Lab Report Scenario 2: Detection of Lateral Movement via SMB/PSExec (T1021.002)

Objective

Simulate and detect lateral movement activity using PsExec via SMB (port 445) by monitoring Sysmon logs in Elastic

Environment Setup

- Sysmon installed and configured.

 - Event ID 3: Network connection

- Elastic Agent deployed to forward Sysmon logs to Elastic Cloud.

- Elastic Security configured to ingest and analyze Sysmon logs.

Sysmon Configuration

```
  <NetworkConnect onmatch="include">

    <DestinationPort condition="is">445</DestinationPort> <!-- SMB (PsExec) -->

    <Image condition="contains">psexec</Image>

    <Image condition="contains">powershell.exe</Image>

    <Image condition="contains">wmic.exe</Image>

   </NetworkConnect>
```

This is need to be configured in sysmon configuration.yaml file

Attack Simulation

PsExec used to run a remote command on Host:

This initiated an SMB connection in Host on TCP port 445.

A remote process (cmd.exe) was created on Host by PsExec.

```
psexec.py Machine1:12345@192.168.1.4
```

Detection Queries

Detect SMB Traffic on Port 445:

```
event.provider:"Microsoft-Windows-Sysmon" and event.code:3 and destination.port:445 and network.transport:"tcp"
```

Correlation Alert Setup

- Created a correlation rule in Elastic Security with conditions:

- Event ID 3 network connection on port 445. - Event ID 1 process creation with PsExec/WMIC/PowerShell remoting keywords.

- Source IP matching and time window of 2 minutes.

- Outcome: Alert triggered successfully when simulated attack was performed.

Conclusion

- The lateral movement via SMB/PSExec attack was successfully simulated.

- Sysmon's Event ID 3 and 1 logs are effective for detecting network and process activity associated with remote

execution.

- Elastic Cloud's correlation rules enabled reliable detection and alerting of suspicious lateral movement behavior.