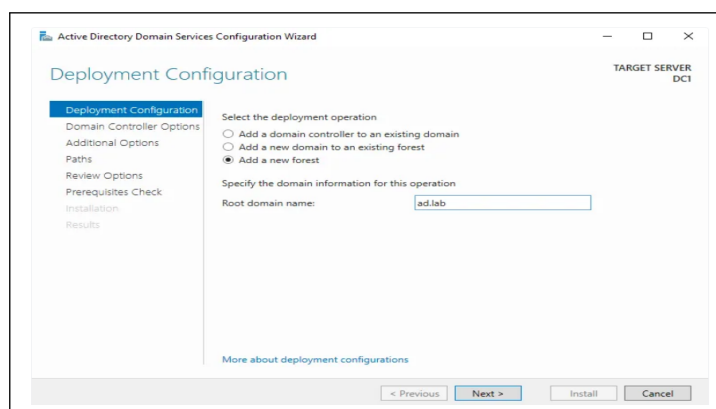


FIGURE A.1 – The "Server Roles" page

A.2 DNS Installation

Having established a Windows Server 2019 environment with a designated hostname and static IP address, we can now take the critical step of promoting this server to a Domain Controller (DC) for our Active Directory lab. This process involves installing the necessary roles using Server Manager. We successfully achieved this by launching the "Add Roles and Features Wizard" and selecting "Active Directory Domain Services" for core DC functionality. Additionally, "DNS Server" was chosen to facilitate hostname resolution within the network. The wizard prompted for additional features required by Active Directory, which were confirmed for installation. Following a final confirmation step, the installation process for both roles commenced. Upon completion, we exited the wizard, ready to proceed with the Active Directory domain configuration and lay the foundation for our lab environment.

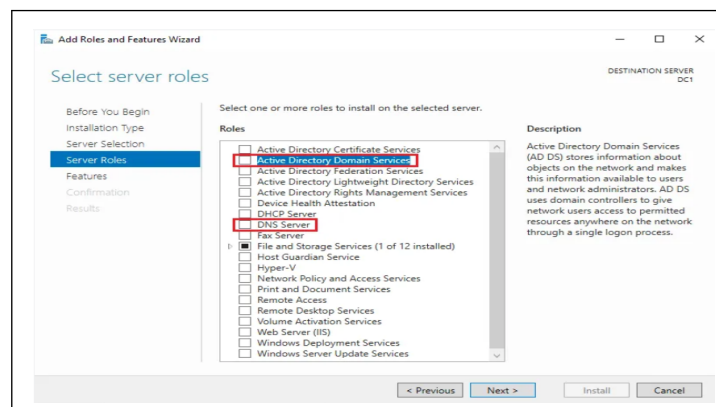


FIGURE A.2 – The "Server Roles" page

A.3 THE PENTESTER FRAMEWORK

PTF serves as a conduit for accessing various security tools, directly sourced from developers' websites. Unlike some platforms, PTF refrains from conducting source code analysis or verification on these tools. Instead, it emphasizes user responsibility, urging individuals to perform their analyses and establish trust with the tool providers. This approach underscores the gravity of trust in the security landscape, where the ramifications of compromised tools can be severe. Thus, users are encouraged to exercise diligence, akin to scrutinizing any software download

from the internet. With this foundation, let's explore how PTF facilitates access to well-known security tools while prioritizing user trust and responsibility.

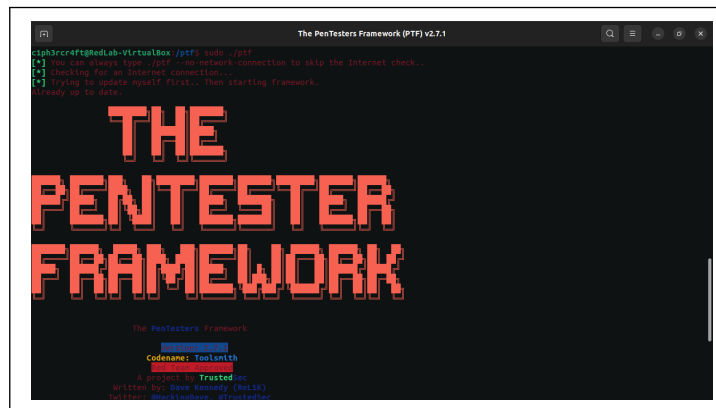


FIGURE A.3 – Welcome interface of ptf

Available from main prompt :

These are the commands you can use directly from the main prompt of PTF.

- **show modules** : Displays a list of available modules (tools) that you can use.
- **show <module>** : Shows information about a specific module.
- **search <name>** : Searches for modules based on a keyword or name.
- **use <module>** : Selects a specific module to use.

Inside modules :

These are the commands available when you're inside a selected module.

- **show options** : Displays the options that can be configured for the selected module.
- **set <option>** : Sets the value of a specific option for the selected module.
- **run** : Executes the selected module with the configured options.

Additional commands :

- **back** : Returns to the previous menu or prompt.
- **help, ?, exit, quit** : Standard commands for getting help, exiting, or quitting the program.

Update or Install :

- **update, upgrade** : Updates or upgrades PTF or its modules to the latest versions.
- **install, run** : Installs or runs PTF or its modules.

A.4 OWASP ZAP

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of The Software Security Project (SSP). ZAP is designed specifically for testing web applications and is both flexible and extensible. At its core, ZAP is what is known as a “man-in-the-middle proxy.” It stands between the tester’s browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application, and as a daemon process.

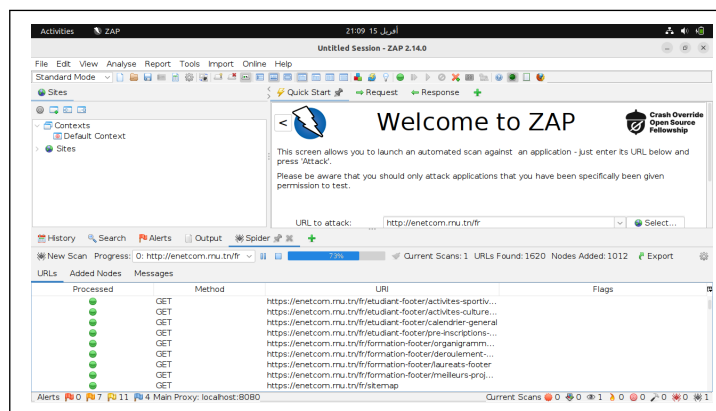


FIGURE A.4 – ZAP attacking interface

A.5 OWASP Nettacker

OWASP Nettacker project is created to automate information gathering, vulnerability scanning and eventually generating a report for networks, including services, bugs, vulnerabilities, misconfigurations, and other information. This software will utilize TCP SYN, ACK, ICMP, and many other protocols in order to detect and bypass Firewall/IDS/IPS devices. By leveraging a unique method

in OWASP Nettacker for discovering protected services and devices such as SCADA. It would make a competitive edge compared to other scanner making it one of the bests.



FIGURE A.5 – OWASP nettacker logo

Cybersecurity test and practice environment

Alaa Eddine Ayedi

Ranim Hassine

Résumé :

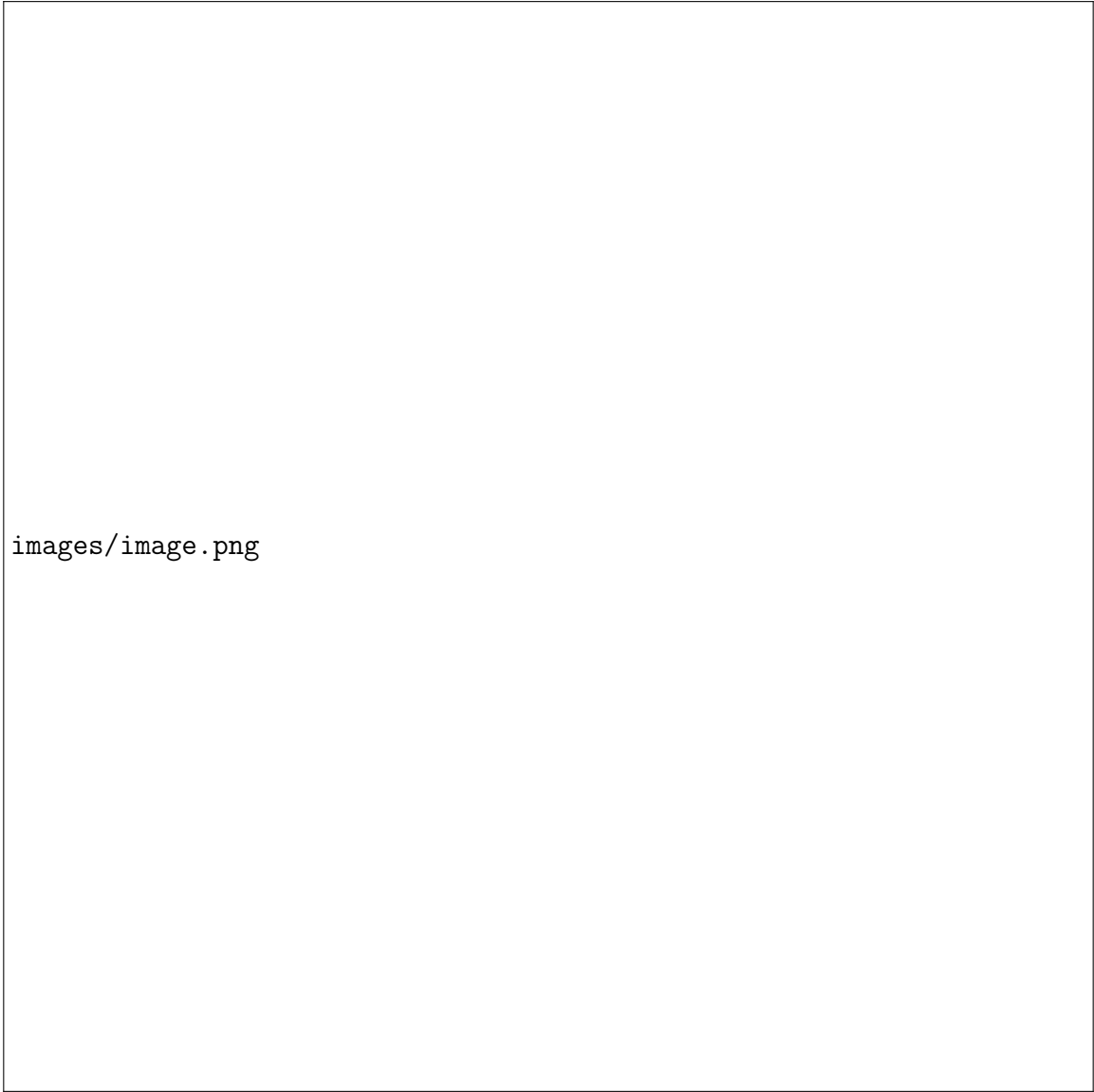
Notre projet propose un environnement de test en cybersécurité avec des capacités de laboratoire portable, comprenant un pare-feu pfSense pour le routage efficace du trafic, et une distribution Linux de pentesting basée sur Raspberry Pi 4 pour le développement de compétences à distance via l'accès SSH.

Mots clés : Cybersécurité, environnement de test, laboratoire portable, pare-feu pfSense, surveillance du trafic, Raspberry Pi 4, distribution Linux pour le pentest, accès distant SSH.

Abstract :

Our project creates a Cybersecurity test platform with a portable pentesting lab. For the blue team, we offer a training environment with a pfSense firewall router for effective traffic monitoring. On the red team side, we provide a beginner-friendly pentesting Linux distribution on a Raspberry Pi 4, enabling remote SSH access for skill development.

Key-words : Cybersecurity, test environment, portable lab, pfSense firewall, traffic monitoring, Raspberry Pi 4, pentesting Linux distribution, remote SSH access.



images/image.png