SIEM LAB SETUP

Objective: Build your own lab environment, understand log sources, and implements basic detection use cases using real tools.

Phase Goals

- Set up a personal cybersecurity lab (your virtual SOC).
- Configure log generation, forwarding, and collection.
- Detect and respond to basic brute-force and login anomalies.
- Create a GitHub repo for weekly progress tracking.

Tools we will work with

- **SIEM:** Wazuh
- **Log Source Simulation:** Ubuntu Machine
- **Monitoring Add-ons:** AuditD and NXLog

1. **Wazuh Installation**
    - First go to the wazuh.com then go documentation and download
    - In this lab we use the Wazuh Machine for log monitoring and analysis. So, we use wazuh OVA File version 4.12.0
    - Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format. This can be directly imported to VirtualBox or other OVA compatible virtualization systems. Take into account that this VM only runs on 64-bit systems with x86_64/AMD64 architecture. It does not provide high availability and scalability out of the box. However, these can be implemented by using distributed deployment.

❖ **Hardware requirements**

- The following requirements have to be in place before the Wazuh VM can be imported into a host operating system:
- The host operating system has to be a 64-bit system with x86_64/AMD64 or AARCH64/ARM64 architecture.
- Hardware virtualization has to be enabled on the firmware of the host.

- A virtualization platform, such as VirtualBox, should be installed on the host system.

Out of the box, the Wazuh VM is configured with the following specifications:

Component	CPU (cores)	RAM (GB)	Storage (GB)
Wazuh v4.12.0 OVA	4	8	50

Download and Install Kali Linux and Ubuntu in VMware

To get started, you'll need VMware installed on your machine. Here are the general steps for downloading and installing **Kali Linux** and **Ubuntu** in VMware, followed by configuring Ubuntu with **Wazuh**.

A. Download Kali Linux and Ubuntu ISOs

1. **Download Kali Linux**:
    - Go to the official Kali Linux website.
    - Choose the appropriate ISO version (e.g., Kali Linux 64-bit).
    - Download the ISO file.
2. **Download Ubuntu**:
    - Go to the official Ubuntu website.
    - Choose the desired Ubuntu version (e.g., Ubuntu 20.04 LTS or Ubuntu 22.04 LTS).
    - Download the ISO file.

B. Install VMware Workstation or VMware Player

1. **Download VMware Workstation Player** (Free for personal use):
    - Go to VMware's website and download the installer.
    - Follow the installation instructions for your operating system (Windows, Linux, or macOS).
2. **Install VMware**:

- Run the installer and follow the on-screen instructions to complete the installation.

C. Create Virtual Machines in VMware

1. **Open VMware Workstation** and click on **Create a New Virtual Machine**.
2. **Configure Kali Linux VM**:
   - Select the **Installer Disc Image File (ISO)** option.
   - Browse and select the Kali Linux ISO you downloaded.
   - Follow the prompts to configure the VM (allocate CPU, RAM, disk space, etc.).
   - Choose **Linux** as the guest operating system and select **Debian 64-bit** for Kali.
   - Finish the setup by clicking **Finish** and then **Power On** the VM.
3. **Install Kali Linux**:
   - Follow the installation prompts (language, timezone, disk partitioning, etc.).
   - Once installation is complete, reboot and login to your Kali Linux machine.
4. **Configure Ubuntu VM**:
   - Similar to Kali, create a new VM, select the Ubuntu ISO, and follow the prompts.
   - Choose **Linux** and **Ubuntu 64-bit** as the OS type.
   - Complete the VM creation and start it.

❖ In this Project we will use the Ubuntu Machine and Wazuh server for monitoring logs. And Monitoring Add-on are for Linux AuditD and NXLog

🛡️ **AuditD (Linux Audit Daemon)**

🔍 **What is AuditD?**

AuditD is the **native Linux auditing framework** used to track system calls and generate detailed logs of user actions, file accesses, permission changes, etc. It's vital for **compliance** (e.g., PCI-DSS, HIPAA) and **intrusion detection**.

🧰 **Use Cases:**

- Monitoring unauthorized access to sensitive files.

- Detecting privilege escalation attempts.
- Tracking changes to system binaries or configs.
- Generating audit trails for incident response or compliance audits.

⚙️ How to Use AuditD

1. Install AuditD (Ubuntu)

- sudo apt update
- sudo apt install auditd audispd-plugins

2. Enable and Start AuditD

sudo systemctl enable auditd

sudo systemctl start auditd

3. View Logs

sudo ausearch

sudo aureport -**a # Summary of audit events**

4. Basic Rule Example: Monitor /etc/passwd

sudo auditctl -w /etc/passwd -p wa -k passwd_changes

- -w: watch this file
- -p wa: watch for write and attribute changes
- -k: attach a keyword for easy searching

5. Permanent Rules

Add them to /etc/audit/rules.d/audit.rules:

-w /etc/shadow -p rwxa -k shadow_file_access

6. Check Logs in Wazuh

If Wazuh is installed:

- AuditD logs are forwarded via the Wazuh agent.
- You can view alerts and events in the Wazuh dashboard (look for auditd or syscheck).

📦 NXLog (Cross-platform Log Collector)

🔍 What is NXLog?

NXLog is a **multi-platform log collection tool** used to collect and forward logs from **Windows, Linux, macOS, and network devices** to destinations like **Wazuh, ELK, Graylog**, etc.

It's especially powerful in environments where you need to collect logs from **non-Syslog-capable systems or Windows machines**.

🧰 Use Cases:

- Collecting Windows Event Logs.
- Forwarding logs from legacy applications.
- Normalizing log formats (JSON, Syslog, GELF).
- Secure forwarding (TLS support).

⚙️ How to Use NXLog

1. Install NXLog (Community Edition)

Windows:

- Download from: https://nxlog.co/products/nxlog-community-edition
- Install and configure via C:\Program Files (x86)\nxlog\conf\nxlog.conf

Linux:

bash

Copy code

```
sudo apt install nxlog
```

2. Sample Config (Windows) – Forward Event Logs to Wazuh

conf

Copy code

```
<Input in>
    Module im_msvistalog
</Input>


<Output out>
    Module om_udp
    Host <wazuh-server-ip>
    Port 514
</Output>
```

<Route 1>

Path in => out

</Route>

3. Start NXLog Service

bash

Copy code

Windows

net start nxlog

Linux

sudo systemctl start nxlog

4. Validate Logs Reaching Wazuh

- Check /var/ossec/logs/ossec.log on the Wazuh server.
- In Kibana or Wazuh UI, search for logs coming from your NXLog hostname.

🔄 AuditD vs NXLog

Feature	AuditD	NXLog
OS	Linux only	Cross-platform (Windows/Linux/macOS)
Focus	System auditing (syscalls, ACLs)	Log collection and forwarding
Ideal for	Compliance, system monitoring	Central log collection, Windows logs
Wazuh integration	Native with Wazuh agent	Custom forwarding
Output formats	Raw audit logs	Syslog, JSON, GELF, XML, etc.

If you're setting up a **Wazuh SIEM** on Ubuntu:

- Use **AuditD** for system activity monitoring.

- Use **NXLog** on Windows clients for Event Log collection if Winlogbeat is not preferred.

Would you like sample configuration files for Wazuh integration using AuditD or NXLog?