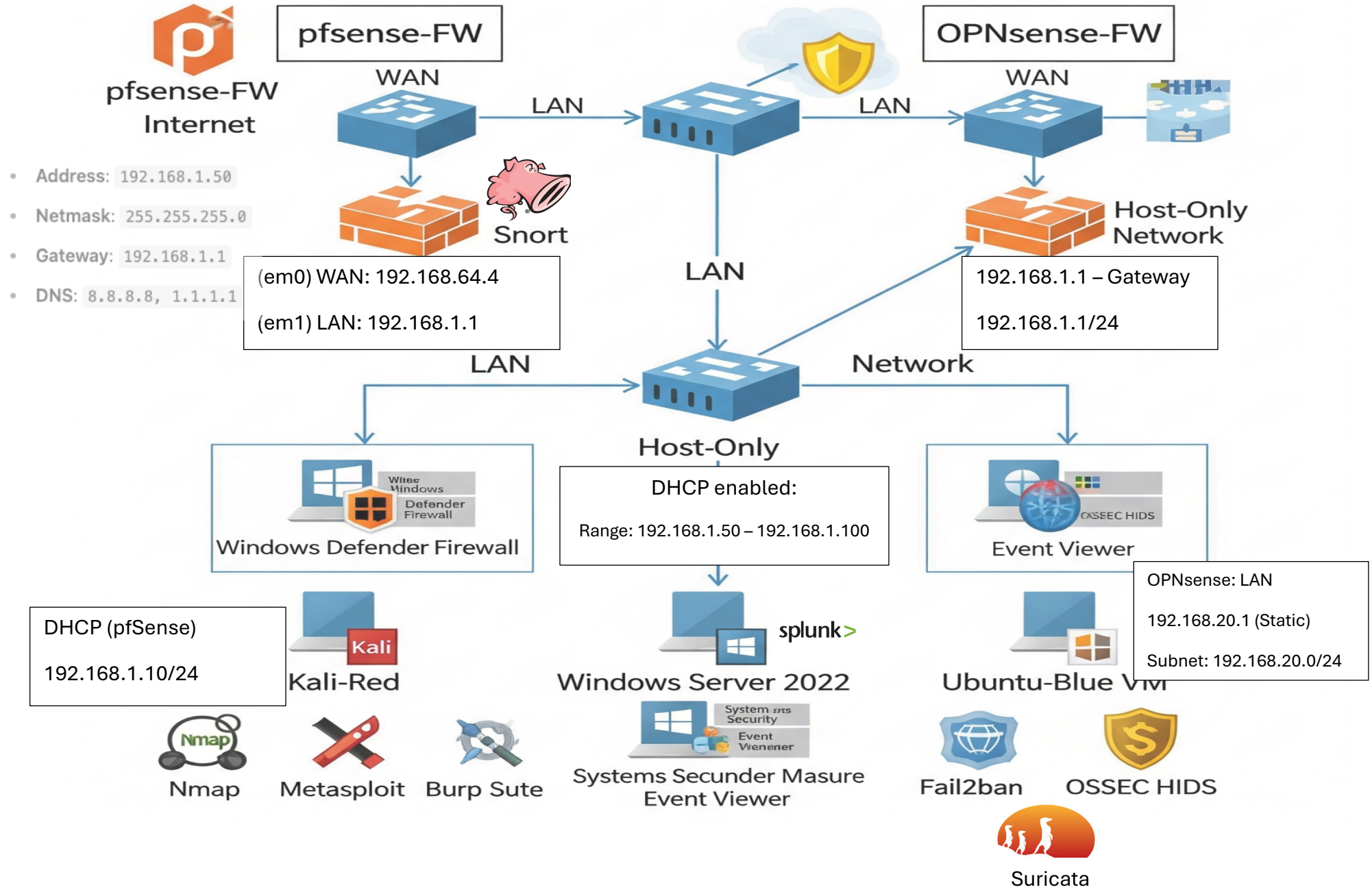
CYBERSECURITY HOMELAB

by HASINA BELTON

May 28, 2025


pfsense-FW
pfsense-FW
Internet
WAN
LAN
OPNsense-FW
WAN
LAN
Address: 192.168.1.50
Netmask: 255.255.255.0
Gateway: 192.168.1.1
DNS: 8.8.8.8, 1.1.1.1
Snort
Host-Only
Network
(em0) WAN: 192.168.64.4
(em1) LAN: 192.168.1.1
LAN
192.168.1.1 – Gateway
192.168.1.1/24
LAN
Network
Host-Only
Windows Defender Firewall
DHCP enabled:
Range: 192.168.1.50 – 192.168.1.100
Event Viewer
OPNsense: LAN
192.168.20.1 (Static)
Subnet: 192.168.20.0/24
DHCP (pfSense)
192.168.1.10/24
Kali
Kali-Red
splunk>
Windows Server 2022
Ubuntu-Blue VM
Nmap
Metasploit
Burp Sute
Systems Secunder Masure
Event Viewer
Fail2ban
OSSEC HIDS
Suricata

Abstract:

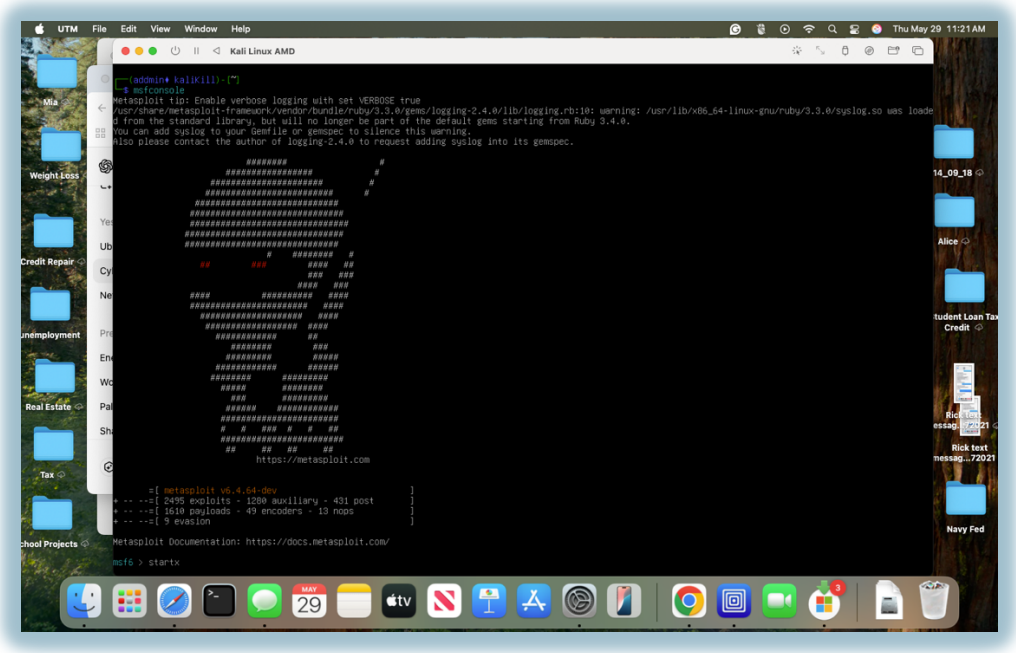
This paper offers a guide and sample to the cybersecurity lab built for hands-on understanding of cyber concepts taught in Phase 1 of the TKH Cybersecurity Fellowship. It walks you through setting up different parts of a virtual network, like firewalls and virtual machines, for practicing real-world security. I'll explore tools found in Kali Linux, understand what pfSense does, and see why systems like Snort or Suricata, are so important for finding and stopping online threats to both enterprise systems and home user. This lab is one option to gain hands-on experience and grow my skills as a cybersecurity engineer to become a great cybersecurity professional.

Kali Linux:

In this cybersecurity lab, a variety of powerful tools are used to provide a comprehensive learning experience for both offensive and defensive security. From the red team's perspective, Kali Linux is employed as the primary attack machine, featuring essential tools such as Nmap for network scanning and reconnaissance, Metasploit and Metasploit 2 for exploit development and execution, and Burp Suite for web application vulnerability testing. These tools enable hands-on practice in identifying and exploiting vulnerabilities within a controlled environment. From the blue team's operations perspective, pfSense acts as a robust firewall, securing the internal network and providing a platform for intrusion prevention. This lab is set up to integrate a Security Information and Event Management (SIEM) system as Splunk for centralized log analysis installed on the Windows Server 2022 Virtual Machine and uses logs provided by Ubuntu Virtual Machine. Suricata, a powerful IDS/IPS, is intended to be used on the Ubuntu-Blue Virtual Machine to monitor internal network traffic for malicious activity and alerts. Windows Server 2022, also serving as a target and blue team component, utilizes Windows Defender Firewall for host-based protection and Event Viewer for crucial system log analysis. Additionally, Ubuntu-Blue incorporates tools like Fail2ban for brute-force attack prevention and OSSEC HIDS for host-based intrusion detection and file integrity monitoring, offering a layered defense approach.

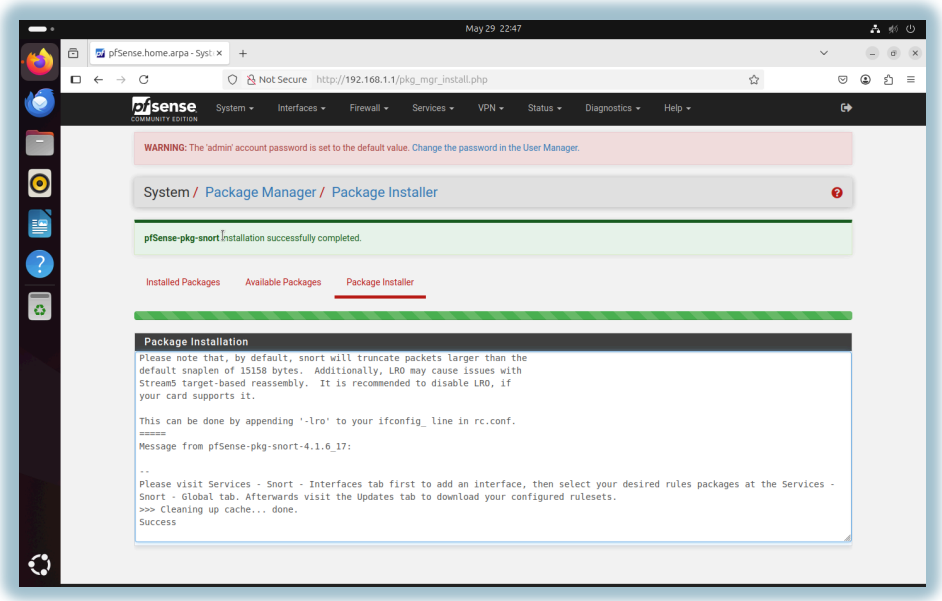
Kali Linux has a variety of special tools to help test computer security. For example, Nmap helps you find other machines and see what services they are running. Hydra can try many passwords quickly to see if a system has weak logins. Metasploit is used to launch known attacks on vulnerable machines like Metasploitable2. Nikto and Burp Suite test websites for security problems. Wireshark also lets you watch network traffic and understand what's happening between multiple machines. These tools are an aid in practicing what real

attackers might do, so I can learn how to stop them. In this lab, they work with pfSense, Suricata, and Splunk to detect and learn from attacks.



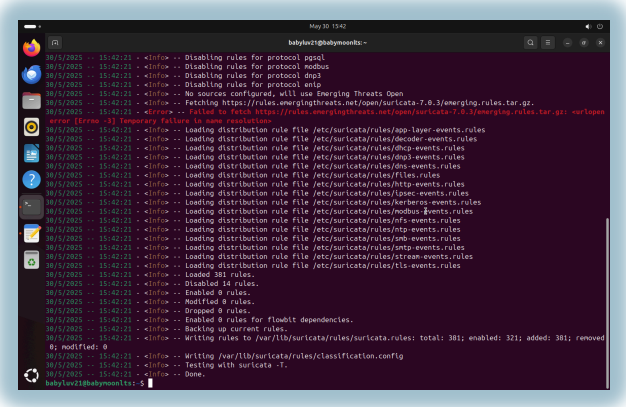
pfSense:

pfSense is a powerful, open-source firewall and router that serves as a core component in this cybersecurity lab. It's based on FreeBSD and acts as a gateway for the internal lab network, controlling all inbound and outbound traffic. Its importance stems from its ability to provide a safe and controlled environment for experimenting with security tools and techniques without impacting the production networks established. Specifically, in this lab, pfSense is crucial for segmenting the network, allowing to isolate the Kali Linux attacker machine and target machines (like Windows Server 2022) from your home network. This isolation ensures that any offensive security exercises, such as vulnerability scanning or exploitation, are confined to this lab environment and do not pose a risk to other personal devices or violate any legal boundaries. Moreover, pfSense allows for the integration of packages like Snort and Suricata, transforming it into an Intrusion Prevention System (IPS) that can monitor and block out malicious activity on the internal lab network. Its robust features, including firewall rules, routing traffic, and support for various security packages, make it a valuable tool for understanding network security fundamentals and practicing defensive strategies in a hands-on manner.



Snort:

Snort is a tool that watches network traffic and looks for signs of attacks. It can work as an IDS, also known as an Intrusion Detection System**,** which alerts you when something suspicious happens. Snort can also work as an IPS, also known as an Intrusion Prevention System**,** which blocks harmful traffic in real-time. IDS and IPS are important because they help protect our computers and data from hackers. They act like hired security, always watching for trouble. Without them, attackers could sneak and penetrate systems without being noticed. Snort uses special rules to detect known threats like viruses, scans, or break-in attempts. It is used by both beginners and professionals to learn and practice network defense. Having an IDS/IPS in this practice lab helps you see attacks clearly and respond quickly to protect assets.



Cyber Home Lab importance:

In the world of cybersecurity, understanding how attackers think and the tools they use is just as important as knowing how to defend. This lab, built carefully with tools like Kali Linux, Metasploitable2, and pfSense, offers a valuable chance to step inside the mind of both the adversary and the protector. It's not a simulated textbook exercise, a system that mirrors the messy, unpredictable nature of the real digital world. This lab becomes a story in itself: one where experience through trial and error, curiosity, and hands-on discovery become the teachers.

By working with this lab, there are small details to see that can lead to big insights. An open port, a weak password, the correct way to install an operating system on different underlying hardware, or a misconfigured rule in a firewall, these aren't just technical flaws. They are the symptoms in a larger narrative about risk, trust, and awareness. Each attack launched and each alert generated builds muscle memory and intuition. Over time, the experience adds to solving larger, more complex issues, no longer just reacting; the experience allows one to begin to anticipate. That shift, from reaction to foresight, is what separates the beginner from the true experienced professional.

Most importantly, this lab fosters something that every great cybersecurity analyst needs to overcome that confidence through experience. One can no longer just read about threats; they are facing real-world scenarios, managing them, and learning how to communicate what matters in a digestible and useful way. That practice, in a safe and controlled space, becomes the foundation for real-world readiness for a learning professional.

Demonstrated Ability:

During Phase One of my cybersecurity training, I successfully demonstrated the ability to apply foundational technical skills by designing and building a fully functional virtual security lab. Using UTM on a Mac Mini, I created and configured multiple virtual machines, including Kali Linux, Ubuntu Server, Windows Server 2022, pfSense, OPNsense, and Metasploitable2. I designed the lab network topology to include both NAT and host-only segments, simulating realistic enterprise traffic flow and segmentation between attacker, defender, and victim systems.

Each component in this lab had a purpose. I configured pfSense as a firewall and gateway, Suricata as an IDS/IPS, and Splunk for log analysis and centralized security monitoring. On Kali Linux, I utilized tools like Nmap, Hydra, and Metasploit to simulate common attacker

behavior, while Ubuntu was used to host Suricata and forward logs. Metasploitable2 served as the vulnerable target, allowing me to test detection and response. Throughout this process, I documented configurations, IP addressing, routing, and interface mapping to ensure clarity and reproducibility.

This project showcases my ability to integrate hands-on technical knowledge with a deep understanding of cybersecurity concepts. I can now confidently describe how firewalls, IDS/IPS, and endpoint logging work together to support a defense-in-depth strategy. More importantly, I've proven I can build and operate these systems in a controlled, safe environment. This experience not only strengthened my technical skills but also deepened my situational awareness, critical for any cybersecurity analyst or defender in training.

Bibliography

1. **How to install Windows Server 2022 on a Mac hosted VM**
   https://www.youtube.com/watch?v=gHpSZ-1eO3w

2. **Cyberwox Blog building a Cyber Homelab**
   https://www.cyberwoxacademy.com/post/building-a-cybersecurity-homelab

3. **Create a virtual Hacking Lab on Apple Silicon Mac**
   https://patrick-rottlaender.medium.com/create-a-virtual-hacking-lab-on-apple-silicon-mac-a86d9b3b2e5f