Wazuh SIEM Home Lab Project

📌 Overview

This project demonstrates the deployment and configuration of **Wazuh SIEM** for log collection, brute-force attack detection, and file integrity monitoring (FIM).
It was built as part of my SOC Analyst learning journey to gain **hands-on experience** with SIEM tools and incident detection.

The goal of this lab is to simulate **real-world SOC scenarios** and document the process in a structured, professional manner.

Lab Environment

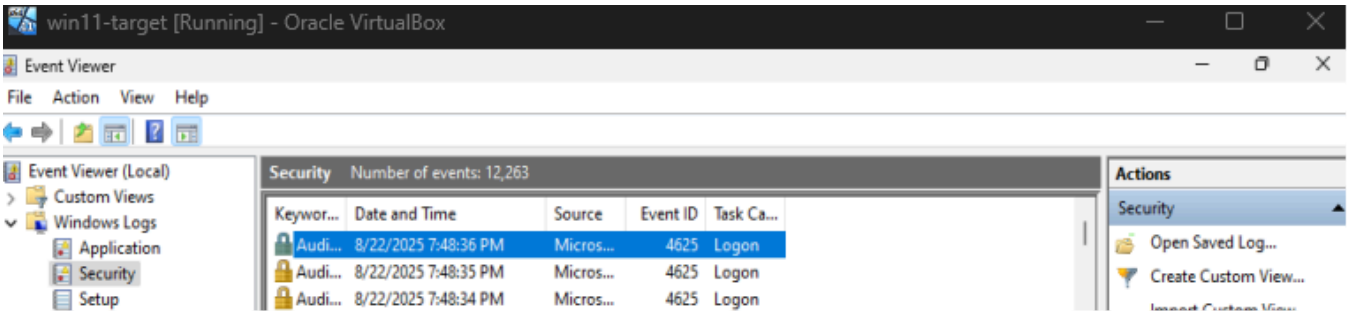
- **Wazuh Manager** → Ubuntu Server (on VMware/VirtualBox)
- **Windows 11** → Target machine with RDP enabled
- **Kali Linux** → Attacker machine for brute force simulation

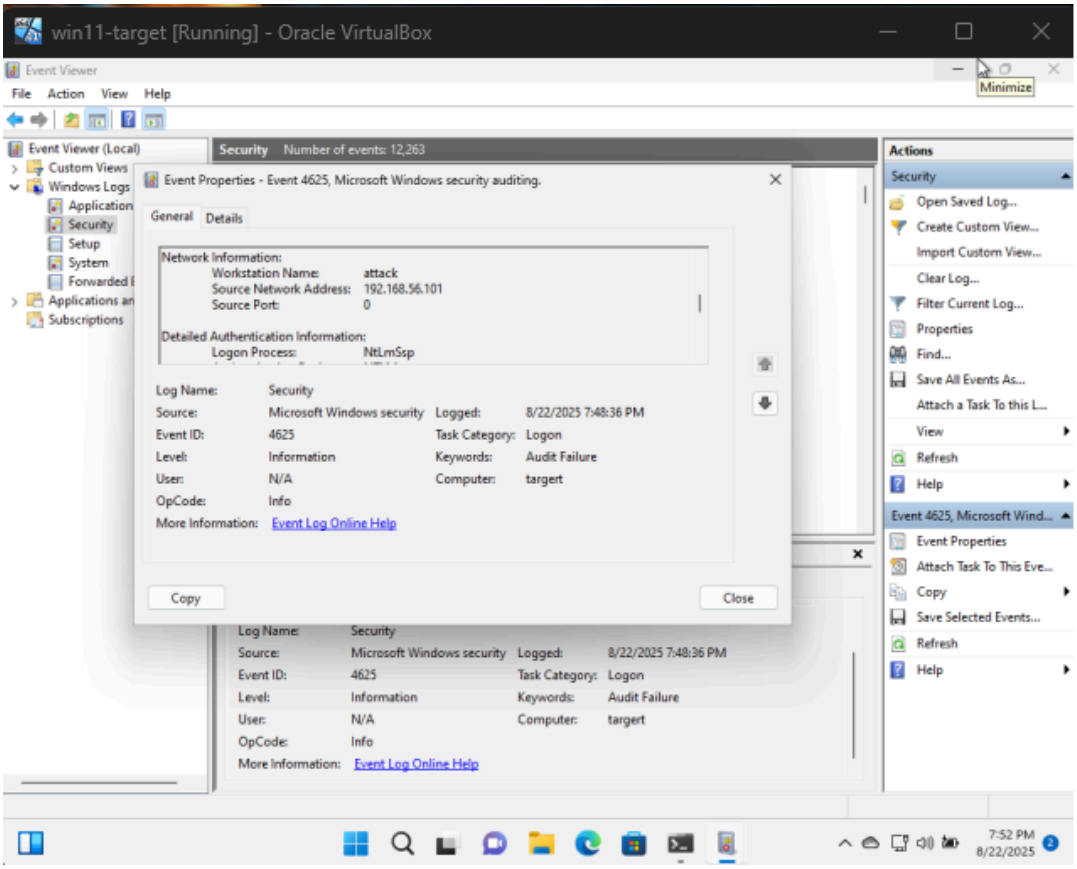
---

🔹 Step 1: Log Collection & Parsing

✅ Configured Wazuh agents on **Windows**
✅ Verified all endpoints reporting logs to the Wazuh dashboard.
✅ Tested log collection using:

- **Failed Windows login attempts** (Event ID `4625`)
- **Nmap scan from Kali → Windows**





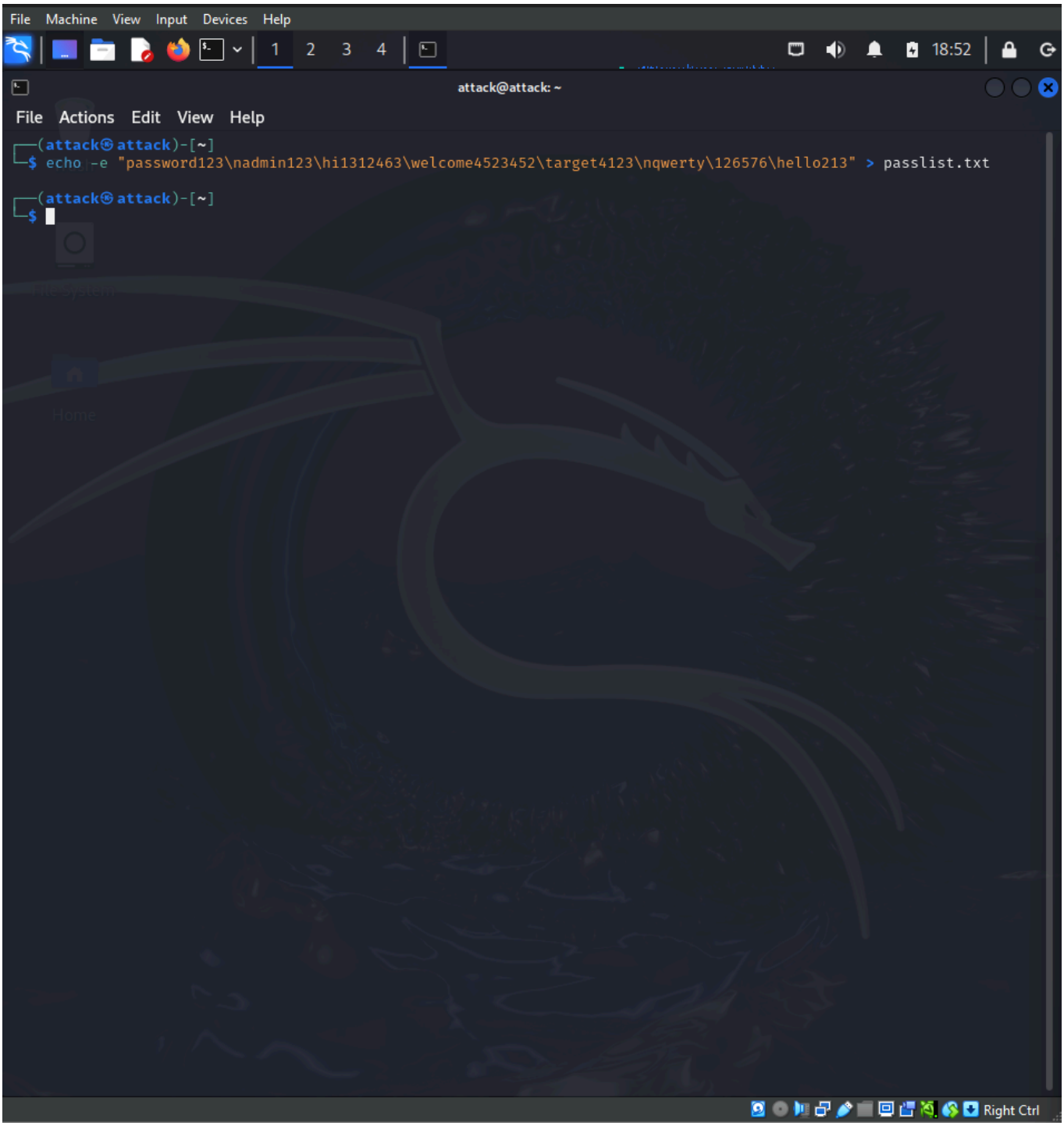
- Windows Event Viewer showing Event ID 4625
- Wazuh dashboard with collected logs

📌 Skill Gained:

- Understanding how logs flow from endpoints to SIEM.
- Identifying failed logins and scan attempts in raw logs.

🔹 Step 2: Brute-Force Attack Simulation

✅ Enabled **RDP on Windows** and allowed through firewall.
✅ Created a **custom password list** for brute force.
✅ Launched brute force attack from Kali using Hydra:

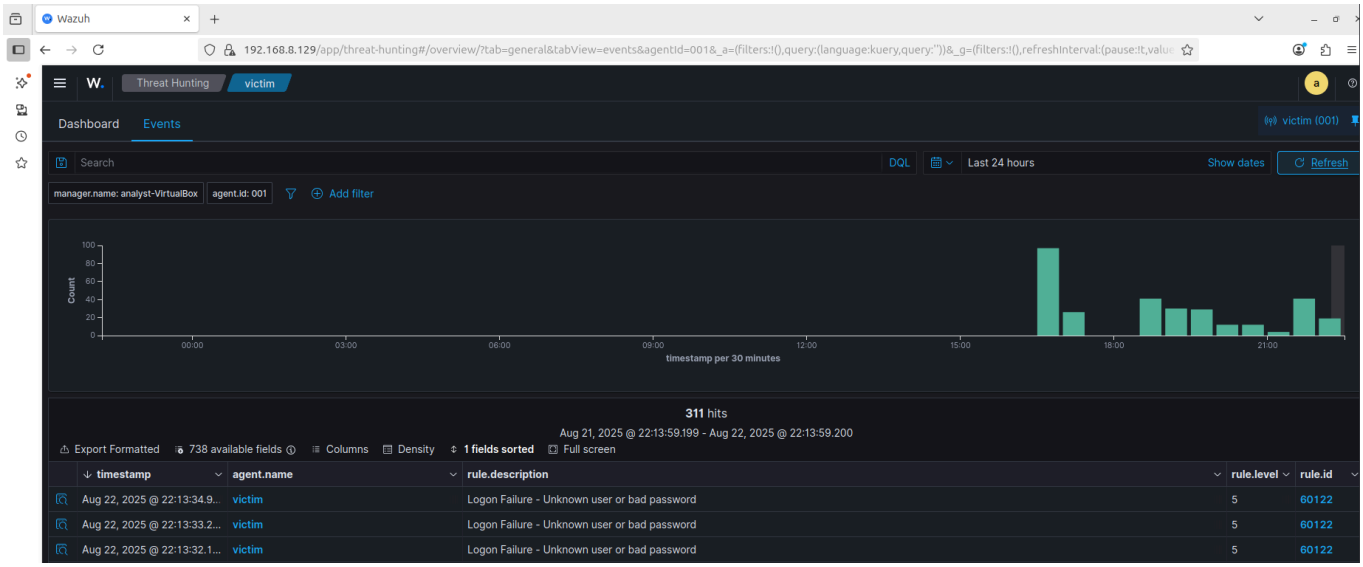



```
hydra -t 1 -V -f -s 3389 -w 5 -l Administrator -P passlist.txt rdp://<Windows-IP>
```

```
┌──(attack㉿attack)-[~]
└─$ hydra -t 1 -V -f -s 3389 -w 5 -l Administrator -P ~/passlist.txt rdp://192.168.56.104

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-22 19:48:30
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 3 login tries (l:1/p:3), ~3 tries per task
[DATA] attacking rdp://192.168.56.104:3389/
[ATTEMPT] target 192.168.56.104 - login "Administrator" - pass "password123" - 1 of 3 [child 0] (0/0)
[ATTEMPT] target 192.168.56.104 - login "Administrator" - pass "admin123\hi1312463\welcome4523452       arget4123" -
 2 of 3 [child 0] (0/0)
[ATTEMPT] target 192.168.56.104 - login "Administrator" - pass "qwerty\126576\hello213" - 3 of 3 [child 0] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-22 19:48:35

┌──(attack㉿attack)-[~]
└─$
```

- ✅ Detected **multiple failed login attempts** in Wazuh.
- ✅ Created a **custom correlation rule** in `local_rules.xml` to detect repeated failed logins.
- ✅ Restarted Wazuh manager and validated the rule triggered alerts.

```
<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>



<group name="windows,authentication_failures">
  <rule id="100002" level="10">
    <field name="event_id">4625</field>
    <description>windows failed logins</description>
    <group>authentication_failed,windows,rdp,</group>
  </rule>

  <rule id="100003" level="10" frequency="3" timeframe="120" ignore="60">
  <if_matched_sid>100002</if_matched_sid>
  <description>multiple login attempts detected</description>
  <group>authentication_failed,windows,rdp,bruteforce,</group>
  </rule>
</group>
```



📌 **Skill Gained:**

- Hands-on with brute force attack simulation.
- Correlation of multiple failed logins into a security alert.
- Creating **custom SIEM rules** for detection.

🔹 Step 3: File Integrity Monitoring (FIM)

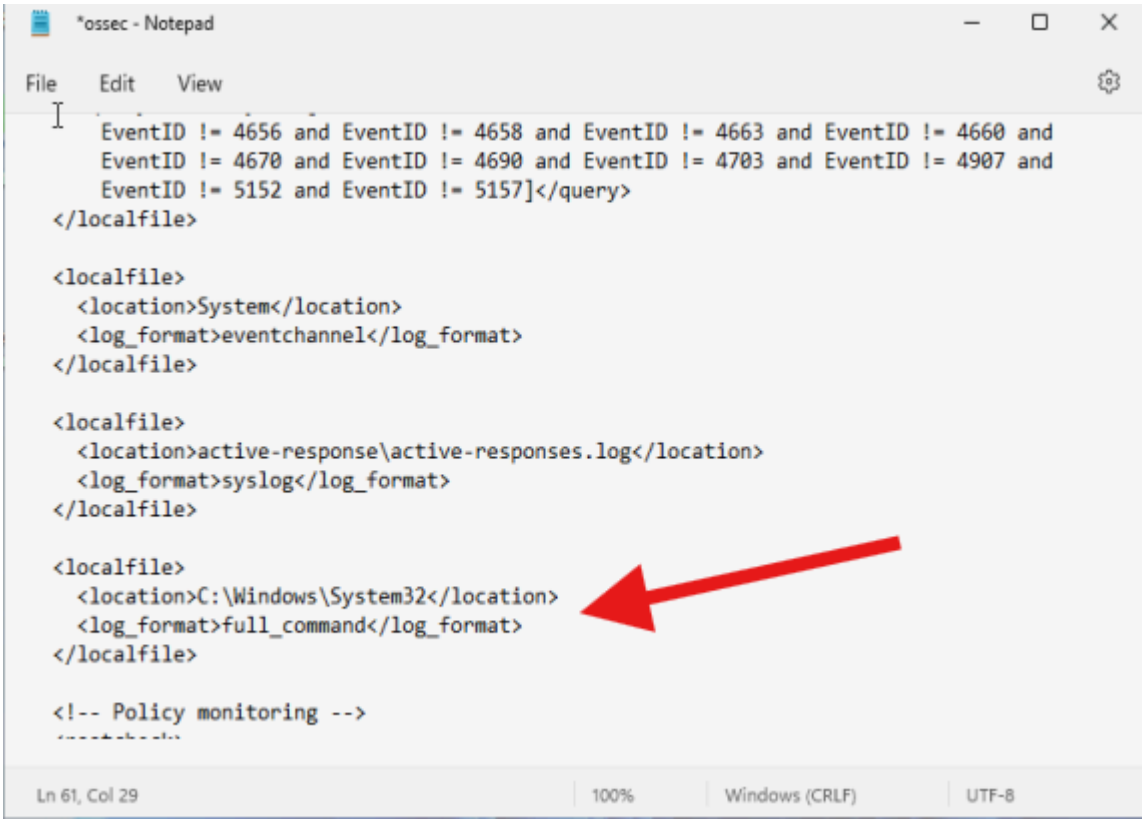
✅ Configured Wazuh FIM on:

- **Windows** → `C:\Windows\System32`

✅ Restarted agents to apply configurations.
✅ Modified test files:

- Edited `C:\Windows\System32\drivers\etc\hosts` on Windows

✅ Wazuh detected file changes and raised alerts.



📌 **Skill Gained:**

- Understanding **file integrity monitoring** for system protection.
- Detecting unauthorized modifications to critical files.

✅ Phase Completion

At the end of this phase:

- All endpoints successfully send logs to Wazuh.
- Brute force attacks are detected and alerted.
- File integrity monitoring is working.

🎯 SOC Analyst Skills Learned

- **Log Collection & Analysis** → Reading Event IDs, understanding raw logs.
- **Threat Detection** → Identifying brute-force and failed login attempts.
- **Rule Creation** → Writing custom SIEM rules for detection.
- **File Integrity Monitoring** → Detecting system file modifications.
- **Alert Handling** → Understanding how alerts appear in SIEM dashboards.

Why This Project Matters

This project simulates real SOC tasks such as:

- Monitoring security events from multiple endpoints.
- Detecting and investigating brute-force attacks.
- Setting up file integrity monitoring for sensitive files.
- Writing custom detection rules.

📌 **Value for SOC Role:**
Completing this project gave me practical experience in **SIEM monitoring, log analysis, incident detection, and response workflows** — the **core skills** expected from a **Tier-1 SOC Analyst**.

👉 This documentation, screenshots, and configs are uploaded here as part of my **SOC Home Lab Journey**.

Author: Nimesh Akalanka Peiris
Year: 2025