

## **INTERNET OF THINGS (IOT) HACKING: SMART IP CAMERA HACKING**

In this report the threats and vulnerabilities posed by IoT devices will be analyzed and effective mitigation systems or procedures will be discussed.

Later in the report, the Foscam FI8910W IP smart camera was attacked from different attack surfaces and a spoofing attack, sniffing attack, as well as DoS attack was successfully carried out on the camera as a proof of concept. Hence the need for a stronger authentication mechanism, usage of secure protocols, and other mitigation techniques are elaborated in this report.

### **1.1 Aim of Study**

This study aims to suggest effective strategies for addressing security vulnerabilities within the realm of the Internet of Things (IoT). Given the rapid proliferation of IoT devices and systems, ensuring robust security measures has become increasingly vital. Through a comprehensive analysis, this research seeks to identify and evaluate these security weaknesses, while also proposing actionable solutions to enhance the overall security landscape of IoT systems. This endeavour contributes to the existing knowledge base in this domain.

This research primarily strives to uncover vulnerabilities that could compromise the privacy, reliability, and availability of IoT systems. By meticulously investigating existing gaps in security measures, the study aims to pinpoint areas where deficiencies or inadequacies exist. Furthermore, the research examines the criticality of addressing these issues to mitigate the risks associated with IoT deployments. To preempt future security breaches in IoT systems, the proposed research also aims to offer effective mitigation strategies. By examining current security practices and conducting thorough studies, this project intends to identify and recommend practical solutions for enhancing the security of IoT networks, devices, and data. Establishing straightforward mitigation measures is crucial for individuals and companies alike to safeguard their IoT infrastructure against cyber threats.

### **The Research Topic's Relevance and Significance**

The study topic on IoT security vulnerabilities and mitigation methods has broad significance and relevance. By spotting flaws and suggesting practical ways to reduce security risks, this research has the potential to make a significant contribution to the creation of safe IoT systems (Atzori et al., 2010).

The study begins by discussing the urgent need for comprehending and resolving the risks prevalent in IoT systems. The potential hazards and security issues related to IoT systems become more apparent as the usage of IoT technology spreads across numerous industries. Researchers, business experts, and legislators may devise and put into place effective security measures thanks to the research's identification and understanding of these vulnerabilities (Angelova et al., 2017)

## Internet of Things (IoT) Camera Hacking

### Introduction

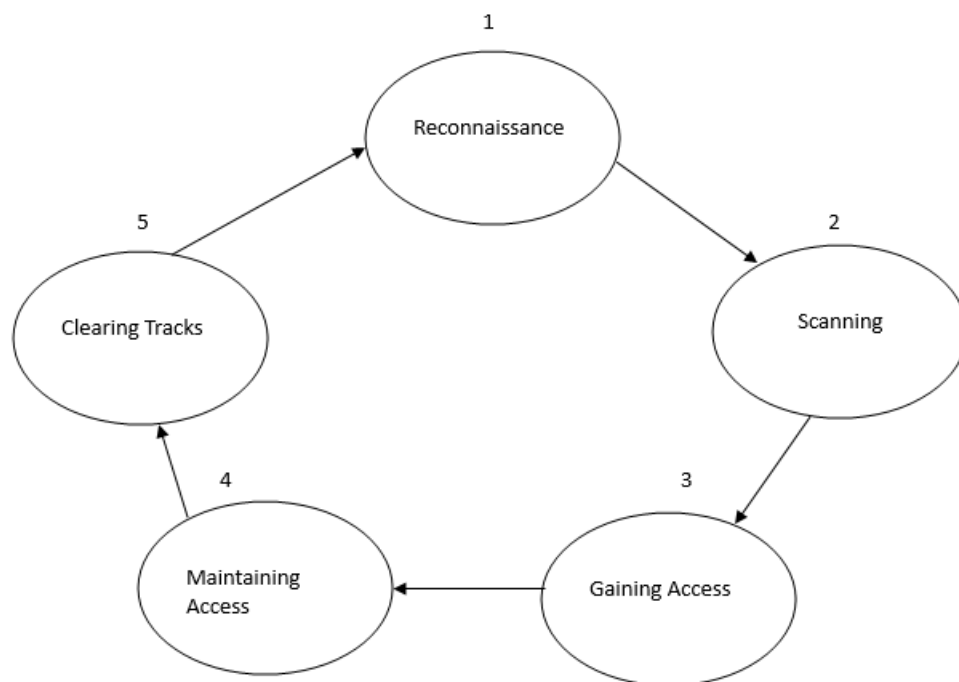
IoT cameras are internet-connected cameras that can send data over a network through the internet. They possess capabilities such as remote access, motion detection, SD card & cloud storage, and so on. They are widely used for surveillance purposes as well as incorporated into smart home systems. IoT cameras can be used for home security, monitoring babies, and monitoring pets, and are controlled through computers, smartphones, and tablets, which allow users to view the camera's feed and operate the camera from a remote location.

*FI8910W Smart IP camera*



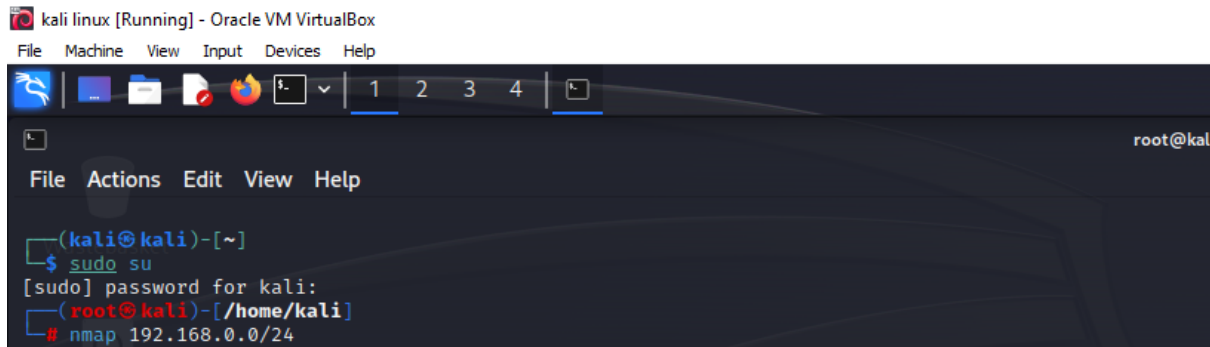
## Methodology

Hacking an IoT camera can take many forms, and attackers usually start by simply finding information online about the camera device. Attackers may use tools like Shodan to search for exposed cameras to hack. Generally, there are phases an attacker goes through to hack an IoT camera. Attackers start from reconnaissance to the scanning phase, to gaining access to the device, then they move to maintain access to the device through backdoors, and finally clear the tracks to avoid suspicion or being caught. The hacking phases are shown



### Scanning for the IP Address of the Camera

The camera and the host machine are both connected to the same router on the IP address range 192.168.0.0- 255. The entire IP address range was scanned using Nmap to find ports and services and also to possibly discover the IP of the Foscam camera because the pack of the camera does not include the IP address. The command for the Nmap scan is shown

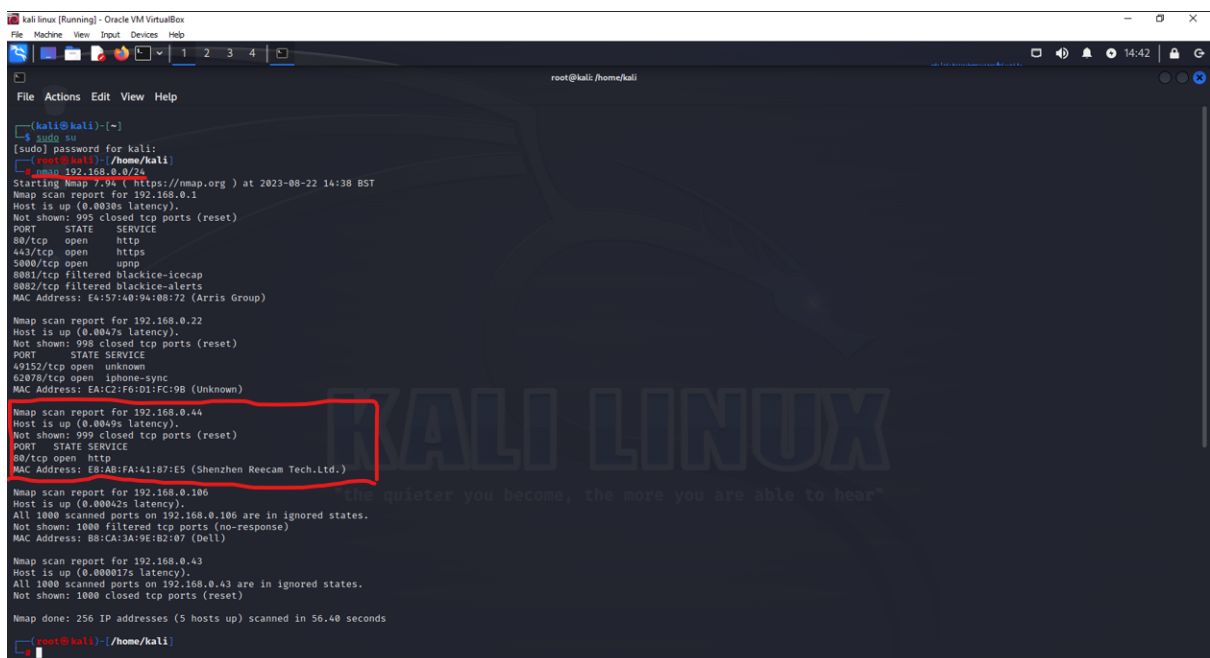


```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(kali@kali)-[/home/kali]
# nmap 192.168.0.0/24
```

After a while, Nmap returned the search result, and details about the addresses in the IP range were returned. the IP address 192.168.0.44 is likely to be the camera we are targeting as it has details such as ‘Shenzhen Reecam” Reecam contain the token “cam” makes it a suspicious name for the Foscam camera.

Investigating further by running an aggressive scan on the IP address 192.168.0.44 shows that my guess is right, as it can be seen below, the name ‘Foscam FI8910W’, the keyword ‘surveillance camera’ and the device type as “specialized webcam’ were returned by Nmap.



```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(kali@kali)-[/home/kali]
# nmap 192.168.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 14:38 BST
Nmap scan report for 192.168.0.1
Host is up (0.0038s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
5000/tcp  open  upnp
8081/tcp  filtered blackice-iccap
8082/tcp  filtered blackice-alerts
MAC Address: E4:57:48:94:08:72 (Arris Group)

Nmap scan report for 192.168.0.22
Host is up (0.0047s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
60152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: EA:C2:F6:D1:FC:9B (Unknown)

Nmap scan report for 192.168.0.44
Host is up (0.0049s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: E8:AB:FA:41:87:E5 (Shenzhen Reecam Tech.Ltd.)

Nmap scan report for 192.168.0.106
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.0.106 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 88:CA:3A:9E:B2:07 (Dell)

Nmap scan report for 192.168.0.43
Host is up (0.000017s latency).
All 1000 scanned ports on 192.168.0.43 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 56.40 seconds
(kali@kali)-[/home/kali]
```

Investigating further by running an aggressive scan on the IP address 192.168.0.44 shows that my guess is right, as it can be seen below, the name ‘Foscam FI8910W’, the keyword ‘surveillance camera’ and the device type as “specialized webcam’ were returned by Nmap.

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/kali

(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
root@kali: /home/kali
└─$ nmap -sS 192.168.0.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 14:38 BST
Nmap scan report for 192.168.0.1
Host is up (0.0038s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
5000/tcp   open  uupnp
8081/tcp   filtered blackice-icecap
8082/tcp   filtered blackice-alerts
MAC Address: EA:57:48:94:08:72 (Arris Group)

Nmap scan report for 192.168.0.22
Host is up (0.0047s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
49152/tcp open  unknown
62878/tcp open  iphone-sync
MAC Address: EA:C2:F6:D1:FC:9B (Unknown)

Nmap scan report for 192.168.0.44
Host is up (0.0049s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: E8:AB:FA:41:87:E5 (Shenzhen Reecam Tech.Ltd.)

Nmap scan report for 192.168.0.106
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.0.106 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 88:CA:3A:9E:02:07 (Dell)

Nmap scan report for 192.168.0.43
Host is up (0.00087s latency).
All 1000 scanned ports on 192.168.0.43 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 56.48 seconds

root@kali: /home/kali
```

```
(root@kali)-[~]
└─$ nmap -A 192.168.0.44
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-22 14:45 BST
Nmap scan report for 192.168.0.44
Host is up (0.0044s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Boa 0.94.13
|_http-server-header: Boa/0.94.13
|_http-title: Site doesn't have a title (text/html).
MAC Address: E8:AB:FA:41:87:E5 (Shenzhen Reecam Tech.Ltd.)
Device type: specialized webcam
Running: AirMagnet embedded, Foscam embedded, Instar embedded, Linux 2.4.X
OS CPE: cpe:/h:airmagnet:smartedge cpe:/h:foscam:fi8904w cpe:/h:foscam:fi8910w cpe:/h:foscam:fi8918w cpe:/h:instar:in-3010 cpe:/o:linux:linux_kernel:2.4
OS details: AirMagnet SmartEdge wireless sensor; or Foscam FI8904W, FI8910W, or FI8918W, or Instar IN-3010 surveillance camera (Linux 2.4)
Network Distance: 1 hop

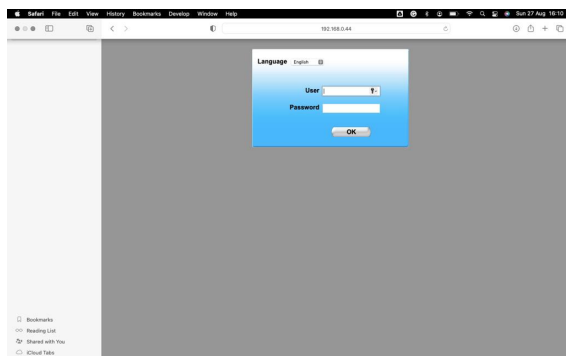
TRACEROUTE
HOP RTT      ADDRESS
1   4.45 ms  192.168.0.44

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.04 seconds

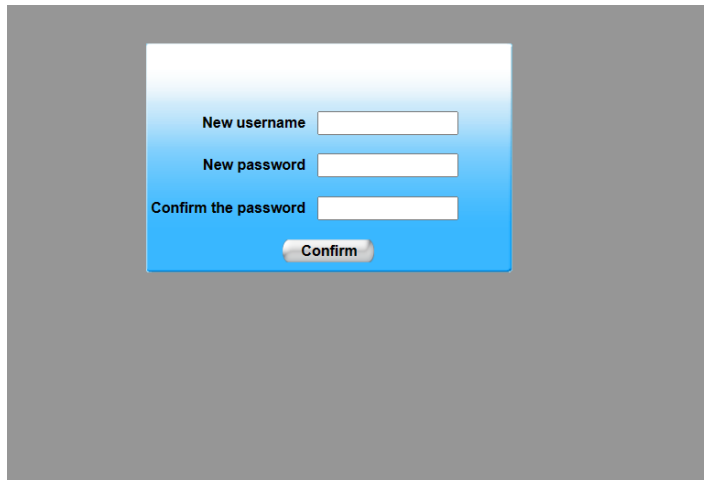
root@kali: /home/kali
```

Also, running a Nmap vulnerability script on the IP address confirms the MAC address and an open port 80 on the camera.

Now that it has been confirmed that the IP address of the camera is 192.168.0.44, the address was entered on browser and the login page for the camera was returned as below



The default username “admin” and blank password was entered on the camera and the login was successful. I then changed the password from the blank default password to “admin1234” using the camera interface shown



A screenshot of a web interface for changing a password. It features three input fields labeled "New username", "New password", and "Confirm the password", each followed by a white text box. Below these fields is a "Confirm" button. The interface has a blue gradient background.

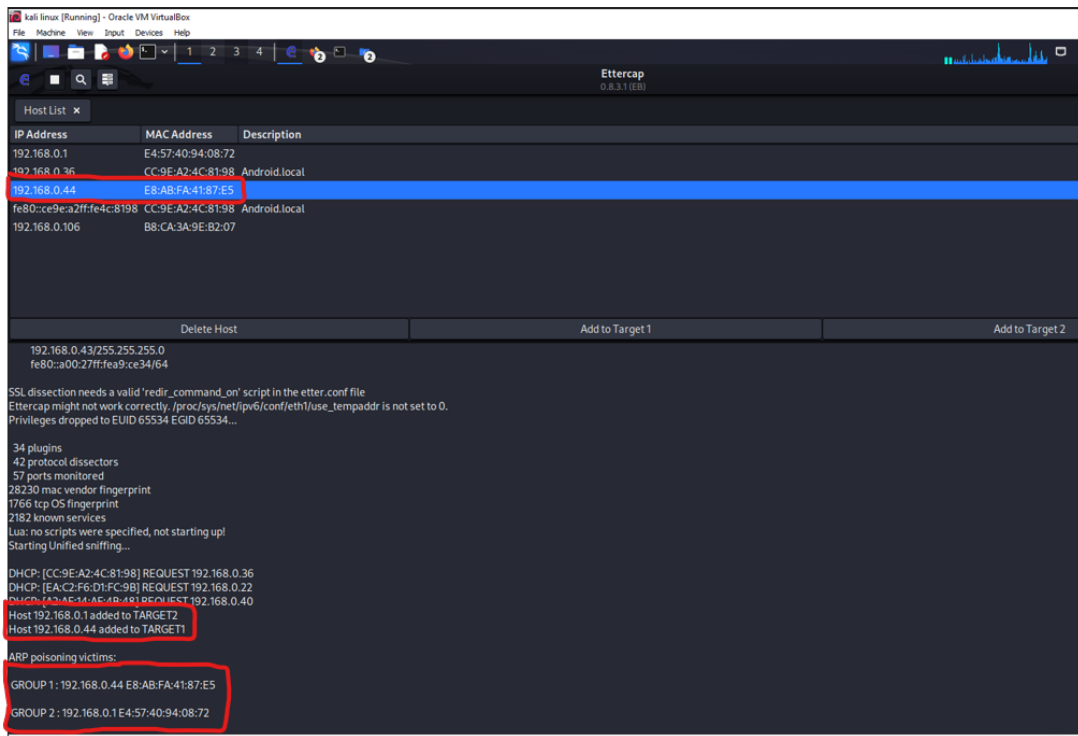


A screenshot of a web interface for selecting a login mode. At the top right is the "FOSCAM" logo and the URL "www.foscam.com". Below this are three buttons: "ActiveX Mode", "Server Push Mode", and "Mobile Phone". At the bottom, there is a "Note:" section with text explaining the three login methods: "Please note that there are three login methods: for IE browser, please choose ActiveX mode; for Safari, Firefox, Google Chrome, please choose Server Push mode; for mobile phone, please choose the third mode".

## Sniffing Attack on the Camera

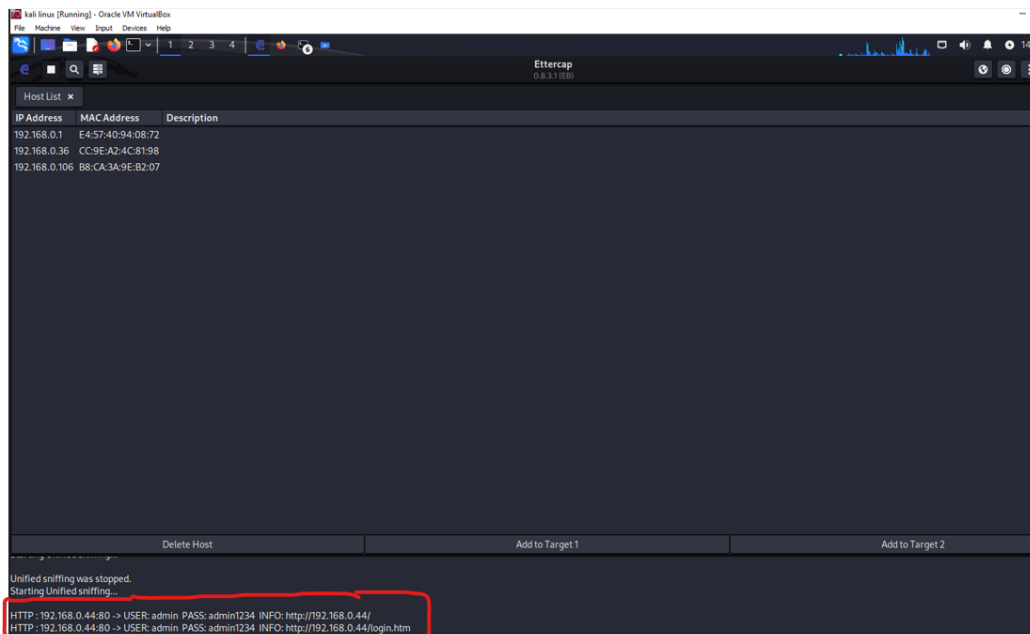
A sniffing attack was carried out on the camera using Ettercap. Ettercap is a kali Linux tool that can be used to carry out so many attacks on the target including man-in-the-middle attack, DoS attack, and so on. The Ettercap was started to capture the network interface that the camera is running on which is eth1 network interface.

Host scan was carried out on the network interface using the Ettercap and the camera IP address was also listed as shown



he camera IP address was added as target 1 and the IP address of my router as target 2, and thereafter Address Resolution Protocol (ARP) poisoning was started.

Soon after, Ettercap was able to sniff on the username and password used in logging into the camera as shown



Ettercap was also able to give the details of the page that the log in credentials will be successfully used as <http://192.168.0.44/login.htm>.

More details about Ettercap sniffing activities are shown

```
Delete Host      Add to Target 1      Add to Target 2

Listening on:
eth1 -> 08:00:27:A9:CE:34
192.168.0.43/255.255.255.0
fe80::a00:27ff:fea9:ce34/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth1/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

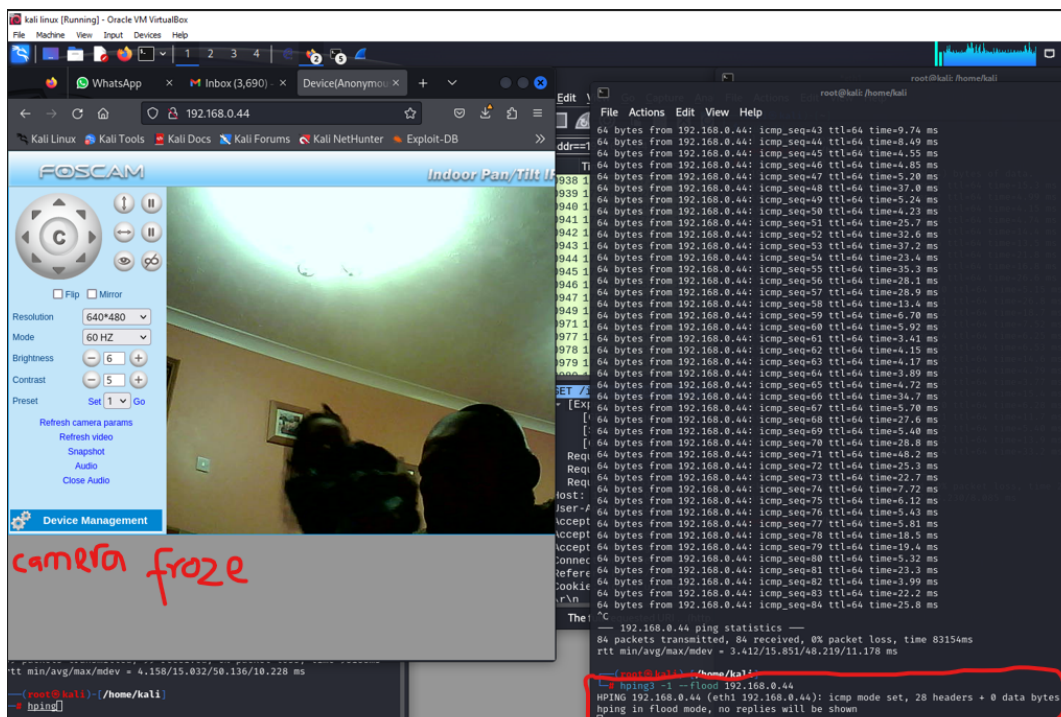
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Unified sniffing was stopped.
Starting Unified sniffing...

HTTP: 192.168.0.44:80 -> USER: admin PASS: admin1234 INFO: http://192.168.0.44/
HTTP: 192.168.0.44:80 -> USER: admin PASS: admin1234 INFO: http://192.168.0.44/login.htm
DHCP: [E8:AB:FA:41:87:E5] DISCOVER
DHCP: [E8:AB:FA:41:87:E5] REQUEST 192.168.0.44
DHCP: [E8:AB:FA:41:87:E5] DISCOVER
DHCP: [E8:AB:FA:41:87:E5] REQUEST 192.168.0.44
HTTP: 192.168.0.44:80 -> USER: admin PASS: admin1234 INFO: http://192.168.0.44/live.htm
HTTP: 192.168.0.44:80 -> USER: admin PASS: admin1234 INFO: http://192.168.0.44/camera.htm
HTTP: 192.168.0.44:80 -> USER: admin PASS: admin1234 INFO: http://192.168.0.44/camera.htm
```

## DoS attack on the Camera

A Denial of Service (DoS) attack was also found to be successful on the camera. First lots of ping request were sent to the camera to overload it with multiple ICMP packets but the camera appeared to still be working fine. Then the hping3 tool was used and immediately the camera froze in less than 5 seconds of running the hping3 command,





## Conclusion

This project critically examined and explored the significance of IoT devices and the potential threats and vulnerabilities of these devices in today's growing demand for IoT systems. This report explored the several ways IoT devices can be compromised such as susceptibility to DoS attacks, insufficient access control mechanisms, insecure firmware, device tampering issues, insufficient data protection, usage of insecure communication protocols, usage of weak authentication mechanisms, data leaks, physical security risks, and lack of a widely accepted security patch (es).

The Foscam camera used for this report demonstrated how attackers can gain entry into the network of an IoT device through the router and carry out several attacks like sniffing, spoofing, DoS attacks to name a few. Also, the camera was unable to handle huge amount of traffic as the camera became unresponsive when flooded with ICMP packets.

To continue to safeguard and protect this huge numbers of IoT devices in today's interconnected world, we must employ the usage of secure communication protocols like TLS and SSH, enforce the usage of a more secure login credentials before the device can be used, limit login attempts to avoid brute forcing, implement intrusion detection and prevention systems. Also, manufacturers should make it easy for users to update IoT devices while in operation without taking it offline, and finally organizations should employ the use of an adaptive and secure policy that can block known and zero-day threats. The race between manufacturers to compete on lower priced cameras and by extension IoT devices make them to relegate these security concerns while rolling out these devices, it is my hope that manufacturers put security first in designing and manufacturing these devices especially now that the numbers of IoT devices begin to accelerate as a result of advance technologies like the 5G network.