

BUILDING A SECURE HOME NETWORK

by

Dale Scott Griffiths

Supervisor: Carlene Campbell

Project submitted as part of the requirements
for the award of BSc (Hons) Computer Networks

April 2018

Declaration of Originality

I, Dale Scott Griffiths declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed :

Date :

FORM OF CONSENT

I Dale Scott Griffiths hereby consent that my Project, submitted in candidature for the B.Sc.(Hons) Computer Networks degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed :

Date :

Copyright Acknowledgement

I acknowledge that the copyright of this project report, and any product developed as part of the project, belong to University of Wales Trinity Saint David, Swansea.

ABSTRACT/SYNOPSIS

This project is based on building a secure home network, this will be completed in two parts. The first section of the document will be used to cover the research and literature review. This will provide the author with the appropriate background knowledge that will be required to continue with the project. The second part of the project will include creating a methodology, this will then guide the author through the design and implementation and testing and evaluation sections of the project.

The design and implementation section will be used to create a network design that will allow the author to conduct the experiment's that will be selected from chapter two research. The design will then be implemented, and documentation of the implementation added to chapter four of the report. This will enable the author to continue to the testing and evaluation section of the project. This section will be where the experiments are conducted, and the evaluation will be written up.

TABLE OF CONTENTS

CHAPTER 1

1.1	Introduction	8
1.2	Aim	8
1.3	Objectives	9
1.4	Structure of The Project.....	9

CHAPTER 2 – RESEARCH & REVIEW OF LITERATURE

2.1	Introduction	11
2.2	Network Overview.....	11
2.3	Network Devices.....	12
2.4	Network Threats.....	14
2.4.1	Browser Attack.....	14
2.4.2	Denial of Service Attack	17
2.4.3	Brute Force Attack.....	19
2.4.4	Malware	21
2.5	Network Security	22
2.5.1	Physical Security	22
2.5.2	Virtual Private Network	22
2.5.3	Firewalls	22
2.6	Related Work	22
2.6.1	WPA2 password crack	23
2.6.2	Network Scan Attack	23
2.7	Conclusion	24

CHAPTER 3 – RESEARCH METHODOLOGY

3.1	Introduction	25
3.2	Research Overview	25
3.2.1	Research Process	26
3.2.2	Research Philosophy	26
3.2.3	Research Approaches	26
3.2.4	Research Strategies	26
3.2.5	Time Horizons	27
3.2.6	Data Collection.....	27
3.3	Research Design	29

3.3.1	Research Deliverables	29
3.4	Triangulation	29
3.5	Conclusion.....	29
CHAPTER 4 – DESIGN & IMPLIMENTATION		
4.1	Introduction	31
4.2	Problem Formulation	31
4.3	Design.....	32
4.4	Implementation.....	34
4.4.1	Router Setup.....	35
4.4.2	Connecting Devices.....	37
4.4.3	Software Installation.....	38
4.5	Conclusion.....	39
CHAPTER 5 – TESTING & EVALUATION		
5.1	Introduction.....	40
5.2	WPA2 Password Cracking.....	40
5.2.1	Simple Password.....	40
5.2.2	Complex Password.....	47
5.2.3	Conclusion	52
5.3	Man-in-the-middle attack	54
5.3.1	Conclusion	58
5.4	Port scanning	59
5.4.1	Conclusion	63
5.5	Conclusion.....	64
CHAPTER 6 – CONCLUSIONS AND RECOMMENDATIONS		
6.1	Summary.....	65
6.2	Conclusion.....	65
6.3	Recommendations for Future Research	66
CHAPTER 7 – REFLECTIONS		
7.1	Introduction	67
7.2	Positives	67
7.3	Negatives	67
7.4	Objectives.....	68
7.5	Conclusion.....	69

LIST OF FIGURES

Figure 1 – Browser Attack [5]	15
Figure 2 – Denial of Service Attack [9]	17
Figure 3 – Brute Force Attack [13].....	19
Figure 4 – Malware [16].....	21
Figure 5 – Research Onion [18]	25
Figure 6 – Network Blueprint	34
Figure 7 – Router Setup (1).....	35
Figure 8 – Router Setup (2).....	35
Figure 9 - Router Setup (3).....	36
Figure 10 - Router Setup (4).....	36
Figure 11 - Router Setup (5).....	37
Figure 12 – Connecting the devices (1).....	37
Figure 13 – Connecting the devices (2).....	38
Figure 14 - Connecting the devices (3)	38
Figure 15 – Kali Linux [19].....	39
Figure 16 – WPA2 simple password (1)	41
Figure 17 - WPA2 simple password (2).....	41
Figure 18 - WPA2 simple password (3).....	42
Figure 19 - WPA2 simple password (4).....	43
Figure 20 - WPA2 simple password (5).....	44
Figure 21 - WPA2 simple password (6).....	45
Figure 22 - WPA2 simple password (7).....	46
Figure 23 - WPA2 complex password (1).....	47
Figure 24 - WPA2 complex password (2)	48
Figure 25 – WPA2 complex password (3)	49

Figure 26 - WPA2 complex password (4)	50
Figure 27 - WPA2 complex password (5)	51
Figure 28 - WPA2 complex password (6)	52
Figure 29 – Man-in-the-middle attack (1)	54
Figure 30 - Man-in-the-middle attack (2)	55
Figure 31 – Man-in-the-middle attack (3)	55
Figure 32 - Man-in-the-middle attack (4)	56
Figure 33 - Man-in-the-middle attack (5)	56
Figure 34 - Man-in-the-middle attack (6)	57
Figure 35 - Man-in-the-middle attack (7)	57
Figure 36 - Man-in-the-middle attack (8)	58
Figure 37 – Port scanning (1)	59
Figure 38 – Port scanning (2)	60
Figure 39 - Port scanning (3)	60
Figure 40 – Port scanning (4)	61
Figure 41 – Port scanning (5)	61
Figure 42 – Port scanning (6)	62

LIST OF TABLES

Table 1 – Data Collection Methods 28

Table 2 – Devices in network design 33

Table 3 – Port scanning 63

Chapter 1

1.1 Introduction

This chapter will be used to demonstrate background knowledge of the authors project building a secure home network. The second section of this chapter will describe the research aims that will be used to build a solution for the scenario. The third section of this chapter will be used to describe the objectives of the project. The final section of this chapter will cover the structure of the report.

This project is based upon building a secure home network. This is essentially a network that can help protect its users and data from certain attacks/threats. A network will never be 100% safe. As new threats are introduced all the time, it would be impossible to say that any network is totally secure. This project may be about creating a secure home network however, it will not defend against every attack/threat possible. There will be variety of different threats/attacks that will be selected to defend against.

The author will be using a mixture of different types of papers, articles and books to provide the research information for this project. Firstly, survey papers will be used as this will allow the author to learn about tools, threats and measures that can be used to secure the network. The author will then read technical papers, these will cover previous experiment's that have been done. This will then give the author an idea of how the experiment for the project can be undertaken. The author will additionally use articles and books to learn more details about the different tools, threats and measures learned in the survey papers.

1.2 Aim

The main aim of this project is to build a home network that can be used to conduct experiments to find the vulnerabilities and provide solutions to secure the network.

1.3 Objectives

The objectives of this project are to look at what different attacks/threats and vulnerabilities there are and how to defend against them.

- Research different devices that are in home networks
- Research threats/vulnerabilities
- Research solutions for the identified threats
- Design and implement a home network
- Conduct the experiment by completing the attacks

1.4 Structure of The Project

The structure of this report is broken up into two sections. The first section of the report is a review of literature. This will be conducted on the project title building a secure home network. This will cover what is a home network and what devices are most commonly used within this type of network. It will also cover different types of threats and vulnerabilities within a network. This will then allow the author to continue into the second section of this report. This will be to carry out the experiments (attacks) to see the weaknesses of the home network. This will then allow the author to document the attacks. This will additionally allow for the author to investigate ways of securing the network from the attacks. The experiment's will then be compared to the literature review to see if the outcome was successful. The author will document all attacks and solutions to share their knowledge with others.

Chapter one

This chapter is used to give an overview of the report. It is used to show the aims, objectives and structure of the project. Once the project is completed the author can see if they have achieved the aims and objectives of the report. This will then demonstrate if the project was successful.

Chapter two

This chapter is used to cover the research needed to complete the project. The author will look at devices, network security and threats. This will allow the author to have the background information required to continue with the project.

Chapter three

This chapter is used to cover the research on the methodology. This will be used to complete the process, philosophy and methodology required to complete the project.

Chapter four

This chapter is used to cover the design and implementation. The design section will be used to document the design of the home network that will be used for the project. The implementation section will be used to ensure the network is built to the design specifications.

Chapter five

This chapter is used to cover the testing and evaluation. The testing section will be used to conduct the attacks. The evaluation section will be used to evaluate the results from the experiments. These will then be compared to aims, objectives and research to ensure the requirements are met.

Chapter six

This chapter is used to conclude the project. It will use information from previous chapters to conclude on if the project was successful. It will look at the aims and objectives of the project and if they have been completed it should demonstrate that the project was successful.

Chapter 2 - RESEARCH & REVIEW OF LITERATURE

2.1 Introduction

This chapter will be used to complete the research that is required to conduct the project. The first section of this chapter will be a network overview, this will contain general information gathered on home networks. The next section of this chapter will cover network devices, this will contain information on what devices are connected to home networks. The next section of this chapter will contain information on threats, this will be used to document different threats. The next section will contain information on network security, this will be used to document security solutions that can help to secure a network. The last section of this chapter will cover related work, this will be used to cover any research that is related to the project.

2.2 Network Overview

Computer networks are a huge part of everyday life, without them life would be a struggle therefore it is important to ensure they are secured. Houses are becoming smarter with the addition of internet of things devices. [1]The paper explains some uses for a smart home. These include lighting, heating, cooling and security systems. To create these smart systems, smart devices need to be added. Smart devices can include light bulbs, thermostats, and camera systems etc. However, this means more devices need to be added to home networks.

This is one of the reasons why computer networks are growing rapidly. According to the report [2], the total amount of traffic in 2017 was 121,694 petabytes per month. However, by 2021 this is expected to rise to 278,108 petabytes per month. This shows a 128.5% increase in monthly traffic in just four years. This shows that home networks are growing, this means there will be more security vulnerabilities within the networks. The report [3], indicates three vulnerabilities within the IoT smart home application. Limited authentication, authorisation and accounting is the first security issue. Central application control security is the second security issue. The lack of encryption on smart devices is the final security issue. The impact of these vulnerabilities could lead to the compromise of user's data. This again providing the reasoning for this project on how to secure a home network.

2.3 **Network Devices**

This section of the report will look at what different devices are currently connected to home networks. It will look at everything from the basic networking devices to how devices connect to the network. It will look at what end devices are currently being connected to home networks, and how smart devices are being used within home networks.

Routers

A router is a device that is used to connect two or more networks so that traffic can be routed between them. This is usually between the network and an internet service provider (ISP). Therefore, a router is generally the entrance/exit point for the network. Typically, in any home network a router will have a firewall built into it, this allows the firewall to filter traffic between the internal network and external network. According to the report [3], home routers are a security vulnerability due to the lack of cryptography and weak default authentication. The report additionally investigates behavioural malware detection on routers to help to secure home networks.

Switch's

A switch is a device that is used to connect multiple devices into a wired network. A switch that would be used within a home network would generally have between 5-10 ports, this means that you can connect to 5-10 devices into the network through the switch. Switches are an effective way of connecting the network, they also allow you to create virtual local area networks (VLANs). This allows you to separate your network traffic to ensure it is more secure. An example of this would be having a guest network on one VLAN and other traffic on the main VLAN. This would mean that there would be no risk of guests accessing anything within the main VLAN.

Servers

There are not many home users that would have a server however, most people are aware that backing up all data is very important. For this reason, the author thinks that most homes would have network attached storage (NAS). This would typically be a hard drive connected to the internet. This would allow the data on the network to be backed up on an hourly or daily basis depending upon the user's requirements.

Workstations/mobile devices

Almost all homes have mobile phones and workstations as end devices in their network. These are essentially what the network is there for however, now days these devices are being used to control peoples smart home devices. Workstations and mobile devices that do not have a strong security implementation can be a vulnerability to the network. These devices are generally what is most lightly to get infected by viruses, malware and spyware when they are not properly secured.

Smart home devices

[4]Now it is realistically possible to have just about any device as a smart device. They allow you to have connectivity and control of your home from anywhere with a wireless connection. This does have one big issue, if the network isn't secure then people could hack people's homes and drive them crazy. There are many smart home devices, thermostats to control ac or heating. Kitchen appliances like smart fridges, smart cookers and smart kettles. Security devices like security camera systems with remote monitoring. There are also general items like smart window controls, smart blinds etc.

2.4 Network Threats

This section of the report will look at different threats that could be an issue for any network. The author will look at what the threat is, previous attacks made with the threat and finally a solution to the threat.

2.4.1 Browser Attack

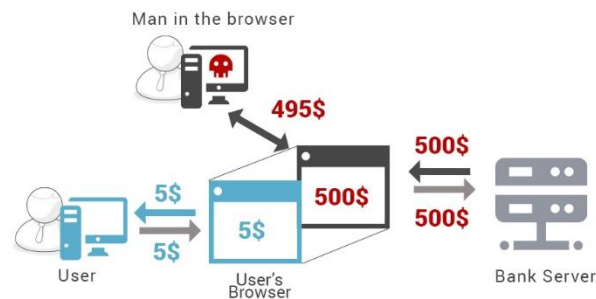


Figure 1 – Browser Attack [5]

[6],[7] A browser attack is also known as a man in the browser attack. The attack involves installing a trojan horse onto the victim's device. The trojan horse is capable of intercepting user's transactions made on the internet. Browser attacks are usually conducted by organised criminals. The reason for this is that the technology is expensive to have the capability to launch a browser attack. Browser attacks have been successfully conducted on Google Chrome, Internet Explorer, and Mozilla web browsers. This type of attack is very hard to detect and prevent as the modifications take place within the user's browser. This means that when the information is sent to the destination, security checks will not detect the modifications they will believe it is the user that sent the exact request.

Example Attack

An example of a browser attack would be logging into an online bank account. Then going to send £100 to a friend's bank account. The user would enter the transaction details and then approve the transaction to send to the bank. However, this is when the trojan horse is used to modify the transaction. The attacker would modify the transaction and for example send £900 to their bank account. This would happen within a few seconds and the transaction then be sent to the bank. The user would see £100 sent to their friend within the transaction. They would not know about the £900 sent to the attackers account until they checked their account balance. Even if the user noticed the balance difference after the attack was completed it would be too late to stop it from happening.

Solution

According to the report [8], there is not any specific method to prevent a browser attack. Security software with real time threat detection and user education are the only possible solutions to this type of attack. Some banks offer "out of band trusted verification" through phone call to verify transactions. However, basic security knowledge like ensuring updates are performed and minimising browser addons will all help to protect from browser attacks.

2.4.2 Denial of Service Attack

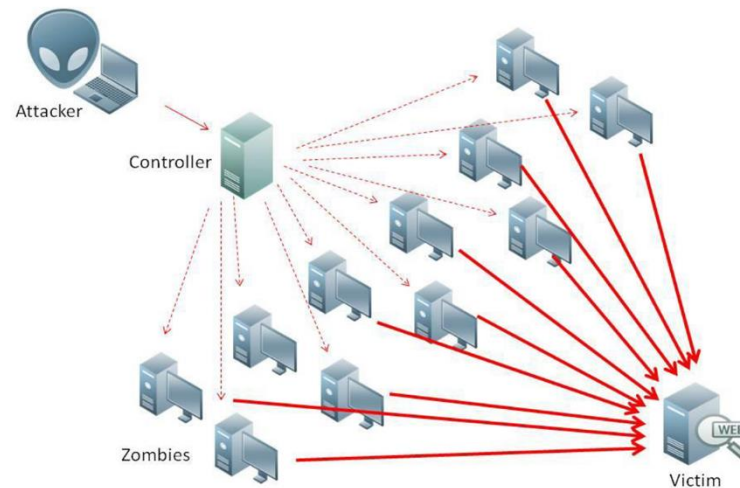


Figure 2 – Denial of Service Attack [9]

[10], [11] Denial of service attack is also known as a DoS attack. A denial of service attack is created by installing software devices to make them a zombie, this is done on between a few thousands to millions of devices to allow the attacker to create the denial of service attack. When the attacker chooses a victim, the attacker will get the zombies to send fake requests to the resource. This will then flood the victims resource forcing it to crash. It is hard to trace a denial of service attack back to the attacker, this is as requests are sent from innocent users that have no idea their devices were used for the attack. Denial of service attacks usually are used against corporate companies and large businesses, so they cannot operate.

According to the report [12], IoT based devices are being launched without the security aspects being considered. This making it easier for attackers to install their software on more devices to allow them to create more zombies. This means that when they launch any attack they have a better success rate. Additionally, it means that there is a bigger risk than ever to dedicated denial of service attacks. With more devices being added daily, this risk is only going to increase.

Recent Attacks

[13] On the 28th February 2018, the world's largest dedicated denial of service attack was launched against GitHub website. The attacker used a vulnerability where network administrators has misconfigured Memcached servers, the majority of these have still not been reconfigured. This means that a duplication of this attack is very likely to happen at some point in the future.

The attack was launched from over one thousand Memcached servers, which in return created requests from tens of thousands of end devices. This type of attack is known as an amplification attack. It can be used to launch an attack over 51,000 times as powerful to its original strength. The attack was created by the attacker sending a spoofed IP addresses to a server vulnerability on Memcached server port 11211. There was 1.35 terabytes (TB) of data sent to the website, this was sent via 126.9 million packets per second.

Solution

There are several solutions that can be implemented to reduce the risk of a denial of service attack. The first step is to communicate with the internet service provider, they can use load balancers to limit the effect of the attack. Other solutions include intrusion detection system's (IDS), intrusion prevention systems (IPS), firewalls. Another way to reduce the effect of a denial of service attack is to have a network that can deal with many requests, typically three or four times the amount of traffic it would normally receive. In the report [14], the author looks at how effective intrusion detection and prevention systems can be during a denial of service attack.

2.4.3 Brute Force Attack

```

Opening /root/Desktop/-01.cap
Reading packets, please wait...

Aircrack-ng 1.2 beta3

[00:00:00] 192 keys tested (1409.45 k/s)

KEY FOUND! [ notsecure ]

Master Key   : 42 28 5E 5A 73 33 90 E9 34 CC A6 C3 B1 CE 97 CA
               06 10 96 05 CC 13 FC 53 B0 61 5C 19 45 9A CE 63

Transient Key : 86 D0 43 C9 AA 47 F8 03 2F 71 3F 53 D6 65 F3 F3
               86 36 52 0F 48 1E 57 4A 10 F8 B6 A0 78 30 22 1E
               4E 77 F0 5E 1F FC 73 69 CA 35 5B 54 4D B0 EC 1A
               90 FE D0 B9 33 06 60 F9 33 4B CF 30 B4 A8 AE 3A

EAPOL HMAC   : 8E 52 1B 51 E8 F2 7E ED 95 F4 CF D2 C6 D0 F0 68

root@kali:~#

```

Figure 3 – Brute Force Attack [14]

[15][13] A brute force attack a method of password cracking. This method works very well when trying to figure out a password, however sometimes it can be slightly slow. A brute force attack involves a password file, this file can be as large as needed. It can include every possible password ever. Then this is run in a trial and error method, it tests each password until it has cracked the password. It will only find the password using this method if it is in the list exactly as the password is.

A brute force attack is commonly used within organisations to test the security strength of their passwords. This being one way that hackers can gain unauthorised access to a system, it is important to ensure any weak passwords are found and fixed before any hacker can find them. When a brute force attack is started it will find any weak or default passwords very quickly, this being one of the reasons it is commonly used for WPA2 password cracking. This is as people do not change their simple default passwords.

Recent Attacks

In 2014 the us utility's control system was attacked by brute force. It has been stated that the attack was successful in gaining access to the system, however no critical systems were compromised. This attack just demonstrates how weak passwords can be easily comprised to gain unauthorised access. The attack was made against the online portal, this only give the attackers access to limited basic control systems. However, it highlighted the importance of strong passwords.

In 2013 one of the largest brute force attacks was made against GitHub. This attack was again successful, and several accounts were compromised in the process. GitHub stores its passwords in a secure method however, weak passwords still existed within the company's network. It remains unclear of exactly how many accounts were compromised as GitHub has not realised this information. This attack was created from around 40,000 different IP addresses. It like the last attack was executed using a username and password list and then all passwords were tested within the list until the attack found the passwords.

Solution

[13] According to the report [16], password security is a major problem for users all over the internet. It is not just about the password but additionally how it is stored. This report investigates using a unique algorithm to secure passwords within a database. Another solution is to use complex passwords, by implementing a password policy. This enables you to ensure all passwords are a certain length, have upper case and lower-case letters and include both numbers and symbols. An example of this would be a simple password being "password" and a complex password of "Exa1Mple@Pas5-Word!". Both passwords can be broken using the brute force method if they are in the word list however, the simple one will be cracked in a matter of minutes. The complicated password is more than likely to take a few days to a few weeks to crack.

2.4.4 Malware

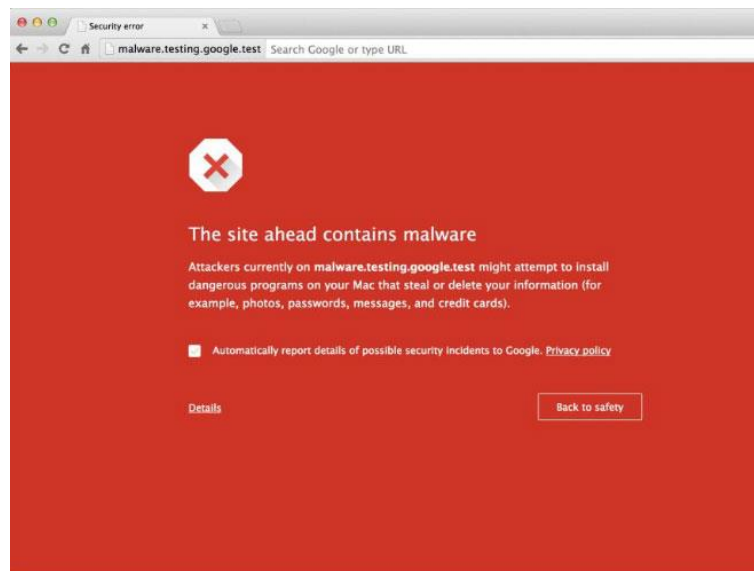


Figure 4 – Malware [17]

[18], [19] Malware is a code that is written to steal, modify, or delete data within devices. There are several types of malware these are viruses, trojans, spyware, worms, ransomware, adware, and botnets. The report [20], states a virus is a program that tries to duplicate itself onto other devices. Viruses are usually spread between different devices over the internet. A trojan is a code that can hide within legitimate programs to stay unnoticed. A trojan can be used for creating backdoors, spyware, turning a device into a zombie, and sending costly SMS messages. A trojan can be hidden within any type of file images, music, software, and applications. Once they have been opened or installed then the trojan sets to work hidden in the background.

[21] Spyware is usually hidden within legitimate programs and is used to steal passwords, bank details, and credit card information. [22] Ransomware is a software that is hidden in a file, once it is opened then the device files get encrypted. The only way to decrypt the files is to pay a sum of money to the hackers, this is usually done in bitcoin. [23] Adware is used to produce unwanted advertisement's, these are usually in one of two ways. The first is a pop-up window and the second is a window that will not close.

2.5 Network Security

This section of the document will look at different security implementations that can be put into place to help secure the network. The author will explain what each of the different security mechanisms is and how it will benefit the network that is being build.

2.5.1 Physical security

This is a security mechanism that is often overlooked, spending large sums of money on state of the art security devices will not protect the network from physical access. The network needs to be both physically secure and secured from authorized access over the internet.

2.5.2 Virtual Private Networks

[24] This is a security mechanism that is widely available on the internet. A virtual private network can be used to encrypt the network traffic between a client and destination over the internet. A virtual private network can be used to secure a device from a man-in-the-middle attack.

2.5.3 Firewalls

[25], [26] A firewall is a device that can be used to filter network traffic depending on a set of rules. A firewall can be either physical or virtual and allows for rules to be created to allow or deny traffic entering or exiting the network. In a home network environment generally, there will be a firewall on the router that is used to connect to the internet,

2.6 Related Work

This section of the report will look at related work. This is work that is based around a similar project to the one being undertaken by the author. The author will explain what each of the related work is about. If they have any results, then the author will additionally look into the details of these.

2.6.1 WPA2 Password Crack

According to the report [27], the paper gives a new dictionary method for cracking WPA2 passwords. The method that this paper uses based on the SA and HMM algorithms to create a new dictionary file. This paper then states John the Ripper will be used for the password cracking and the new dictionary file will be used to find the WPA2 password. This paper states using this type of dictionary attack has a higher success rate than what a brute force attack has.

According to the report [28], The paper explains how a WPA2 attack is performed using Kali Linux. The paper details a testbed design for the simulated network to be created for the attack to take place. This paper is attempting to break the password using the brute force method. This paper manages to break the WPA2 password in 12 hours 12 minutes and 50 seconds, the attack had to test 129832652 keys before it found the correct one. This shows that the brute force method is effective however, it is slower than what a dictionary attack would be.

2.6.2 Network Scan Attack

The report [29] looks at an approach that can be used to create a network scan attack using P-SCAN. According to the report P-SCAN is a very configurable and scalable network scanning tool. This software can be used to challenge all network devices security however, in this report it looks at evaluating Internet of things device security.

According to the report [30][30], Internet of things devices are being added to networks with their basic default authentication. The report looks at how Internet of things devices are being targeted to be used for denial of service attacks as most of these devices have little to no authentication. This report demonstrates how a scanning tool called Shodan can be used to scan for weak passwords or open ports. The report then goes on to explain how the open ports within the network can be used by attackers to use exploits to gain unauthorised access to the devices.

2.7 Conclusion

In conclusion this chapter has given the author the background knowledge to support the project. The author has looked at different threats and solutions, devices within the network, and related work based around what the author is aiming to achieve from the project.

Chapter 3 - RESEARCH METHODOLOGY

3.1 Introduction

This chapter will cover the research overview, process, philosophy, methodology, data collection and research design. This will allow the author to understand exactly how to complete the project. This chapter is based around the aims and objectives. This allows the author to know what is required to achieve a successful outcome from this project.

3.2 Research Overview

This chapter is used to cover the research overview that is required to complete the methodology, to enable the author to achieve the aim and objectives of the project. Figure 5 below shows the research onion, this provides a detailed plan that covers everything from the research to concluding the project.

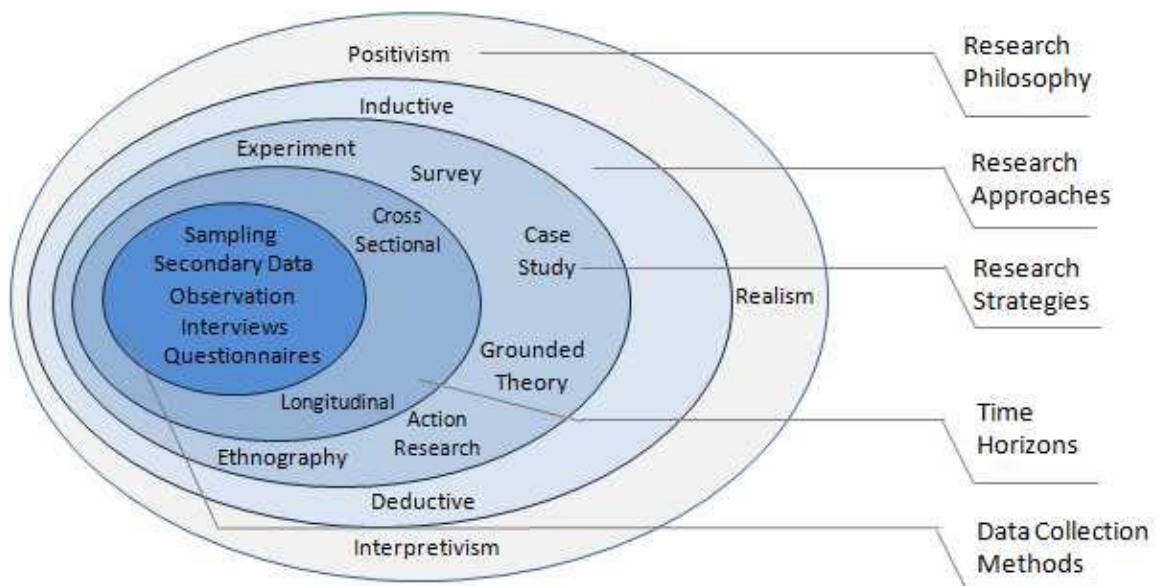


Figure 5 – Research Onion [31]

3.2.1 Research Process

The research process will be used to develop a method that can be used to create a secure home network. The author will explain each section of the research onion and how they relate to the project on building a secure home network. Once the project is completed the author will then cross reference their work with the research. This will allow the author to have an idea of how this project relates to others that have been done in the past.

3.2.2 Research Philosophy

In the philosophy section of the research onion there are three different methods. The research philosophy that will be used within this project is positivism. Positivism research philosophy is when the research is mainly based upon scientific evidence, this is usually statistics or experiments. The author believes that this is an important for the research as the project is based around experiment's.

3.2.3 Research Approaches

In the approaches section of the research onion there are two methods, inductive and deductive. The research approach that will be used within this project is deductive. Deductive is used to test a theory that the author has, in this project the author has a theory that home networks are not very secure so how can they be secured.

3.2.4 Research Strategies

In the strategies section of the research onion there are six methods. These are experiment, survey, case study, grounded theory, action research and ethnography. The research strategy that will be used in this project is experiment. Experiment research strategy is when the author changes one or more variables to conduct the experiment and then recode the data. The author will be creating several different attacks; this will be the changing variable. The author will then recode the results from the experiments, this will allow them to be compared the findings found within the research.

3.2.5 Time Horizons

In the time horizons section of the research onion there are two methods, cross sectional and longitudinal. The time horizon that will be used within this project is cross sectional. Cross sectional time horizon is when something is done at a single point of time. The author will be conducting each experiment once so this is why cross sectional time horizon was selected for this project.

3.2.6 Data Collection

In the data collection section of the research onion there are five methods. These are sampling, secondary data, observation, interviews, and questionnaires. The data collection methods that will be used within this project will be observation and secondary data. The observation data collection method is used to observe the results of something and explain it. The author will be observing the results from the experiments and documenting them. The secondary data collection method is when existing data is researched that is based on that of a similar project. The author will be using secondary data for the research. The author will also use this to compare the findings of the project to findings of similar projects.

Data collection methods this is used to demonstrate what methodology that has to be used within each chapter. The author will use this to understand exactly what method is required to successfully complete each chapter of the project. This will help to ensure that the project has a successful outcome.

Component	Research Approach
Introduction Chapter 1	Deductive - used to test a theory that already exists
Research & Review of literature Chapter 2	Action Research – Researching and understanding findings Qualitative Research – Reviewing current network vulnerabilities
Research Methodology Chapter 3	Action Research – Researching and understanding findings
Design & Implementation Chapter 4	Action Research – Researching and understanding findings Experiment – Changing a variable to obtain results
Evaluation Chapter 5	Qualitative Research – Obtaining Results Action Research – Understanding findings Triangulation - Ensuring results are similar to previous experiments
Conclusion Chapter 6	Action Research – Understanding findings
Reflection Chapter 7	Action Research – Understanding findings

Table 1 – Data Collection Methods

3.3 Research Design

This section of the report will be used to cover the research deliverables, in this section the author will state what the research deliverables for the project are and why they are important. It will also cover triangulation; the author will explain how they aim to use triangulation within their project to ensure the data collected is accurate and correct.

3.3.1 Research Deliverables

The research that the author has completed in chapter two will allow the author to understand different network vulnerabilities. This will allow the author to produce better results within the experiments, this will increase the chances of success during the attacks. The results and findings can be found in chapter five of this project. This section will cover exactly what attacks have been implemented and how to secure a network from this type of threat.

3.4 Triangulation

This project is based around research and experiments. The author will conduct the experiments, from these the author will have some results. This is when research triangulation will be important; the author will compare their results to their research. This should provide validity to the authors work and allow for a conclusion knowing the results and findings are accurate.

3.5 Conclusion

In conclusion the author finds that this chapter has been very helpful, by ensuring that the correct methods are in place to have a successful outcome. The research philosophy will be helpful in guiding the author through the remainder of the project. This is as the research onion guides the author step by step on what to do within the project. The author additionally found the data collection methods very helpful in providing different ways of collecting information for the project. With the project moving towards the design and implementation section, it is important that this chapter is clear as it will guide the author on what needs to be done for the remainder of the project. However, the part that the author believes is the most important is research triangulation. This section will help support the authors work in providing clarification to support the findings from the project.

The following chapter explores the design and implementation section of the report. This chapter will look at how the author can create the network for the experiments to take place on. Additionally, it will look at how each experiment can be carried out giving the author a plan to proceed to chapter five with.

Chapter 4 - DESIGN & IMPLEMENTATION

4.1 Introduction

Chapter four is essentially split into two sections design and implementation. The design section of the network needs to look at what devices are going to be within the network. This includes how each of the devices will connect to each other. There will need to be implementation of security based on the devices connected to the network. The author will then have to look at what vulnerabilities could exist within the network design. This will give the author an idea of how attackers could exploit the network and gain unauthorised access.

When these points have been considered and a final design proposal is made then the author can begin with the implementation. This will be done to the design that will be created during the first part of chapter four. The author will then document the implementation and conclude this chapter.

4.2 Problem Formulation

This project is based upon building a secure home network. The author will build a network that will involve workstations, mobile phones, printers, and smart devices. This will allow for a real-world test of the vulnerabilities within the network to be discovered. When designing the network there will be no major security systems or software added to the design. The author will then implement the network within the home environment. This will allow the author to test the network in chapter five. These tests will involve software within Kali Linux as this is a very strong tool for testing network security. The results from the testing should allow the author to make suggestions to improve the security of the network, doing so will give the author a successful project.

4.3 **Design**

When designing a network, the first thing that needs to be considered is what devices are going to be connected to the network. The next consideration is how are the devices going to connect to each other. The last consideration is what software is required on the devices to conduct the experiments. Only after these points have been considered can the network design begin.

There will be 14 different devices that will be included within the network design. Table two below shows each device that the author would like within the network. It also shows each device connection type and what different devices should be connected to within the network.

Device Name	Device Type	Connection Type	Connection to
Virgin Media Super Hub	Wireless Router	Coaxial Cable	Internet service provider
HP laptop	Laptop	Category 5 Ethernet cable & Wi-Fi	Virgin Media Super Hub
Phillips television	Smart Television	Wi-Fi	Virgin Media Super Hub
HP printer	Network Printer	Wi-Fi	Virgin Media Super Hub
Dales TiVo box	Smart TV Box	Wi-Fi	Virgin Media Super Hub
Main TiVo box	Smart TV Box	Wi-Fi	Virgin Media Super Hub
Dyson Fan	Smart Fan	Wi-Fi	Virgin Media Super Hub
iPhone	Mobile Phone	Wi-Fi	Virgin Media Super Hub
HP desktop	Desktop Computer	Wi-Fi	Virgin Media Super Hub
CCTV System	IoT NVR	Category 5 Ethernet cable	Virgin Media Super Hub
CCTV Camera 1	Smart CCTV Camera	Category 5 Ethernet cable	CCTV System
CCTV Camera 2	Smart CCTV Camera	Category 5 Ethernet cable	CCTV System
CCTV Camera 3	Smart CCTV Camera	Category 5 Ethernet cable	CCTV System
CCTV Camera 4	Smart CCTV Camera	Category 5 Ethernet cable	CCTV System

Table 2 – Devices in network design

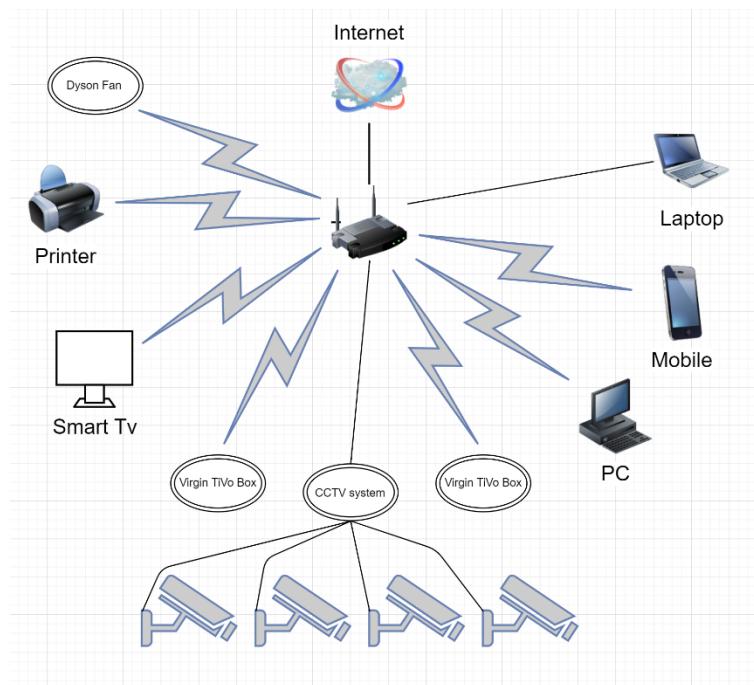


Figure 6 – Network Blueprint

The blueprint in the figure above is a demonstration of how each of the devices should connect. It gives the author a clear idea of how to implement the network in the next section of this chapter. The blueprint and table two both give the same information however; the blueprint is easier to work with when creating the implementation as it creates a visualisation for the author to follow. To create the attacks within the network the author will need to install Kali Linux operating system onto one of the devices. This will enable the author to create the attacks chosen within the network to find the vulnerabilities.

4.4 **Implementation**

This section of the report is used to document the implementation for the project. It is essentially in three parts, router setup this section will document how the router will be set up within the network. The next part will be connecting to the router, this section will document how devices can be connected to the router. The final part of this section will cover the software that has to be installed to enable the author to create the experiments.

4.4.1 Router Setup

Figure 7 below shows the very first screen on setting up a virgin media router. This is when the author had to select a language for the installation. The author chose English as this is the language that they understand and then clicked next.

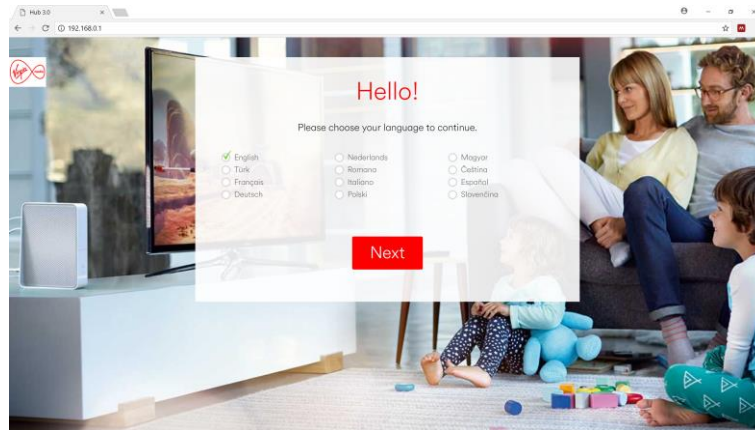


Figure 7 – Router Setup (1)

Figure 8 below shows second step to setting up a virgin media router. This is when the author had to input the default settings password and click next.

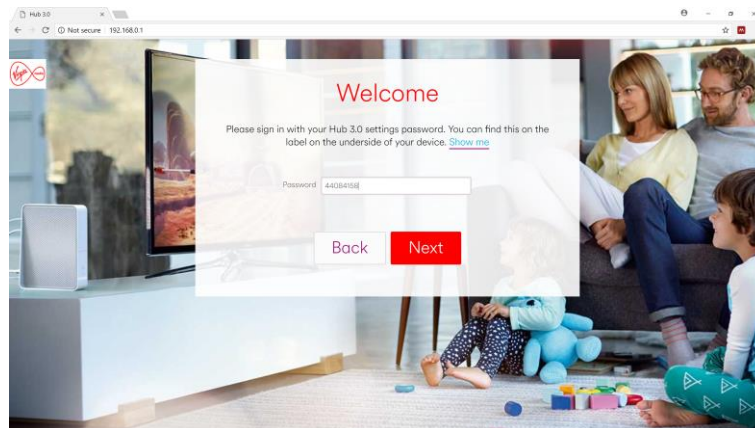


Figure 8 – Router Setup (2)

Figure 9 below shows the third step to setting up a virgin media router. This is when the author had to change the default password for the administrator login then click next.

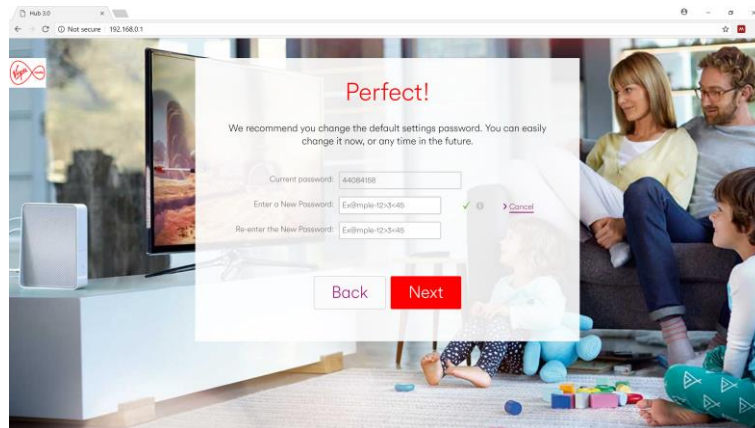


Figure 9 - Router Setup (3)

Figure 10 below shows the forth step in setting up a virgin media router. This is when the author had to reboot the router to apply the new settings by clicking finish.

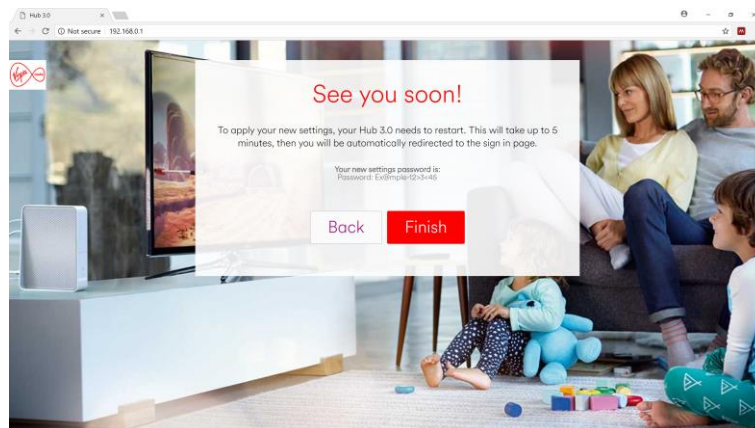


Figure 10 - Router Setup (4)

Figure 11 below shows that the virgin media router has been set up correctly. To access the routers administration settings the author had to login using the password that was created earlier.

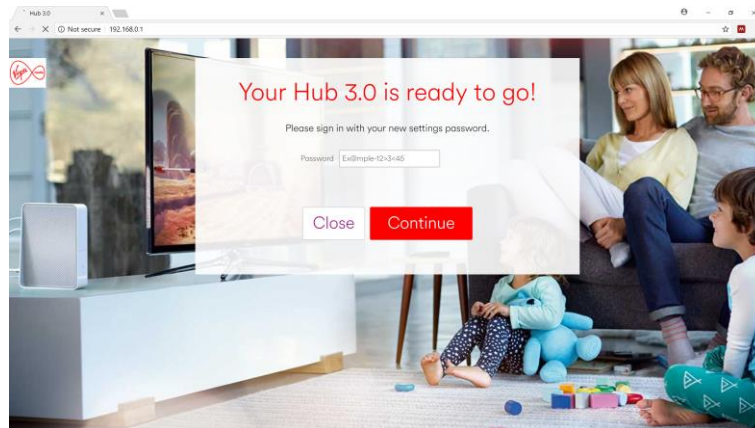


Figure 11 - Router Setup (5)

4.4.2 Connecting Devices

Figure 12 below shows the network that was created within the last section of the document. To connect to the network the author must click connect.

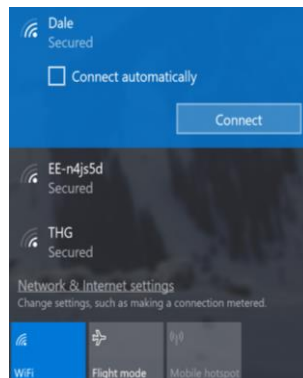


Figure 12 – Connecting the devices (1)

Figure 13 below shows the author must type in the password that they created within the administration settings of the router earlier.

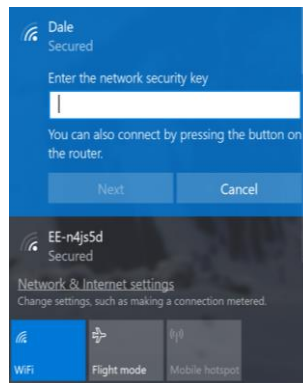


Figure 13 – Connecting the devices (2)

Figure 14 below shows that the password has successfully entered, and the device is now connected to the network. This process must be repeated on all Wi-Fi devices to enable them to connect to the network. Wired devices can just be connected directly to the router using category 5 ethernet cable.

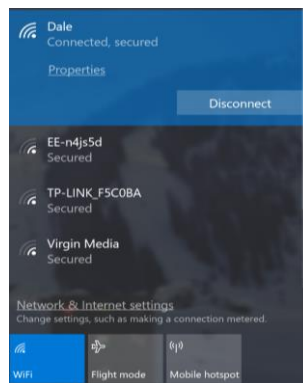


Figure 14 - Connecting the devices (3)

4.4.3 Software Installation

The author had to install Kali Linux to their laptop. This was done by creating a windows partition, this is where the second operating system will be stored. The author then followed the installation steps to install the dual boot operating system. Once completed the author rebooted the system and there was an option for Kali Linux boot or Windows 10 boot. Figure 15 below shows what the Kali Linux operating system looks like once it is installed. At this stage the author is ready to move onto the testing and evaluation in chapter five.



Figure 15 – Kali Linux [32]

4.5 **Conclusion**

In conclusion the author has found chapter four to be very helpful within the project. It has ensured that the network was designed correctly, allowing the author to connect the devices that were required. During the implementation section of the report the author documents setting up the router, connecting the devices, and installing Kali Linux. There was only one issue the author had during the implementation, thus was that the network adaptor within the workstation was not compatible with Kali Linux. The author had to use an external wireless adaptor that was compatible with Kali Linux to connect using Wi-Fi.

Chapter 5 – Testing & Evaluation

5.1 Introduction

This chapter will be used to document the experiments that will be done for the project. The author will be looking at a variety of different attacks, WPA2 password cracking, man-in-the-middle attack, and port scanning. The author will conduct the WPA2 password cracking and man-in-the-middle attack in Kali Linux operating system. The port scanning will be conducted in windows operating system.

5.2 WPA2 password cracking

In this section of the report the author will be conducting two WPA2 password cracking attacks. The author will set up the WPA2 attack so that the first one will have a simple password and the second one will have a complex password. This will allow the author to compare the difference in password strength.

5.2.1 Simple Password

Figure 16 below shows the network settings that have been implemented for the simple WPA2 password attack to be conducted. The router has been set up with an SSID of “Dale” as seen in chapter four, the router has also been given a password of “aboutadobe”. The author has verified the settings to ensure they are correct before the attack is started.

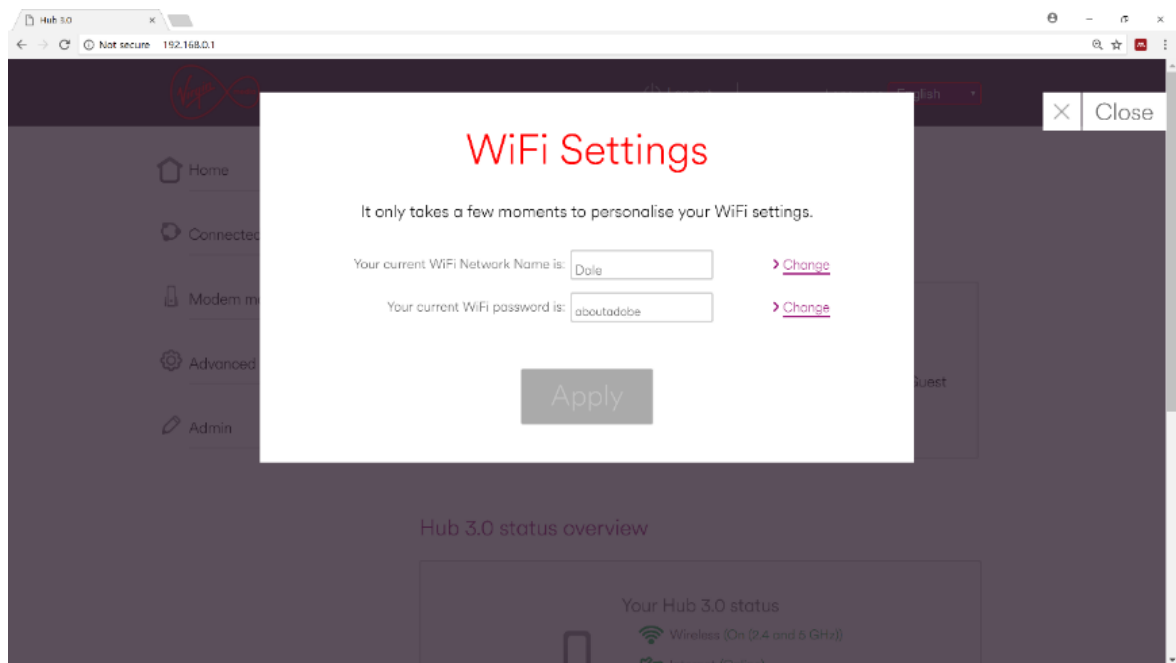


Figure 16 – WPA2 simple password (1)

Figure 17 below shows the author is utilising Kali Linux to perform the attack. Firstly, the author opened a new terminal window. The next step is to start the wireless monitoring. This was done using the command “airmon-ng start wlan0”. This command will search for the wireless networks that are within range of the attacker.

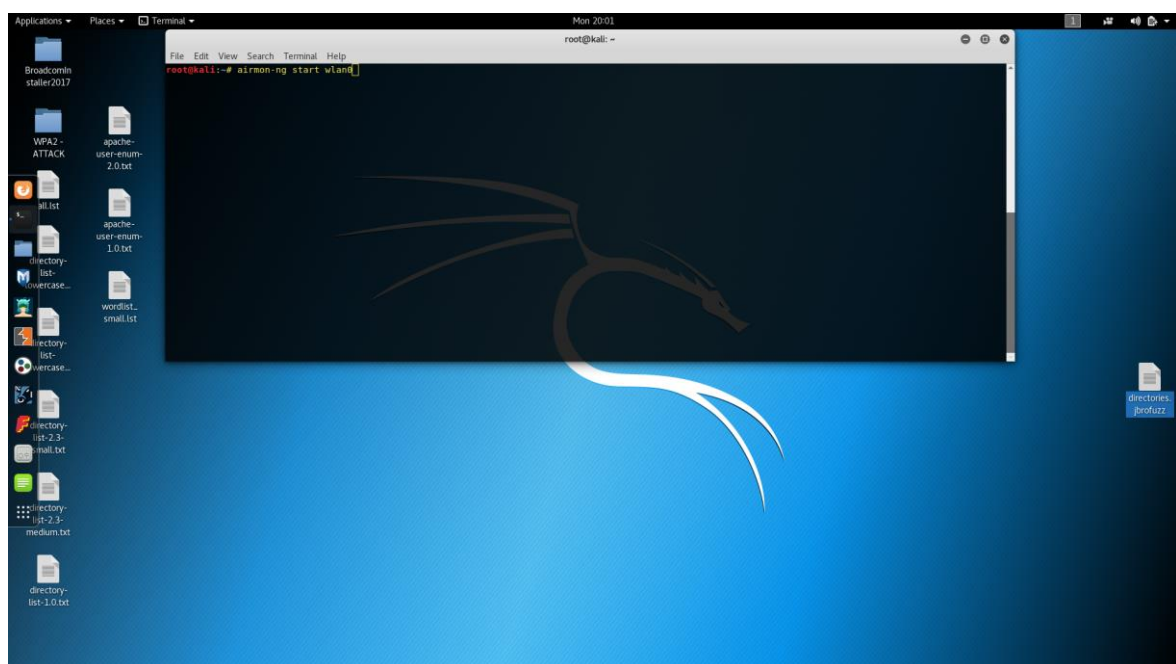


Figure 17 - WPA2 simple password (2)

Figure 18 below shows the author has successfully started the wireless monitoring in the last step. The next stage is to identify different network SSID's this is done by typing in the command "airodump-ng wlan0mon". This allows the author to continue to the next stage of the attack.

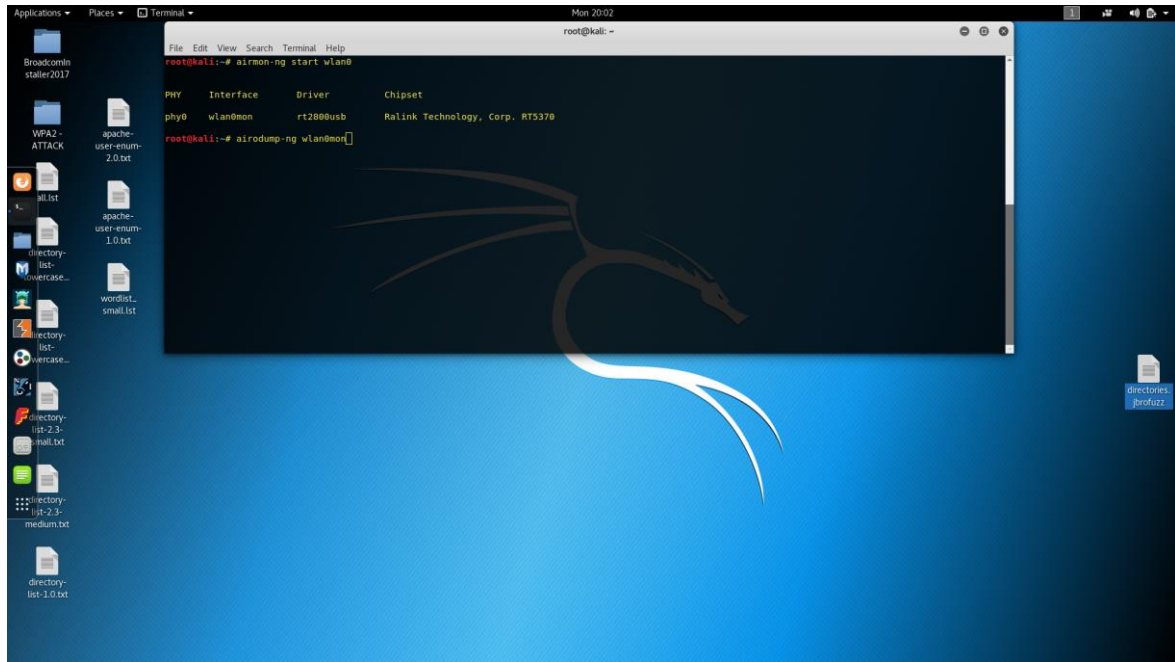


Figure 18 - WPA2 simple password (3)

Figure 19 below shows the last step of the attack was successful as it enabled the attacker to find the wireless networks that were within range. The network that the author set up had an SSID of “Dale”, which the attacker found. The next step of this attack is to monitor the traffic on the Dale network. This is done by entering the command “airodump-ng -c 6 -w dg2 --bssid 00:8E:F2:72:7E:3C wlan0mon”.

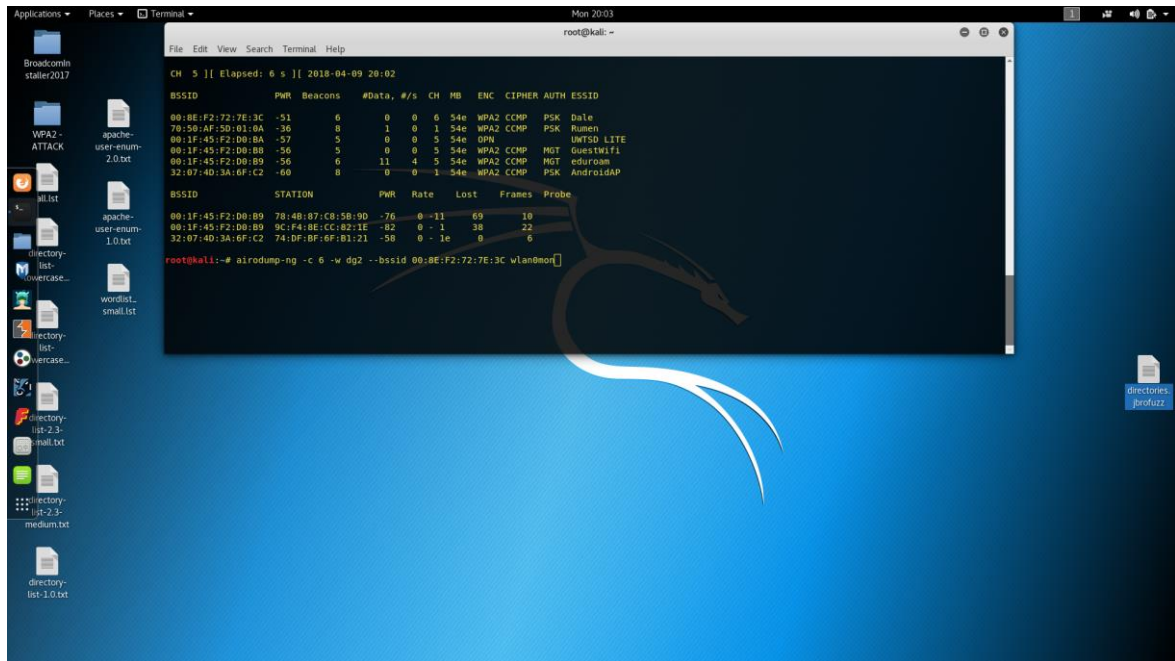
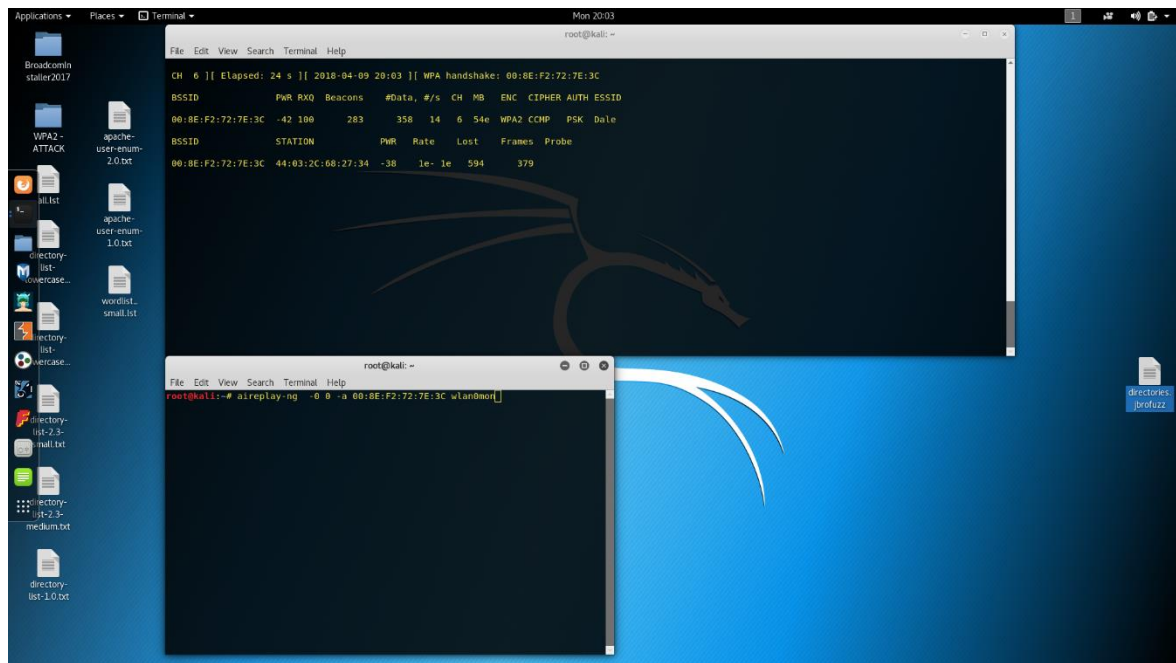


Figure 19 - WPA2 simple password (4)

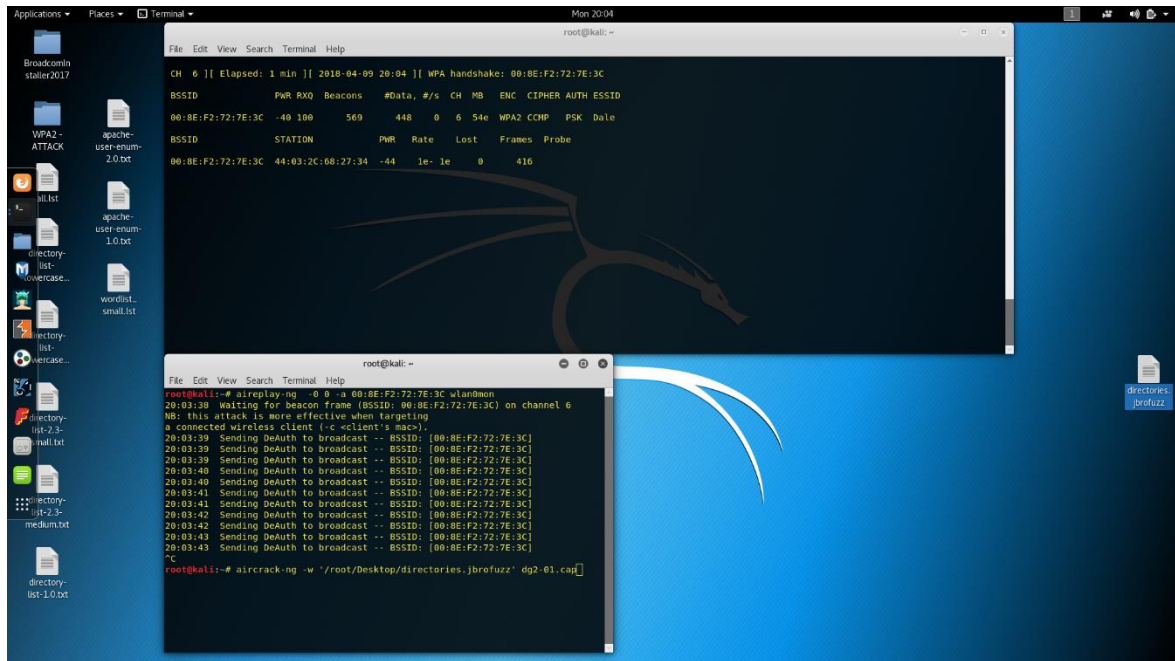
Figure 20 below shows that the last step of the attack was successful as the attacker is monitoring the network traffic. When traffic is sent to the wireless router it allows the attacker to get a WPA handshake that can be seen in the top right of the terminal. The author then begins to once again monitor for traffic using the command “aireplay-ng -0 0 -a 00:8E:F2:72:7E:3C wlan0mon”.



```
root@kali: ~  
CH 6 ][ Elapsed: 24 s ][ 2018-04-09 20:03 ][ WPA handshake: 00:8E:F2:72:7E:3C  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
00:8E:F2:72:7E:3C -42 100 283 358 14 6 54e WPA2 CCMP PSK Dale  
BSSID STATION PWR Rate Lost Frames Probe  
00:8E:F2:72:7E:3C 44:03:2C:60:27:34 -38 1e- 1e 594 379  
  
root@kali: ~  
root@kali:~# aireplay-ng -0 0 -a 00:8E:F2:72:7E:3C wlan0mon
```

Figure 20 - WPA2 simple password (5)

Figure 21 below shows that the last step was successful in monitoring the network for traffic as now the author has data being sent to the network. The author then stops the monitoring of the network traffic. This enables the password list to be opened. This is done by using the following command “aircrack-ng -w '/root/Desktop/directories.jbrofuzz' dg2-1.cap”.



```
root@kali:~# airodump-ng -0 0 -a 00:8E:F2:72:7E:3C wlan0mon
20:03:39 Waiting for Beacon frame (BSSID: 00:8E:F2:72:7E:3C) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:03:39 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:39 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:39 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:40 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:40 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:41 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:41 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:42 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:42 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:43 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
20:03:43 Sending DeAuth to broadcast -- BSSID: [00:8E:F2:72:7E:3C]
^C
root@kali:~# aircrack-ng -w '/root/Desktop/directories.jbrofuzz' dg2-01.cap
^C
```

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:8E:F2:72:7E:3C	-40	100	569	448	0	6	54e	WPA2	CCHP	PSK	Dale

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
00:8E:F2:72:7E:3C	44:03:2C:60:27:34	-44	1e-1e	0	410	

Figure 21 - WPA2 simple password (6)

Figure 22 shows that the last step of the attack was again implemented correctly by running the password file. This password file included 10 million different password combinations. It was run on the network and it cracked the WPA2 key “aboutadobe”. This was the key that was created at the start of this attack, so this demonstrates that the attack was successful.

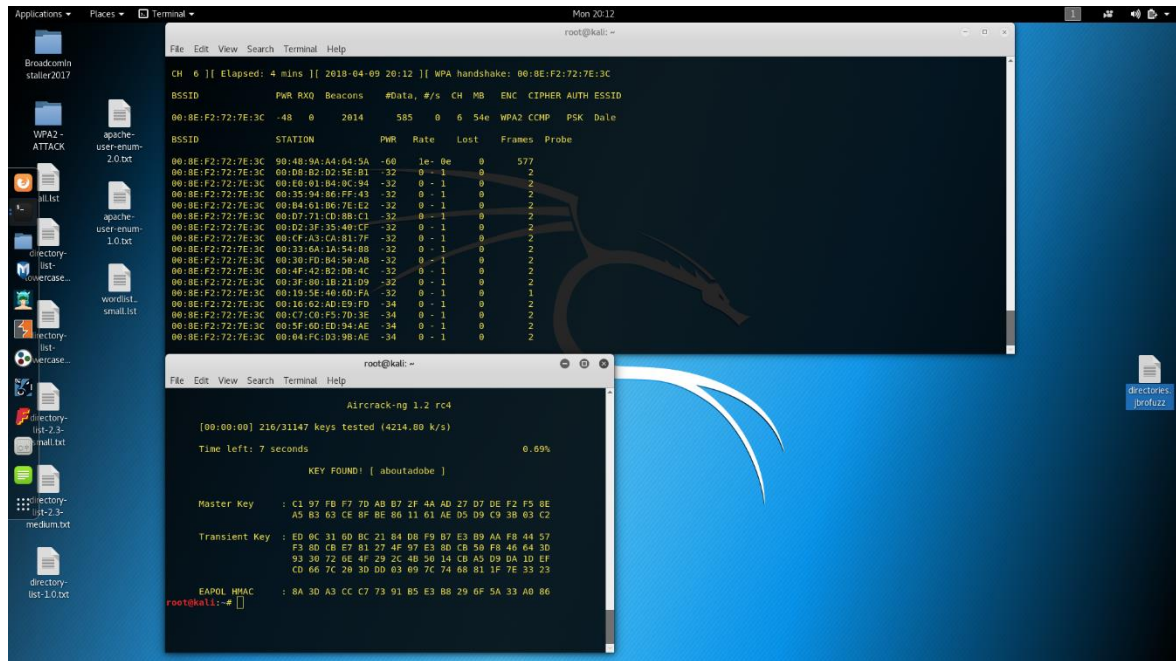


Figure 22 - WPA2 simple password (7)

5.2.2 Complex password

Figure 23 below shows the network settings that have been implemented for the complex WPA2 password attack to be conducted. The router has been set up with an SSID of “Dale” as seen in chapter four, the router has been given a password of “X-Win32_v6”. The author has again verified the settings to ensure they are correct before the attack is started.

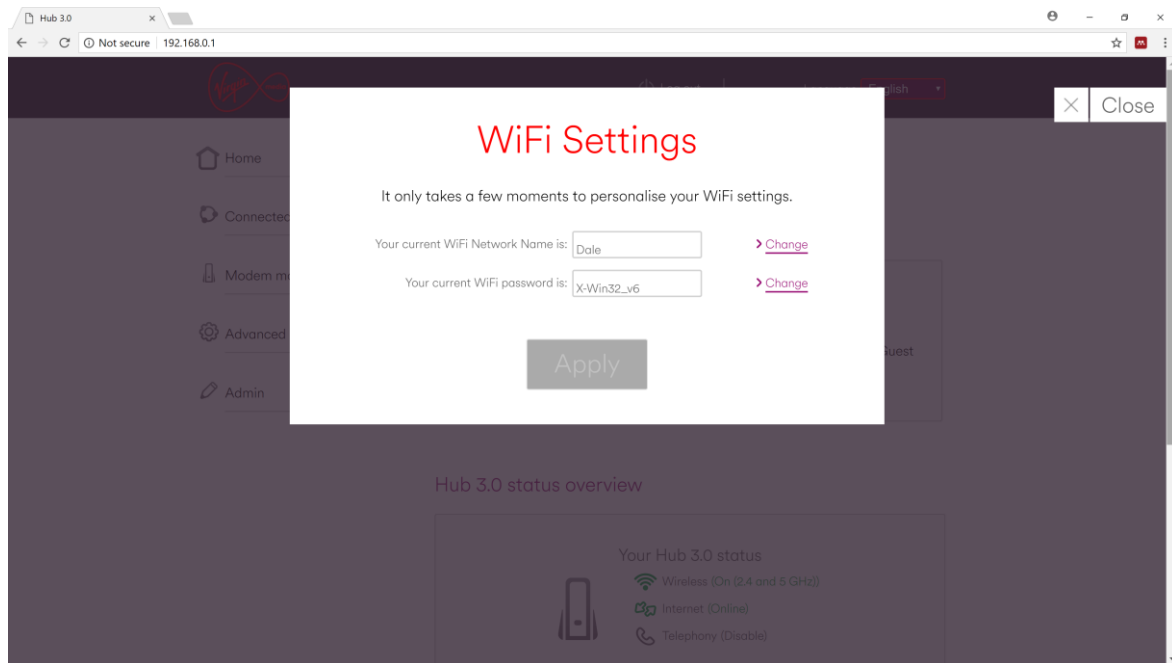


Figure 23 - WPA2 complex password (1)

Figure 24 below shows the author is utilising Kali Linux to perform the attack. Firstly, the author opened a new terminal window. The next step is to start the wireless monitoring. This was done using the command “airmon-ng start wlan0”. This command will search for the wireless networks that are within range of the attacker. The next stage is to identify different network SSID's this is done by typing in the command “airodump-ng wlan0mon”.

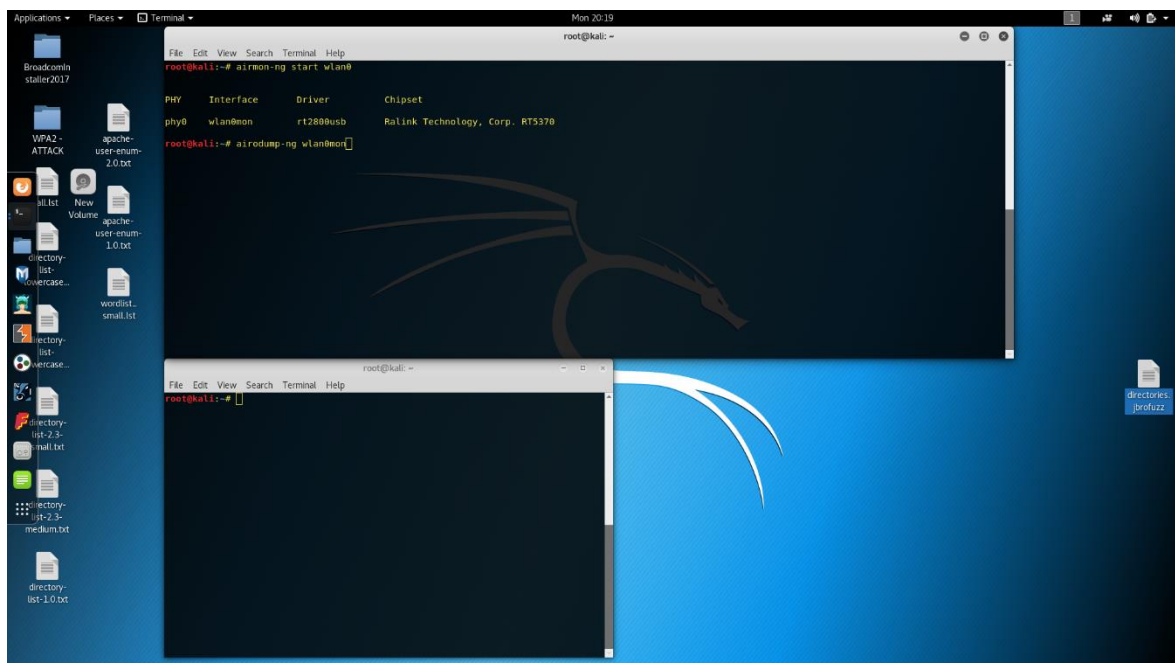


Figure 24 - WPA2 complex password (2)

Figure 25 below shows the last step of the attack was successful as it enabled the attacker to find the wireless networks that were within range. The network that the author set up had an SSID of “Dale”, which the attacker found. The next step of this attack is to monitor the traffic on the Dale network. This is done by entering the command “airodump-ng -c 6 -w dg2 --bssid 00:8E:F2:72:7E:3C wlan0mon”.

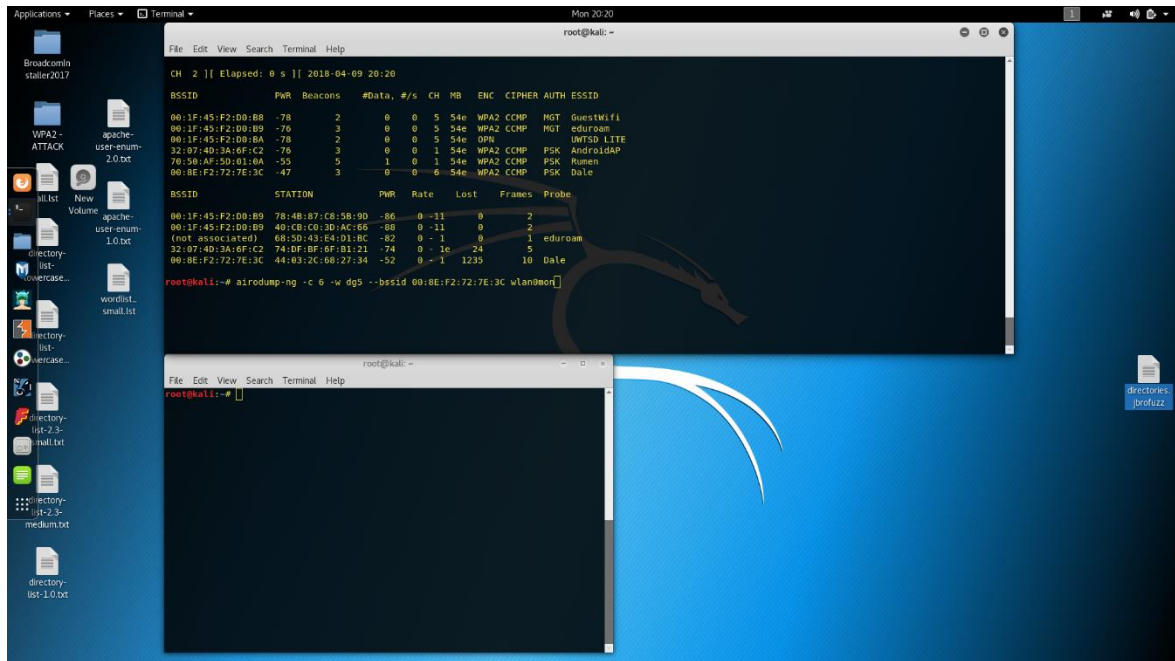


Figure 25 – WPA2 complex password (3)

Figure 26 below shows that the last step of the attack was successful as the attacker is monitoring the network traffic. When traffic is sent to the wireless router it allows the attacker to get a WPA handshake that can be seen in the top right of the terminal. The author then begins to once again monitor for traffic using the command “aireplay-ng -0 0 -a 00:8E:F2:72:7E:3C wlan0mon”. This is done so that the author can get a WPA handshake.

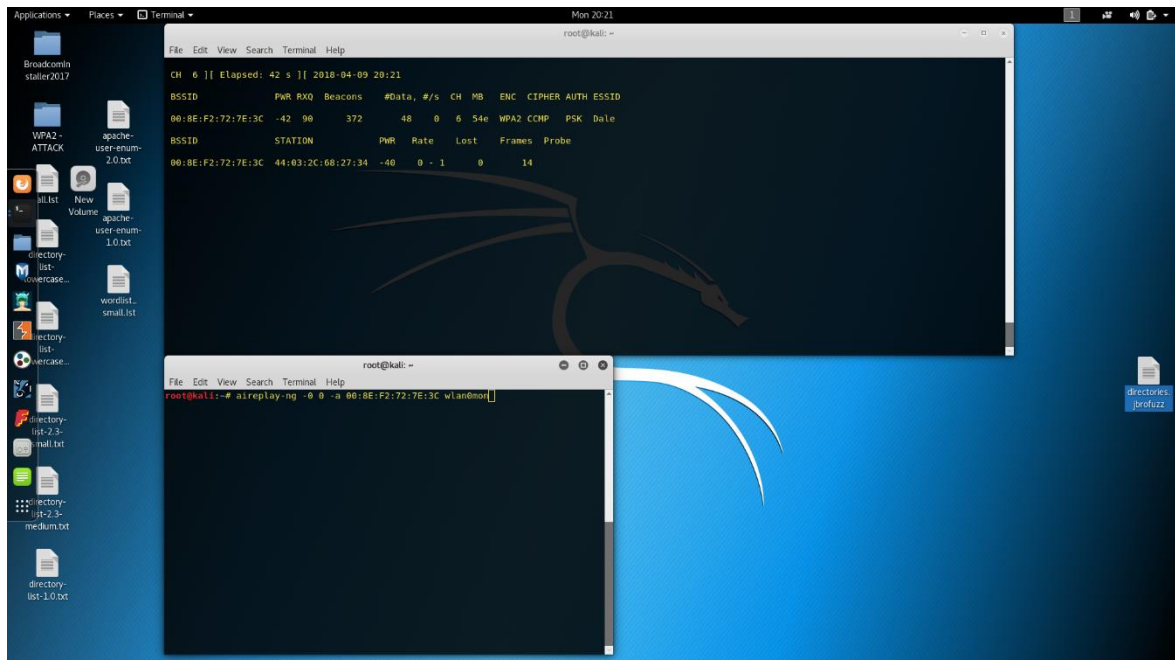


Figure 26 - WPA2 complex password (4)

Figure 27 below shows that the last step was successful in monitoring the network for traffic as now the author has data being sent to the network. Once the author has the handshake then the monitoring of the network traffic can be stopped. This enables the password list to be run. This is done by using the following command “aircrack-ng -w '/root/Desktop/directories.jbrofuzz' dg5-04.cap”.

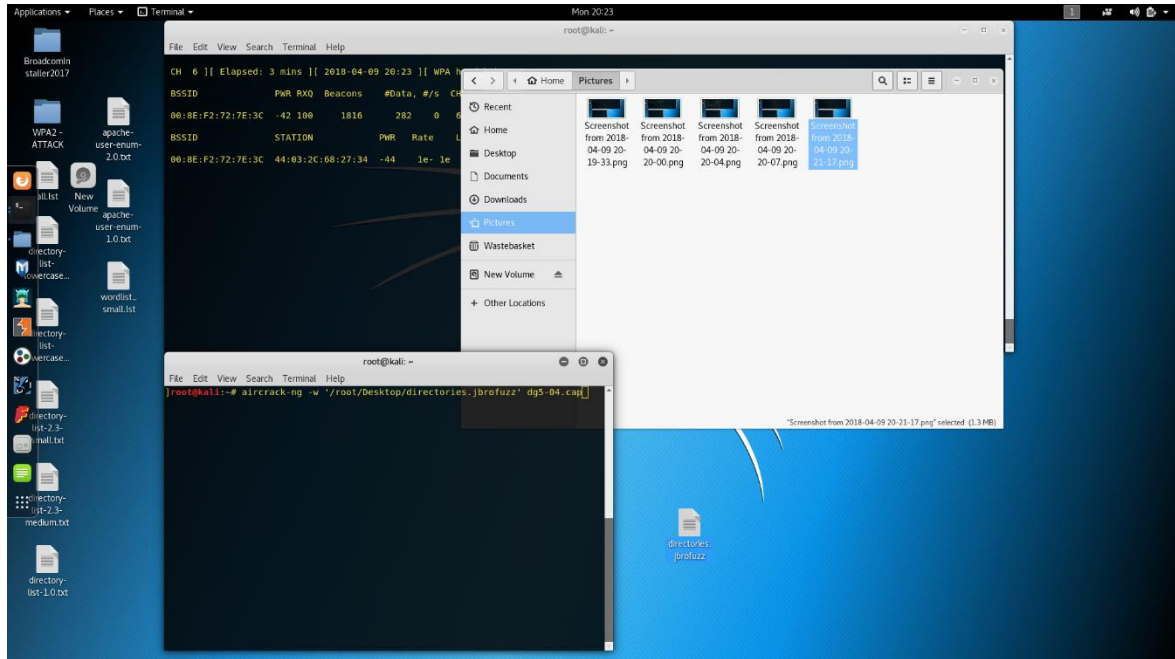


Figure 27 - WPA2 complex password (5)

Figure 28 shows that the last step of the attack was again implemented correctly by running the password file. This password file included 10 million different password combinations. It was run on the network and it cracked the WPA2 key “X-Win32_v6”. This was the key that was created at the start of this attack, so this demonstrates that the attack was successful.

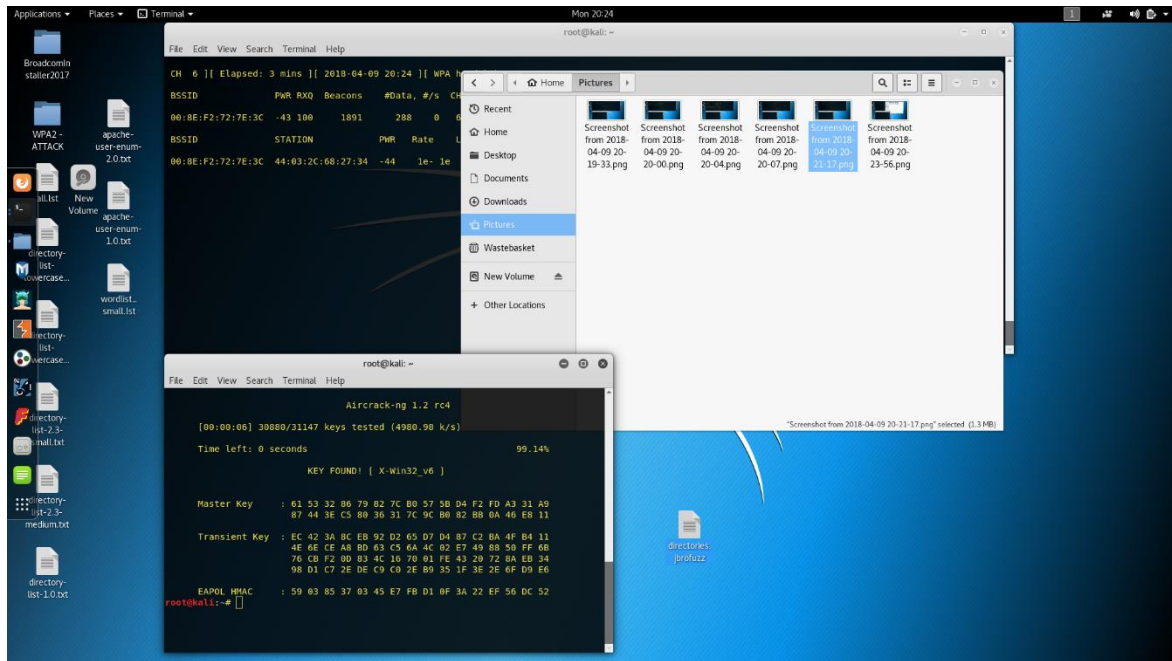


Figure 28 - WPA2 complex password (6)

5.2.3 Conclusion

In conclusion the author believes that the two WPA2 attacks were successful, by demonstrating one method that WPA2 passwords can be found. The attacker found both the simple and complex password. The simple password attack was cracked at 0.67% through the password file. The complex password attack was cracked at 99.14% through the password file. This could give the wrong conclusion that simple passwords are easier to crack than complex passwords.

In general, from the authors research in chapter two, the WPA2 password crack doesn't always take longer to crack more complex passwords than simple ones. This attack uses the brute force cracking method. This means that it goes through a password list one by one. This means that if the list has the complex passwords at the start they will theoretically be broken before the simple passwords.

The author would still recommend complex passwords however, try to ensure the passwords are not going to be included in password lists. This can be done by making a password about something that nobody else would know. Then by adding in numbers, capitalisation and symbols it should help ensure that passwords are kept safe. It doesn't mean the password isn't breakable, but it will be harder for an attacker to break the password. The author would additionally recommend checking default passwords and ensuring that they are changed into a complexed algorithm to create a stronger password.

5.3 Man-in-the-middle attack

In this section of the report the author will be conducting a man-in-the-middle attack. The author will use Kali Linux to create the attack that will be used to capture images off the websites that are visited by the targeted host. Kali Linux has software that is called Ettercap. This part of the report will document how the attack is completed and the provide solutions to help prevent the man-in-the-middle attack.

Figure 29 below shows the author started the attack by opening a new terminal. The next step was to open ettercap, this was done by using the command “ettercap -G”. The next step is to start the unified sniffing the screenshot below provides evidence of the author doing this.



Figure 29 – Man-in-the-middle attack (1)

Figure 30 below shows the popup that occurs upon starting the sniffing tool. This part of the attack involves the attacker selecting the network interface that will be used to perform the attack, the interface wlan0 was selected for this.

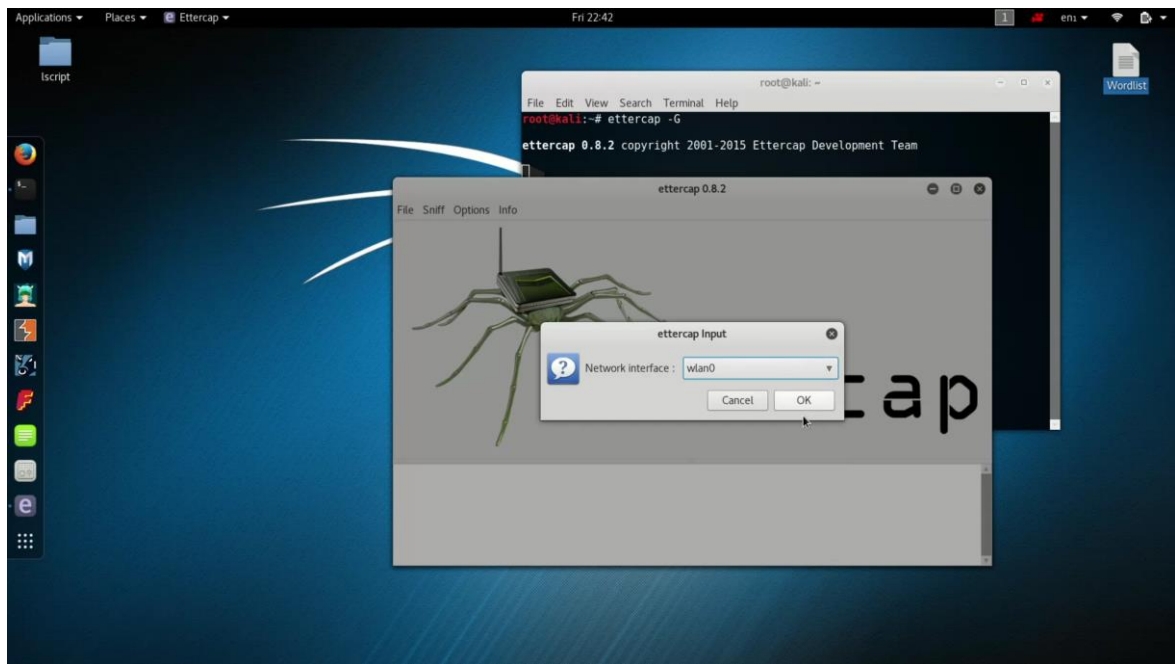


Figure 30 - Man-in-the-middle attack (2)

Figure 31 below shows that the next step of the attack is to click on the host button. This will give a dropdown menu that will allow the attacker to scan for hosts. The attacker started the scan and the output can be seen in figure 32 of this document.

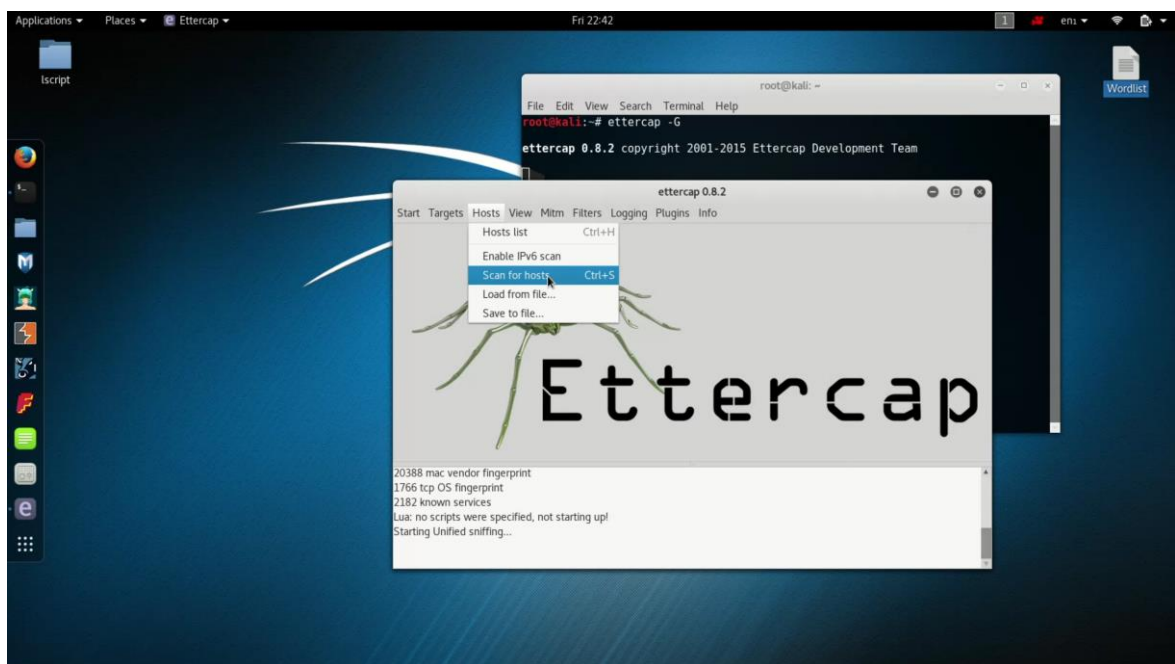


Figure 31 – Man-in-the-middle attack (3)

Figure 32 below shpws that the scan for hosts was sucessful in the last section of the attack. The attacker found two hosts within the network so that the attack could continue.



Figure 32 - Man-in-the-middle attack (4)

Figure 33 below shows the two hosts that have been identified within the network. The screenshot below shows the author adding these devices and making them target one and target two for the attack.

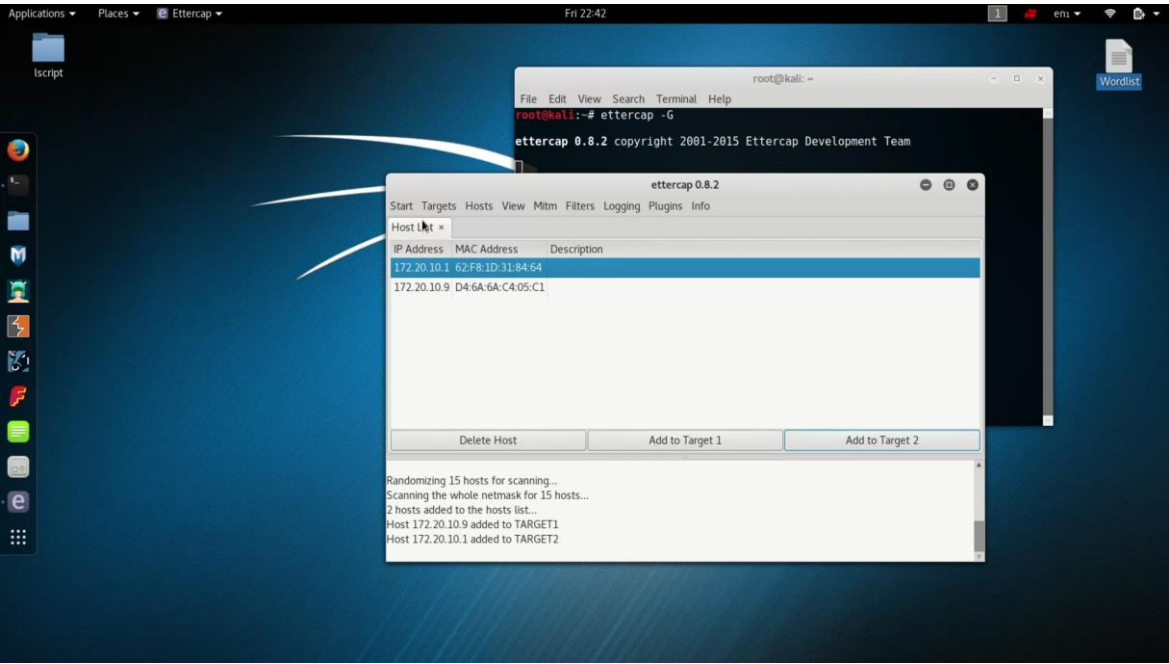


Figure 33 - Man-in-the-middle attack (5)

Figure 34 below shows the next stage of the attack starting the ARP poisoning. The author had to click sniff remote connections and then the attack will begin.

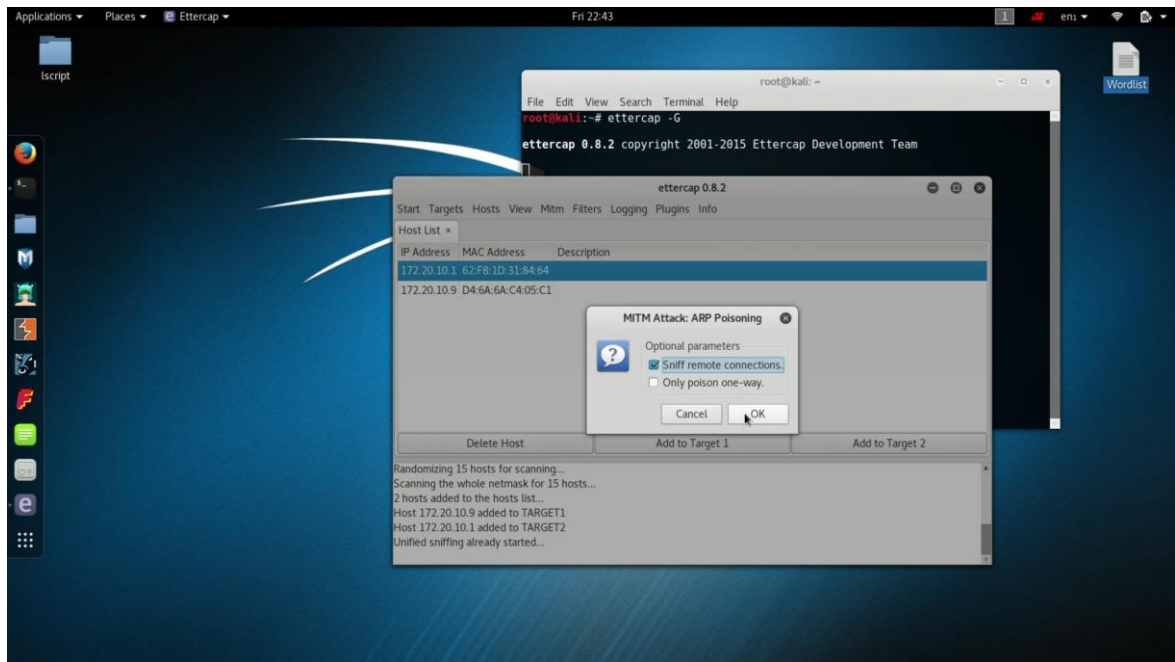


Figure 34 - Man-in-the-middle attack (6)

Figure 35 below shows the next step of the attack is to open a new terminal and type in the command to open driftnet. This is done using the command “driftnet -i wlan0”.

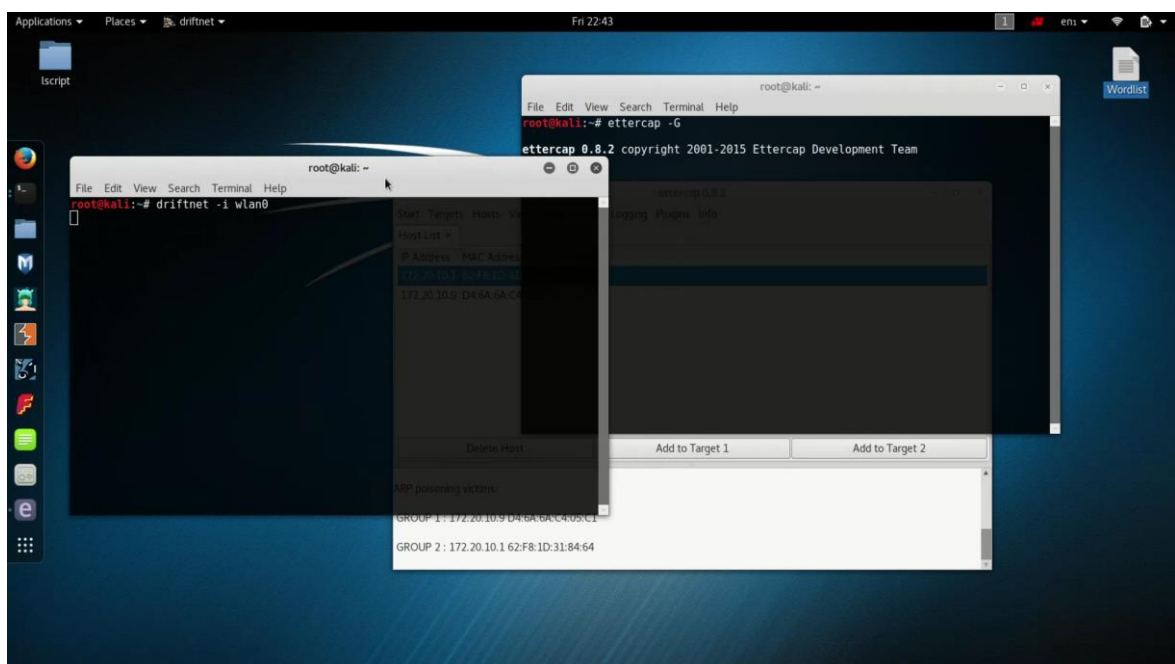


Figure 35 - Man-in-the-middle attack (7)

Figure 36 below shows the client traffic, this is from the different websites that are visited. The attack is then designed to show the images within the driftnet screen. Figure 36 provides the author with evidence that the attack was successful.

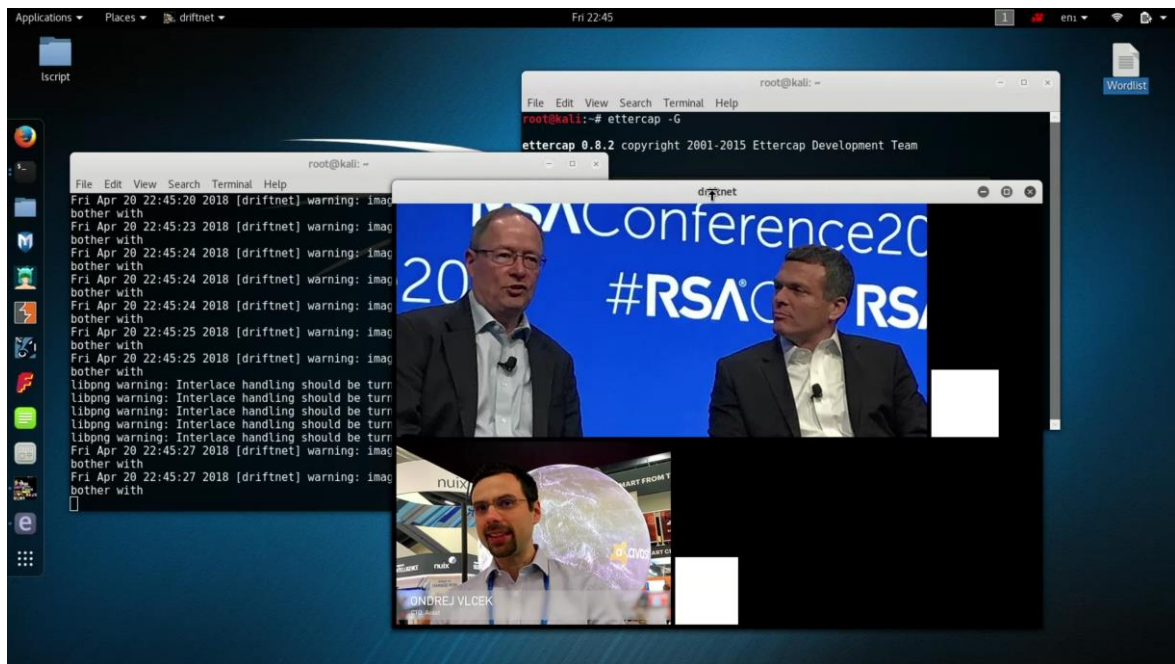


Figure 36 - Man-in-the-middle attack (8)

5.3.1 Conclusion

In conclusion the author believes that the man-in-the-middle attack was successful. The author demonstrated how this type of attack can be used to gather images from unsecure websites that the clients browse on. The author has identified several solutions within the research in chapter two. However, the author would recommend using a virtual private network to prevent this type of attack. A virtual private network does not totally block all man-in-the-middle attacks, but it will stop any attacks happening between the home router and the virtual private network gateway.

5.4 Port scanning

In this section of the report the author will be performing port scanning on the home network. The idea behind this attack is to find the different vulnerabilities within the network. Different devices will have different ports open for different reasons, the author will explain what ports are open and look at what solutions can be made.

Figure 37 below shows the first step that needs to be taken when performing a port scan. This is to create a ping scan, this will enable the attacker to find what devices are within the network. The ping scan was performed and the author found all 14 devices that are connected to the network.

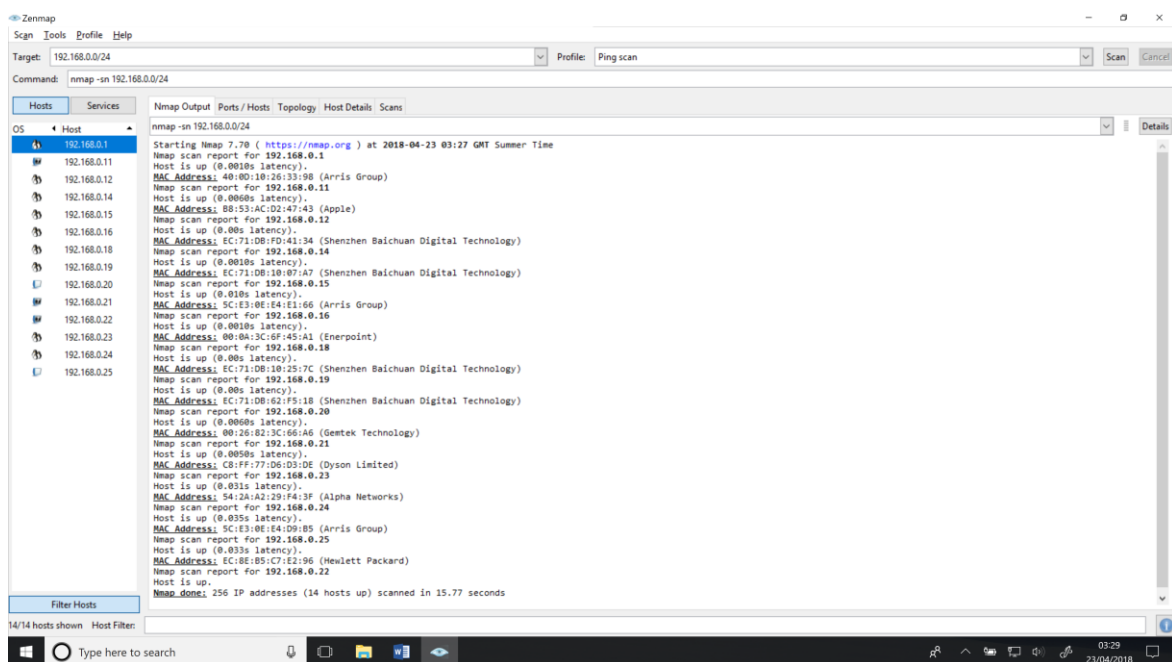


Figure 37 – Port scanning (1)

Figure 38 below shows the results from the network scan. The author chose to scan the wireless router to see if there were any weaknesses within this device. The wireless router has an IP address of 192.168.0.1.

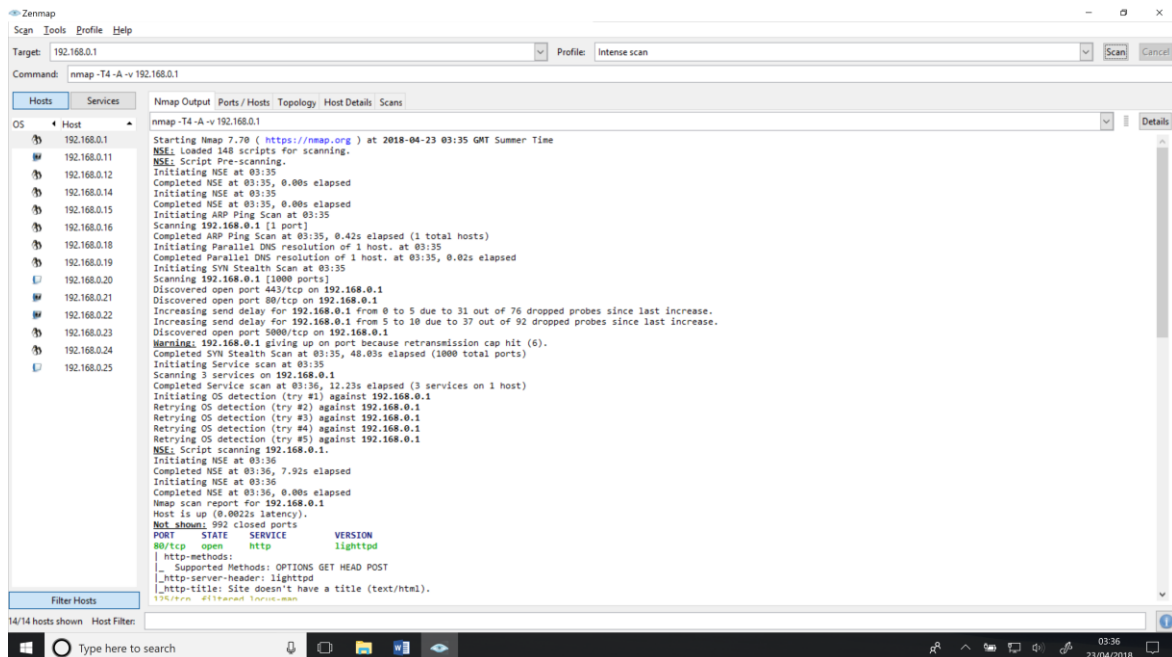


Figure 38 – Port scanning (2)

Figure 39 below shows the remaining results from the wireless router scan. The author can see that port 5000 is open, this is the first vulnerability within the network that has been found.

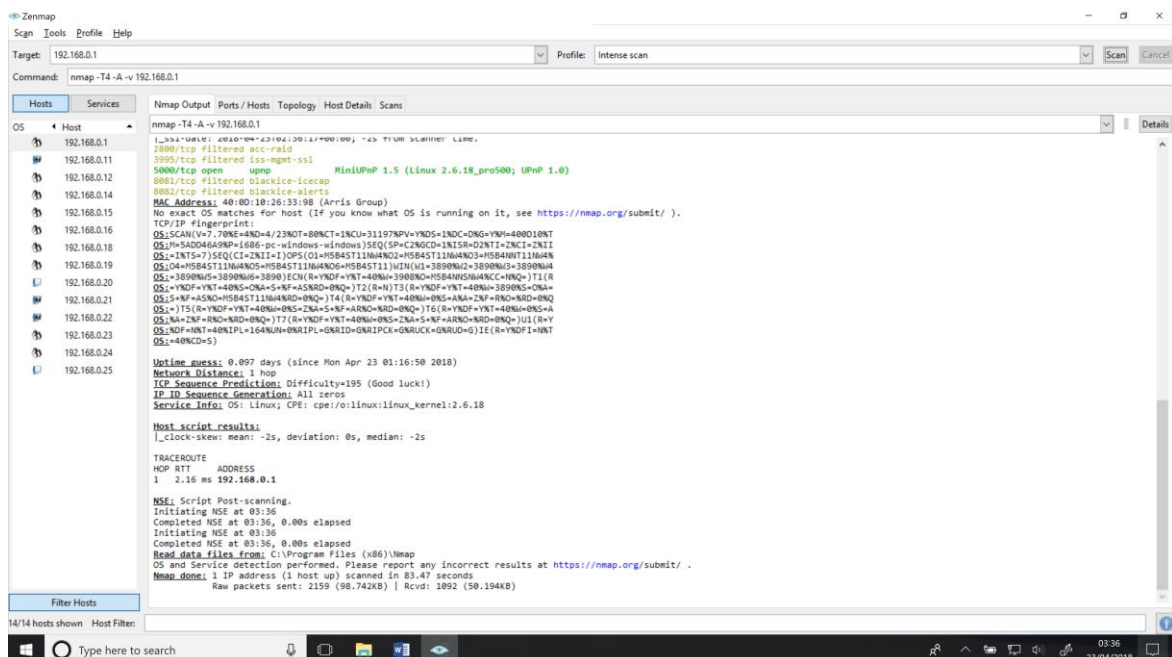


Figure 39 - Port scanning (3)

Figure 40 below shows the results from scanning the Dyson fan that is installed within the network, this device has an IP address of 192.168.0.21. The scan has demonstrated that this device is secure by all 1000 tested ports being closed.

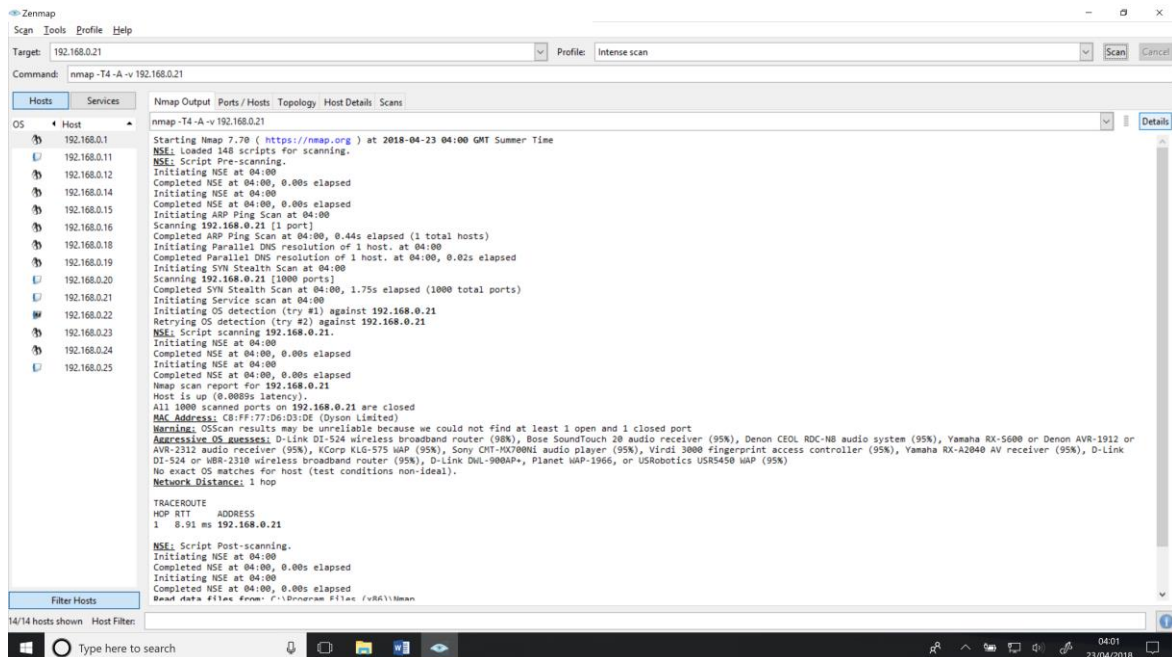


Figure 40 – Port scanning (4)

Figure 41 below shows the remaining results from the scan on the Dyson fan. The author was unsure if the device was safe as there is no anti-virus or firewall that can be installed. However, these results provide clear evidence that the device is safe.

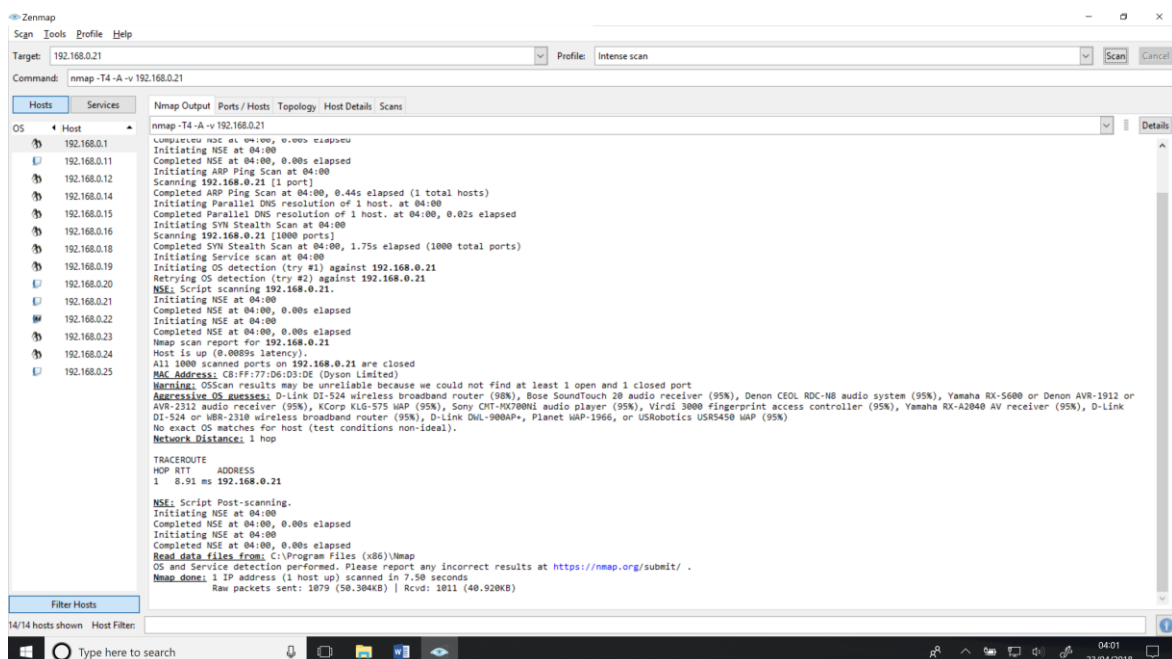


Figure 41 – Port scanning (5)

Figure 42 below provides the results from the scan on the laptop on the network with the IP address 192.168.0.22. The author had a theory that this would be one of the most secure devices within the network. The reason for this is this device has a strong firewall to protect it from being attacked within this manner. The scan results provide clear evidence of this by showing all 1000 scanned ports are filtered by the firewall. The scan did not reveal information about the device, that the same scan on other devices did. This again provides clear evidence that a strong firewall can prevent this type of attack.

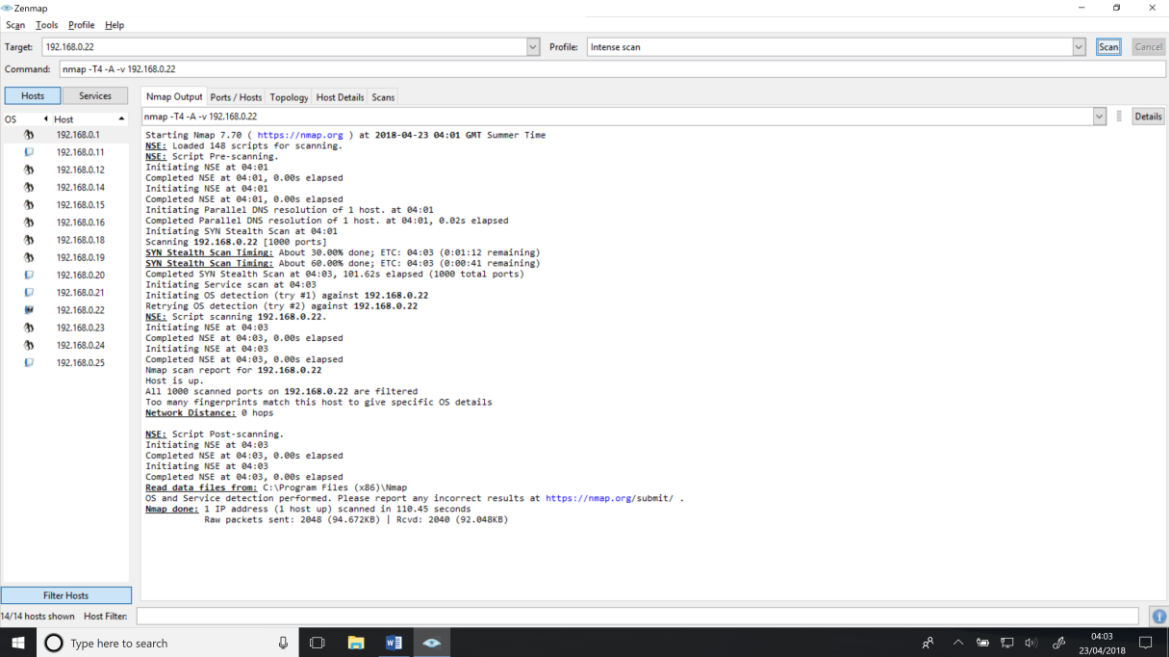


Figure 42 – Port scanning (6)

Table 3 below is used to document the port scanning that was performed within the network. It is used to show any open ports within the network, this will then allow the author to investigate ways of securing the open ports. The author has made two classifications' secure or insecure. A secure device is any device that has been scanned with two or less ports open. An insecure device is any device that has been scanned with more than two open ports. Devices with more than two open ports need to be looked at in more detail to investigate how to secure them. The table is used to document every device name, IP address, open ports, and security classification. Once the table is completed the author will discuss the findings and provide a solution to secure any insecure devices.

Device Name	IP address	Open Ports	Secure or Insecure
Virgin Media Super Hub	192.168.0.1	80, 5000	Secure
HP laptop	192.168.0.22	None	Secure
Phillips television	192.168.0.23	2323, 8000, 49154	Insecure
HP printer	192.168.0.25	80, 443, 515, 631, 8080, 9100, 9220	Insecure
Dales TiVo box	192.168.0.15	443, 1503, 2191, 49152	Insecure
Main TiVo box	192.168.0.24	443, 1503, 2191, 49152	Insecure
Dyson Fan	192.168.0.21	None	Secure
iPhone	192.168.0.11	62078	Secure
HP desktop	192.168.0.20	135, 139, 445	Insecure
CCTV System	192.168.0.12	85, 9000	Secure
CCTV Camera 1	192.168.0.14	554, 6001, 800, 900	Insecure
CCTV Camera 2	192.168.0.16	554, 6001, 800, 900	Insecure
CCTV Camera 3	192.168.0.18	554, 6001, 800, 900	Insecure
CCTV Camera 4	192.168.0.19	554, 6001, 800, 900	Insecure

Table 3 – Port scanning

The scan has identified that there are only two devices within the network with no open ports, this provides clear evidence that these are very secure devices. Additionally, the scan has identified three more secure devices with two or less ports open. However, the scan has identified eight insecure devices within the network. These are devices with more than two ports open, these devices will need additional security mechanisms to ensure that they are safe. The author will provide details of this future work in chapter six.

5.4.1 Conclusion

The author believes that the port scanning attack has been very successful in identifying security vulnerabilities within the network. The solution to this issue that the author would provide is a strong firewall before the traffic enters or exits the network, this should help in preventing unauthorised access to the network.

5.5 Conclusion

In conclusion the author believes that this chapter has been very successful. All of the attacks demonstrated weaknesses within the network and the author has provided at least one solution to each of the issues. However, the port scanning attack identified an area for future research. This is to identify different ports by their uses and research methods of securing each of the open ports to provide a more secure home network.

Chapter 6 - CONCLUSIONS AND RECOMMENDATIONS

This section of the report will provide a summarisation of the work that has been completed within the project. It will then conclude and discuss if the project was successful. This chapter will then provide recommendations for further work.

6.1 Summary

The project was based upon building a secure home network. Chapter two provided the author with research that was required to complete the project. This was very helpful as it assisted the author with background knowledge to complete the project. Chapter three provided a clear and structured methodology for the project to be conducted. This ensured that the author had a clear idea of what was required at each stage of the project.

Chapter four was used to create a design and implement the network. This chapter was an essential part of the project, without it the project would have not been completed. It provided the author with a network that could be used to conduct the experiment's on. Chapter five covers the main section of the document, testing and evaluation. In this chapter the author conducted three experiment's WPA2 password cracking, man-in-the-middle attack, and port scanning. Conducting these experiments allowed the author to find the vulnerabilities within the network and provide solutions for each of the vulnerability's. Doing this allowed the author to achieve the aim that was set out at the start of the project.

6.2 Conclusion

This section of the report will look at the aim of the project and see how each chapter relates to these. This will enable the author to come to a definitive conclusion on if the project was successful. The aim of this project was set out in chapter one, the aim of this project was to build a home network that can be used to conduct experiments to find the vulnerabilities and provide solutions to secure the network.

Chapter two was used to give the author background knowledge on network devices, network threats, and network security and related work. This enabled the author to conduct the project with the appropriate knowledge that was required to meet the aim set out.

Chapter three was used to research a methodology that was suitable to conduct the project upon. The author used the research onion to build the methodology as this was one of the most suitable methodologies for the project. This then give the author a plan of exactly what was required and how to successfully achieve the aims. Chapter four was used to design and implement the network enabling the author to continue onto chapter five to conduct the experiments.

Chapter five was used for the testing and evaluation for the project. In this section of the report the author was able to successfully conduct three separate experiment's. Each experiment was designed to find vulnerabilities within the network, this enabled the author to provide solutions on how to secure the network from these attacks. Overall the author believes the project met the aim and objectives that were set out in chapter one. This demonstrates that the overall outcome of the project was successful, as the author achieved everything that was set out at the beginning of the project.

6.3 Recommendations for Future Research

This project has enabled the author to several different arears for future research, however the author is going to talk about the two most significant areas for future research. The first recommendation for future research is to research Kali Linux. This will enable the author to have a better understanding of different commands that the author could use to conduct future work. The second recordation that the author will provide is to continue this project. Technology is changing daily, this means threats and vulnerabilities are changing constantly. The author would like to conduct further research on different experiment's that can be conducted to find additional vulnerabilities within the network. This will enable the author to further improve the security on home networks.

Chapter 7 – Reflections

7.1 Introduction

This chapter is used to discuss how the project went. This chapter will cover both the positives and the negatives of the project and come to an overall conclusion. The positives of the project will cover what sections of the project went well and how did they go so well. The negatives of the project will cover what did not go that well and what went wrong. The conclusion will then discuss how the project met the aim and objectives and what could have been improved.

7.2 Positives

The author found chapter two was a huge benefit to this project. Chapter two provided the background knowledge to enable the author to undertake the different sections required to finish the project successfully. Chapter three was additionally very helpful in providing the author with a detailed action plan of exactly what needed to be done to progress through the project. The author feels without a detailed plan of what had to be done, work could have been done incorrectly. However, this was not the case as chapter three plan and the Gantt chart covered what needed to be done and when it had to be done.

Time management was another positive aspect within the project as the author knew what had to be done and when it had to be done by, this enabled the author to ensure that the project was finished on time. The final positive aspect that the author is going to talk about is the attacks. In chapter five the author conducted three attacks. These were WPA2 password cracking, port scanning, and man-in-the middle attacks. The attacks were all very successful in providing the author with vulnerabilities within the network.

7.3 Negatives

The first negative aspect that the author would like to discuss is the evaluation in chapter five. Generally, time management was a positive aspect of this project. However, as the author was ill during the period that was set out by the Gantt chart it delayed the project by one week. It did stop the author from finishing before the deadline as when planning the Gantt chart, the author left three weeks between the finish of the project and deadline to allow for any delays.

The second negative point that the author would like to discuss is Kali Linux. The author did not have enough experience at using the operating system to complete the experiment's. This forced the author to conduct additional research on how to conduct the attacks, the author should have added a section on how to do some of these attacks in chapter two. This would have allowed the author to conduct more attacks therefore, it would have improved the outcome of the project.

The last point that the author would like to discuss is not attending as many project meetings as the author should have. If the author had attended more of the project meetings, there would have been additional guidance on how to improve the project. If the author was to conduct another project this is one mistake that would not be made again.

7.4 **Objectives**

In chapter one the author set out five different objectives, this section of the report will look at how each objective completed during the project. The first objective was "Research different devices that are in home networks". This was covered in chapter 2.3 network devices. This section of the research gave a brief description of different devices that are generally used within home networks. The second and third objectives were "Research threats/vulnerabilities and solutions for the identified threats". This was covered again within the research section of the project in chapter 2.4 network threats. It discussed what the threat was, example attacks, and provided at least one solution to each attack.

The fourth objective that has been completed is "design and implement a home network". This was covered within chapter four of the project. This section was used to plan the network and then document the implementation of the network. The final objective that has been completed is "Conduct the experiment by completing the attacks". This objective was completed in chapter five, where the author conducted three different attacks and then provided at least one solution to prevent each of the attacks.

7.5 **Conclusion**

Overall the author feels that the project was conducted successfully. The author achieved the aim and objectives that were set out during chapter one. The project could have been improved, by adding more attacks and getting more guidance by attending more project meetings. In any future projects the author will obtain all the guidance possible to improve the quality of the work that is completed.

Chapter 8 – REFERENCES

- [1] J. Waleed, "Smart Home as a New Trend , a Simplicity Led to Revolution," *Int. Sci. Conf. Eng. Sci. - 3rd Sci. Conf. Eng. Sci.*, pp. 30–33, 2018.
- [2] Cisco, "Cisco Visual Networking Index: Forecast and Methodology, 2016–2021," 2017.
- [3] J. Ahamed and A. V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities," in *2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, 2016, pp. 1–5.
- [4] C. Drubin, "More than Half a Billion Wireless Smart Home Monitoring Devices to be Installed Worldwide by 2018 - ProQuest," *Microw. J.*, no. May 2014, p. 2018, 2014.
- [5] "man-in-the-browser-attack.png (1103×523)." [Online]. Available: <https://securebox.comodo.com/theme/images/man-in-the-browser-attack.png>. [Accessed: 24-Apr-2018].
- [6] R. Rogowski, M. Morton, F. Li, F. Monroe, K. Z. Snow, and M. Polychronakis, "Revisiting Browser Security in the Modern Era: New Data-Only Attacks and Defenses," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2017, pp. 366–381.
- [7] K. Sai and A. Ayyagari, "Man in the Browser Attacks," 2017.
- [8] Chris Cain, "Analyzing Man-in-the-Browser (MITB) Attacks," pp. 1–23, 2014.
- [9] "ddos-reflectorattacks1.png (1134×768)." [Online]. Available: <http://oversitesentry.com/wp-content/uploads/2015/07/ddos-reflectorattacks1.png>. [Accessed: 24-Apr-2018].
- [10] R. Rabie and M. Drissi, "Applying sigmoid filter for detecting the low-rate denial of service attacks," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 2018, pp. 450–456.
- [11] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–10, 2018.
- [12] V. Adat, A. Dahiya, and B. B. Gupta, "Economic incentive based solution against distributed denial of service attacks for IoT customers," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1–5.
- [13] M. C. Ghanem and D. N. Ratnayake, "Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by

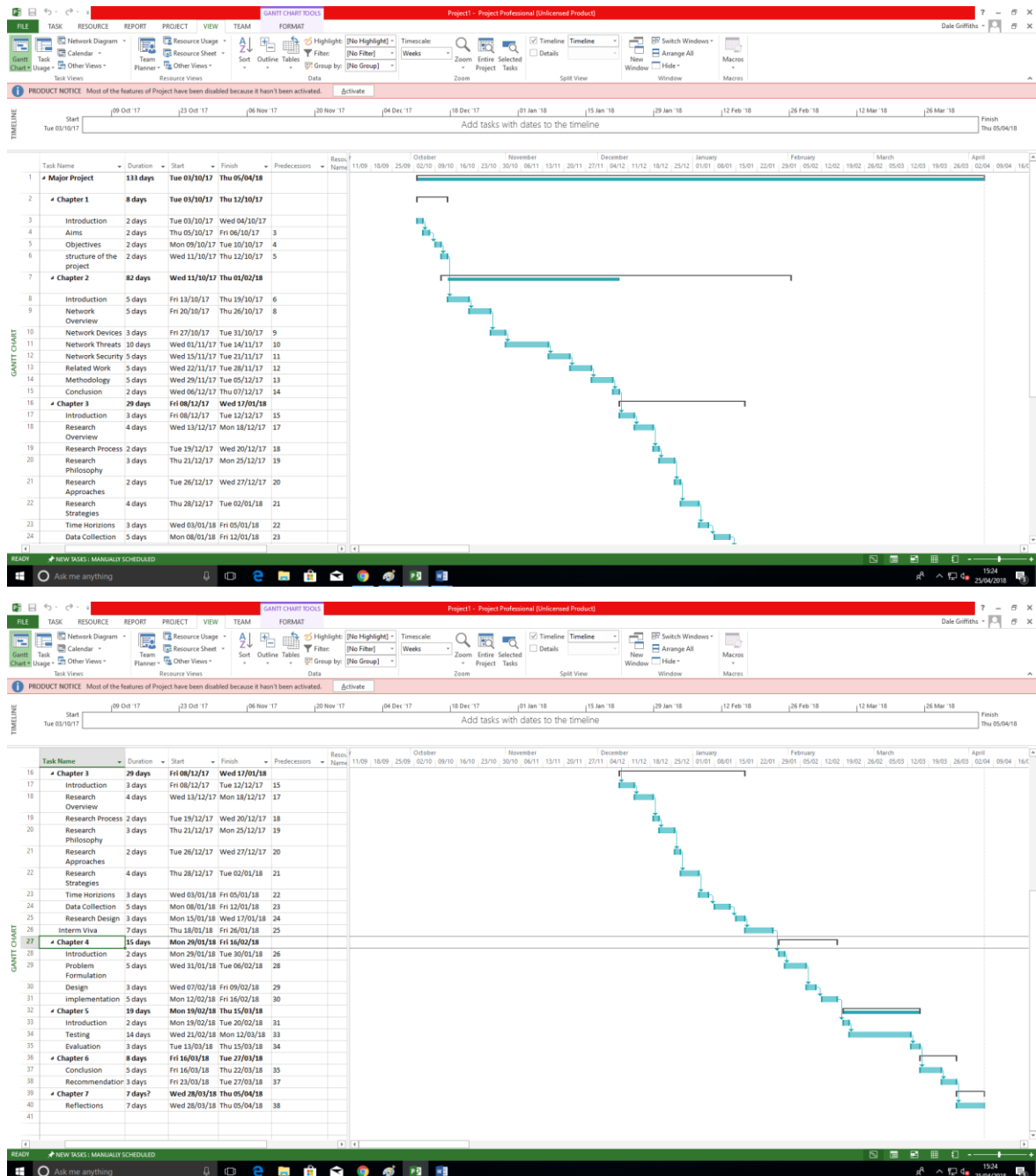
- brute-force attack a novel re-authentication protocol,” in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, 2016, pp. 1–7.
- [14] D. C. Grant, “Distributed detection and response for the mitigation of distributed denial of service attacks,” in *2018 International Conference on Information Networking (ICOIN)*, 2018, pp. 495–497.
- [15] S. Bhowal, S. R. Dutta, and S. Mitra, “An efficient reduced set brute force attack technique for a particular steganographic tool using vername algorithm,” in *2017 Fourth International Conference on Image Information Processing (ICIIP)*, 2017, pp. 1–4.
- [16] K. S. M. Moe and T. Win, “Improved hashing and honey-based stronger password prevention against brute force attack,” in *2017 International Symposium on Electronics and Smart Devices (ISESD)*, 2017, pp. 1–5.
- [17] “googlemalwareattack.jpg (661×496).” [Online]. Available: <https://www.drupalaid.com/sites/default/files/assets/images/webform-malware/googlemalwareattack.jpg>. [Accessed: 24-Apr-2018].
- [18] C. Kotkar and P. Game, “Prevention mechanism for prohibiting SMS malware attack on android smartphone,” in *2015 Annual IEEE India Conference (INDICON)*, 2015, pp. 1–5.
- [19] B. Min and V. Varadharajan, “Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT),” in *2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS)*, 2015, pp. 80–89.
- [20] M. Rafiq, M. S. Arif, A. Raza, and M. O. Ahmad, “Numerical modeling of virus outbreak in a computer network with limited anti-virus ability,” in *2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2018, pp. 415–421.
- [21] M. A. Sheta, M. Zaki, K. A. E. S. El Hadad, and H. A. M, “Anti-spyware Security Design Patterns,” in *2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)*, 2016, pp. 465–470.
- [22] D.-Y. Kim, G.-Y. Choi, and J.-H. Lee, “White list-based ransomware real-time detection and prevention for user device protection,” in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1–5.

- [23] *IEEE-SA Industry Connections & AMTSO Mobile Adware Guidelines : IEEE-SA Industry Connections and AMTSO Mobile Adware Guidelines - Version 1.0.* IEEE, 2015.
- [24] S. Jing, Q. Qi, R. Sun, and Q. Li, "Study on VPN Solution Based on Multi-campus Network," in *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, 2016, pp. 777–780.
- [25] S. Raje, S. Vaderia, N. Wilson, and R. Panigrahi, "Decentralised firewall for malware detection," in *2017 International Conference on Advances in Computing, Communication and Control (ICAC3)*, 2017, pp. 1–5.
- [26] N. Maheshwari and H. Dagale, "Secure communication and firewall architecture for IoT applications," in *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, 2018, pp. 328–335.
- [27] L. Ge, L. Wang, and L. Xu, "A Method for Cracking the Password of WPA2-PSK Based on SA and HMM," in *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*, 2016, pp. 59–62.
- [28] M. M. Hafiz and F. H. Mohd Ali, "Profiling and mitigating brute force attack in home wireless LAN," in *2014 International Conference on Computational Science and Technology (ICCST)*, 2014, pp. 1–6.
- [29] T. Maurin, L.-F. Ducreux, G. Caraiman, and P. Sissoko, "IoT security assessment through the interfaces P-SCAN test bench platform," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2018, pp. 1007–1008.
- [30] H. Al-Alami, A. Hadi, and H. Al-Bahadili, "Vulnerability scanning of IoT devices in Jordan using Shodan," in *2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS)*, 2017, pp. 1–6.
- [31] "The-research-process-onion-Saunders-et-al-2003.jpg (610×311)." [Online]. Available: https://www.researchgate.net/profile/Jesus_Mascareno/publication/277753340/figure/fig1/AS:395655043403777@1471342921168/The-research-process-onion-Saunders-et-al-2003.jpg. [Accessed: 19-Apr-2018].
- [32] "kali-linux-sensorstechforum.png (1024×768)." [Online]. Available: <https://sensorstechforum.com/wp-content/uploads/2017/07/kali-linux-sensorstechforum.png>. [Accessed: 25-Apr-2018].

APPENDICES

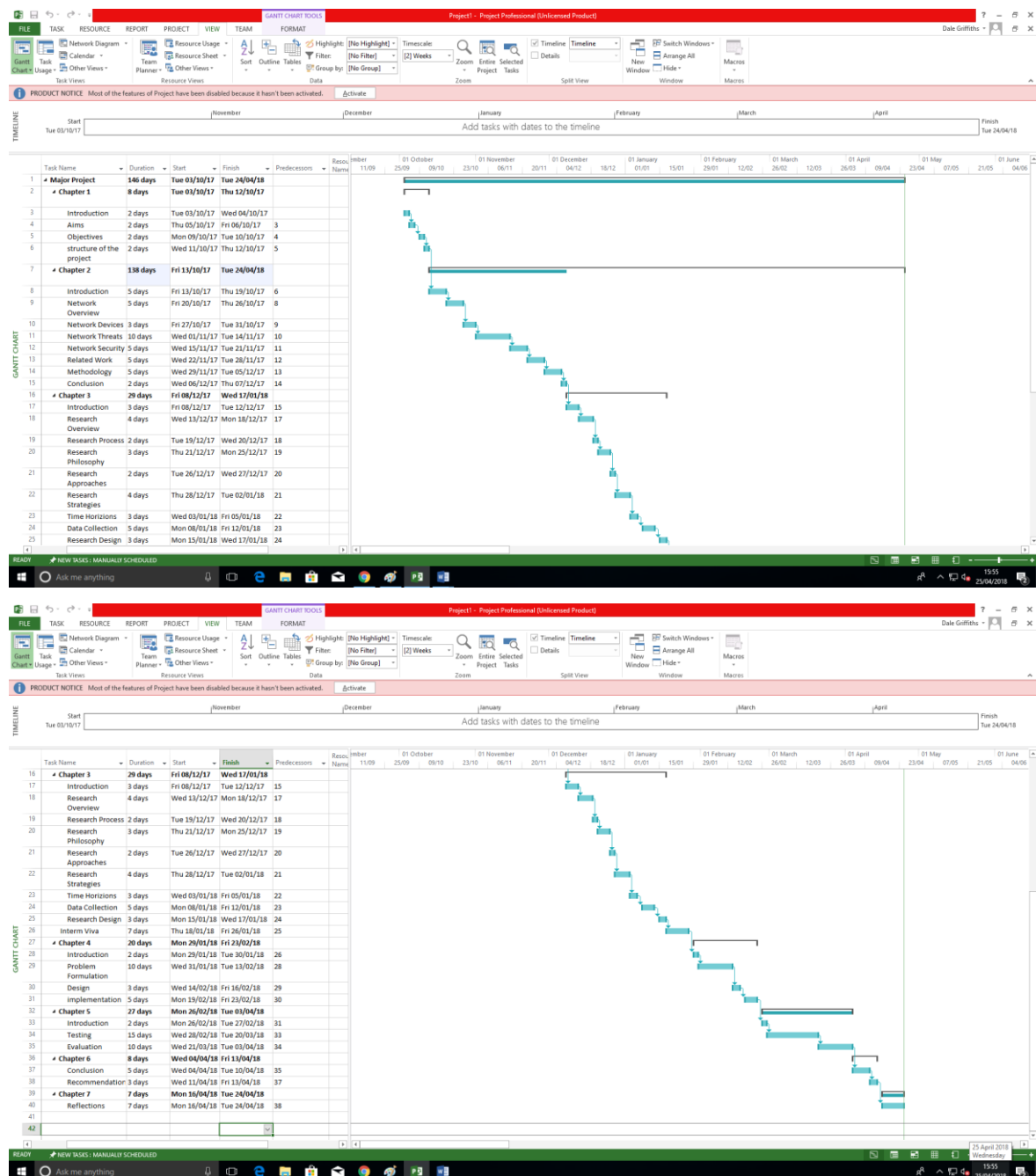
PROJECT MANAGEMENT

Original Gantt chart



Form the original Gantt chart when the original project plan was created the author should have finished on the 05/04/2018. However, it can be seen in the revised Gantt chart below that some things did not finish on time. This did not mean the project was not finished in time for the deadline just it was finished on the 24/04/2018 instead of the original date.

Revised Gantt Chart



Methodology

The author believes that the onion that was used to create the project methodology helped them during the project. It was very good in providing a clean plan of exactly how each step of the process had to be completed. The Gantt chart additionally went alongside the methodology set out in chapter three to ensure that the project was completed before the deadline.