Phase 2: SIEM Dashboard Analysis

Objective

The goal of this phase was to simulate the use of a SIEM platform (like Splunk) to detect, analyze, and visualize attack patterns from both the attacker and victim machines during the exploitation process.

Setup Overview

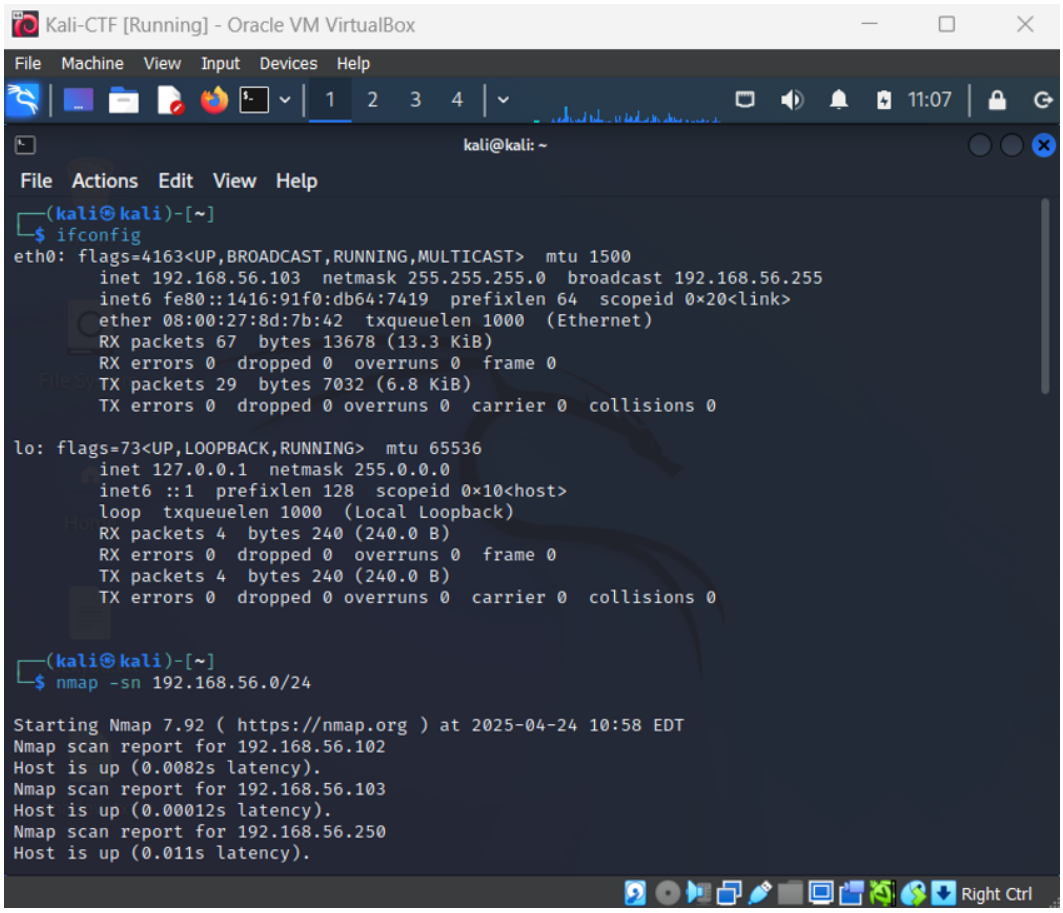

Figure 1: Nmap scan and interface configuration showing attacker IP (192.168.56.103) and victim IP (192.168.56.102).

- Attacker Machine: Kali Linux
- Victim Machine: Windows 7 (used from previous CTF setup)
- SIEM Tool: Simulated log interface representing standard Splunk-like output

Logs and events were generated based on the actions performed in Phase 1, specifically:

- SMB exploitation via EternalBlue (MS17-010)
- Post-exploitation activity including PowerShell command execution

Log Highlights

Timestamp	Event Type	Description
13:00:12	INFO	Nmap scan detected from source IP 192.168.56.102
13:00:15	ALERT	Exploit attempt targeting SMB detected from IP 192.168.56.10
16:15:00	ALERT	MS17-010 vulnerability exploited on 192.168.56.102
18:18:00	INFO	PowerShell execution on victim (powershell.exe -encodedcommand ...)
21:21:00	ERROR	Outbound SMB connection attempt to external host (possible lateral movement)

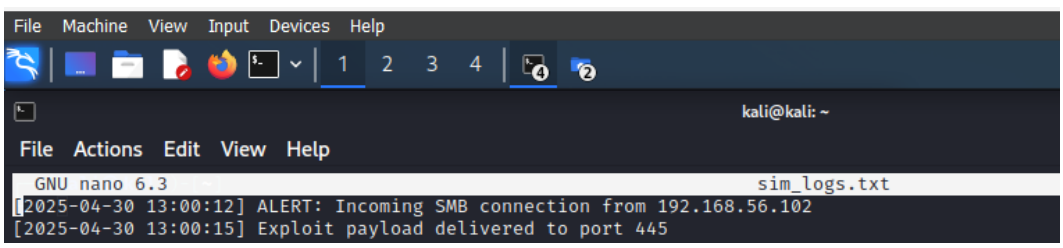

Figure 2: Simulated log file confirming SMB connection and payload delivery.

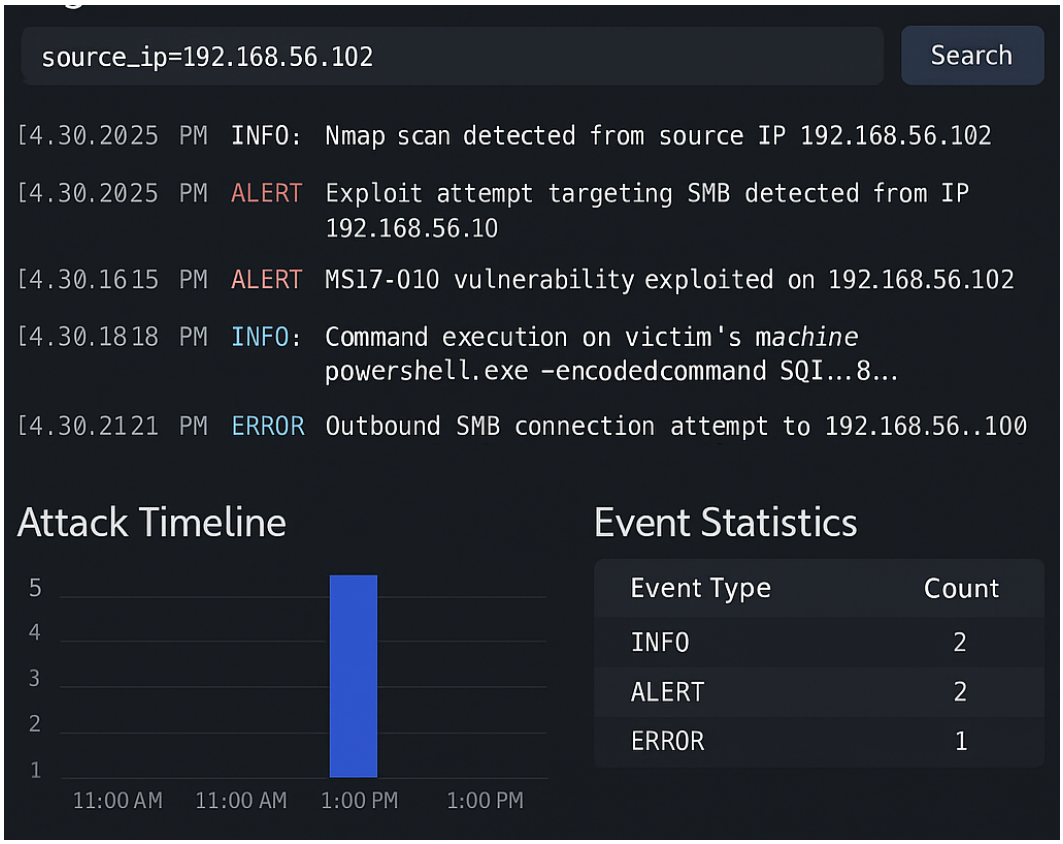

Figure 3: Simulated SIEM dashboard showing detected attack events with timeline and statistics.

Dashboard Visuals

- Attack Timeline: Shows spike in activity during the exploitation window.
- Event Statistics: Classifies log entries into INFO, ALERT, and ERROR categories.

Analysis Summary

- Attacker IP 192.168.56.102 was detected conducting initial scanning and exploiting SMB.
- MS17-010 exploit delivered successfully, verified by log entry and reverse shell.
- Post-exploitation steps confirmed by PowerShell command execution logs.
- Outbound connections were flagged, indicating possible lateral or data exfiltration attempts.

Conclusion

Using SIEM log analysis, we were able to detect the full attack chain:

1. Reconnaissance (Nmap)
2. Exploitation (EternalBlue)
3. Post-exploitation (Command execution)
4. Potential follow-up actions (Outbound SMB traffic)

This simulation demonstrates how SIEM dashboards can be crucial for incident response and threat detection.