Cybersecurity Attack Simulation Report

📄 Introduction

This report details a controlled cybersecurity attack simulation conducted in a lab environment using virtual machines. The objective was to emulate a common real-world attack scenario involving port scanning, payload creation, reverse shell exploitation, and detection via a SIEM (Splunk). The attacker used Kali Linux and the victim system was a Windows machine. The simulation was intended for educational purposes and ethical hacking practice.

🎯 Objectives

- Simulate a penetration test using known techniques and tools.
- Understand and demonstrate how attackers establish a reverse shell.
- Monitor and analyze the attack lifecycle using a SIEM (Splunk).
- Evaluate the visibility and effectiveness of Splunk in detecting key stages of an intrusion.

🧪 Methodology

🖥️ Virtual Environment Setup

- **Attacker:** Kali Linux VM (Metasploit, Nmap, Python 3)
- **Victim:** Windows VM (target of the attack)
- Both machines configured in the same internal network via VirtualBox.

🔬 Step-by-Step Simulation

1. **Connectivity Check:**
   Verified communication between attacker and victim using ICMP (ping).
2. **Port Scanning:**
   Used Nmap to identify open ports on the victim machine.
3. **Payload Generation:**
   A reverse shell executable was created using msfvenom with the payload: windows/x64/meterpreter/reverse_tcp
4. **Web Server Deployment:**
   Python 3 HTTP server was used to host the payload file.

5. **Delivery and Execution:**
   Victim downloaded and executed the payload, establishing a reverse shell.
6. **Session Establishment:**
   A Meterpreter session was opened, allowing remote interaction with the victim.
7. **System Exploration:**
   The attacker ran basic commands to gather system information and demonstrate access.

🕵️ Detection and Monitoring with Splunk

🔎 Log Sources Monitored

- Windows Security Logs (Sysmon)
- Network traffic logs (if available)
- Splunk alerts and dashboards

✅ Notable Detections in Splunk

1. **Nmap Scan Detected:**
   Unusual port scan activity was visible in the network logs.
2. **Payload Download:**
   HTTP request logs showed the victim downloading the suspicious .exe file.
3. **Execution of Unknown File:**
   Sysmon logs indicated execution of a new unsigned executable (shell_reverse.exe).
4. **Reverse Shell Connection:**
   Outbound connection from the victim to the attacker's IP and port was logged.
5. **Splunk Alert Triggered:**
   A correlation search detected suspicious process creation and outbound connections, flagging possible remote control activity.

🧠 Conclusion

The attack simulation successfully demonstrated a complete lifecycle of a basic cyber intrusion using common tools and techniques. The use of Splunk as a SIEM platform proved effective in detecting multiple stages of the attack:

- Reconnaissance (Nmap scan)
- Delivery (HTTP download)
- Execution (Payload run)
- Command and Control (Reverse shell session)

This highlights the importance of robust logging, endpoint visibility (e.g., Sysmon), and real-time alerting to identify and respond to threats quickly. In a real-world environment, such visibility could enable timely incident response and mitigation before significant damage occurs.