Final Project Summary – TaZahnae Matthews

Project Title: Kali Linux Attack on Metasploitable 2 through pfSense Firewall

**Project Objective:** The goal of this final project was to build a fully functional and isolated network environment to simulate a cyber-attack scenario. Using Kali Linux as the attacker machine and Metasploitable 2 as the target, the simulation involved routing all traffic through a pfSense firewall to monitor, control, and evaluate network activity. This approach demonstrates essential penetration testing skills and practical understanding of secure network configurations.

---

Network Configuration:

| Machine | IP Address | Network Interface | Subnet | Purpose |
|---|---|---|---|---|
| Kali Linux (Attacker) | 192.168.64.7 | Host-only | 192.168.64.0/24 | Launch attacks |
| pfSense (WAN) | 192.168.64.8 | Host-only | 192.168.64.0/24 | External-facing firewall |
| pfSense (LAN) | 192.168.1.1 | Internal | 192.168.1.0/24 | Routes traffic to LAN |
| Metasploitable 2 | 192.168.1.162 | Host-only/internal | 192.168.1.0/24 | Vulnerable target |
| Ubuntu (Management) | 192.168.64.9 | Host-only | 192.168.64.0/24 | GUI access to pfSense |

---

## ➢ Step-by-Step Process:

- ➢ Setup Virtual Machines: All VMs were installed using UTM on a Mac with M1 chip. Machines included Kali Linux, Metasploitable 2, Ubuntu, and pfSense.

- **Network Configuration**: Networking was carefully configured. Host-only adapters were assigned to allow intra-VM communication while keeping the environment isolated. pfSense was configured with a WAN interface on the same subnet as Kali and Ubuntu and a LAN interface on the same subnet as Metasploitable.

- **Initial Connectivity Test:** Basic connectivity was verified with ping. When issues occurred, such as unresponsive machines or unreachable IPs, IP addresses and subnet settings were checked and corrected in each VM.

- **Accessing pfSense GUI:** Ubuntu was used to access the pfSense GUI at 192.168.1.1. Initial attempts produced a browser warning due to an untrusted SSL certificate. Firefox and Chromium required manual security exceptions to be added to proceed.

- Firewall Configuration: The pfSense firewall was configured by logging into the web GUI. Rules were examined to ensure proper routing between the attacker and target machines. Option 11 in the pfSense terminal was used to restart the web configuration when needed.

- **Troubleshooting Networking Issue**s: Multiple challenges emerged, such as:
    - Machines showing the wrong IP
    - Inaccessible pfSense interface
    - Constant resets to the welcome screen These were resolved by adjusting UTM network settings, setting the interface to "Host-only," and restarting VMs.

- **Port Scanning and Reconnaissance:** With proper routing in place, Nmap was used on Kali to scan Metasploitable 2. Open ports like 443/tcp (HTTPS) confirmed visibility through pfSense.

➢ Conducting Simulated Attacks: Metasploit Framework was initiated on Kali to identify vulnerabilities and exploit open services on Metasploitable. The attack was monitored via pfSense to observe traffic behavior.

---

## Challenges and Fixes:

| Issue/Challenge | Root Cause/Details | Fix/Resolution |
|---|---|---|
| • pfSense repeatedly going to welcome screen | • Improper shutdown or failure to complete setup | • Rebooted pfSense VM and used console option 11 to restart web configurator |
| • "Not Secure" warning in browser | • SSL certificate was self-signed | • Added a security exception manually in Firefox and Chromium |
| • Blank pfSense web GUI page | • Network mismatch or service failure | • Restarted pfSense, verified IP, and reloaded page |
| • HTTP Error 401 (Unauthorized) | • Incorrect login credentials or session timeout | • Retried login after refreshing and verifying credentials |
| • Ubuntu network changed after VM settings | • Changing from Shared to Host-only altered IP | • Checked network settings and corrected subnet to match host-only configuration |
| • Metasploitable unreachable from Kali | • Routing misconfiguration or no firewall pass rules | • Ensured LAN/WAN rules allowed traffic and interfaces matched VM settings |
| • Kali could not reach Metasploitable | • pfSense not routing properly | • Verified pfSense LAN rules, confirmed IP addressing on all machines |

---

Reflections and Lessons Learned:

This project taught me valuable skills in virtual networking, system troubleshooting, and security awareness. One major takeaway was the importance of correctly assigning and managing network interfaces in virtual machines. Any misconfiguration, even as small as the wrong subnet, can cause extensive delays.

I also learned how browser security handles self-signed certificates. Being able to distinguish between genuine threats and controlled test environment limitations helped improve my confidence in managing web and firewall tools. Accessing pfSense through browsers involved repeated steps of adding exceptions and confirming port access.

Another critical learning point was understanding how a firewall like pfSense operates. Not only does it route traffic, but it can also log, control, and block attacks. Observing packets during simulated scans from Kali allowed me to visualize the firewall's function in a real network.

Overall, the successful demonstration of a full attack route from Kali to Metasploitable 2 through pfSense confirmed that a secure, segmented lab can be built using free tools like UTM, open-source OSes, and standard configuration steps.

---

Conclusion:

This project combined network configuration, security simulation, and practical troubleshooting. Despite encountering various hurdles—from pfSense startup errors to connectivity issues—each problem offered an opportunity to gain deeper technical knowledge.

My final setup created a safe environment for testing cybersecurity tools and simulated real-world threats in a closed system. The knowledge gained will directly support my transition into the cybersecurity field.

---

Prepared by:
TaZahnae Matthews
May 2025