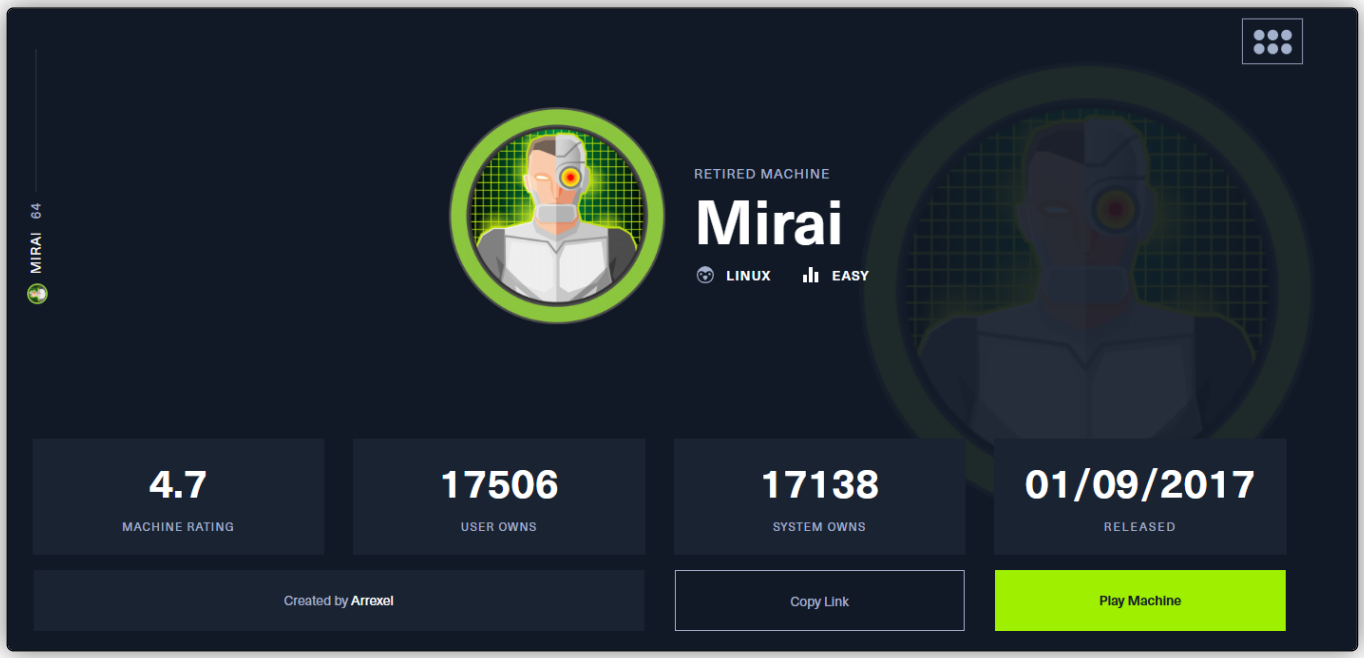
268- MIRAI

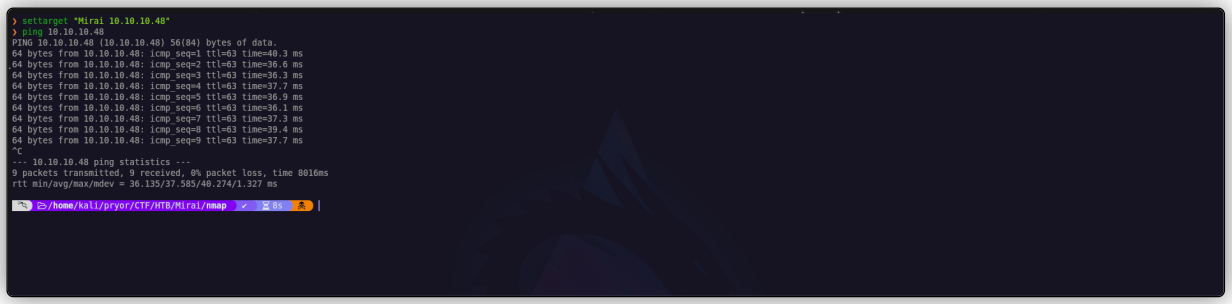
1. MIRAI

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

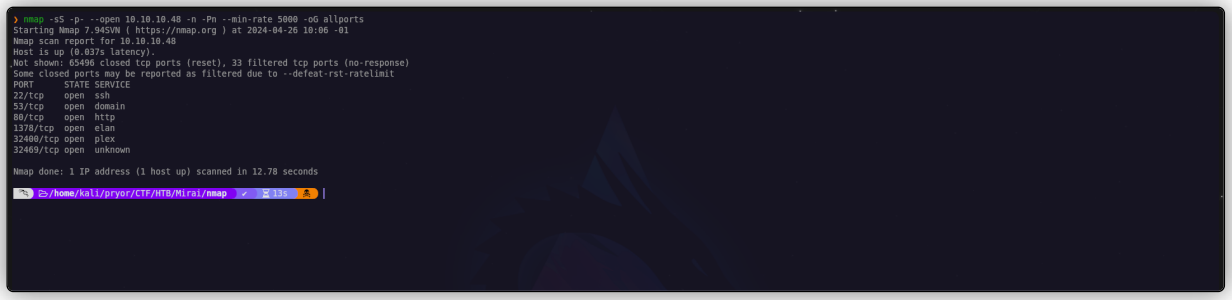


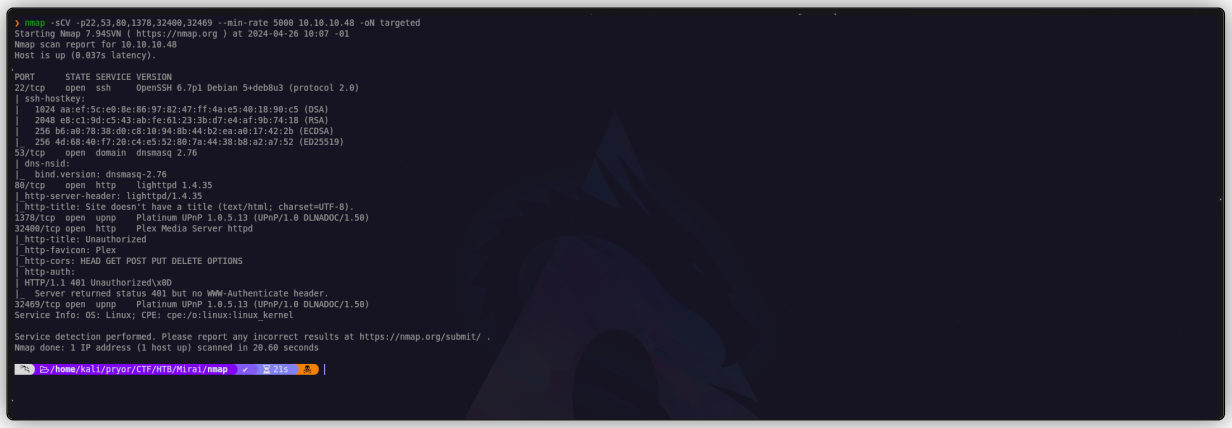
1.1. Preliminar

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

- 

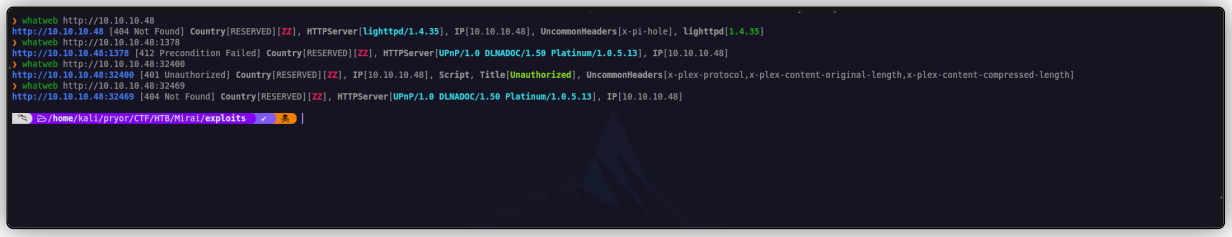
1.2. Nmap

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

- 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.
  - 

> - **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*.
    - 

> - **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.

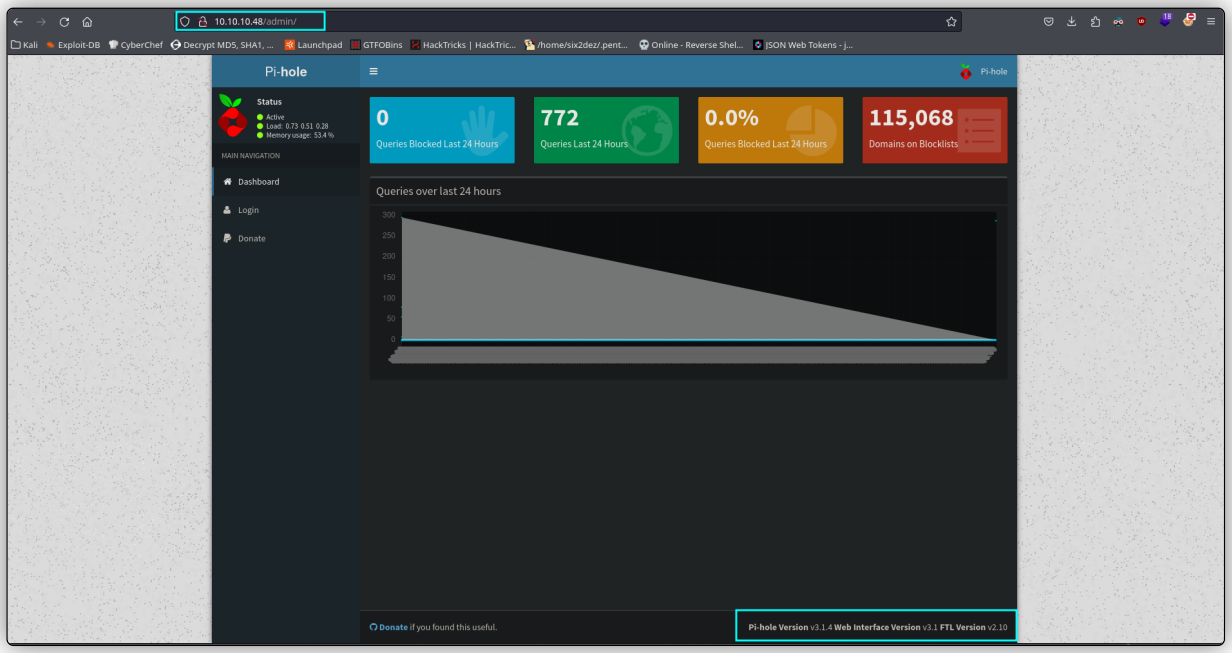
> - **Plex Media Server** es una aplicación de servidor multimedia que te permite organizar, gestionar y transmitir tu colección de medios digitales, como películas, programas de televisión, música, fotos y videos caseros, a una variedad de dispositivos. Estos dispositivos pueden incluir televisores 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.

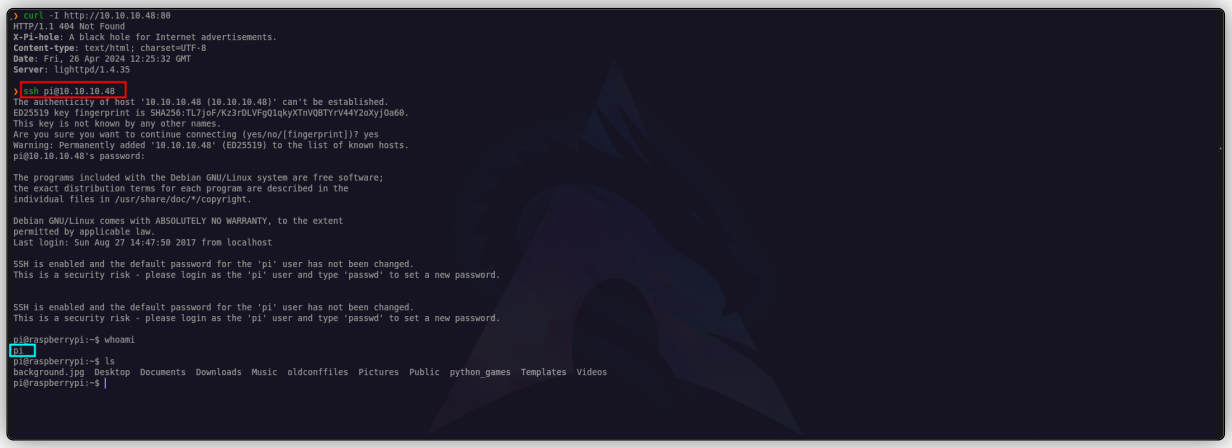
```
gobuster dir -u http://10.10.10.48 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 20 -b 403,404,503 -x php,html,txt,bak,asp,aspx
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@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%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 351907 / 1543927 (22.79%)
===============================================================
Finished
===============================================================
/home/kali  16m 13s
```

- 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**.

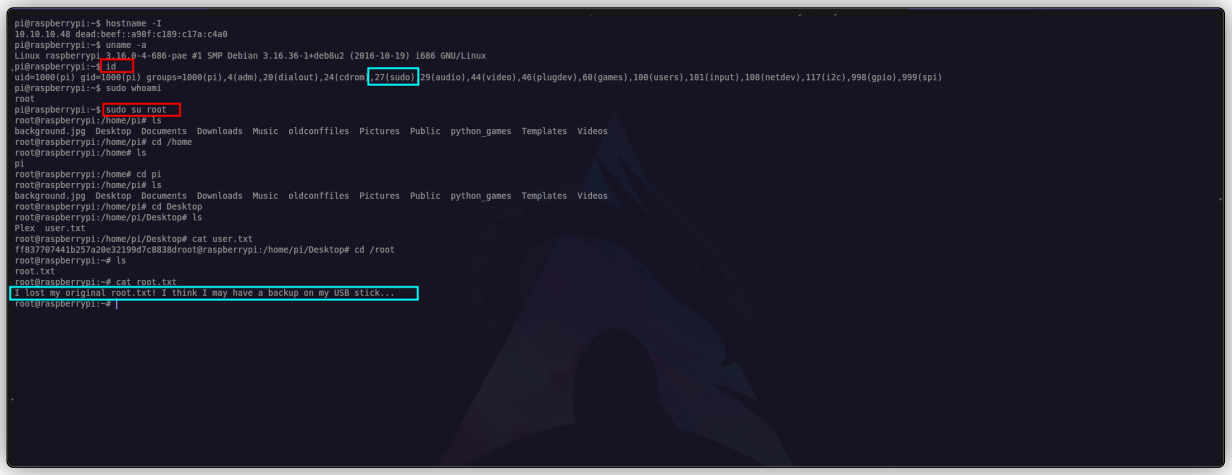


> - **Pi-Hole** es un proyecto de software de código abierto diseñado para actuar como un *servidor DNS (Sistema de Nombres de Dominio)* y bloqueador de anuncios en una red local. Se ejecuta en dispositivos basados en Raspberry Pi, aunque también se puede instalar en otros sistemas Linux. El objetivo 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.

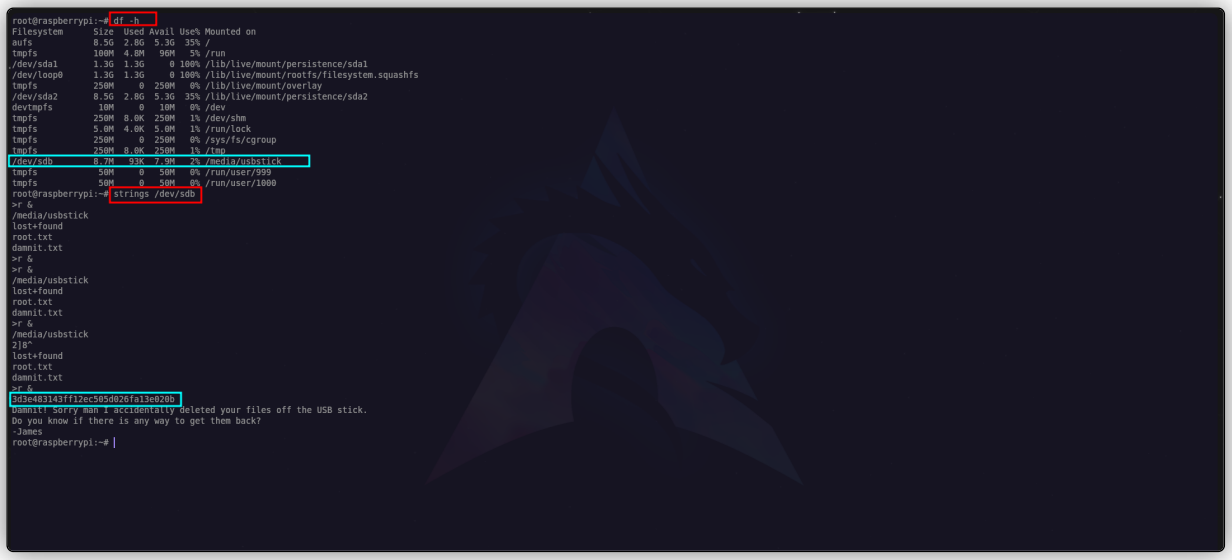
1.5. Raspberry Pi SSH Default credentials

- 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*.
    - 

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.
    - 

- 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.



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