Network4Newbs
Eric Jones

1. Project Overview

Objective:

The objective of this lab is to build a virtual security environment using a mini PC, enabling network simulation, penetration testing and containerized application deployment. The project leverages Proxmox, Kali Linux, Docker, Portainer, Metasploit and various other security tools to create a flexible and secure environment for cybersecurity research and testing.

Key Features:

- **Proxmox-** virtualization management
- **PFSense-** firewall configuration
- **Kali Linux-** penetration testing
- **Caldera-** emulation
- **Wazuh-** security monitoring
- **Nessus-** vulnerability scanning
- **Security Onion-** threat hunting
- **TheHive & Cortex-** security incident management
- **bWAPP & DVWA-** web security testing
- **VulnHub-** hosting vulnerable machines
- **Windows Active Directory-** enterprise security testing
- **Windows 10 & 11-** endpoint security testing
- **Ubuntu-** additional Linux
- **Docker & Portainer-** containerized applications

2. Network Architecture

Infrastructure Setup:

The project is hosted on a MIni PC with the following specs:

- **CPU:** Celeron 3.4 GHz
- **RAM:** 16GB
- **Storage:** 512 SSD
- **Network:** Gigabit Ethernet

Virtualized Environment: