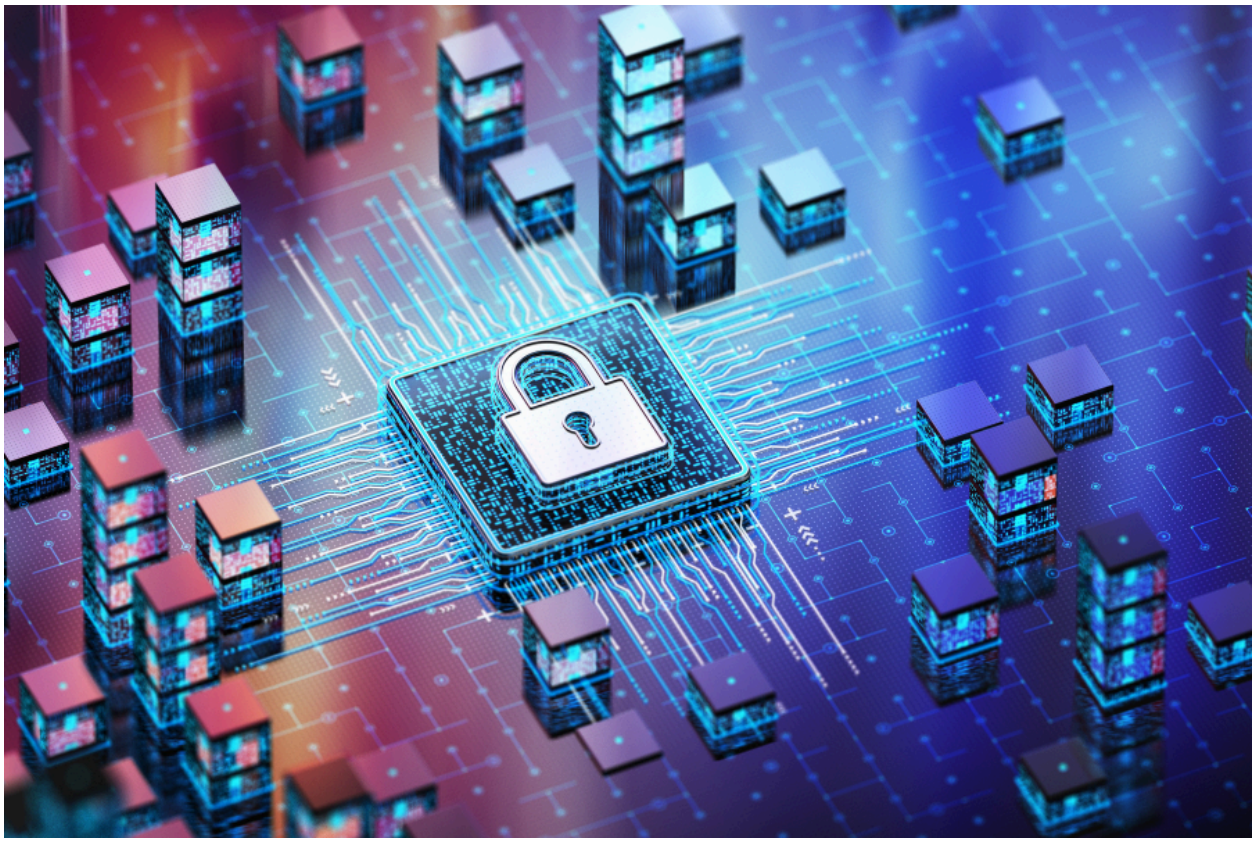
Digital Battleground:

Learning Defensive & Offensive Tactics



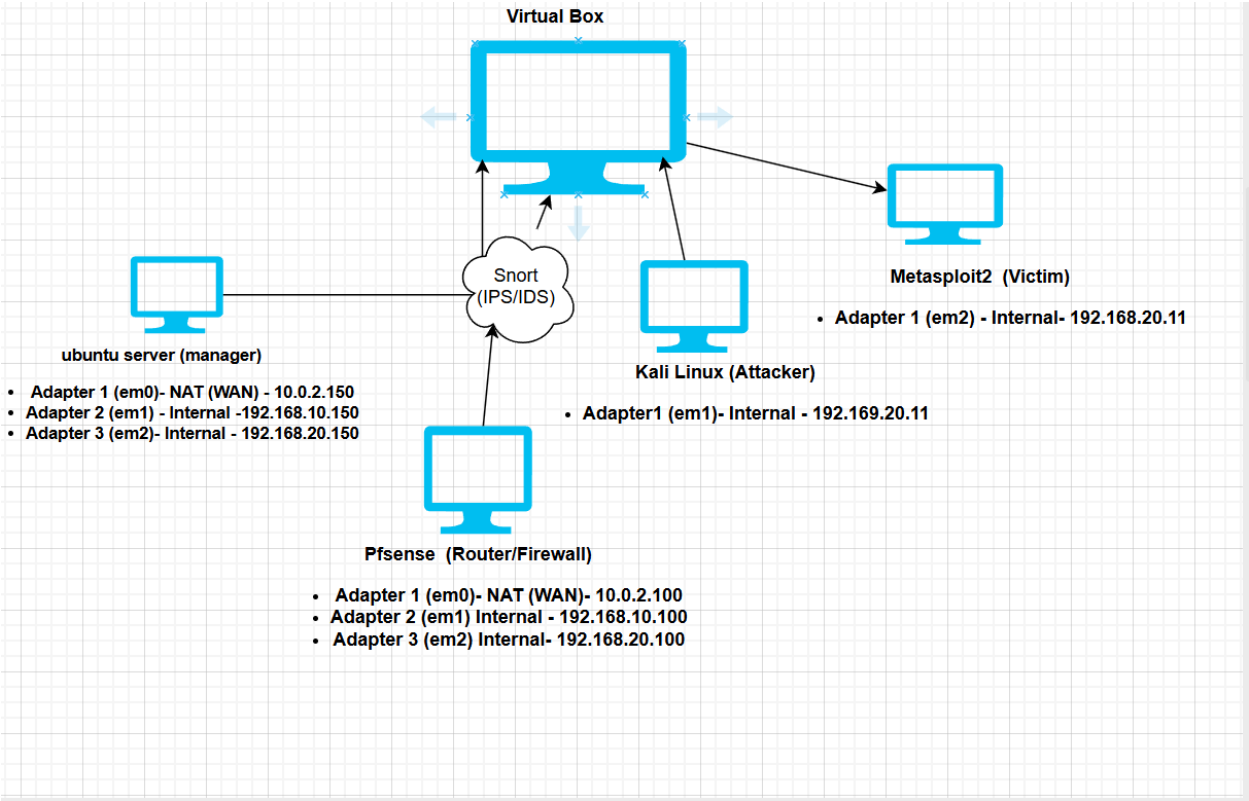
Author: Marshae Bryant

Institution: The Knowledge House

May 25, 2025

Lab Topology

Role	System	IP Address & Adapters
Attacker	Kali Linux	• Adapter 1 (em1): Internal- 192.168.10.5
Victim	Metasploit	• Adapter 1 (em2): Internal 192.168.20.11
Firewall/ IDS/Ips	PfSense & Snort	• Adapter 1 (em0) NAT - WAN - 10.0.2.100 • Adapter 2 (em1) - Internal -192.168.10.100 • Adapter 3 (em2)- Internal- 192.168.20.150
Management	Ubuntu	• Adapter 1 (em0) - NAT - WAN - 10.0.2.150 • Adapter 2 (em1) - Internal -192.168.10.150 • Adapter 3 (em2) - Internal - 192.168.20.150



Introduction:

In today's digital landscape, cybersecurity skills have become more essential for both individuals and organizations seeking to protect their data from malicious attackers. As technology evolves at a rapid pace, so do attackers on the hunt for data

and privacy information have grown exponentially. Everyday new attacks emerge causing one to wonder, “How can I stay protected against cyber attackers?” The answer is being offensively and defensively trained by practicing real-world scenarios – that is how you protect yourself for the digital battleground. Hands-on experience is a critical component in developing skills to defend and mitigate vulnerabilities. The safest and most practical way to practice hands-on cybersecurity skills is in a home lab environment.

This report outlines the design, setup and usage of a personal cybersecurity home lab focusing on both offensive and defensive security techniques. The objective of this lab is to simulate real-world attacks and defense scenarios in order to train and prepare for the current digital battleground we all face today. This lab will help with gaining a deeper understanding of vulnerabilities, threat detection and mitigation strategies.

Tools:

Just like any other battle in history, the way you prepare for battle is contingent on what tools you have in your arsenal. Identify the best tools and their function to accomplish the lab's goal. The lab setup includes virtualized systems configured to support penetration testing (Red team techniques) and defensive monitoring and security hardening (Blue team techniques).

The tools we will include:

- ☐ Kali Linux as the attack machine,

- ☐ Pfsense as the firewall/router,
- ☐ Metasploit 2 as the target machine, and
- ☐ Snort as the IDS/IPS (Intrusion detection/intrusion prevention systems).

Offensive Security (Red Team):

Offensive security is a proactive and adversarial approach to protecting network systems from attacks. Oftentimes, offensive security consists of conducting penetration testing designed to identify vulnerabilities in the system before they are exploited.

To simulate real-world attacks, Kali Linux is used to scan and exploit services on Metasploit. On Kali Linux, there is a tool called Nmap that is widely known and used to scan your victim for vulnerabilities. Common vulnerabilities that can be discovered with Nmap are open ports, vulnerable services detected, and misconfigurations.

In this portion of the lab, we will take our Kali linux machine to do a vulnerability scan using nmap. Before we do the nmap scan, we must go to the Pfsense GUI on our server manager (Ubuntu) and update the firewall rules to allow any packets from other networks to be delivered. If the default firewall settings are not changed, Kali will not be able to ping or do a scan of metasploit. To change the firewall rules, start up the server manager virtual machine and access PfSense through the GUI method. Open a web browser and type in the IP address of your PfSense which in this case is 192.168.10.100 and press search. This should load the pfSense home page where you can log in using the credentials that were created during the initial setup. Once you're logged in, navigate to the ‘Firewall’ tab and click on rules. Click ‘add’ to add a rule. Check for the following fields and tabs: **Action**: Pass, **Interface**: WAN, **Protocol**: Any,

Source: Any, **Destination**: LAN Subnet (pfSense Ip address). Lastly click ‘Save’ and ‘Apply’. This should allow traffic from Kali to Metasploit.

From the Kali terminal, type the command `nmap -A 192.168.20.11`

The output displayed sends a lot of information about metasploit but one line in particular stood out. One of the lines showed ‘vsftpd_234_backdoor’ vulnerability. This indicates that there is a back door that allows attackers to bypass normal authentication and gain unauthorized access. This vulnerability can also be researched on the list of ‘Common Vulnerabilities and Exposures’ as vulnerability number : CVE-2011-2523. If a user attempted to log in with the username “:)”, the back door would activate and open the command shell. This gives the attacker remote command execution capabilities that could lead to full system compromise.

Exploitation steps:

Penetration testing can be a form of ethical hacking. Ethical hacking is the use of hacking skills for legitimate purposes. Ethical hacking helps professionals use techniques to identify and address vulnerabilities in the systems and networks. Ethical hackers typically do not have a malicious goal in mind but the goal of improving security. As an ethical hacker if we want to exploit the system we would want to run;

```
Msfconsole
Use exploit/unix/ftp/vsftpd_234_backdoor
Set RHOST 192.168.56.101
run
```

This portion of the lab helps fully understand the mind and actions of an attacker. It is critical to decipher the moves of a real-world attacker because it will help you have an individual or company defend against an attack. Attacks can happen at any moment

and the proper skills and training can help recognize the patterns of attacks before it even happens.

Defensive Security (Blue Team):

The defensive side of security is more proactive and focuses on prevention, detection and response to cyber threats. This approach is executed before any attacks even happen. On this side of the lab, this is where pfSense will do its job and act as the network's primary firewall. To be proactive PfSense must be configured in a way that interfaces are segmented to isolate internal and external traffic. The rules should be set to only allow necessary traffic from the WAN to LAN. It is best practice when it comes to defending and security hardening to make sure you only allow traffic from devices on the network and no traffic should be allowed from unknown networks.

Another tool that is best used in defensive security is Snort. Snort is a free open-source network intrusion detection and prevention system that monitors network traffic for suspicous activity. Snort is a tool that is deployed on pfSense and is configured with community rules that tigger alerts on known attacks. This means that during the Nmap scan and exploitation, Snort will generate alerts indicating suspicious activity. Once suspicious activity is identified, the next step in defending would be Mitigation. The purposes of mitigation is a technique that is used to reduce the severity of an attack. If there is any indication of malicious activity the blue team must act swiftly. Mitigation stratgies once the suspicious activity is reported would be: blocking IP addresses after repeated scanning attempts, logging and alerting for known exploit

signatures, limiting services exposed on the LAN, creating firewall rules that restrict unnecessary ports.

Security Hardening:

Beyond reacting to attacks, securit hardening is an essential part of defensive security. In order to have a good security posture, it is best practices to get ahead of attacks before they even happen. Security hardening can consists of: regular vulnerability scanning, patch management to update services, disabling unnecessary services, network segementation to minimize attack surfaces, and using honeypots to detect and trap intrusions. Security hardening your network is going to significantly reduce the attack surface and make it harder for attackers to find vulnerabilities to exploit.

Observations:

During this lab, I did run into many errors such as during the pentration testing my Kali would not ping metasploit. I wanted to do a ping of metasploit to test it before i did the nmap scan from my Kali machine. I had to reconfigure the firewall rules and metasploit's network. Another error I observed was, when I tried to install Snort on pfsense, I got an 'Installion failed' error messgae. It would not install Snort because it said anothehr instance of pfSense-upgrade is running. To rectify this issue I changed the WAN on pfSense to DHCP and for the LAN I changed the configurations to static.