

|  |
| --- |
| Investigating Vulnerabilities in IoT devices in the context of a smart home  Michael W Crow  BSc Ethical Hacking and Countermeasures, 2017 |

|  |
| --- |
| School of Arts, Media and Computer Games  Abertay University |

# Abstract

Jfjfgjgjg gobbledegook

Table of Contents

[Abstract i](#_Toc480664665)

[Table of Figures iv](#_Toc480664666)

[Table of Tables v](#_Toc480664667)

[Acknowledgements vi](#_Toc480664668)

[University of Abertay Dundee Permission to Copy vii](#_Toc480664669)

[Abbreviations, Symbols, Notation and Glossary of Terms viii](#_Toc480664670)

[1. Introduction 1](#_Toc480664671)

[1.1. Introduction to IoT 1](#_Toc480664672)

[1.2. History of IoT 2](#_Toc480664673)

[1.3. The Modern Smart Home 3](#_Toc480664674)

[1.4. Penetration Testing and IoT 4](#_Toc480664675)

[1.5. Devices Tested in this project 5](#_Toc480664676)

[1.6. Research Questions 5](#_Toc480664677)

[1.7. Research Aims 5](#_Toc480664678)

[1.8. Research Objectives 5](#_Toc480664679)

[1.9. Statement of Structure 5](#_Toc480664680)

[2. Background 7](#_Toc480664681)

[2.1. IoT Market Projections 7](#_Toc480664682)

[2.2. Cyber Security Implications 10](#_Toc480664683)

[2.3. IoT in Industry 11](#_Toc480664684)

[2.4. IoT Architecture 12](#_Toc480664685)

[2.5. IoT Attack Vectors 14](#_Toc480664686)

[2.6. IoT and Botnets 15](#_Toc480664687)

[2.7. OWASP IoT top Ten 16](#_Toc480664688)

[3. Methodology 19](#_Toc480664689)

[3.1. Data Collection Methods 19](#_Toc480664690)

[3.1. Ethical Considerations 19](#_Toc480664691)

[3.2. IP Security Camera 1 19](#_Toc480664692)

[3.3. IP Security Camera 2 23](#_Toc480664693)

[3.4. Baby Monitor 27](#_Toc480664694)

[3.5. Bluetooth Heart Rate and Blood Pressure Monitor 29](#_Toc480664695)

[3.6. Smart Power Plug 31](#_Toc480664696)

[3.7. Bluetooth Weight scales 32](#_Toc480664697)

[4. Results 35](#_Toc480664701)

[4.1. IP Security Camera 1 36](#_Toc480664702)

[4.2. IP Security Camera 2 36](#_Toc480664703)

[4.3. Baby Monitor 36](#_Toc480664704)

[4.4. Bluetooth Blood Pressure and Heart Rate Monitor 37](#_Toc480664705)

[4.5. Smart Power Plug 37](#_Toc480664706)

[4.6. Bluetooth Weight Scales 37](#_Toc480664707)

[4.7. Security Concerns Grouped by Vulnerability 37](#_Toc480664708)

[5. Discussion 39](#_Toc480664709)

[5.1. Case Studies 39](#_Toc480664710)

[5.2. Real World Implications 39](#_Toc480664711)

[5.3. Countermeasures 39](#_Toc480664712)

[6. Conclusion 40](#_Toc480664713)

[6.1. Future work 40](#_Toc480664714)

[7. Appendices 41](#_Toc480664715)

[7.1. IP Security Camera 1 – ipcam.sh output 41](#_Toc480664716)

[7.2. IP Security Camera 2 - ipcam.sh output 50](#_Toc480664717)

[7.3. Smart Scale Database Dump 60](#_Toc480664718)

[8. List of References 64](#_Toc480664719)

[Bibliography 68](#_Toc480664720)

# Table of Figures

[Figure 1 – Aspects of life effected by IoT 7](#_Toc480664721)

[Figure 2 – IoT Market trends by Sector 8](#_Toc480664722)

[Figure 3 – Home Internet Enabled devices by category 9](#_Toc480664723)

[Figure 4 – Preparing for IoT in the workplace 12](#_Toc480664724)

[Figure 5 – Three Layer IoT architecture 13](#_Toc480664725)

[Figure 6 – Four Layer IoT architecture 13](#_Toc480664726)

[Figure 7 – Distribution of Mirai Botnet 16](#_Toc480664727)

[Figure 8 – Nmap Scan IP Camera 1 20](#_Toc480664728)

[Figure 9 – Telnet IP Camera 1 20](#_Toc480664729)

[Figure 10 – IP Camera 1 file system 21](#_Toc480664730)

[Figure 11- ipcam.sh file location 21](#_Toc480664731)

[Figure 12 – Username and password dump 22](#_Toc480664732)

[Figure 13 – Password change test 22](#_Toc480664733)

[Figure 14 – User Information dump after password change 23](#_Toc480664734)

[Figure 15 – Nmap Scan IP Camera 2 24](#_Toc480664735)

[Figure 15 – Telnet login to IP Security Camera 2 24](#_Toc480664736)

[Figure 15 – IP Security Camera 2 file system 25](#_Toc480664737)

[Figure 16 – ipcam.sh file position IP Camera 2 25](#_Toc480664738)

[Figure 17 – Logins and password dump IP Camera 2 26](#_Toc480664739)

[Figure 18 – Password change test IP Camera 2 26](#_Toc480664740)

[Figure 19 – information dump after password change IP Camera 2 27](#_Toc480664741)

[Figure 20 – Baby Monitor Nmap Scan Results and telnet connection 28](#_Toc480664742)

[Figure 21 – Packet sniffing of Baby Monitor 28](#_Toc480664743)

[Figure 22 – Man in the middle Cain 29](#_Toc480664744)

[Figure 23 – Cloud interface connection 30](#_Toc480664745)

[Figure 24 – mitmproxy blood pressure monitor 30](#_Toc480664746)

[Figure 25 – Personal information Blood pressure monitor 31](#_Toc480664747)

[Figure 26 – smart plug remote network 32](#_Toc480664748)

[Figure 27 – Smart Plug Desktop Application 32](#_Toc480664749)

[Figure 28 – Smart Scales Cloud Connection 33](#_Toc480664750)

[Figure 29 – Smart scales user information count 34](#_Toc480664751)

[Figure 30 – No. of Vulnerabilities by Device 36](#_Toc480664752)

[Figure 31 – No. of Security Concerns Grouped by vulnerability 38](#_Toc480664753)

# Table of Tables

[Table 1 – Fourth Industrial Revolution 1](#_Toc480664149)

[Table 2 – IoT Units Installed by Category 9](#_Toc480664150)

[Table 3 – IoT Vulnerability Results Table 35](#_Toc480664151)

# Acknowledgements

I would like to thank my supervisor, Xavier Bellekens and head of course Colin Mclean for their advice and support throughout this project and years of study.

I would also like to thank my friends, family and peers who also supported me through my years of study at Abertay University.

# University of Abertay Dundee Permission to Copy

Author: Michael W Crow

Title: Investigating Vulnerabilities In IoT devices in the context of a smart home

Qualification: Ethical Hacking and Countermeasures

Date of Submission: 26/04/2017

~~\* I agree that a copy may be made of the whole or any part of the above-mentioned project report without further reference to the undersigned~~

or

\* A copy shall not be made of the whole or any part of the above-mentioned project report without the written consent of the undersigned.

(\* Please strike out whichever does not apply)

Signature: Michael Crow

Address: Riverview, Main Street, Killin, Perthshire, Scotland, FK218XE

Date: 4/04/2017

# Abbreviations, Symbols, Notation and Glossary of Terms

IoT

P&G – proctor and gamble

Smart Device

Smart Home

Penetration or Pen Test

Penetration tester

White Hat hacking

Black Hat hacking

## Introduction

In the modern age in which we live very few aspects of life are hidden from the ever-advancing wave of modern technology, according to the office for national statistics in 2016, 89% of households in the UK had access to the internet [1] this compared to just ten years before in 2006 when only 57% of UK households had access to the internet highlights the extraordinary popularisation and advancement of the industry in the last decade alone.

With the benefits of technology now firmly cemented into the daily routine of the everyday person, developers of the industry are constantly producing new and intriguing ways in which technology can benefit people in making their lives easier and more productive.

At the forefront of this exciting time in technological advancement lies the subject of the Internet of Things or IoT.

### Introduction to IoT

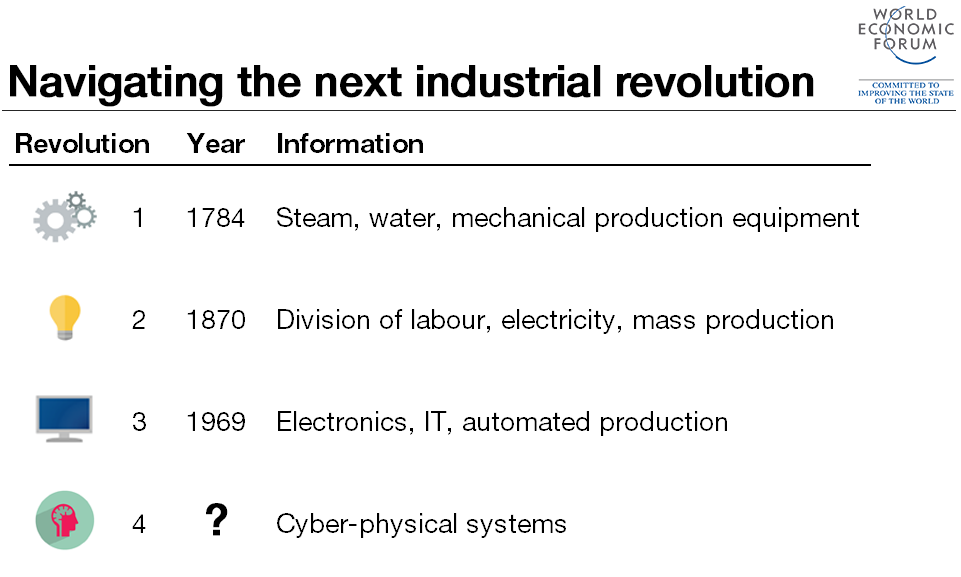
Since its invention in the late 1960s as a part of the third industrial revolution, the internet as we know it has underwent many transformations most notably the invention of the World Wide Web by Sir Tim Berners-Lee in 1990 which introduces the world to the concepts and advantages of interconnectivity. The most modern development in the internet is represented by the concept of the Internet of Things (IoT) is considered by many industry and economic experts as the possible fourth industrial revolution combined with artificial intelligence[2].

Table 1 – Fourth Industrial Revolution – World Economic forum (Klaus, 2016) [2]

The role of the internet of things in the progression of technology appears to be a substantial one in both the near and distant future and therefore it is a very hot topic in the technological world however, many main stream media outlets through using Internet of Things as a “buzz phrase” tends to confuse the general population as to what IoT actually is. As simply defined by the oxford dictionary the internet of Things is; “The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data” (Oxford Dictionary, 2016) [3]. These interconnected devices and everyday objects are often referred to as “smart devices” and form what can be described as the “building blocks” of which the Internet of Things is formed upon.

### History of IoT

The topic of interconnected devices is not by any means a new concept as the idea itself can be traced back to the year 1926 when Nikola Tesla stated;

*"When wireless is perfectly applied the whole earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole.........and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."* (Tesla, 1926).

The concept of interconnectivity continues through the decades until the creation of what many consider the first ever interconnected device in 1990 when John Romkey invented “The Internet Toaster” which used TCP/IP networking to allow itself to be turned off and on over the internet [4].

The term “Internet of things” Is claimed to be coined even as far back as 1999 by Kevin Ashton when he used it as a title of a presentation he was making to Procter & Gamble (P&G) about RFID chip connectivity. [5]

Fast forward to 2011 when the public launch Internet Protocol version 6 (IPv6) produced the scope in which current and future developments of the internet of things can occur as IPv6 allows for 2128 unique internet IP addresses compared to only 232 (4.29Billion) Which IPv4 had almost completely been allocated by the year 2011. The almost limitless amount of IP addresses that IPv6 can assign therefore increasing the rate at which IoT devices can be produced.

### The Modern Smart Home

In 2016 the internet was accessed daily by 82% of adults over the age of 16 in the UK [6], That Amounts to 41.8 Million individuals across the country this compared to 35% (16.2 million) of adults that access the internet daily in 2006 demonstrates that in the last ten years alone internet access has become an integral part of our society, however it is not only the percentage of the population that access the internet that has changed the way in which they access the internet has also seen a dramatic change.

In 2016 70% of adults used a mobile phone or “smart phone” to connect to the internet “on the go” which is a rise of 4% from 2015 [7]. Another device which was not traditionally connected to the internet was televisions, in 2016 28% of adults in the UK used televisions or “smart TVs” to connect to the internet which has also seen a rise of 4% since 2015 [8].

As such devices become more and more popular amongst the general population the concept of the “smart home” is becoming of increasing interest to business and consumer alike.

A “smart home” is a household in which many “smart devices” are used to aid and entertain in everyday life, these devices are often interconnected to a main controller system which can be accessed from a smart phone or remote device which can be used to control devices such as smart lighting, washing machines fridges etc. with the concepts of the internet of things any device can be accessed and controlled remotely over internet connection.

### Penetration Testing and IoT

With the Internet of things quickly becoming an exciting revolution in technological innovation organisations are keen to produce and develop as many devices as the can as quickly as they can, thus many devices are being produced without the proper security testing being carried out. The internet of things at this point has no worldwide standards agency setting a benchmark for security, as a result many smart devices are being purchased by businesses and consumers alike which contain multiple security flaws and therefore may pose risks to personal and private data.

In other sectors of information technology one technique which can be used to assess the security levels of devices and systems is penetration testing. Penetration testing involves the active gathering of information about the device or system in question in an attempt to identify the security weaknesses and entry points in which an attacker or “hacker” may use to compromise the device or system. The person or persons performing the penetration test are often referred to as “white hat” hackers as opposed to “black hat” hackers who aim to exploit security vulnerabilities for unauthorised purposes [9].

In this investigation, existing penetration techniques will be used against multiple “smart devices” in order to assess their current state of security. The penetration testing methodology that will be used in this investigation is the OWASP IoT Methodology.

### Devices Tested in this project

The “smart devices” tested in this project are listed below, all names make and models of the devices are withheld for security purposes:

1. IP Security Camera 1 – Internet based security camera.
2. IP Security Camera 2 – Internet based security camera with audio capabilities.
3. Baby Monitor – Internet based baby monitor with audio capabilities.
4. Bluetooth Heart Rate and Blood Pressure Monitor.
5. Smart Power Plug – Internet based power socket controller.
6. Bluetooth weight scales.

### Research Questions

How can IoT devices adversely affect the security of a “smart home” and its users. What techniques can be deployed against IoT devices to expose their vulnerabilities? Are IoT devices vulnerable? If so what countermeasures can be implemented in order to protect them and their users?

### Research Aims

The overall aim of this investigation is to analyse the possible vulnerabilities of various internet of things devices which could be present in a smart home and were applicable provide suggested suitable countermeasures which could be put in place in order to protect the internet of things devices and their users.

### Research Objectives

This investigation aims to achieve the following objectives:

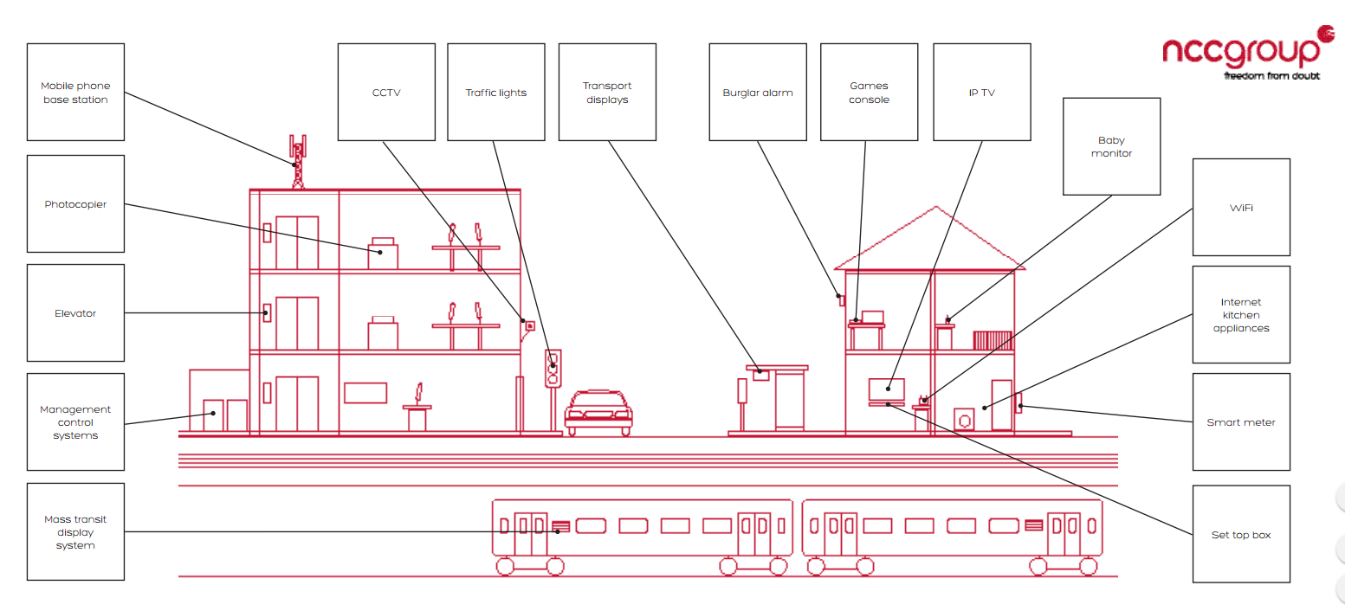
* Analyse the various techniques used to compromise IoT devices.
* Identify Vulnerabilities in all IoT devices Tested.
* Review the level of security present in all IoT devices tested and recommend possible countermeasures to prevent future attacks.

### Statement of Structure

This investigation was based mainly on practical penetration testing of IoT devices with research fundamental to the learning and developing attacks which could be deployed against popular IoT devices thus backing up the practical work carried out. The results of the practical aspects of this investigation were used in conjunction with research to highlight the current state of security in IoT devices and the possible repercussions which users may face as a result. This section of the investigation has been an introduction to the concepts of IoT, Smart Homes and penetration testing. The following section of this investigation is the background and review of current literature which will provide evidence of the current state of play of IoT in the business and consumer markets and will highlight the current academic efforts which aim to assess IoT security. Following the investigation background will be the methodology section documenting the practical steps which were taken to produce the results which will then be discussed with reference to the aims and objectives of this investigation before any conclusions are drawn.

## Background

### IoT Market Projections

The connection of everyday objects to the internet is one of the most discussed about and exciting revelations in modern day technology, this excitement is shared by developers and consumers alike. The main reason for the recent interest in the Internet of Things is its ability to impact on every aspect of modern life.

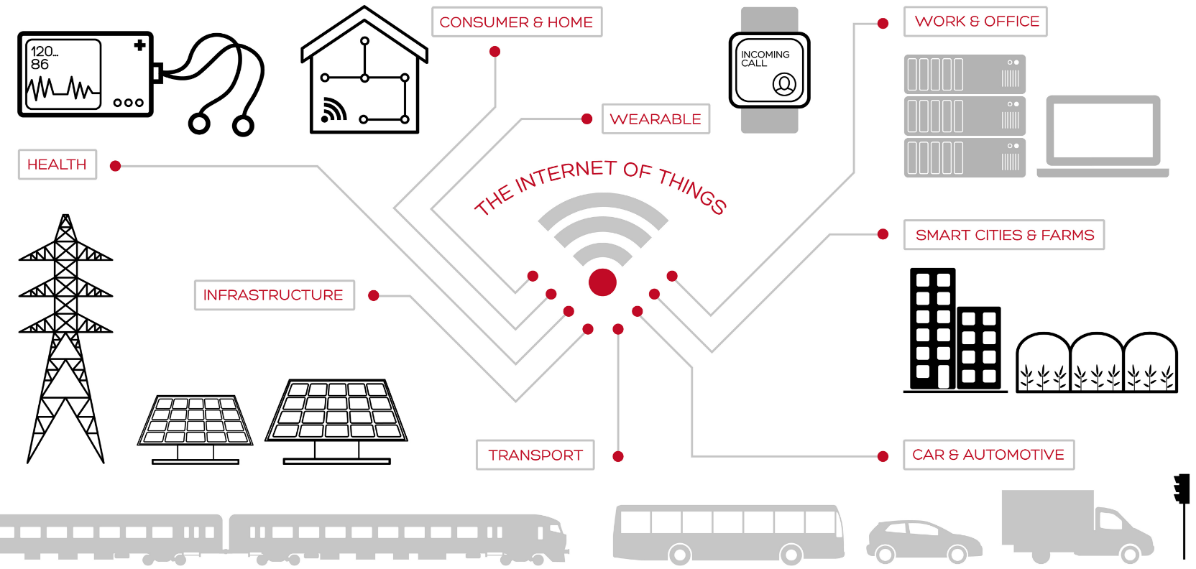


Figure 1 – Aspects of life effected by IoT (NCC Group, 2016) [10]

Which figure is better?

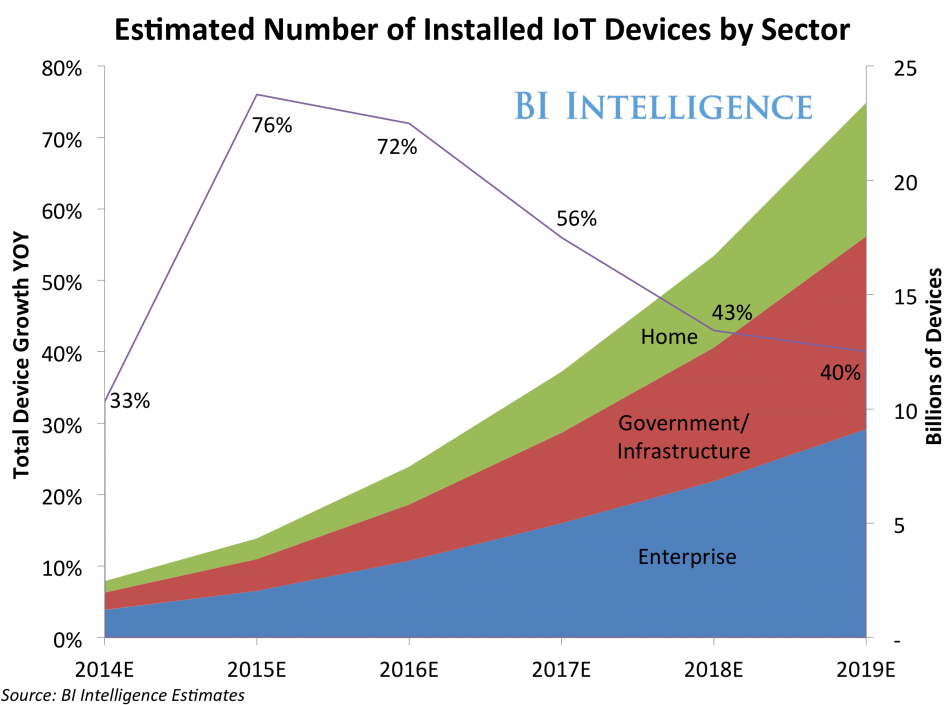
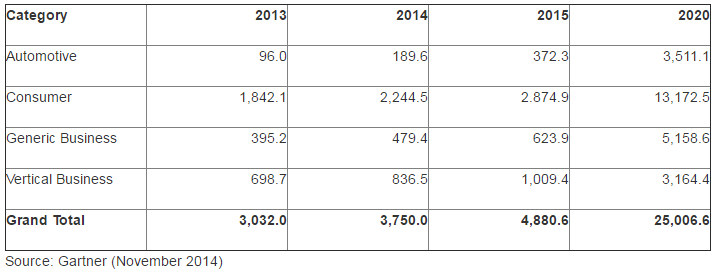
As depicted in figure 1 the Internet of Things is set to influence every sector of industry from home users to enterprise and even government and infrastructure and the rapid developments seem to show no sign of slowing down.

Figure 2 – IoT Market trends by Sector (Business Insider UK, 2014) [11]

Figure 2 above from a report produced by Business Insider UK depicts the current and future market trends of IoT, it estimates that by 2019 the internet of things will have become the “largest device market in the world” [11] more than twice that of the smart phone, PC, tablet, connected car and wearable markets combined [11] this will result in IoT adding $1.7 trillion in value to the global economy in 2019 thus highlighting the huge interest from business in relation to IoT.

Currently the enterprise sector has the largest market share of IoT technologies, however future trends dictate that this share will decline with government and home sectors set to expand rapidly in the near future [11].

According to Gartnerthere will be 25 Billion devices connected to the internet of things in 2020 [12].The vast majority of these devices will be in the consumer sector with over 13 Billion devices.

Table 2 – IoT Units Installed by Category in Million (Gartner, 2014) [12]

The future growth of the home sector which is set to drive global IoT investments provides the scope for this investigation which will focus on the domestic consumer sector “smart devices” and their users.

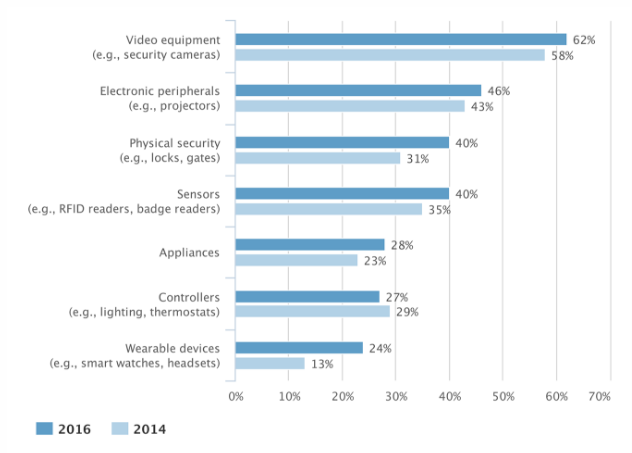
The domestic consumer market consists of a wide verity of technologies from wearable technologies to security cameras, this verity of consumer IoT devices is evidenced in a report by the marketing research organisation “Spiceworks” who surveyed 440 IT professionals across the globe [13].

Figure 3 – Home Internet Enabled devices by category (Spiceworks, 2016) [13]

This report by SpiceWorks shows that currently the most popular IoT devices in the consumer sector are video related devices, it is for this reason that a larger focus on video based IoT devices was adopted with three video based devices being selected to test.

### Cyber Security Implications

#### 2.2.1 Current Landscape

The topic of cybersecurity as a whole, has become a valid and excepted expense in the most modern business models, this has come to be after years of high profile breaches which has opened the eyes of big business to the losses which can be incurred both in relation to financial loss and logical data loss. Recent research conducted by the UK government

Government research found that in the last year 46% of UK businesses experienced a cyber security breach of some kind [14], the study also revealed that 67% of the surveyed businesses have a budget for cyber security but only 11% have a cyber security incident plan [14]. As a direct result of this research governmental bodies are urging businesses to take a more no nonsense approach to the threats of cybersecurity as government themselves has as they recently announced a further £1.9 Billion investment in cybersecurity [14], this large investment highlights the fact that cybersecurity reaches every department of modern life.

This current cybersecurity landscape imposed on government and business is a result of the various legislative and compliance frameworks that now exist within the industry such as PCI DSS compliance for example, which focuses on securing the IT infrastructure and software of businesses which handle card payment transactions, if businesses don’t comply they face large fines. This is just one example of how international legislature can act as an incentive to organisations in relation to increasing their levels of cybersecurity.

#### 2.2.2 Introduction of IoT

As internet of Things devices become more and more prevalent in business and government as they are forecast to, it will only become harder for these sectors to defend against cyber-attacks. This is due to the diverse range of IoT devices which will be used in various areas of business performing a range of tasks from physical security such as IP cameras to sensor based systems at the customer facing front end. The increased usage of these devices will therefore increase the number of potential entry points which attackers could exploit. Currently at the time of writing there is no standards authority regulating the security level of existing or newly developed internet of things devices, the prospect of this wave of technology being introduced to every sector of life without proper scrutiny is a daunting prospect for business, government and consumers alike.

Recent research conducted by Sadeghi, Wachsmann and Waidner (2015)[15] details the security and privacy challenges facing the industrial internet of things, supporting the argument that industry’s current urge to “connect the unconnected” is leaving itself open to further potential entry points for attackers. Sadeghi, Wachsmann and Waidner (2015) [15] state that industry cannot afford to adapt to the threats posed by IoT as slowly as it did to the now accepted threats and common practices of cyber security. Although this statement is agreeable the concepts of IoT security must be viewed upon holistically and organisations must be educated on the threats which may put their systems at risk. This may not be as easy as some may think due to industry’s resilience to inherent further costs and procedures without substantial proof.

### IoT in Industry

In a recent report by SpiceWorks [16], which surveyed 440 industry professionals worldwide, 84% of professionals agreed that the most concerning aspect of Internet of Things integration into industry is that the devices themselves “create more entry points into the network”. The study also details that three quarters of IT pros are also extremely worried that the manufactures of IoT “aren’t implementing sufficient security measures” [16]. Further research conducted by Borgohain, Kumar and Sanyal, (2015) [17] goes as far as to state that based on its survey of vulnerabilities in internet of things devices and systems industry must first focus on securing the IoT infrastructure and devices that currently exist and halt the rapid development of new devices until a point which it can be assured that they can be secured in order to protect consumer and industrial privacy. This strong opinion highlights the severity of the situation according to industry experts.

However this warning to industry seems to have been ignored, again referring to the recent survey carried out by SpiceWorks (2016) [16] in which they asked if organisations are preparing for IoT in the workplace:

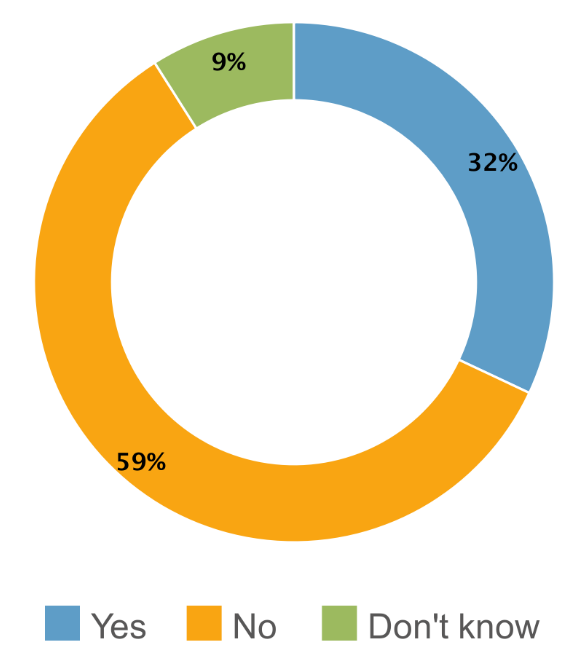


Figure 4 – Preparing for IoT in the workplace (SpiceWorks 2016) [16]

As depicted in figure 4 above, 59% of professionals confessed that they were not in fact preparing for the introduction of IoT in the workplace.

### IoT Architecture

In order to fully understand the vulnerabilities facing the Internet of Things and whether or not they are vulnerable, a large focus on the architecture of IoT, According to research conducted by Yousuf, Mahmoud and Imran Zualkernan, (2015) [18] IoT operates on three layers; The Perception layer, The Network Layer, and the Application layer. The Perception or “Sensors” layer is the layer in which data is acquired, the data is collected and processed in this layer, this data is then sent to the network layer. The network layer of the architecture is responsible for data transmission and routing, it achieves this through making use of wireless technologies such as Wifi, Bluetooth or 3G/4G. These technologies filter and transmit the data to and from the IoT device.

The final layer of architecture proposed by Yousuf, Mahmoud and Imran Zualkernan, (2015) [18] is the application layer, this layer validates the sending and receiving of data to and from the network layer, it achieves this through various authenticity and confidentiality techniques. This research by Yousuf, Mahmoud and Imran Zualkernan, (2015) [18] defines IoT architecture in its simplest form as demonstrated by figure 5 below;

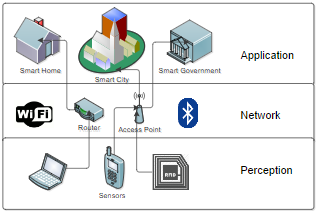


Figure 5 – Three Layer IoT architecture (Yousuf, Mahmoud and Imran Zualkernan, 2015) [18]

However further research conducted by Farooq et al, (2015) [19] proposes a slightly more detailed architecture for the Internet of things with a “Middle-Ware Layer” being added as a fourth layer in between the network layer and the application layer as depicted in figure 6 below;

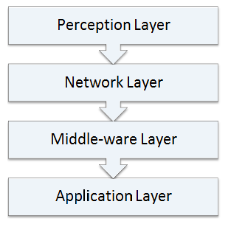


Figure 6 – Four Layer IoT architecture (Farooq et al,2015) [19]

This Middle ware layer acts as a further information processing system automating the delivery of data to relevant databases providing storage capabilities, this then allows the application layer to process the more practical aspects of the architecture with extra resource such as user interaction and the implementation of smart environments and transportation.

### IoT Attack Vectors

Understanding the way in which Internet of Things devices are constructed and operate is vital to identifying the possible techniques which attackers could employ in order to exploit their vulnerabilities.

Research conducted by Abomhara and Køien (2015) [20] details an extensive list of attacks which can exploit vulnerabilities existing in modern IoT devices face. Abomhara and Køien (2015) [20] group the attacks as follows;

* Physical Attacks – Attacks in which the tampering of hardware and connection ports is performed.
* Reconnaissance Attacks – The mapping and discovery of open ports and services as well as gathering IP address information by an attacker.
* Denial of service (DoS) Attacks – An attack which can disable the functionality of the device or the system in which it is a part of.
* Access Attacks – These types of attacks can be grouped into physical access attacks and remote access to attacks. An access attack involves unauthorised access to the device or its network.
* Privacy Attacks – Attacks which aim to steal private user data, privacy attacks can entail data mining, espionage, sniffing and password cracking attacks.

This grouped list off attacks facing IoT devices is testament to the diverse nature of IoT technologies as any number of these attacks can be performed on an IoT device or network. Research carried out by Nawir et al, (2017) [21] mirrors much of this opinion, that the Internet of Things faces substantial amounts of security related issues, this research places an interesting blame on a recent inactivate in china called “Sensing China” an attempt to “rapidly accelerate the development of IoT across the country” (Nawir et al, 2017) [21] , a keen interested is also taken in this research to the usage of IoT devices in denial of service attacks of which several high-profile cases have been documented recently.

### IoT and Botnets

In recent years Distributed Denial of Service (DDoS) attacks have grown in popularity amongst attackers, the attack itself aims to make an online service unavailable to its users, this is achieved through flooding the services servers with extremely large amounts of information or “traffic” (Mirkovic, Prier and Reiher, 2003) [22], this traffic is sent to the services servers from multiple sources often making use of a “botnet”. A “botnet” is a “large collection of well-connected compromised machines that can be co-ordinated to partake in malicious activities” (Rajab et al., 2007) [23]. As conventional DDoS attacks have grown in popularity over recent years as to has the defence against them, organisations are monitoring their traffic and communications with the outside world with a lot more scrutiny this has resulted in attackers resorting to think outside the box in terms of approach and scale of DDoS attacks, especially the size and scale of the botnets used.

In September 2016 the Mirai botnet announced its presence as the key behind the largest DDoS attack in history (Newman, 2016) [24]. Mirai operated by implanting malware onto vulnerable IoT devices such as IP Cameras, smart DVRs and routers, in doing so Mirai managed to compromise as many as “half a million devices” in 164 countries according to research conducted by Angrishi (2017) [25]. This huge number of compromised devices allowed the Mirai botnet to produce a record braking 1.1Tbps DDoS attack (Angrishi 2017) [25] and through doing so managed to take out a number of high profile internet based services such as Amazon, Spotify, Twitter and many, many more (Cox, 2016) [26].

Figure 7 below depicts the distribution of the Mirai Botnet as of 26th October 2016;



Figure 7 – Distribution of Mirai Botnet (Angrishi 2017) [25]

The current academic climate clearly dictates a feeling of unrest in relation the IoT security amongst security professionals and researchers alike as evidenced through numerous sources, through the latest research of the Mirai botnet it appears as though these feelings of unrest are well warranted as many feel as though this is just the beginning. However the academic climate seems to be overwhelmingly focused on the big picture of IoT security and therefore much of the current research fails to detail exactly how vulnerable the internet of things is through practical methods. The following sections of this investigation aims to build upon the evidenced current research that documents the possible security vulnerabilities and architecture structures with the overall aim of creating a step to step guide to exploit some of these vulnerabilities to judge if IoT devices are on an individual level as vulnerable as security experts dictate.

### OWASP IoT top Ten

In order to assess the level of security present on the internet of things devices tested in this investigation the Open Web Application Security Project (OWASP) Internet of Things testing methodology was adopted [27]. OWASP is a non-profit organisation operated by security professionals all over the world. The main reason for choosing this methodology is its open source nature and therefore its free to use and distribute. The OWASP IoT methodology itself replicates the original OWASP penetration testing methodology which is based on the OWASP top ten which is a list of vulnerabilities which OWASP deem to be the most crucial to systems.

The OWASP IoT top Ten vulnerabilities are as follows;

1. Insecure Web Interface

The assessment of insecure web interfaces will not be explored in this investigation as explicit consent has not been granted, this will form part of the future work section of this document.

1. Insufficient Authentication

To test for insufficient authentication analysis of default system passwords will be performed. Network traffic analysis will lso be performed with Wireshark.

1. Insecure Network Services

The NMAP tool will be used to assess the IoT devices their open ports and services which are running on those ports.

1. Lack of Transport Encryption

The lack of transport encryption will be assessed using Wireshark to determine whether data is being properly encrypted when transported or if data is transported in plain text.

1. Privacy Concerns

Privacy concerns will be explored with the use of sniffing and file exploration depending on the existing vulnerabilities of the IoT device

1. Insecure Cloud Interface

Devices using a cloud interface will be assessed through account enumeration. Traffic analysis will be performed with Wireshark to determine any exposed credentials or account vulnerabilities.

1. Insecure Mobile Interface

Mobile interface vulnerabilities will be explored using packet sniffing techniques with Wireshark and account enumeration.

1. Insufficient Security Configurability

The configurability of all devices will be investigated focusing on the extent which permissions can be configured and configurability options available.

1. Insecure Software/Firmware

Insecure software present on the devices will be investigated to determine file encryption levels, verification methods and update functionality as well as a further focus on firmware containing sensitive information.

1. Poor Physical Security

The devices will be analysed in relation to the accessing of software via physical ports such as USB and the possible presence or use of removable storage media.

The following section of this investigation documents the practical steps which were taken to assess the level of security of each individual Internet of Things Device tested in the scope of this investigation.

## Methodology

As previously discussed the practical aspects of this investigation were carried out referencing the OWASP IoT Top ten testing project and methodology.

### Data Collection Methods

A total of six IoT devices were tested in this investigation, the devices were all tested in a lab and home environments using a PC computer and IPhone 6s for the mobile interface applications. All results have been kept strictly confidential with the investigator and project supervisor.

### Ethical Considerations

Only proof of concept data was using the testing of all applications therefore no personal user information was obtained or distributed. Any testing which could impact negatively on the devices services was not performed, therefore some areas of the OWASP IoT methodology testing was not performed such as web application testing due to ethical and legal reasons.

### IP Security Camera 1

The first device which was tested in this investigation was IP Security Camera 1, this generic IP camera operated over Wi-Fi and through Ethernet connection. It operates as a live CCTV network camera which has the capability of mobile, browser and desktop application viewing. Mobile viewing can also be done remotely via a mobile application. The camera allows for the user so store images and video at set intervals or constantly.

IP Security camera was set up in a lab testing environment connected via Ethernet to begin with for calibration until Wi-Fi capability was set up.

The first stage of testing this camera involved performing a Nmap scan against the ip address of the camera. Nmap is a free to use tool which is used for port scanning and network exploration including what services are running on the open ports of the device [28]. The IP address of the camera in this case was found to be 192.168.1.104.

The Nmap scan results for IP Camera 1 can be evidenced in figure 8 below;

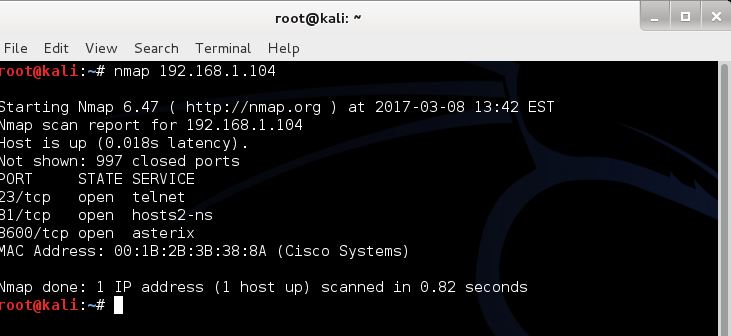


Figure 8 – Nmap Scan IP Camera 1

The Nmap scan clearly shows three open ports on the device;

* TCP Port 23- Telnet
* TCP Port 81 – hosts2-ns
* TCP Port 8600 – asterix

The presence of an open telnet service running on its default port was of much interest as telnet is a service which allows for the remote connection to network devices.

The next stage of the test was to attempt to remotely connect to the camera via its telnet service.



Figure 9 – Telnet IP Camera 1

As evidenced in figure 9 above access to the IP Camera was granted, this was achieved by simply guessing the root password of the device, the following credentials were used to connect via telnet to the camera;

* Login – **root**
* Password – **123456**

Once connected to the camera exploration of the files present on the IP Camera could be carried out. Files present on the device are presented in in figure 10 below;

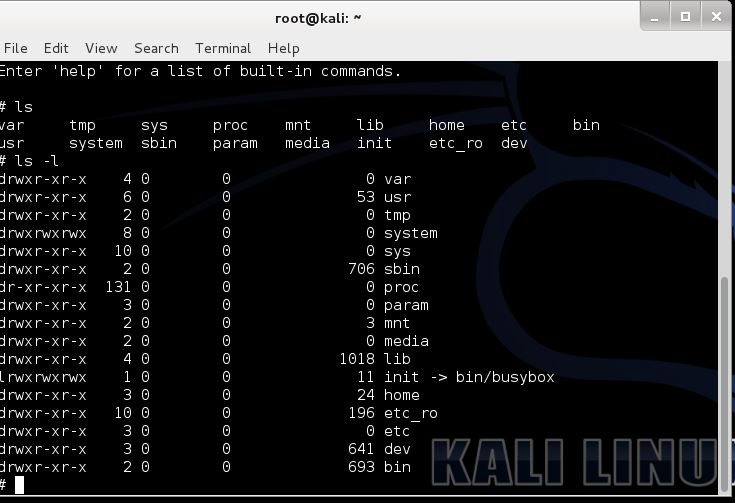


Figure 10 – IP Camera 1 file system

After further exploring the files within the IP Cameras system an interesting file called “ipcam.sh” was discovered, the location of this file within the system was “/system/init/ipcam.sh” which can be seen in figure 11 below;

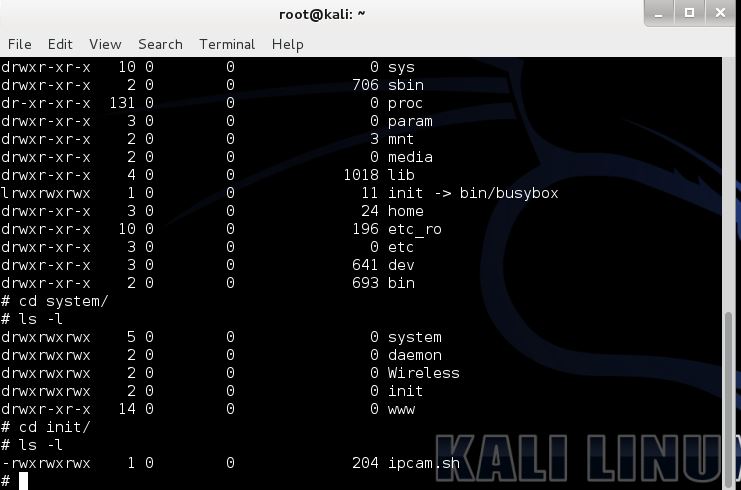


Figure 11- ipcam.sh file location

When the file “ipcam.sh” was run it returned interested results as the complete system setup and configuration of the IP Camera was dumped to the screen, as full export of the system configuration dump can be referenced in Appendices 7.1.

Upon close inspection of the system configuration dump it was discovered that all username and password information was displayed as shown in figure 12 below;

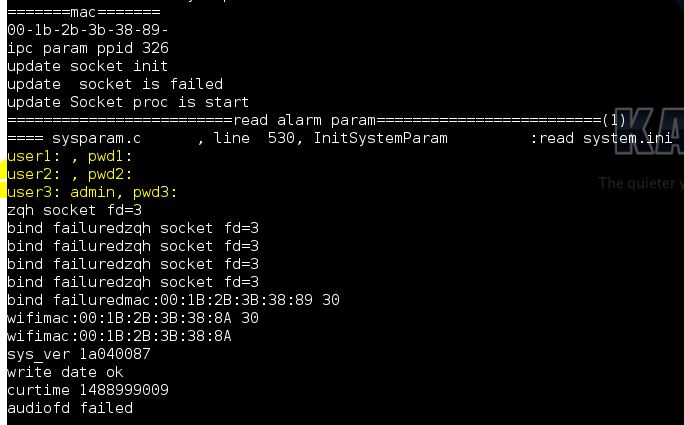


Figure 12 – Username and password dump

In order to confirm that this was in fact the usernames and passwords of the user accounts the password was changed using the mobile application evidenced in figure 13 below;

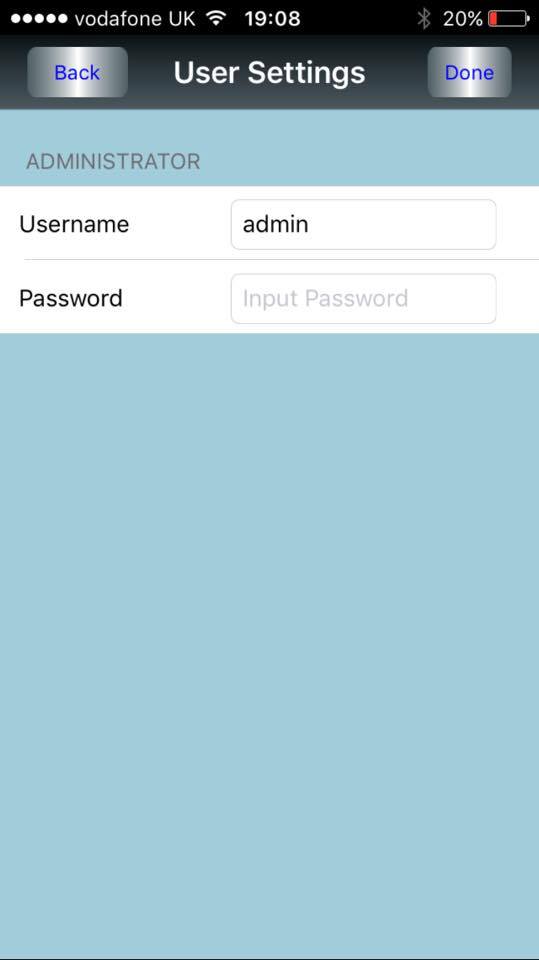
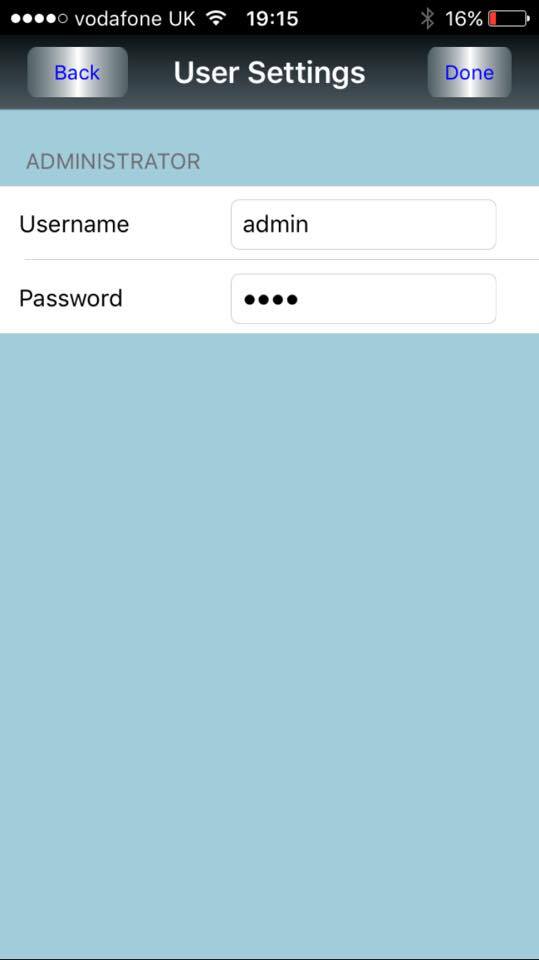


Figure 13 – Password change test

The password was changed to “test” using the mobile application.

Once the password was changed the “ipcam.sh” file was executed once again which confirmed suspicions that the dumped usernames and password in question were in fact accurate. Evidence of the dumped usernames and passwords after the changing of the user’s passwords is demonstrated in figure 14 below;

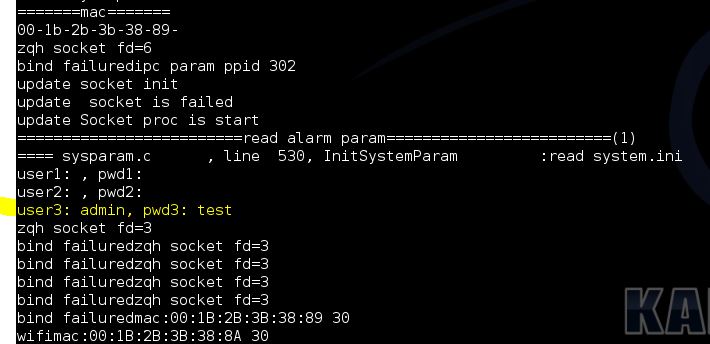


Figure 14 – User Information dump after password change

### IP Security Camera 2

The second device to be tested was a secondary IP Security Camera, it must be noted that this camera was of an entirely separate brand to IP Security camera 1. This IP Camera operated in much the same was as IP Security Camera 1 in that it produced a live video feed which can be sent to a mobile application to allow the user to view it. This camera also allowed for rotation on two axis as well as the ability to both listen to and send live audio to and from the camera. The camera was connected to the network via Ethernet connection until Wi-Fi settings could be configured. The mobile application was also install and set up allowing connection to the camera via Wi-Fi.

The first stage in testing IP Security Camera 2 was to perform a Nmap port and service scan against its IP Address. The IP address of IP Camera 2 was “192.168.1.216”.

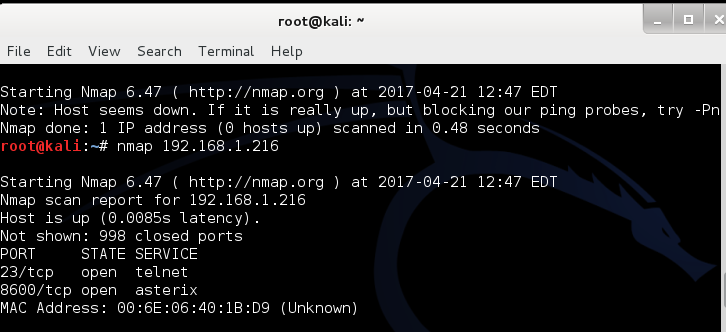


Figure 15 – Nmap Scan IP Camera 2

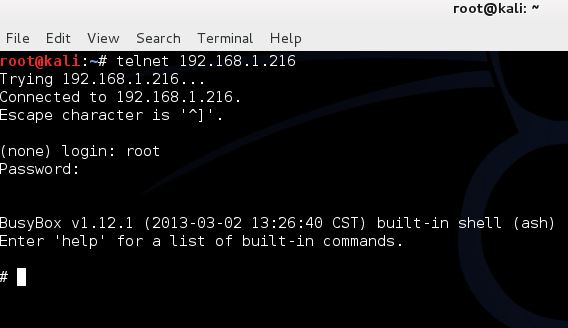
Figure 15 above displays the Nmap port and service scan results for IP Security Camera 2. The two ports open are;

* TCP Port 23 - telnet
* TCP Port 8600 – asterix

An attempt to connect to the IP camera through telnet was then carried out. With the use of password guessing, the telnet login and password were found to be;

* Login – **root**
* Password – **123456**

The process of the connection to IP Security Camera 2 is demonstrated in figure 15 below;

Figure 15 – Telnet login to IP Security Camera 2

Once connection to the IP Camera was established its file system was explored, the files present on IP Security Camera 2 are shown in figure 16 below;

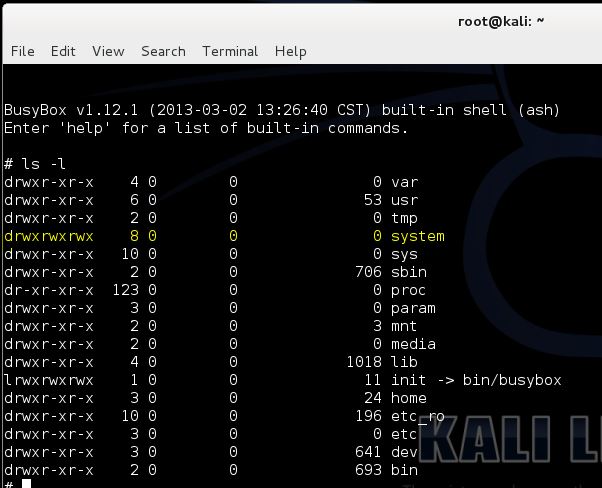


Figure 15 – IP Security Camera 2 file system

As the file system appeared to be very similar to that of IP Security Camera 1 the “/system/init” directory was explored for similar files as “ipcam.sh” which was discovered in IP Camera 1.



Figure 16 – ipcam.sh file position IP Camera 2

The Linux executable file “ipcam.sh” was located in the “system/init” file directory as evidenced by figure 16 above. When executed this file dumped all system configuration to the screen similar to IP Security Camera 1, the full output of the “ipcam.sh” for IP Security Camera 2 can be reference in Appendices 7.2.

Within the output of “ipcam.sh” was a list of usernames and passwords as shown in figure 17 below;

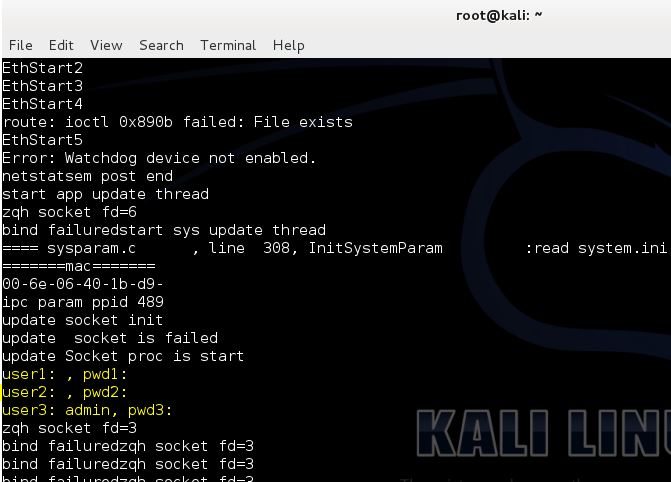


Figure 17 – Logins and password dump IP Camera 2

As with IP camera 1 the password of the user account was changed in order to confirm that the accounts displayed when executing the “ipcam.sh” file were in fact the correct user account details.

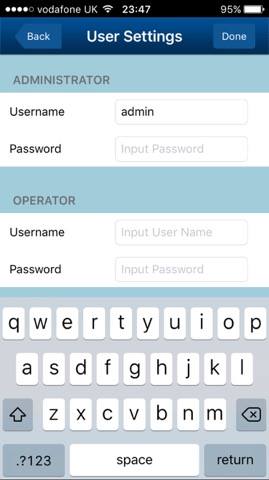
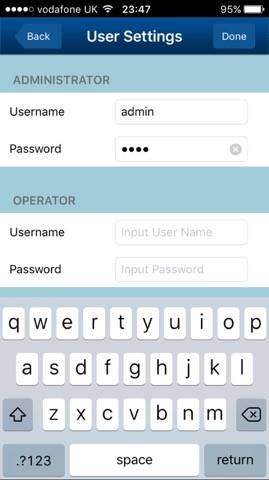


Figure 18 – Password change test IP Camera 2

Figure 18 above evidences the change in password to “test”. Following this change the “system/init/ipcam.sh” file was re executed and the user information had infact changed to “test” as evidenced in figure 19 below;

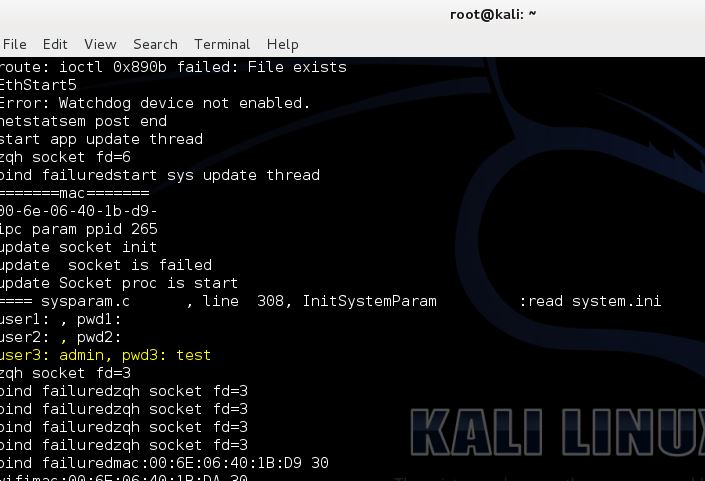


Figure 19 – information dump after password change IP Camera 2

### Baby Monitor

The third device tested was an IP security camera which was marketed as a home baby monitor which has been “secured” for the users protect. The device worked in much of the same way as the other IP Security Camera devices tested in this investigation. The camera allows for live streaming of images to a dedicated mobile and browser applications.

The first stage in testing the baby monitor was to perform a Nmap ports and services scan against its IP address, the IP address of the baby monitor in this case was 192.168.1.214. The baby monitor was found to have only one port open;

* TCP Port 14987 – Unknown Service

After further investigation port 14987 was found to be running a telnet service.

Figure 20 below demonstrates the output of the Nmap scan performed against the baby monitor and the attempt to connect to the telnet service;

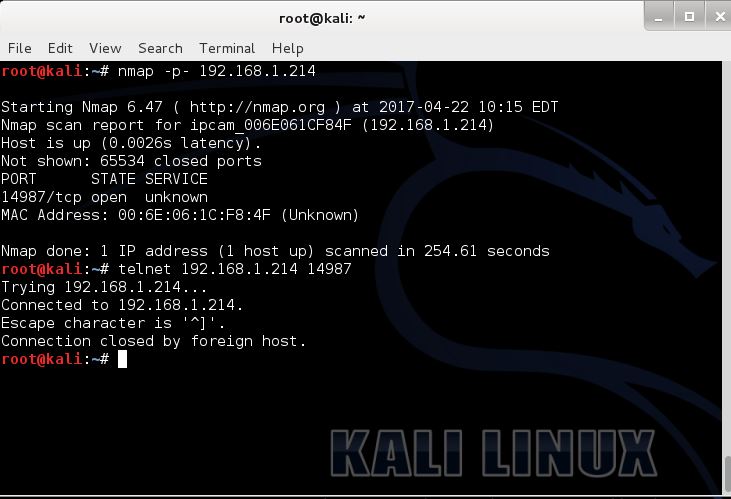


Figure 20 – Baby Monitor Nmap Scan Results and telnet connection

The baby monitor device has disabled remote connection to its systems over telnet however the next stage of the testing, packet sniffing, revealed that the telnet service running on port 14987 was unencrypted.

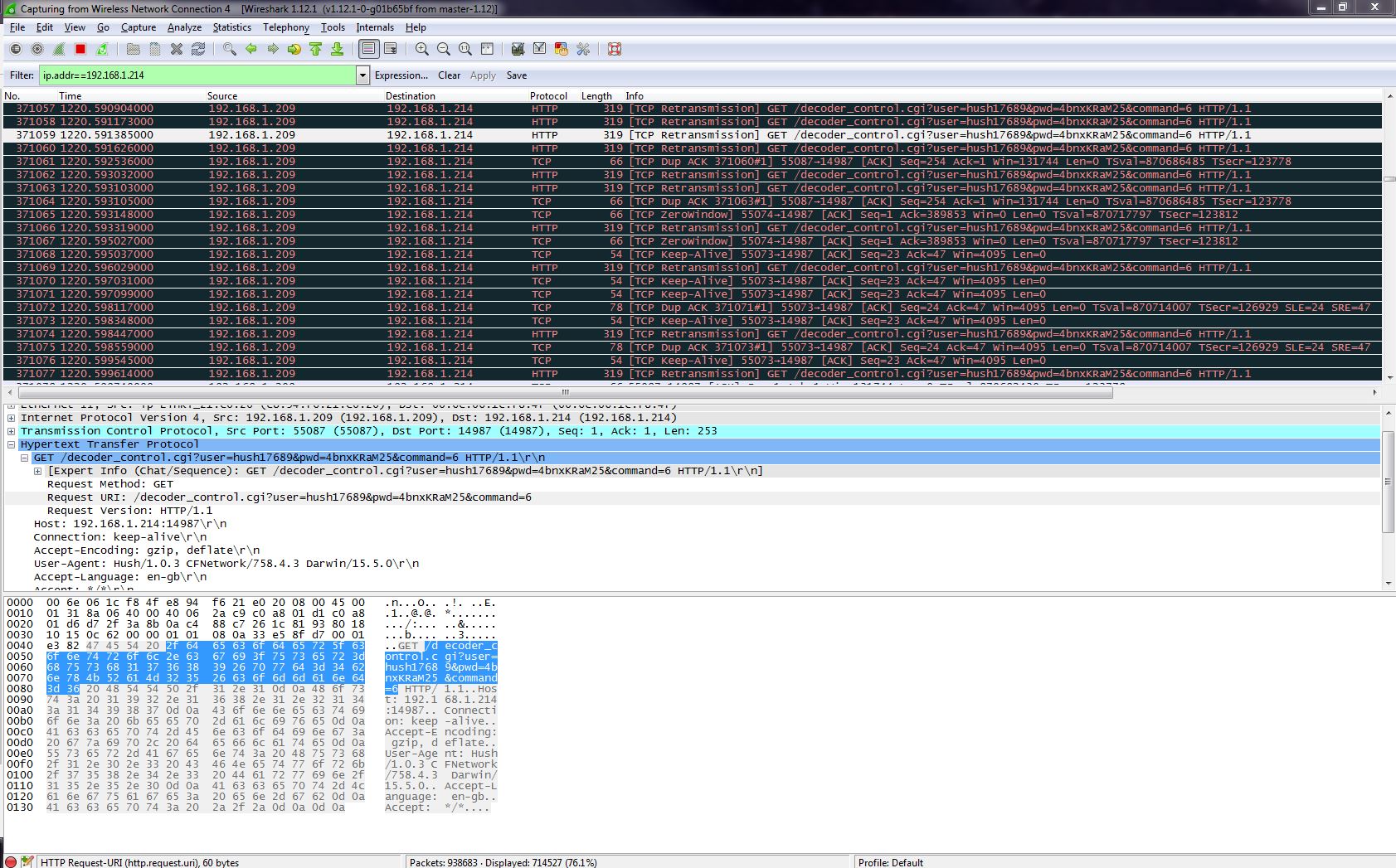


Figure 21 – Packet sniffing of Baby Monitor

Figure 21 above shows the Wireshark [?] analysis of the data packets transferred to and from the baby monitor, within one of the data packets is the user credentials used to connect to “192.168.1.214” port “14987”. The credentials discovered are as follows;

* User – **hush17689**
* Password – **4bnxKRaM25**

### Bluetooth Heart Rate and Blood Pressure Monitor

The fourth device tested was a wireless blood pressure and heart rate monitor, this device used Bluetooth to communicate to and from a dedicated mobile application. The mobile application itself allowed the user to capture and store blood pressure and heart rate information within the mobile device itself. The user is provided with the option to export all data to a healthcare professional or friend/ family member, this functionality of the application makes use of email to export the data.

The first stage of testing the Bluetooth blood pressure monitor was to perform a man in the middle attack between the mobile application and cloud interface. The process was completed using the Cain and able penetration testing tool [?] and Wireshark [?]. Figure 22 below evidences the process of the man in the middle attack on the device;

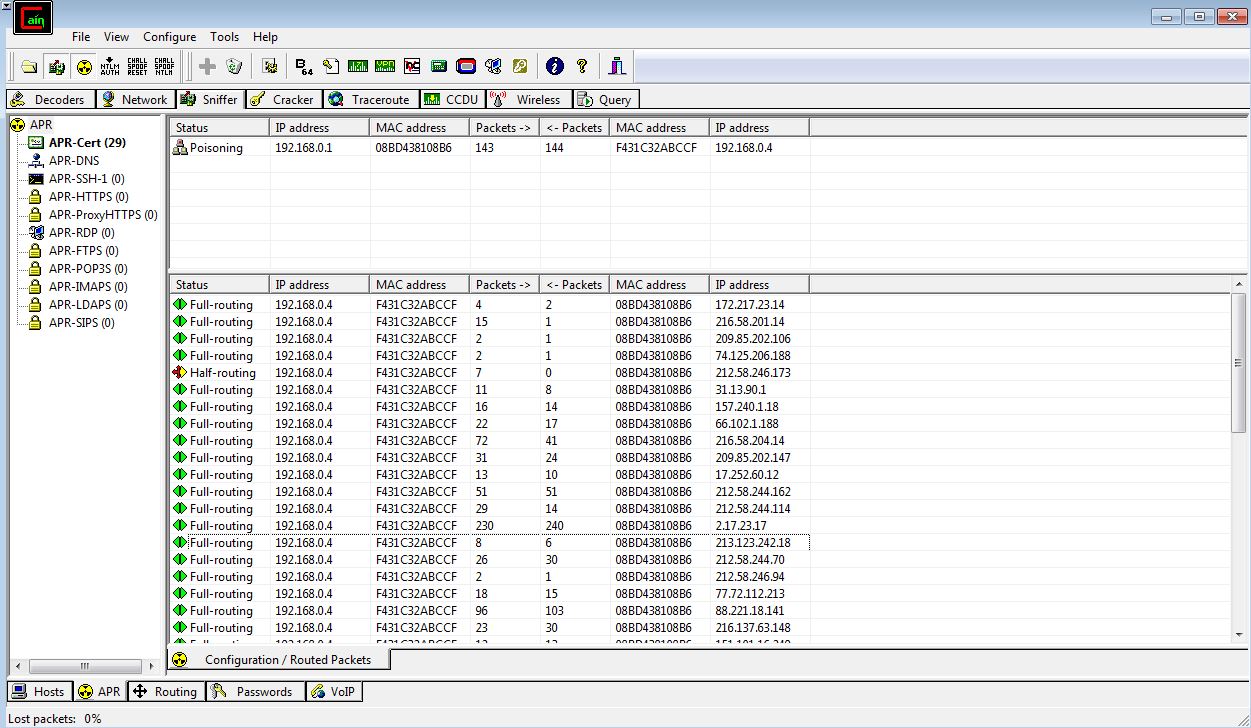


Figure 22 – Man in the middle Cain

Analysis of the certificates generated when performing the man in the middle attack showed a connection to the devices cloud interface as shown in figure 23 below;

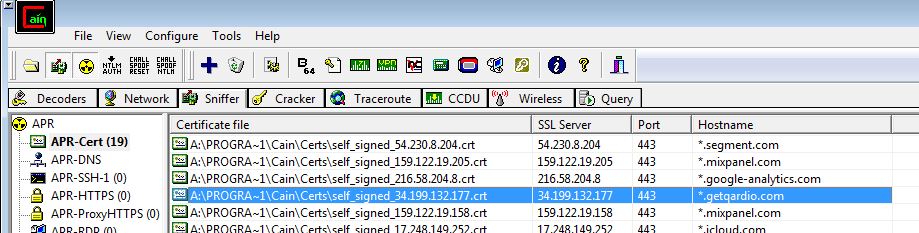


Figure 23 – Cloud interface connection

Analysis of the data packet transfer to this cloud interface via Wireshark showed that all traffic was in fact encrypted using SSL (TLS v1.2). In order to circumnavigate this encryption a too called man in the middle proxy (mitmproxy) was used in order to receive the data unencrypted. Figure 24 below evidences the unencrypted traffic using mitmproxy;

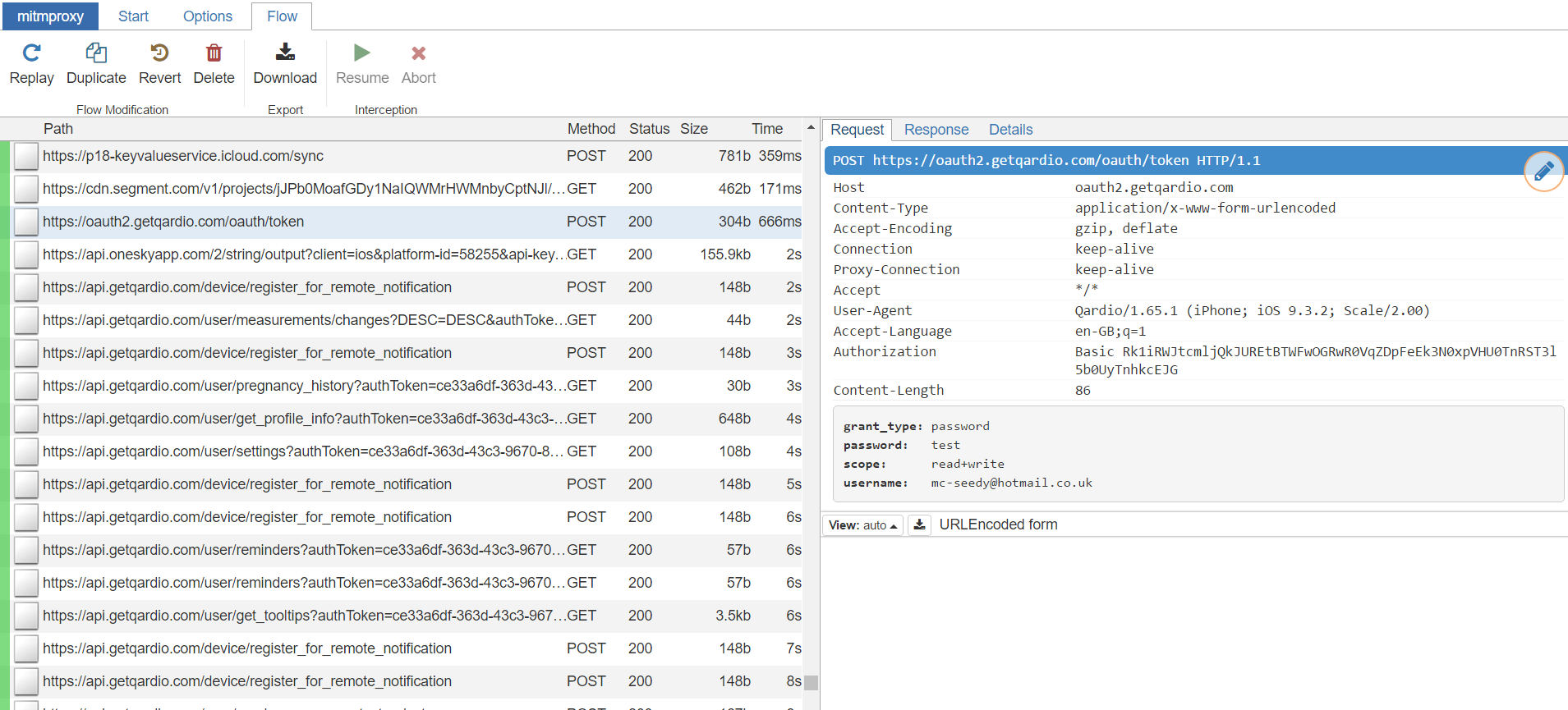


Figure 24 – mitmproxy blood pressure monitor

Within the viewable unencrypted connections and data was the username and password of the user as shown in figure 24 above. Upon further inspection of the data transfers was the complete user profile and information being transferred to the cloud interface of the device as detailed in figure 25 below;

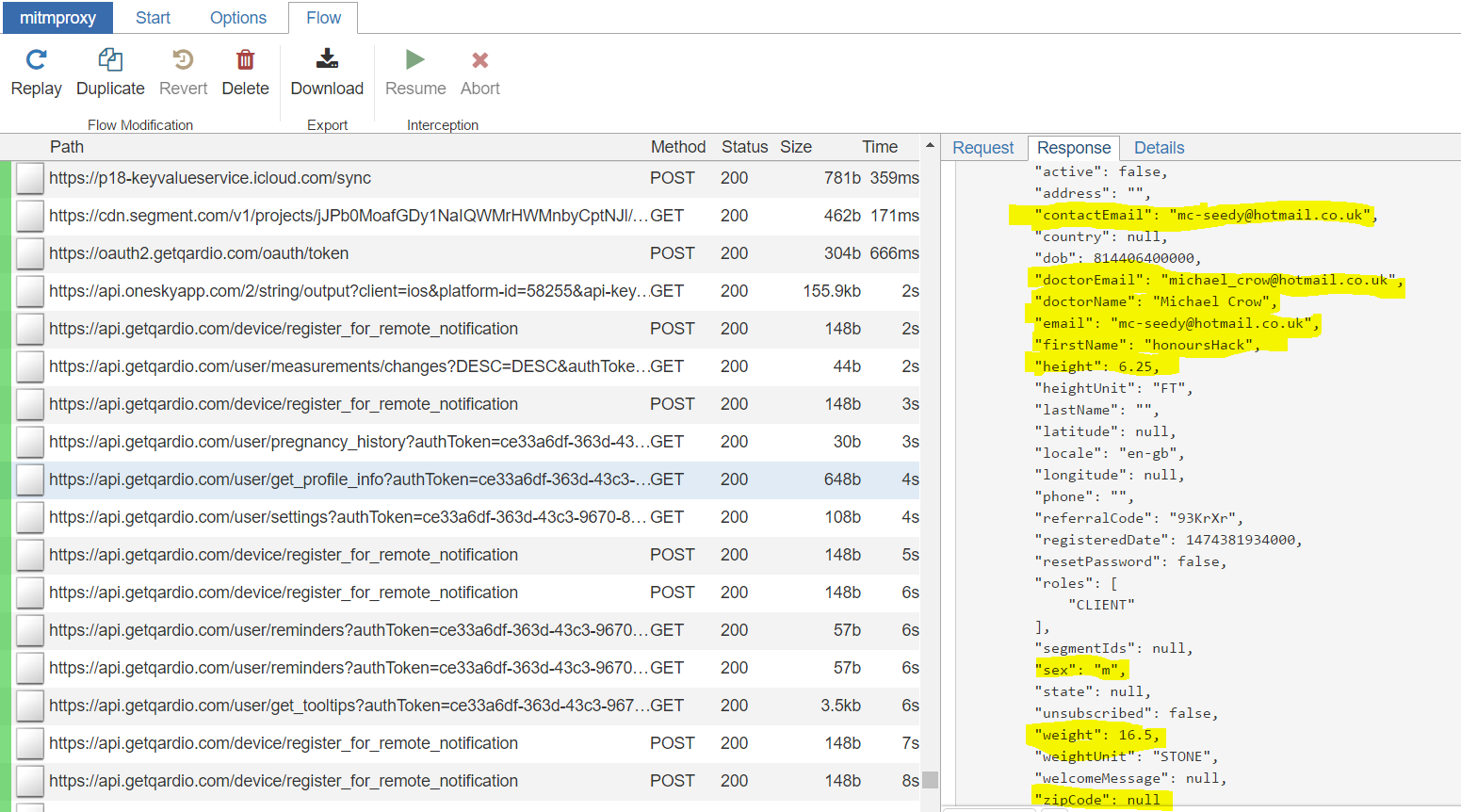


Figure 25 – Personal information Blood pressure monitor

This information included the doctor information and user information such as height, geographical location, phone number, sex, weight and postal code. When the user exported the data within the email functionality of the mobile app the complete contents of the email could be captured including any notes, it should also be noted that using mitmproxy allows for the editing of this data for example email address and then by replaying the connection the data could be sent to another email address chosen by the attacker.

### Smart Power Plug

The next device tested was a generic smart power socket device, this device allows a user to control the turning on and off any electrical device connected via mains plug socket, the device advertises that connection and control of the smart plug is only available through its dedicated mobile application. The device also provides the user with time setting functionality which allows the user to a specific time to allow or disallow power to the electrical item connected via the smart power plug.

The first stage in testing was to attempt to Nmap scan the device in search for open ports and services present on the device however, all communication ports were closed on the device. The next stage of testing was to assess the level of security present on the mobile application, upon inspection it was discovered that there was numerous applications present on the apple app store which would allow any mobile user in the vicinity of the smart plug to add it as a device without a specific password, the user could also access the plug outwith the network in which it is set up, in the case of this investigation the smart plug could be controlled using a second mobile device using 4G as shown in figure 26 below;

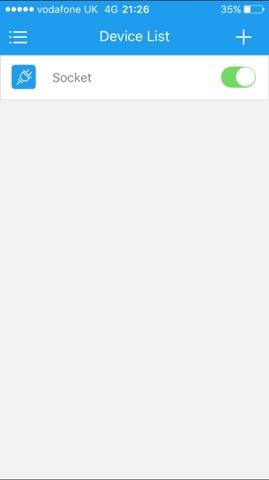


Figure 26 – smart plug remote network

After further research into the smart plug itself, it was discovered that a desktop application had been created by a previous user that when run would allow for the connection to the plug connected to the same network as the desktop itself. The application created by [?] is freely available on GitHub. Figure 27 below is a combination of screenshots evidencing the applications functionality in relation to the turning off and on of the smart plug;

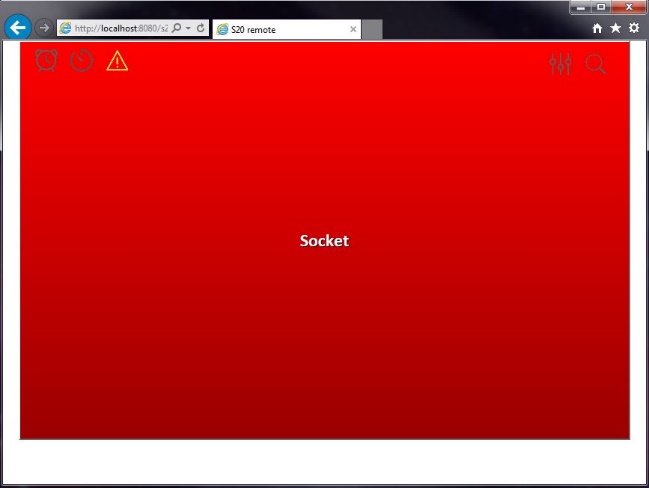
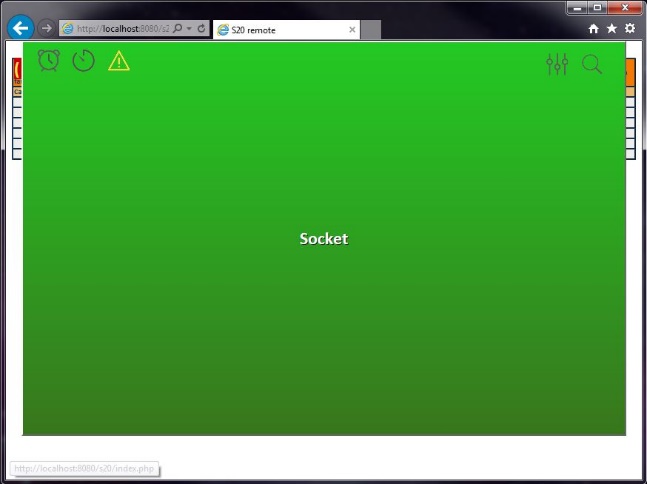


Figure 27 – Smart Plug Desktop Application

### Bluetooth Weight scales

The sixth device tested was a smart weight scale, the scale makes the use of Bluetooth technology to connect to a mobile device which has been pre-installed with a dedicated mobile application. The mobile application acts as a general health tool which contains information on the user’s weight history, height and other personal details. The application also provides an email functionality which can export all health data to a specified email address.

The testing of this device was conducted using mitmproxy in order to capture the communication of the smart scale mobile application. The first interesting communication captured was the immediate connection to the applications cloud interface, this connection displayed the username and password in the request packet, however the user’s password was in fact encrypted. Figure 28 below is details the capture of the cloud connection with username and encrypted password;

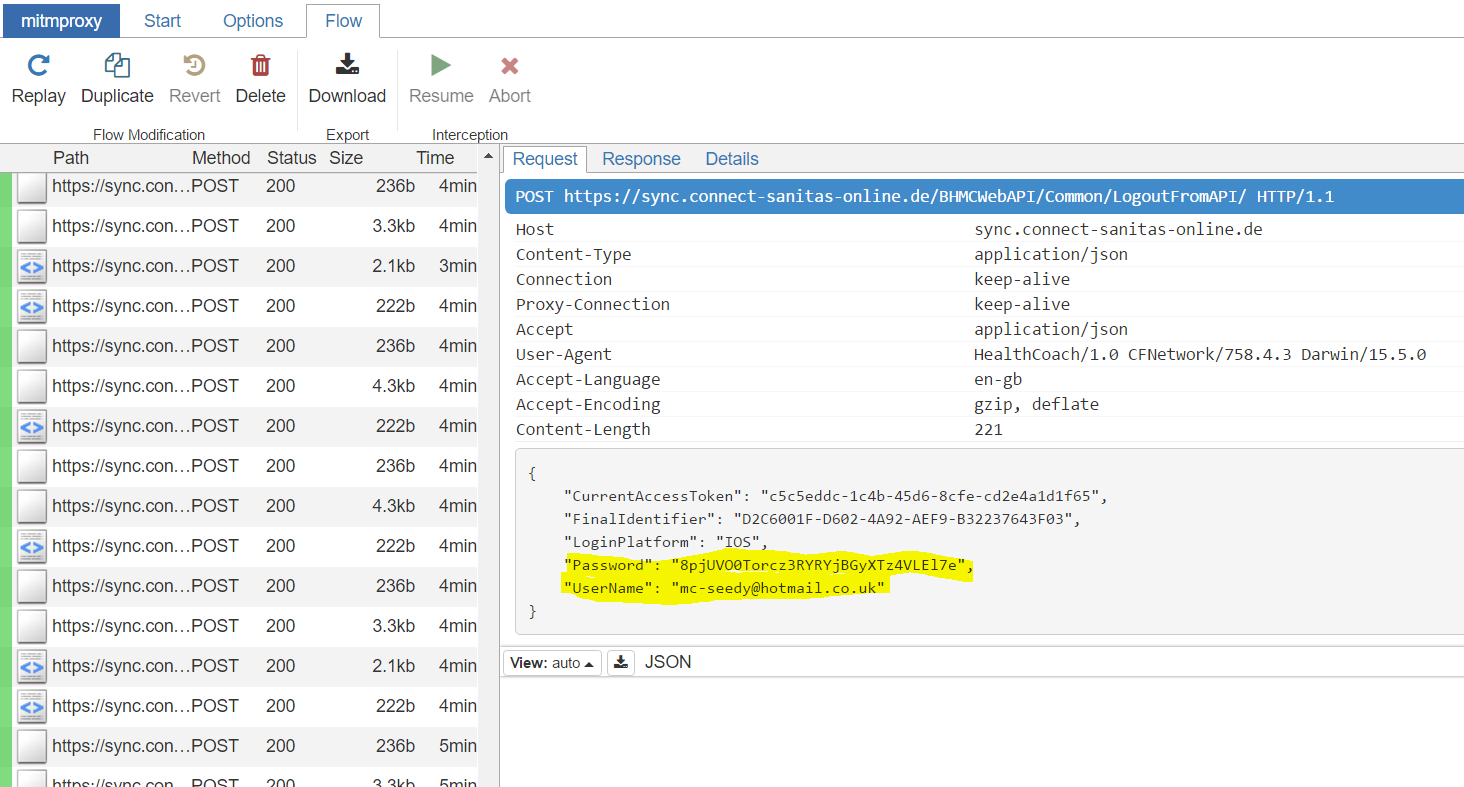


Figure 28 – Smart Scales Cloud Connection

The next stage of the testing involved the analysis of further connection to the cloud interface from the mobile interface, one connection to the cloud interface returned the entire personal profile of the user, information such as medication counters and sleep counters were displayed, furthermore a full database upload was captured which included multiple counts of private information, a full dump of the database upload can be referenced in Appendices 7.3. A summary of the private user information counts can be evidenced in figure 29 below;

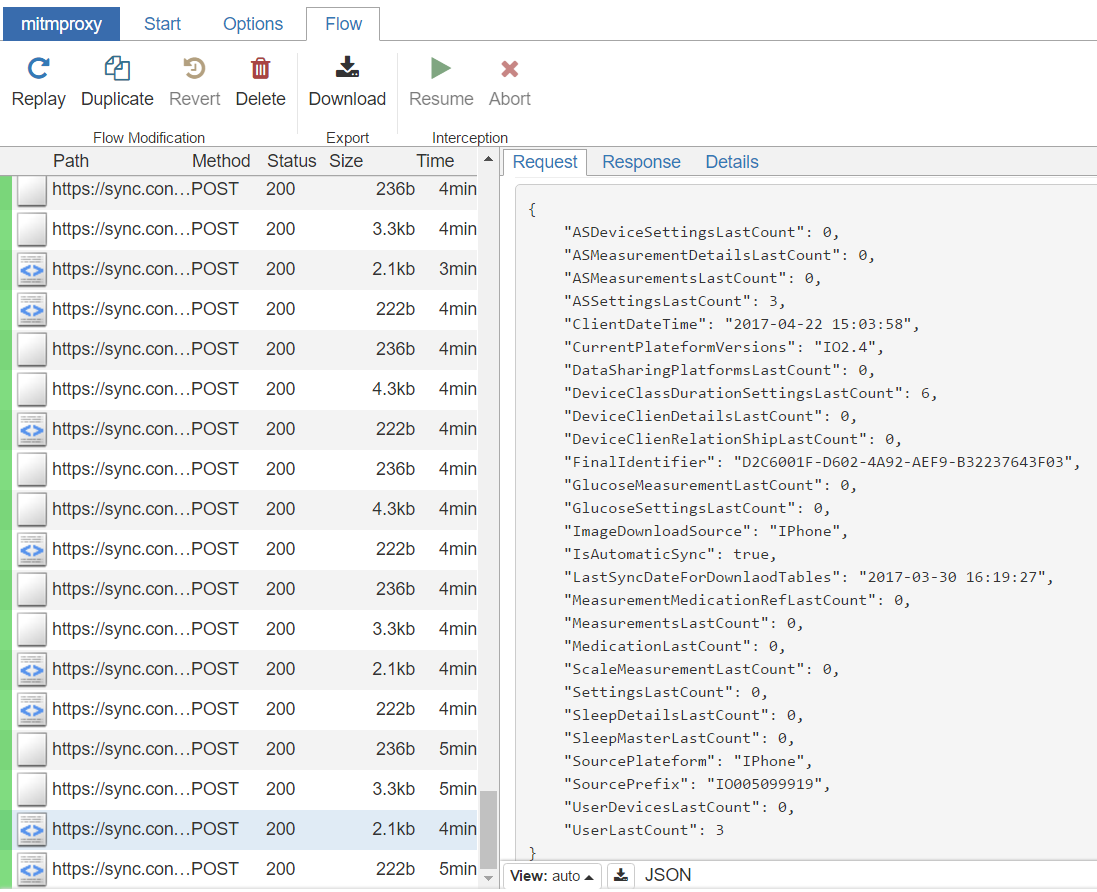


Figure 29 – Smart scales user information count



## Results

Table three bellows depicts the number of vulnerabilities found in each device which was tested in this investigation;

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IOT Device Vulnerability table | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Vulnerabilities --> | Insufficient Authentication / Authorization | Insecure Network Services | Lack of Transport Encryption | Privacy Concerns | Insecure Cloud Interface | Insecure Mobile Interface | Insufficient security configurability | Insecure software/firmware | Poor Physical Security |
| ID No. | Device |  |  |  |  |  |  |  |  |  |
| 1 | IP Camera 1 |  |  |  |  |  |  |  |  |  |
| 2 | IP Camera 2 (With Sound) |  |  |  |  |  |  |  |  |  |
| 3 | Blood pressure Monitor |  |  |  |  |  |  |  |  |  |
| 4 | Smart Power Plug |  |  |  |  |  |  |  |  |  |
| 5 | IP Camera 3 (Baby Monitor) |  |  |  |  |  |  |  |  |  |
| 6 | Bluetooth Scales |  |  |  |  |  |  |  |  |  |

Table 3 – IoT Vulnerability Results Table

Figure 30 below details the number of vulnerabilities grouped by device;

Figure 30 – No. of Vulnerabilities by Device

### IP Security Camera 1

The first IP Security Camera that was tested in this investigation was found to have a total of six vulnerabilities. The vulnerabilities found were;

* Insufficient Authentication / Authorization
* Insecure Network Services
* Privacy Concerns
* Insufficient security configurability
* Insecure software/firmware
* Poor Physical Security

### IP Security Camera 2

The second IP Security Camera that was tested in this investigation was found to have a total of six vulnerabilities. The vulnerabilities found were;

* Insufficient Authentication / Authorization
* Insecure Network Services
* Privacy Concerns
* Insufficient security configurability
* Insecure software/firmware
* Poor Physical Security

### Baby Monitor

The third IP Security camera tested in this investigation which was marketed as a baby monitor contained a total of six vulnerabilities. The vulnerabilities found consisted of;

* Insufficient Authentication / Authorization
* Insecure Network Services
* Lack of Transport Encryption
* Privacy Concerns
* Insufficient security configurability
* Poor Physical Security

### Bluetooth Blood Pressure and Heart Rate Monitor

The Bluetooth Blood pressure and heart rate monitor tested in this investigation was found to have a total of five security vulnerabilities. The vulnerabilities found consisted of;

* Lack of Transport Encryption
* Privacy Concerns
* Insecure Cloud Interface
* Insecure Mobile Interface
* Insufficient security configurability

### Smart Power Plug

The smart power socket testing in this investigation was found to have a total of four existing vulnerabilities. The vulnerabilities found consisted of;

* Insufficient Authentication / Authorization
* Insecure Mobile Interface
* Insufficient security configurability
* Insecure software/firmware

### Bluetooth Weight Scales

The Bluetooth weight scales tested in this investigation had a total of four security related vulnerabilities. The vulnerabilities found consisted of;

* Lack of Transport Encryption
* Privacy Concerns
* Insecure Cloud Interface
* Insufficient security configurability

### Security Concerns Grouped by Vulnerability

Overall there was a total of thirty-one vulnerabilities found when testing all devices in this investigation. Figure 31 below details the number of vulnerabilities found during testing grouped by the type of vulnerability present on devices;

Figure 31 – No. of Security Concerns Grouped by vulnerability

## Discussion

### Case Studies

### Real World Implications

### Countermeasures

## Conclusion

### Future work

## Appendices

### IP Security Camera 1 – ipcam.sh output

# ./ipcam.sh

# Watchdog device not enabled.

zqh socket fd=3

InitSystemParam 0

=========================read system param from file==================================

mac:00:1B:2B:3B:38:89 30

wifimac:00:1B:2B:3B:38:8A 30

wifimac:00:1B:2B:3B:38:8A

bind failuredie param ppid 329

zqh socket fd=3

daemon:===== wifi.c, line 71, WifiConfig(): SSID=Flat 5

daemon:===== wifi.c, line 347, WifiDriversInit(): insmod From kernal

bind failuredie param ppid 336

insmod: cannot insert '/lib/modules/2.6.21/kernel/drivers/net/wireless/rt2860v2\_sta/rt2860v2\_sta.ko': Success

daemon:===== wifi.c, line 355, WifiDriversInit(): [insmod /lib/modules/2.6.21/kernel/drivers/net/wireless/rt2860v2\_sta/rt2860v2\_sta.ko mac=00:1B:2B:3B:38:8A] OK

EthMacInit2

ifconfig: SIOCSIFHWADDR: Device or resource busy

EthMacInit3

EthMacInit4

brctl: bridge br0: File exists

switch reg write offset=14, value=5555

switch reg write offset=40, value=1001

switch reg write offset=44, value=1001

switch reg write offset=48, value=1001

switch reg write offset=4c, value=1

switch reg write offset=50, value=2001

switch reg write offset=70, value=ffffffff

switch reg write offset=98, value=7f7f

switch reg write offset=e4, value=7f

done.

EthMacInit5

EthMacInit5

switch reg write offset=14, value=5555

switch reg write offset=40, value=1001

switch reg write offset=44, value=1001

switch reg write offset=48, value=1001

switch reg write offset=4c, value=1

switch reg write offset=50, value=2001

switch reg write offset=70, value=ffffffff

switch reg write offset=98, value=7f7f

switch reg write offset=e4, value=7f

done.

eth is start

=====InitNetDrivers=======

======dns failed===========:

pid 323

NetThreadProc

Error: Watchdog device not enabled.

netstatsem post

Daemon...=======network change=======

Daemon...netok -1 link 2

net is work on eth

enter ethernet dhcp mode

EthStart1

route: ioctl 0x890c failed: No such process

EthStart2

EthStart3

EthStart4

EthStart5

Error: Watchdog device not enabled.

netstatsem post end

start app update thread

start sys update thread

zqh socket fd=6

bind failured=======mac=======

00-1b-2b-3b-38-89-

ipc param ppid 326

update socket init

update socket is failed

update Socket proc is start

=========================read alarm param=========================(1)

==== sysparam.c , line 530, InitSystemParam :read system.ini

user1: , pwd1:

user2: , pwd2:

user3: admin, pwd3: test

zqh socket fd=3

bind failuredzqh socket fd=3

bind failuredzqh socket fd=3

bind failuredzqh socket fd=3

bind failuredzqh socket fd=3

bind failuredmac:00:1B:2B:3B:38:89 30

wifimac:00:1B:2B:3B:38:8A 30

wifimac:00:1B:2B:3B:38:8A

sys\_ver 1a040087

write date ok

curtime 1492789427

audiofd failed

ie param ppid 415

ie param ppid 415

==== encrypt.c , line 809, CheckAudioChip :iRet=0, rdat=0xfd

==== encrypt.c , line 839, CheckAudioChip :=============Audio Chip Check FAILED!!!!!!!

=======mac=======

00-1b-2b-3b-38-89-

============autio init=========

Ethnet Dhcp

udhcpc (v1.12.1) started

audio capture:421

==== stream.c , line 564, VideoEnable :---VideoEnable(bysize=0)---Initing...

Sending select for 192.168.1.103...

Lease of 192.168.1.103 obtained, lease time 86400

deleting routers

route: ioctl 0x890c failed: No such process

adding dns 192.168.1.254

Unable to set format: Device or resource busy.

init thread ok

capture video:452

Socket proc is start pid=456

send live jpeg:457

send live jpeg:458

send live jpeg:459

send live jpeg:460

send video jpeg:461

send video jpeg:462

send video jpeg:465

send live audio:466

send live audio:467

send live audio:468

send live audio:469

AudioPlayProc:470

send video jpeg:463

send record file:471

=============Error grabbing=-3, nCount = 1

send record file:472

send record file:473

send record file:474

iRet 0 upnp:/system/system/bin/upnpc-static -a 192.168.1.103 81 81 TCP

iRet 0

start gpio check

start motion check

start alarm proc

==== dns.c , line 179, DnsSendAlarmProc :start alarm to DNS server...

web pid:489

init thread ok

========ipaddr 192.168.1.103===========

========port 81===========

FrameRate proc:490

p2p init proc

P2P cmd thread is start...

P2P media thread is start...

P2P play thread is start...

==== moto-new.c , line 5381, InitMoto :Init, alarminhappen = 1

==== moto-new.c , line 1945, ReadVertSteps :Read maxverttime = 160

==== moto-new.c , line 1999, GetVertTime :get vertime 144

==== moto-new.c , line 5604, MotoThreadStart :=========Start, verttime = 144, maxverttime=160======

==== moto-new.c , line 1636, ReadLevelSteps :Read maxleveltime = 516

==== moto-new.c , line 1663, GetLevelTime :get levelime 0

P2P media thread is start...

P2P cmd thread is start...

[ error: /mnt/hgfs/vm\_share-2/svn-down/app-jpg\_V2.0/func/lens\_moto.c, 1468]=> !!! ERROR : GetLensMotoSitStoreInfo !!!

dhcp is start...=0

daemon:===== network.c, line 601, DhcpStart(): Set DNS 1 and 2 to NULL

daemon:===== network.c, line 627, DhcpStart(): 2 = []

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[0] = 1

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[1] = 9

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[2] = 2

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[3] = .

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[4] = 1

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[5] = 6

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[6] = 8

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[7] = .

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[8] = 1

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[9] = .

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[10] = 2

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[11] = 5

daemon:===== network.c, line 632, DhcpStart(): Change DNS2[12] = 4

daemon:===== network.c, line 660, DhcpStart(): 1 = []

daemon:===== network.c, line 661, DhcpStart(): 2 = [192.168.1.254]

run route by zqh

==== network.c , line 3436, Networkhread :Create Thread WfiCheckProc

==== network.c , line 3342, WfiCheckProc :===wifi check status===

==== capture.c , line 370, SetBrightness :size iRet=0, value=1

==== capture.c , line 393, SetContrast :size iRet=0 value=16

sat1

sat2

==== video.c , line 994, VideoParamInit :--------------VideoParamInit----------

set mirr flip=5

==== video.c , line 1122, VideoParamInit :set mirr flip, Param = 5, Saturation = 5

=============Error grabbing=-3, nCount = 2

[Biz\_API.cpp �� 2728 �� ]; pkt\_recvTh start!!

[Biz\_API.cpp �� 2741 �� ]; pkt\_recvTh start sucessfully!!

[Biz\_API.cpp �� 2751 �� ]; sendThread start!!!

[Biz\_API.cpp �� 2764 �� ]; sendThread create success!!!

[Biz\_API.cpp �� 2774 �� ]; timerThread start!!!

[Biz\_API.cpp �� 2787 �� ]; timerThread create success!!!

sat1

sat2

write -1

==== main.c , line 300, main :SystemVerion==================[ 26.4.0.135 ]==============

write -1

==== encrypt.c , line 1188, CheckEncryptProc :start CheckEncryptProc !!!

==== encrypt.c , line 1192, CheckEncryptProc :CheckEncrypt now

==== encrypt.c , line 1197, CheckEncryptProc :CheckEncrypt ok

=============Error grabbing=-3, nCount = 3

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 4

gate way:0.0.0.0 192.168.1.254 0.0.0.0 UG 0 0 0 eth2

======dns failed===========:

--------------SaveSystemParam----------

bparam.stNetParam.szIpAddr = 192.168.1.103

link:2 status:2

=============Error grabbing=-3, nCount = 5

==== dns.c , line 1203, FactoryRegisterProc :Start FactoryRegisterProc

========version:1010907===========

========DeviceID:MEYE-158538-EEBCB=========

=============Error grabbing=-3, nCount = 6

==== moto-new.c , line 5498, MotoCentProc :=====moto is start=====

==== moto-new.c , line 5499, MotoCentProc :moto start, read moto sit

==== moto-new.c , line 5500, MotoCentProc :presend = 0, speed = 5

==== moto-new.c , line 5507, MotoCentProc :Set Moto to Center-----

==== moto-new.c , line 4557, SendMotoCmd :Motocmd=0

start run ddns

write date ok

=============Error grabbing=-3, nCount = 7

=============Error grabbing=-3, nCount = 8

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 9

=============Error grabbing=-3, nCount = 10

def key proc

=============Error grabbing=-3, nCount = 11

externwifistatus=0

=============Error grabbing=-3, nCount = 12

=============Error grabbing=-3, nCount = 13

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 14

iRet 0

bFlagInternet 1

bFlagHostResolved 1

bFlagServerHello 1

NAT\_Type 2

PPPP\_Share\_Bandwidth(1) iRet 0

P2P init =1

=============Error grabbing=-3, nCount = 15

=============Error grabbing=-3, nCount = 16

=============Error grabbing=-3, nCount = 17

=============Error grabbing=-3, nCount = 18

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 19

=============Error grabbing=-3, nCount = 20

==== moto-new.c , line 3633, MotoCenter :------verttime = 0

=============Error grabbing=-3, nCount = 21

=============Error grabbing=-3, nCount = 22

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 23

=============Error grabbing=-3, nCount = 24

==== moto-new.c , line 3669, MotoCenter :==========Will Center, verttime = 160

dircnt 64 verttime 160

=============Error grabbing=-3, nCount = 25

=============Error grabbing=-3, nCount = 26

===onstart===1

=============Error grabbing=-3, nCount = 27

on start = 0

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 28

=============Error grabbing=-3, nCount = 29

=============Error grabbing=-3, nCount = 30

=============Error grabbing=-3, nCount = 31

=============Error grabbing=-3, nCount = 32

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 33

=============Error grabbing=-3, nCount = 34

=============Error grabbing=-3, nCount = 35

=============Error grabbing=-3, nCount = 36

=============Error grabbing=-3, nCount = 37

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 38

=============Error grabbing=-3, nCount = 39

=============Error grabbing=-3, nCount = 40

=============Error grabbing=-3, nCount = 41

=============Error grabbing=-3, nCount = 42

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 43

=============Error grabbing=-3, nCount = 44

=============Error grabbing=-3, nCount = 45

=============Error grabbing=-3, nCount = 46

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 47

=============Error grabbing=-3, nCount = 48

=============Error grabbing=-3, nCount = 49

=============Error grabbing=-3, nCount = 50

=============Error grabbing=-3, nCount = 51

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 52

=============Error grabbing=-3, nCount = 53

=============Error grabbing=-3, nCount = 54

=============Error grabbing=-3, nCount = 55

=============Error grabbing=-3, nCount = 56

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 57

Connection closed by foreign host.

root@kali:~#

### IP Security Camera 2 - ipcam.sh output

# ./ipcam.sh

# Watchdog device not enabled.

InitSystemParam 0

=========================read system param from file==================================

mac:00:6E:06:40:1B:D9 30

wifimac:00:6E:06:40:1B:DA 30

wifimac:00:6E:06:40:1B:DA

zqh socket fd=3

zqh socket fd=3

bind failuredie param ppid 302

bind failuredie param ppid 300

daemon:===== wifi.c, line 311, WifiDriversInit(): insmod From kernal

insmod: cannot insert '/lib/modules/2.6.21/kernel/drivers/net/wireless/rt2860v2\_sta/rt2860v2\_sta.ko': Success

daemon:===== wifi.c, line 316, WifiDriversInit(): [insmod /lib/modules/2.6.21/kernel/drivers/net/wireless/rt2860v2\_sta/rt2860v2\_sta.ko mac=00:6E:06:40:1B:DA] OK

EthMacInit2

ifconfig: SIOCSIFHWADDR: Device or resource busy

EthMacInit3

EthMacInit4

brctl: bridge br0: File exists

switch reg write offset=14, value=5555

switch reg write offset=40, value=1001

switch reg write offset=44, value=1001

switch reg write offset=48, value=1001

switch reg write offset=4c, value=1

switch reg write offset=50, value=2001

switch reg write offset=70, value=ffffffff

switch reg write offset=98, value=7f7f

switch reg write offset=e4, value=7f

done.

EthMacInit5

EthMacInit5

switch reg write offset=14, value=5555

switch reg write offset=40, value=1001

switch reg write offset=44, value=1001

switch reg write offset=48, value=1001

switch reg write offset=4c, value=1

switch reg write offset=50, value=2001

switch reg write offset=70, value=ffffffff

switch reg write offset=98, value=7f7f

switch reg write offset=e4, value=7f

done.

eth is start

=====InitNetDrivers=======

daemon:===== network.c, line 383, DnsConfig(): Save to File, 1 = [8.8.8.8]

daemon:===== network.c, line 384, DnsConfig(): Save to File, 2 = [192.168.1.254]

pid 289

NetThreadProc

Error: Watchdog device not enabled.

netstatsem post

=======network change=======

netok -1 link 2

net is work on eth

enter ethernet dhcp mode

EthStart1

route: ioctl 0x890c failed: No such process

EthStart2

EthStart3

EthStart4

route: ioctl 0x890b failed: File exists

EthStart5

Error: Watchdog device not enabled.

netstatsem post end

start app update thread

zqh socket fd=6

bind failuredstart sys update thread

=======mac=======

00-6e-06-40-1b-d9-

ipc param ppid 295

update socket init

update socket is failed

update Socket proc is start

==== sysparam.c , line 308, InitSystemParam :read system.ini

user1: , pwd1:

user2: , pwd2:

user3: admin, pwd3: test

zqh socket fd=3

bind failuredzqh socket fd=3

bind failuredzqh socket fd=3

bind failuredzqh socket fd=3

bind failuredzqh socket fd=3

bind failuredmac:00:6E:06:40:1B:D9 30

wifimac:00:6E:06:40:1B:DA 30

wifimac:00:6E:06:40:1B:DA

sys\_ver 5102008c

write date ok

curtime 1492793149

audiofd failed

ie param ppid 379

ie param ppid 379

WRITE I2C : Write Error - TX Data==== encrypt.c , line 472, CheckEncrypt :==========encrypt is error===========

fp == null

WRITE I2C : Write Error - Sub Addrwrite i2c not ack

==== encrypt.c , line 1122, CheckChipOk :es8388 isn't exist...

audio capture:383

=======mac=======

00-6e-06-40-1b-d9-

============autio init=========

audio play:384

==== stream.c , line 368, VideoEnable :---VideoEnable(bysize=0)---Initing...

Ethnet Dhcp

udhcpc (v1.12.1) started

Unable to set format: Device or resource busy.

init thread ok

capture video:397

Socket proc is start pid=401

=============Error grabbing=-3, nCount = 1

send live jpeg:406

send live jpeg:407

send live jpeg:408

send live jpeg:409

send video jpeg:410

send video jpeg:411

send video jpeg:412

send video jpeg:413

send live audio:414

send live audio:415

send live audio:416

send live audio:417

AudioPlayProc:418

send record file:419

send record file:420

send record file:421

send record file:422

Sending select for 192.168.1.216...

Lease of 192.168.1.216 obtained, lease time 86400

iRet 0 upnp:/system/system/bin/upnpc-static -a 192.168.1.216 14987 14987 TCP

iRet 0

start gpio check

start motion check

start alarm proc

==== dns.c , line 107, DnsSendAlarmProc :start alarm to DNS server...

init thread ok

web pid:442

========ipaddr 192.168.1.216===========

========port 14987===========

FrameRate proc:443

p2p init proc

P2P cmd thread is start...

P2P media thread is start...

==== moto-new.c , line 4418, InitMoto :Init, alarminhappen = 0

==== moto-new.c , line 1318, ReadVertSteps :Read maxverttime = 140

==== moto-new.c , line 1372, GetVertTime :get vertime 56

==== moto-new.c , line 1026, ReadLevelSteps :Read maxleveltime = 510

==== moto-new.c , line 1053, GetLevelTime :get levelime 268

P2P play thread is start...

P2P media thread is start...

P2P cmd thread is start...

deleting routers

route: ioctl 0x890c failed: No such process

==== network.c , line 2897, Networkhread :Create Thread WfiCheckProc

==== capture.c , line 366, SetBrightness :size iRet=0, value=1

==== video.c , line 664, VideoParamInit :--------------VideoParamInit----------

set mirr flip=5

==== video.c , line 717, VideoParamInit :set mirr flip, Param = 5, Saturation = 5

=============Error grabbing=-3, nCount = 2

==== network.c , line 2832, WfiCheckProc :===wifi check status===

adding dns 192.168.1.254

write -1

=============Error grabbing=-3, nCount = 3

dhcp is start...=0

daemon:===== network.c, line 488, DhcpStart(): Set DNS 1 and 2 to NULL

daemon:===== network.c, line 514, DhcpStart(): 2 = []

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[0] = 1

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[1] = 9

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[2] = 2

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[3] = .

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[4] = 1

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[5] = 6

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[6] = 8

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[7] = .

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[8] = 1

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[9] = .

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[10] = 2

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[11] = 5

daemon:===== network.c, line 519, DhcpStart(): Change DNS2[12] = 4

daemon:===== network.c, line 547, DhcpStart(): 1 = []

daemon:===== network.c, line 548, DhcpStart(): 2 = [192.168.1.254]

run route by zqh

==== main.c , line 441, main :SystemVerion==================[ 81.2.0.140 ]==============

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 4

=============Error grabbing=-3, nCount = 5

=============Error grabbing=-3, nCount = 6

gate way:0.0.0.0 192.168.1.254 0.0.0.0 UG 0 0 0 eth2

daemon:===== network.c, line 383, DnsConfig(): Save to File, 1 = [8.8.8.8]

daemon:===== network.c, line 384, DnsConfig(): Save to File, 2 = [192.168.1.254]

--------------SaveSystemParam----------

bparam.stNetParam.szIpAddr = 192.168.1.216

link:2 status:2

==== dns.c , line 694, FactoryRegisterProc :FactoryRegisterProc

========version:20804===========

==== moto-new.c , line 4438, MotoCentProc :=====moto is start=====

==== moto-new.c , line 4439, MotoCentProc :moto start, read moto sit

==== moto-new.c , line 4440, MotoCentProc :presend = 0, speed = 5

==== moto-new.c , line 4447, MotoCentProc :Set Moto to Center-----

==== moto-new.c , line 3611, SendMotoCmd :Motocmd=0

=============Error grabbing=-3, nCount = 7

start run ddns

iRet 0

bFlagInternet 1

bFlagHostResolved 1

bFlagServerHello 1

NAT\_Type 0

PPPP\_Share\_Bandwidth(1) iRet 0

P2P init =1

=============Error grabbing=-3, nCount = 8

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 9

=============Error grabbing=-3, nCount = 10

=============Error grabbing=-3, nCount = 11

def key proc

check wifi

=============Error grabbing=-3, nCount = 12

=============Error grabbing=-3, nCount = 13

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 14

=============Error grabbing=-3, nCount = 15

=============Error grabbing=-3, nCount = 16

=============Error grabbing=-3, nCount = 17

=============Error grabbing=-3, nCount = 18

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 19

=============Error grabbing=-3, nCount = 20

=============Error grabbing=-3, nCount = 21

=============Error grabbing=-3, nCount = 22

=============Error grabbing=-3, nCount = 23

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 24

=============Error grabbing=-3, nCount = 25

=============Error grabbing=-3, nCount = 26

=============Error grabbing=-3, nCount = 27

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 28

=============Error grabbing=-3, nCount = 29

==== date.c , line 141, NtpThreadProc :Call GetNtpTime

==== date.c , line 90, GetNtpTime :bparam.stDTimeParam.byIsNTPServer = 1

==== date.c , line 91, GetNtpTime :bparam.stDTimeParam.szNtpSvr = time.nist.gov

==== date.c , line 96, GetNtpTime :start connect timer server...=time.nist.gov

=============Error grabbing=-3, nCount = 30

=============Error grabbing=-3, nCount = 31

=============Error grabbing=-3, nCount = 32

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 33

=============Error grabbing=-3, nCount = 34

=============Error grabbing=-3, nCount = 35

=============Error grabbing=-3, nCount = 36

=============Error grabbing=-3, nCount = 37

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 38

dircnt 56 verttime 140

=============Error grabbing=-3, nCount = 39

=============Error grabbing=-3, nCount = 40

===onstart===1

=============Error grabbing=-3, nCount = 41

on start = 0

=============Error grabbing=-3, nCount = 42

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 43

=============Error grabbing=-3, nCount = 44

=============Error grabbing=-3, nCount = 45

=============Error grabbing=-3, nCount = 46

=============Error grabbing=-3, nCount = 47

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 48

=============Error grabbing=-3, nCount = 49

=============Error grabbing=-3, nCount = 50

=============Error grabbing=-3, nCount = 51

=============Error grabbing=-3, nCount = 52

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 53

=============Error grabbing=-3, nCount = 54

=============Error grabbing=-3, nCount = 55

=============Error grabbing=-3, nCount = 56

Error: Watchdog device not enabled.

=============Error grabbing=-3, nCount = 57

Connection closed by foreign host.

root@kali:~#

### Smart Scale Database Dump

"ClientDateTime": "2017-04-22 15:10:20",

"DestinationPlateform": "Cloud",

"FinalIdentifier": "D2C6001F-D602-4A92-AEF9-B32237643F03",

"IsAutomaticSync": 0,

"SourcePlateform": "IPhone",

"SourcePrefix": "IO005099919",

"jsonDataRecordsList": [

{

"RecordData": "{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserId\":1,\"Revision\":0,\"CreatedDate\":\"2017-03-30 17:27:08\",\"lastRecordOfHistoryTable\":0,\"GlobalTime\":\"2017-03-30 16:27:08\",\"SharingPlatform\":\"HealthKit\",\"PermissionType\":\"Write\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",

"TableName": "DataSharingPlatforms"

},

{

"RecordData": "{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserId\":1,\"Revision\":1,\"CreatedDate\":\"2017-03-30 17:27:08\",\"UpdatedDate\":\"2017-04-15 21:49:18\",\"GlobalTime\":\"2017-04-15 20:49:18\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Write\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",

"TableName": "DataSharingPlatforms"

},

{

"RecordData": "{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserId\":1,\"Revision\":2,\"CreatedDate\":\"2017-03-30 17:27:08\",\"UpdatedDate\":\"2017-04-22 15:55:10\",\"GlobalTime\":\"2017-04-22 14:55:10\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Write\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",

"TableName": "DataSharingPlatforms"

},

{

"RecordData": "{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserId\":1,\"Revision\":3,\"CreatedDate\":\"2017-03-30 17:27:08\",\"UpdatedDate\":\"2017-04-22 15:59:23\",\"GlobalTime\":\"2017-04-22 14:59:23\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Write\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",

"TableName": "DataSharingPlatforms"

},

{

"RecordData": "{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserId\":1,\"Revision\":4,\"CreatedDate\":\"2017-03-30 17:27:08\",\"UpdatedDate\":\"2017-04-22 15:59:29\",\"GlobalTime\":\"2017-04-22 14:59:29\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Write\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",

"TableName": "DataSharingPlatforms"

},

{

"RecordData": "{\"globalTime\":\"2017-04-22 14:59:58\",\"Revision\":1,\"Source\":\"WE149106703GSS000002\",\"UpdatedDate\":\"2017-04-22 15:59:58\",\"UserId\":1,\"TargetEndValue\_mgdl\":160,\"CreatedDate\":\"2017-03-30 18:18:49\",\"GlucoseSettingId\":1,\"UpdatedSource\":\"IO005099919GSS000002\",\"TargetStartValue\_mgdl\":110,\"TargetEndValue\_mmol\":8.8,\"TargetStartValue\_mmol\":6,\"RevisionCount\":0,\"IsDeleted\":false,\"IsNewRecord\":false,\"DisplayUnit\":\"mg\_dL\"}",

"TableName": "GlucoseSettings"

},

{

"RecordData": "{\"globalTime\":\"2017-04-22 15:00:21\",\"Revision\":2,\"Source\":\"WE149106703GSS000002\",\"UpdatedDate\":\"2017-04-22 16:00:21\",\"UserId\":1,\"TargetEndValue\_mgdl\":160,\"CreatedDate\":\"2017-03-30 18:18:49\",\"GlucoseSettingId\":1,\"UpdatedSource\":\"IO005099919GSS000002\",\"TargetStartValue\_mgdl\":110,\"TargetEndValue\_mmol\":8.8,\"TargetStartValue\_mmol\":6,\"RevisionCount\":0,\"IsDeleted\":false,\"IsNewRecord\":false,\"DisplayUnit\":\"mg\_dL\"}",

"TableName": "GlucoseSettings"

},

{

"RecordData": "{\"Id\":1,\"Source\":\"IO005099919DSP000001\",\"FieldName\":\"\",\"UserId\":1,\"Revision\":5,\"CreatedDate\":\"2017-03-30 17:27:08\",\"UpdatedDate\":\"2017-04-22 16:08:33\",\"GlobalTime\":\"2017-04-22 15:08:33\",\"SharingPlatform\":\"HealthKit\",\"lastRecordOfHistoryTable\":0,\"UpdatedSource\":\"IO005099919DSP000001\",\"PermissionType\":\"Write\",\"IsAgreedToConnect\":false,\"IsDeleted\":false}",

"TableName": "DataSharingPlatforms"

},

{

"RecordData": "{\"AdvPackagesTimeInterval\":0,\"ActivityGrade\":0,\"pairingBit\":false,\"createUserStatus\":0,\"batteryLevel\":100,\"TXPower\":0,\"UserDetactionLimits\":2,\"UDID\":\"8633A31A-CDCB-E750-FB1B-36FE400F426F\",\"GlobalTime\":\"2017-04-22 15:10:19\",\"UserOnDevice\":0,\"pairingCompleted\":false,\"optionalDeviceName\":\"test \",\"Source\":\"IO005099919DCR000001\",\"firmwareVersion\":5,\"IsNewRecord\":true,\"RSSI\":-56,\"CreatedDate\":\"2017-03-30 17:20:40\",\"isTrusted\":true,\"UpdatedSource\":\"IO005099919DCR000001\",\"DeviceUnit\":1,\"PowerSavingMode\":false,\"ID\":1,\"DeviceId\":4,\"inRange\":false,\"IsDeleted\":false,\"scaleVersion\":5,\"deviceName\":\"SANITAS SBF70\",\"NoOfUsers\":1,\"UserId\":1,\"userExists\":false,\"measurementExists\":false,\"UpdatedDate\":\"2017-04-22 16:10:19\",\"unknownMeasurementsCount\":0,\"Revision\":29}",

"TableName": "DeviceClientRelationship"

}

]

}

View: auto JSON

## List of References

[1] [6] [7] Office for National Statistics, “Internet access – households and individuals: 2016” (4/8/2016) [Online] Available at: <https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016> [Accessed March 2017].

[2] Klaus, Schwab, “The Fourth Industrial Revolution: what it means, how to respond” (14/1/2016) [Online] Available at: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/> [Accessed October 2016].

[3] Oxford Dictionary, “Internet of Things” [Online] Available at:

<https://en.oxforddictionaries.com/definition/internet\_of\_things>

[Accessed September 2016].

[4] Deoras, Srishti, “First ever IoT device- “The Internet Toaster”” (5/8/2016) [Online] Available at: <http://iotindiamag.com/2016/08/first-ever-iot-device-the-internet-toaster/> [Accessed February 2017].

[5] Ashton, Kevin, “That 'Internet of Things' Thing”” (22/6/2009) [Online] Available at: <http://www.rfidjournal.com/articles/view?4986 > [Accessed March 2017].

[8] Deloitte Statistics, “The Internet of Things (IoT): most entertaining” (2016) [Online] Available at: <https://www.deloitte.co.uk/mobileuk/internet-of-things/> [Accessed March 2017].

[9] Rouse, Margaret, “Whatis.com - pen test (penetration testing)” [Online] Available at: <https://www.deloitte.co.uk/mobileuk/internet-of-things/> [Accessed March 2017].

[10] NCC Group, “Internet of Things (IoT)” (2016) [Online] Available at: <https://www.nccgroup.trust/uk/our-solutions/your-sectors/internet-of-things/> [Accessed November 2016].

[11] Greenough, John, “The 'Internet of Things' Will Be the World's Most Massive Device Market and Save Companies Billions of Dollars” (18/11/2014) [Online] Available at:

<http://uk.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10?r=US&IR=T>[Accessed October 2016].

[12] Gartner Inc., “Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015” (11/11/2014) [Online] Available at:

<https://www.gartner.com/newsroom/id/2905717>

[Accessed September 2016].

[13][16] SpiceWorks IT, “2016 IoT Tends: The Devices have Landed, How IT and IoT are learning to peacefully coexist” (2016) [Online] Available at:

<https://www.spiceworks.com/marketing/reports/iot-trends/#section-0>

[Accessed October 2016].

[14] Klahr, R., Shah, J., Sheriffs, P., Rossington, T., Pestell, G., Button, M. and Wang, V. Cyber security breaches survey 2017 Main report (2017). [Online] Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/609186/Cyber\_Security\_Breaches\_Survey\_2017\_main\_report\_PUBLIC.pdf> [Accessed 15 Apr. 2017].

[15] Sadeghi, A., Wachsmann, C. and Waidner, M. (2015). Security and Privacy Challenges in Industrial Internet of Things. [Online] Available at: <http://ieeexplore.ieee.org/document/7167238/> [Accessed 20 February 2017].

[17] Borgohain, T., Kumar, U. and Sanyal, S. (2015). Survey of Security and Privacy Issues of Internet of Things. [Online] Available at: <https://www.researchgate.net/publication/270763270\_Survey\_of\_Security\_and\_Privacy\_Issues\_of\_Internet\_of\_Things> [Accessed 10 Feb. 2017].

[18] Yousuf, T., Mahmoud, R. and Imran Zualkernan, F. (2015). nternet of Things (IoT) Security: Current Status, Challenges and Countermeasures. [Online] Available at: <https://www.researchgate.net/publication/300413927\_Internet\_of\_things\_IoT\_security\_Current\_status\_challenges\_and\_prospective\_measures> [Accessed 10 Feb. 2017].

[19] Farooq, M., Waseem, M., Khairi, A. and Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). [Online] Available at: <https://www.researchgate.net/publication/272488555\_A\_Critical\_Analysis\_on\_the\_Security\_Concerns\_of\_Internet\_of\_Things\_IoT> [Accessed 10 Feb. 2017].

[20] Abomhara, M. and Køien, G. (2015). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. [Online] Available at: <https://s3.amazonaws.com/academia.edu.documents/39628024/Cyber\_Security\_and\_the\_Internet\_of\_Thing20151102-5470-rumluk.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1492727999&Signature=08kKMpmV6nyHIlyIfyWikevYyqQ%3D&response-content-disposition=inline%3B%20filename%3DCyber\_Security\_and\_the\_Internet\_of\_Thing.pdf> [Accessed 10 Feb. 2017].

[21] Nawir, M., Amir, A., Yaakob, N. and Lynn, O. (2017). Internet of Things (IoT): Taxonomy of security attacks - IEEE Xplore Document. [online] Available at: <http://ieeexplore.ieee.org/document/7804660/> [Accessed 20 Feb. 2017].

[22] Mirkovic, J., Prier, G. and Reiher, P. (2003). Attacking DDoS at the source - IEEE Xplore Document. [Online] Available at: <http://ieeexplore.ieee.org/abstract/document/1181418/> [Accessed 10 Feb. 2017].

[23] Rajab, M., Zarfoss, J., Monrose, F. and Terzis, A. (2007). My Botnet is Bigger than Yours (Maybe, Better than Yours. [Online] Available at: <https://www.usenix.org/legacy/event/hotbots07/tech/full\_papers/rajab/rajab.pdf> [Accessed 10 Nov. 2016].

[24] Newman, L. (2016). The Botnet That Broke The Internet. [Online] Wired.com. Available at: <https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/> [Accessed 3 Nov. 2016].

[25] Angrishi, K. (2017). Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets. [Online] Available at: <https://arxiv.org/pdf/1702.03681.pdf> [Accessed 20 Mar. 2017].

[26] Cox, E. (2016). Mirai IoT Botnet: 5 Fast Facts You Need to Know. [Online] Available at: <http://heavy.com/tech/2016/10/mirai-iot-botnet-internet-of-things-ddos-attacks-internet-outage-blackout-why-is-internet-down/> [Accessed 3 Nov. 2016].

[27] OWASP Internet of Things Project Top Ten (10/9/2016) [Online], Available at:

<https://www.owasp.org/index.php/OWASP\_Internet\_of\_Things\_Top\_Ten\_Project>

[Accessed September 2016].

[28] Nmap Tool [Online] Available at:

<https://nmap.org/> [Accessed September 2016]

# Bibliography

If required