📄Mini SOC Project – Task 1 Report + Interview Q&A

🔗FINAL PROJECT REPORT

📌Project Title:

Mini SOC Setup for Detecting Brute-Force Attacks using Wazuh + Suricata

Objective:

To simulate a real-world Security Operations Center (SOC) using open-source tools and detect brute-force login attempts on a Windows machine from a Kali Linux attacker VM.

🛠️Environment Setup:

VM	OS	Role	Key Tools
1	Ubuntu	SOC Server	Wazuh + Suricata
2	Windows 10	Target Machine	Wazuh Agent
3	Kali Linux	Attacker	Hydra (for brute force)

🔐Attack Scenario:

- The attacker (Kali) uses `Hydra` to brute-force RDP and SMB logins on the Windows 10 machine.
- The Windows 10 machine has a Wazuh agent installed that monitors log files and reports to Wazuh Server.
- Suricata passively analyzes network traffic for signs of brute-force activity.

🔍Detection Workflow:

1. **Hydra** was used to launch brute-force attacks:

```
hydra -l justs -P /usr/share/wordlists/rockyou.txt rdp://192.168.52.129 -t 1 -W 3
```

1. **Wazuh Agent** sent logs to Ubuntu server.

2. **Wazuh Dashboard > Security Events** showed:

3. 🔐Authentication failures: 13

4. 🔗Authentication successes: 43

5. Real-time monitoring confirmed Wazuh's capability to detect brute-force attempts accurately.

📏Screenshots Collected:

- Agent successfully connected.
- Hydra attack in progress.
- Wazuh Dashboard alerts.
- Brute-force detection alerts in "Security Events".

📊Outcome:

Metric	Value
Total Agents Connected	1
Brute Force Detection	🔗Yes
Alerts Raised in Wazuh	🔗Yes
Dashboard Visibility	🔗Yes

🕐Skills Demonstrated:

- SIEM setup (Wazuh)
- Suricata deployment
- Windows agent configuration
- Wordlist-based brute-force attack simulation
- Real-time log monitoring & alerting

📁Project Assets:

- Wordlist: `rockyou.txt`
- Protocols used: `SMB`, `RDP`
- Detection Points: Log monitoring + Suricata traffic inspection

---

🕐INTERVIEW Q&A

1. What is the objective of your Mini SOC project?

To simulate a SOC setup using open-source tools that can detect brute-force attacks on endpoints (Windows) using centralized monitoring via Wazuh.

2. What tools did you use?

- **Wazuh**: SIEM and endpoint monitoring
- **Suricata**: Network-based IDS/IPS
- **Hydra**: For simulating brute-force login attacks
- **VirtualBox**: Virtual lab environment

3. How did you simulate the brute-force attack?

Using Hydra from Kali Linux to attempt thousands of RDP login attempts to the Windows 10 machine:

```
hydra -l justs -P /usr/share/wordlists/rockyou.txt rdp://192.168.52.129 -t 1
-W 3
```

4. What did Wazuh detect?

- 13 failed login attempts
- 43 successful logins (from normal interaction)
- Security alerts shown in the Wazuh dashboard's "Security Events" tab

5. How did you ensure the Windows agent was working?

- Installed Wazuh agent on Windows 10
- Registered it using an agent key on the Ubuntu Wazuh server
- Confirmed connection on the Wazuh Dashboard

6. What role did Suricata play in this setup?

It helped inspect network traffic passively to detect patterns (e.g., RDP/SMB brute force behavior). While not heavily used for this task, it can enrich detection in future steps.

7. What challenges did you face?

- Agent registration issues
- Service start errors on Windows (Access Denied)
- Rockyou.txt wordlist decompression
- Low alert count when services were misconfigured

8. How can this setup be improved further?

- Add email/Slack notifications for high-level alerts
- Include Linux targets and web servers
- Fine-tune Wazuh rules and thresholds
- Integrate with ELK or Grafana dashboards

🔗TASK 1: COMPLETE 📀