SOC Lab Setup – Proxmox + Wazuh (v1)

Overview

The goal of this project was to build the foundation of a Security Operations Center (SOC) lab using a dedicated machine running Proxmox as the hypervisor and Wazuh as the SIEM platform.

1. Set up a segmented virtual network
2. Deploy a Wazuh all-in-one SIEM
3. Troubleshoot real-world infrastructure issues
4. Successfully access and operate the Wazuh dashboard

Infrastructure Setup

Hypervisor: Proxmox VE installed on bare metal with static IP configuration.

Network Architecture

1. vmbr0 – management / internet (10.0.0.x)
2. vmbr1 – isolated internal lab network

Virtual Machine Setup

Wazuh VM Configuration:

1. OS: Ubuntu Server 24.04
2. CPU: 4 cores
3. RAM: 8GB
4. Disk: 80GB
5. NIC 1: vmbr1 (lab)
6. NIC 2: vmbr0 (internet)

Major Issues Encountered & Resolved

1. Incorrect Subnet Configuration

```
192.168.100.2 → changed to 10.0.0.50/24
```

2. Wi-Fi Limitation

Proxmox required wired Ethernet connection to function properly.

3. VM Network Interfaces Down

```
sudo ip link set ens18 up
sudo ip link set ens19 up
```

4. Netplan Configuration

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens18:
      dhcp4: true
    ens19:
      dhcp4: true
```

5. DNS Failure

```
nameserver 127.0.0.53 → replaced with 8.8.8.8 / 1.1.1.1
```

6. Wazuh Installer Issues

Initial download returned XML AccessDenied response instead of script.

7. Ubuntu 24.04 Compatibility

```
./wazuh-install.sh -a –ignore-check
```

Wazuh Installation

Installed Wazuh Manager, Indexer, and Dashboard successfully. All services confirmed running.

Dashboard Access

Successfully accessed dashboard after correcting URL formatting issue.

Final Result

1. Proxmox fully operational
2. Segmented lab network implemented
3. Wazuh SIEM installed and running
4. Dashboard accessible

Key Takeaways

1. Wired networking is critical for hypervisors
2. Network segmentation improves realism
3. DNS and interface configuration are common failure points
4. Always verify downloaded scripts
5. Troubleshooting is part of the process