📅Mini SOC Project - Brute Force Detection using Wazuh + Suricata

🕰️Overview

This project simulates a mini Security Operations Center (SOC) environment using:

- **Ubuntu (SOC Server)** running **Wazuh** and **Suricata**
- **Windows 10 VM (Target System)**
- **Kali Linux (Attacker System)**

The objective is to detect and alert brute-force login attempts on a Windows 10 machine using a centralized monitoring solution.

🔧Tools & Technologies Used

Tool	Purpose
Wazuh	SIEM and endpoint detection/alerts
Suricata	Network-based intrusion detection
Hydra	Brute-force attack simulation
VirtualBox	Virtualization
Ubuntu	SOC base OS
Windows 10	Target endpoint
Kali Linux	Attacker machine

💶Architecture

```
+---------------------+           +-----------------------+
|      Kali Linux     |---------->|   Windows 10 Target   |
| (Attacker w/ Hydra) |  SMB/RDP  | (Wazuh Agent Installed)|
+---------------------+           +-----------------------+
                                          |
                                          | Agent Reports
                                          v
                               +------------------+
                               |   Ubuntu Server   |
                               | Wazuh + Suricata |
                               +------------------+
```

🎓Learning Objectives

- Understand how SIEM systems monitor endpoint activity
- Detect brute-force attacks using centralized logging
- Gain experience with Wazuh, agents, and alert rules
- Practice simulated attacks using real tools (Hydra)

🕐Step-by-Step Implementation

🔗Step 1: Environment Setup

- Created 3 VMs in VirtualBox:
- Ubuntu (for Wazuh + Suricata)
- Windows 10 (target machine)
- Kali Linux (attacker)

🔗Step 2: Wazuh Installation

- Installed **Wazuh Server** and **Dashboard** on Ubuntu
- Installed **Wazuh Agent** on Windows 10
- Connected agent to server and verified it appears in the Wazuh dashboard

🔗Step 3: Simulating Brute-Force Attack

- Used Hydra to target Windows 10 login:

```
hydra -l justs -P /usr/share/wordlists/rockyou.txt rdp://192.168.x.x -t 1 -W 3
```

- Tried different services like `rdp` and `smb` on port `3389` and `445`

🔗Step 4: Monitoring Alerts

- Opened **Wazuh Dashboard > Security Events**
- Filtered by Authentication Failures
- Verified detection of brute-force attempts

📊Sample Alert Observations

Metric	Value
Total Alerts	152
Authentication Failures	13
Authentication Successes	43
Level >= 12 Critical Alerts	0

Real-time visibility into login attempts was successfully achieved.

🕠Outcome

We successfully:

- Created a functioning SOC environment
- Simulated a brute-force attack using Hydra
- Detected and verified alerts in Wazuh

This project demonstrates a hands-on understanding of endpoint monitoring and threat detection using open-source tools.

🗜️Next Steps

- Improve detection rules in Wazuh
- Enable email or Slack notifications
- Add more endpoints (Linux, Web Servers, etc.)
- Explore integrating with ELK Stack or Grafana

💼Author

Chinnu\ Offensive Security Learner | Building skills in real-world SOC setups\ GitHub: [your-repo-link]