Lab Report: Scenario 4 – Log Tampering Simulation (T1562.002)

Objective

Simulate a post-compromise scenario where an attacker clears security logs using commands like wevtutil.exe, Clear-EventLog, or auditpol.exe, and detect the behavior using **Winlogbeat**, **Sysmon**, and **Kibana**.

Attack Chain Summary

Step	Description
1	Brute-force attack (via SMB) to gain access.
2	Attacker executes log-clearing command to cover tracks.
3	Sysmon logs process execution (Event ID 1).
4	Winlogbeat forwards logs to Elasticsearch.
5	Kibana detects and alerts on suspicious activity.

Attack Simulation (on Victim Machine)

Commands Used

- $ smbexec.py Machine1:12345@192.168.1.5   - For shell connection after BruteForce
- wevtutil cl Security - Clearing logs

Sysmon Configuration (Event ID 1 & 4104)

Sysmon is configured to log process creation (Event ID 1) and PowerShell script block logging (Event ID 4104).

Winlogbeat Configuration (winlogbeat.yml)

```
winlogbeat.event_logs:
  - name: Microsoft-Windows-Sysmon/Operational
    event_id: 1
  - name: Windows PowerShell
    event_id: 4104
```

Kibana Alert Rule Configuration

```
process.name: "wevtutil.exe" and event.code: "1"
```

Threshold Alert

Field	Value
Count	> 0
Time Window	Last 5 minutes
Exclude Duplicates	Yes
Fields in Alert Details	host.name, process.command_line, user.name

Alert Action

Email Alert (Kibana Action)

Subject: Log Tampering Detected

Conclusion

The lab successfully simulates and detects log tampering attempts using system utilities. Alerts are triggered via Kibana when key commands are run, fulfilling the detection objective under MITRE technique T1562.002.