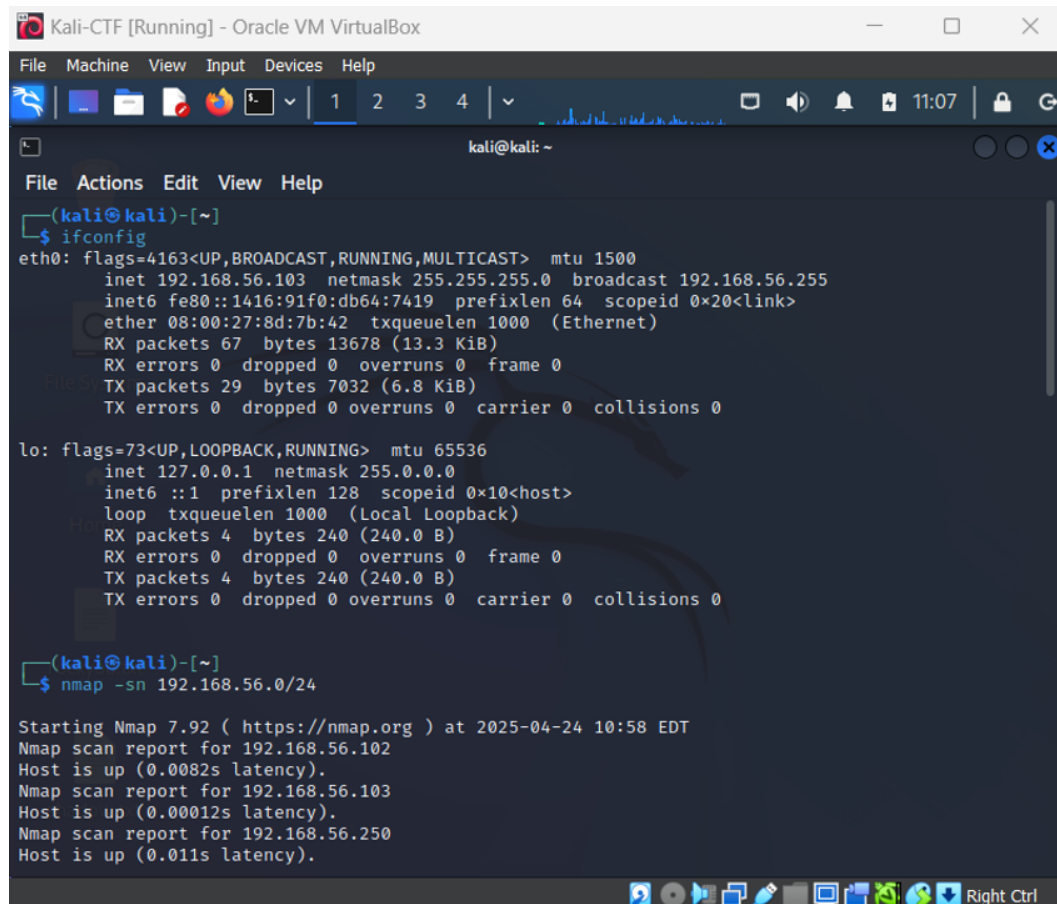


Phase 2: SIEM Dashboard Analysis

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



```
Kali-CTF [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.103 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::1416:91f0:db64:7419 prefixlen 64 scopeid 0<link>
    ether 08:00:27:8d:7b:42 txqueuelen 1000 (Ethernet)
    RX packets 67 bytes 13678 (13.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 7032 (6.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ nmap -sn 192.168.56.0/24

Starting Nmap 7.92 ( https://nmap.org ) at 2025-04-24 10:58 EDT
Nmap scan report for 192.168.56.102
Host is up (0.0082s latency).
Nmap scan report for 192.168.56.103
Host is up (0.00012s latency).
Nmap scan report for 192.168.56.250
Host is up (0.011s latency).
```

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

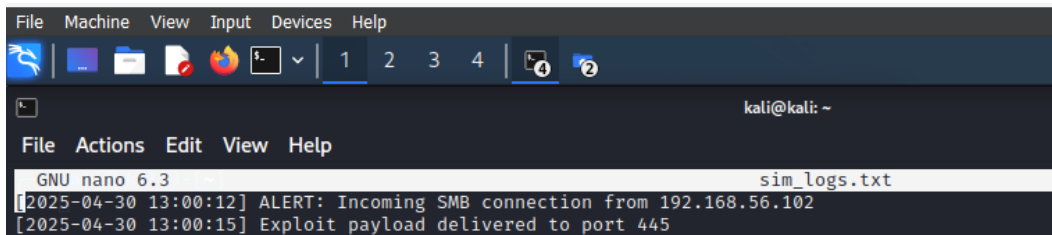
- Attacker Machine: Kali Linux
- Victim Machine: Windows 7 (used from previous CTF setup)
- SIEM Tool: Simulated log interface representing standard Splunk-like output

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)



```

File  Machine  View  Input  Devices  Help
[Icons]
kali@kali: ~
File  Actions  Edit  View  Help
GNU nano 6.3 sim_logs.txt
[2025-04-30 13:00:12] ALERT: Incoming SMB connection from 192.168.56.102
[2025-04-30 13:00:15] Exploit payload delivered to port 445

```

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

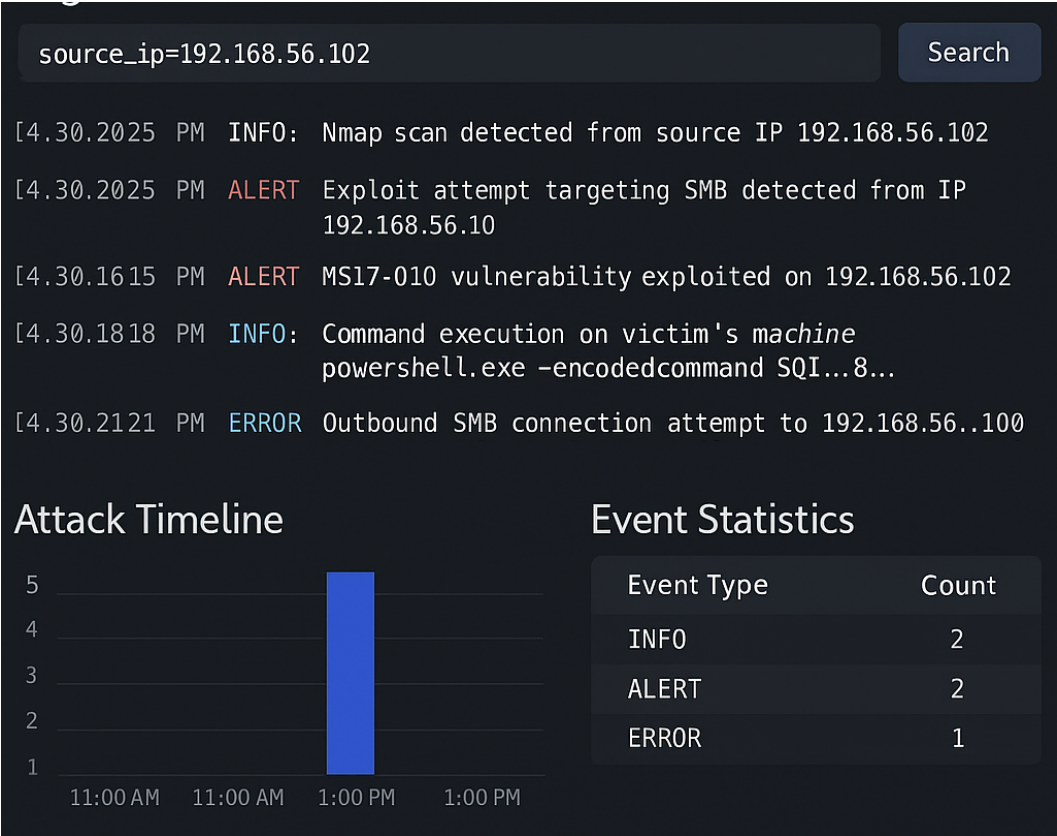


Figure 3: Simulated SIEM dashboard showing detected attack events with timeline and statistics.

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.