🛠 Project 1: Security Monitoring & Incident Simulation Lab

🎯 Goal

Set up a mini SOC (Security Operations Center) environment, simulate an attack, detect it with a SIEM, and document the incident.

You'll show you can:

- Configure monitoring/logging
- Detect suspicious activity
- Investigate and respond
- Write an **incident report**

⚙️ Setup

Virtual Machines (VMs)

- **1 Attacker** → Kali Linux
- **1 Victim/Target** → Ubuntu Server
- **1 SIEM** → Wazuh (open-source SIEM)

(You can use VirtualBox or VMware; allocate ~2GB RAM per VM.)

Tools

- **Wazuh** → SIEM for monitoring/logging
- **Nmap** → network scanning (attacker)
- **Hydra** → brute force login attempts (attacker)

🖥️ Step 1: Install Wazuh SIEM

On your Ubuntu Server (SIEM machine):

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
sudo bash ./wazuh-install.sh -a
```

This installs:

- Wazuh Manager
- Wazuh Dashboard (web interface at `https://<server-ip>:443`)

Default login:

- User: `admin`
- Pass: `admin`

🖥️ Step 2: Install Wazuh Agent on Victim VM

On the **Ubuntu Victim VM**:

```
curl -sO https://packages.wazuh.com/4.9/wazuh-agent-4.9.0.deb
sudo dpkg -i ./wazuh-agent-4.9.0.deb
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Then configure the agent to talk to SIEM:

```
sudo nano /var/ossec/etc/ossec.conf
```

Find `<address>` and replace with your SIEM server IP.
Restart:

```
sudo systemctl restart wazuh-agent
```

Now the victim’s logs will flow into Wazuh.

💻 Step 3: Simulate an Attack from Kali

From **Kali Linux (attacker)** → brute force SSH on the victim:

```
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://<victim-ip>
```

Also run an **Nmap scan**:

```
nmap -A <victim-ip>
```

These should trigger alerts in Wazuh.

💻 Step 4: Detect & Investigate in Wazuh

1. Log into Wazuh Dashboard (`https://<SIEM-IP>:443`)
2. Go to **Security Events** → search for:
   - `authentication failure`
   - `sshd` brute force
   - Port scanning detection
3. Take **screenshots** of the alerts.

💻 Step 5: Document the Incident

Write an **Incident Report** (1–2 pages). Example structure:

Incident Report – SSH Brute Force Attempt

- **Date/Time:** [Timestamp from logs]
- **Source IP:** [Attacker IP]
- **Target IP:** [Victim IP]
- **Detection:** Wazuh alert “Multiple SSH authentication failures”
- **Impact:** Unauthorized access attempt (not successful)
- **Mitigation:** Block attacker IP with firewall, enforce strong passwords, enable MFA

Save this as **incident-report.pdf** and add screenshots.

📂 Deliverables for Portfolio

- **Screenshots:** Wazuh alerts, attack commands, logs
- **Incident Report PDF**
- **GitHub Repo Folder:**
- `project1-soc-lab/`
- `├── incident-report.pdf`
- `├── screenshots/`
  `└── setup-notes.md`