



A Study of the Design and Implementation of a Secure Enterprise Network

by
Dale Griffiths

Supervisor: Carlene Campbell
Second Marker: Kapilan Radhakrishnan

Project submitted as part of the requirements for the award of MSc Computer Networks and
Security

September 2019

DECLARATION

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 has not previously been accepted as part of any other Masters' submission.

Signed: D.S.Griffiths

Date: 19/09/2019

FORM OF CONSENT

I Dale Scott Griffiths hereby consent that my Project, submitted in candidature for the M.Sc. Computer Networks and Security, 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: D.S.Griffiths

Date: 19/09/2019

Abstract

This project was based on the design and implementation of a secure enterprise network. Firstly, the report covered related work and provide the author with the required information related to complete the author's project. The project then investigates a methodology that was used by the author to support the design and implementation and results. The design and implementation chapter are used to document the building of the enterprise network this provided the author with a testbed network to conduct the experiments within a safe environment. The next stage of this project was to complete the experiments and implement solutions to the identified vulnerabilities. The report is then concluded and investigated the outcome of the project to be successful.

Table of Contents

Abstract.....	3
Chapter 1 – Introduction	10
1.2 Aim	10
1.3 Objectives.....	10
1.4 Project Structure.....	10
1.4.1 Chapter One	11
1.4.2 Chapter Two.....	11
1.4.3 Chapter Three	11
1.4.4 Chapter Four.....	11
1.4.5 Chapter Five	11
1.4.6 Chapter Six	11
Chapter 2 – Literature Review	12
2.1 Introduction.....	12
2.2 Enterprise Networks.....	12
2.3 Network Devices.....	12
2.3.1 Routers	12
2.3.2 Switches.....	13
2.3.4 Access Points & Wireless Controllers	13
2.3.5 Servers & End Devices	13
2.4 Network Threats	14
2.4.1 Viruses & Worms.....	14
2.4.2 Drive-by Download Attacks	15
2.4.3 Botnets.....	16
2.4.4 Phishing Attacks.....	17
2.4.5 Ransomware	18
2.4.6 VLAN Hopping Attack.....	19
2.5 Network Defences & Countermeasures	20
2.5.1 Firewall	20
2.5.2 Intrusion Prevention System.....	21
2.5.3 Intrusion Detection System	21
2.5.4 Encryption	22
2.5.5 Virtual Private Network.....	23
2.5.6 Anti-Virus & Anti-Malware.....	24
2.5.7 Physical Security	25
2.5.9 Email Security	26

2.5.10 VLAN Segmentation	27
2.5.11 Wireless Security	28
2.5.12 Access Control	29
2.5.13 Data Loss Prevention	30
2.6 Related Work	31
2.7 Conclusion	31
Chapter 3 – Research Methodology	32
3.1 Introduction	32
3.2 Research Overview	32
3.2.1 Research Philosophy	32
3.2.2 Research Approach	32
3.2.3 Research Strategies	33
3.2.4 Time Horizons	33
3.2.5 Data Collection Methods	33
3.3 Research Deliverables	34
3.4 Triangulation	34
3.5 Conclusion	34
Chapter 4 – Design & Implementation	35
4.1 Introduction	35
4.2 Problem Formulation	35
4.3 Design	35
4.4 Implementation	36
4.4.1 Core Switch Configuration	37
4.4.2 Distribution Switch Configuration	37
4.4.3 Access Layer Switches	38
4.4.4 Adaptive Security Appliance	38
4.4.4 Wireless Access Point	39
4.4.5 Virtual Private Network	40
4.5 Conclusion	40
Chapter 5 – Results and Findings	41
5.1 Introduction	41
5.2 Vlan Hopping Attack	41
5.3 Wi-Fi Password Cracking	45
5.4 Conclusion	48
Chapter 6 – Conclusion & Recommendations	49
6.1 Introduction	49
6.2 Summary	49

6.3 Conclusion	49
6.4 Recommendations for Future Research	50
Chapter 7 – Reflections	51
7.1 Introduction.....	51
7.2 Positives.....	51
7.3 Negatives	51
7.4 Objectives.....	51
7.5 Conclusion	52
References.....	53
Appendices.....	59

List of Figures

Figure 1 - Virus & Worm [4]	14
Figure 2 - Drive-by Download Attack [8]	15
Figure 3 – Botnet [12].....	16
Figure 4 - Phishing Attacks [18].....	17
Figure 5 – Ransomware [22].....	18
Figure 6 - VLAN Hopping Attack [28]	19
Figure 7 – Firewall [29]	20
Figure 8 - Intrusion Prevention & Detection Systems [38]	21
Figure 9 – Encryption [44].....	22
Figure 10 - Virtual Private Network [49]	23
Figure 11 - Anti-Virus & Anti-Malware [54]	24
Figure 12 - Physical Security [59]	25
Figure 13 - Email Security [60]	26
Figure 14 - VLAN Segmentation [64]	27
Figure 15 - Wireless Security [67].....	28
Figure 16 - Access Control [72].....	29
Figure 17 - Data Loss Prevention [77].....	30
Figure 18 - Research Onion [82]	32
Figure 19 - Network Blueprint.....	36
Figure 20 – Core Switch Configuration.....	37
Figure 21 – Distribution Switch Configuration	37
Figure 22 – Access Switch Configuration	38
Figure 23 – Adaptive Security Appliance Configuration	38
Figure 24 – Wireless Access Point (1).....	39
Figure 25 – Wireless Access Point (2).....	39
Figure 26 – Virtual Private Network	40
Figure 27 - Vlan Hopping Attack (1).....	41
Figure 28 - Vlan Hopping Attack (2).....	41
Figure 29 - Vlan Hopping Attack (3).....	42
Figure 30 - Vlan Hopping Attack (4).....	42
Figure 31 - Vlan Hopping Attack (5).....	43
Figure 32 - Vlan Hopping Attack (6).....	43
Figure 33 - Vlan Hopping Attack (7).....	44
Figure 34 - Vlan Hopping Attack (8).....	44
Figure 35 – Wi-Fi Password Crack (1)	45
Figure 36 – Wi-Fi Password Crack (2)	45
Figure 37 – Wi-Fi Password Crack (3)	46
Figure 38 – Wi-Fi Password Crack (4)	46
Figure 39 – Wi-Fi Password Crack (5)	47
Figure 40 – Wi-Fi Password Crack (6)	47
Figure 41 –Gantt Chart (1).....	59
Figure 42 –Gantt Chart (2).....	59

List of Tables

Table 1 - Data Collection Methods.....	33
Table 2 - IP Addressing	35
Table 3 - Device List.....	36

ACRONYMS

Quality of Service – (QoS)
Demilitarized Zone – (DMZ)
Virtual Local Area Network – (VLAN)
Wireless Access Point – (WAP)
Intrusion Detection System – (IDS)
Intrusion Prevention System – (IPS)
File Transfer Protocol – (FTP)
Simple Network Management Protocol – (SNMP)
Rivest-Shamir-Adleman – (RSA)
Advanced Encryption Standard – (AES)
Internet Service Provider – (ISP)
Transport layer security – (TLS)
Point to point tunnelling protocol – (PPTP)
OpenVPN, Secure Socket Layer – (SSL)
IP Security – (IPsec)
Closed-Circuit Television Systems – (CCTV)
Mandatory Access Control – (MAC)
Discretionary Access Control – (DAC)
Role-based Access Control – (RBAC)

Chapter 1 – Introduction

1.1 Introduction

This chapter is used by the author to demonstrate the background knowledge of the project building a secure enterprise-class network. The first section of the report will be the design and implementation of the enterprise-class network and then testing the security of the network. This chapter will then discuss the author's research aims required to implement a solution for the scenario. The chapter will then move on to discuss the objectives outlined by the author before covering the structure that will be used for this report.

This project has been designed by the author to implement an enterprise network and then secure the network from several threats. The author is aiming to implement solutions to the identified threats to secure the network and the data stored on the network from unauthorized access. Threats are always evolving, and this means that no network can ever be completely safe. There will be several different types of research for the project, these include journals, articles, papers, and other online resources provide the author with information relating to this project. The background knowledge will be used to provide several threats and solutions that are commonly used to attack networks. The author will then investigate survey papers that will outline a selection of several tools that be used within the project. The next stage is to investigate technical papers to find related work that has been conducted by different authors in the past, providing a potential method for this project to be conducted upon.

1.2 Aim

The aim of this project is to design and implement an enterprise-class network with a minimum of 30 networking devices. Therefore, allowing the experiments to be conducted on allowing weaknesses within the network to be identified. Therefore, allowing solutions to be implemented to secure the network.

1.3 Objectives

The project objective is to investigate enterprise-class networks and vulnerabilities to implement solutions to prevent these attacks from happening on the network.

- Research enterprise-class networks
- Research networking devices
- Investigate several vulnerabilities and solutions to be used for the project
- Plan and implement an enterprise-class network that consisting of more than 30 networking devices
- Conduct experiments and configure solutions to secure the network

1.4 Project Structure

This report is essentially separated into two sections, firstly the literature review this will focus on enterprise network devices and what vulnerabilities and solutions are commonly used by attackers to obtain unauthorized access. The next section will be used to design, implement and conduct experiments to investigate the vulnerabilities that are in the network. This then allows the author to implement preventative measures to secure the network from the vulnerabilities. The author will then conduct a comparison between the experiments and the literature review to understand if the experiments are successful or not. The final stage of this project is to investigate if the aim and objectives are achieved, this will provide the author with an outcome of if the project is successful or not.

1.4.1 Chapter One

Chapter one provides a brief overview of the report, it outlines the author's aim and objectives during the project. This chapter additionally provides a report structure to outline exactly what should be completed to achieve a successful outcome from the project. Upon completion of the project, the author can verify that the aim and objectives have been successfully met, demonstrating how successful the project was.

1.4.2 Chapter Two

Chapter two provides the author with a section of the report to document information that has been researched as part of this project. This will include information on enterprise-class networks and vulnerabilities and solutions, commonly used to obtain authorized access to networks by attackers. This chapter will then investigate related work to provide the author with previous work that has been conducted, giving the author additional information on how to improve the outcome of the project.

1.4.3 Chapter Three

Chapter three provides a research methodology for the project. This includes the research philosophy, research approach, research strategy, time horizons, and data collection methods that can be used by the author for the project. This provides the author with a clear methodology for the project to be completed upon, ensuring a successful outcome.

1.4.4 Chapter Four

Chapter four is utilized by the author to document the design process and the implementation required to complete the project. The design section will cover the network design and planning process, this will include what devices will be included within the network. It will also cover the blueprint for the network, this is how the author would like the network to be and how different devices should communicate. The implementation chapter will document the installation process of the devices, network, and software to complete the network build.

1.4.5 Chapter Five

Chapter five provides the author with a section to document the testing and evaluation of the project. The testing section will document what experiments the author has carried out and how each experiment has been conducted. The report will then move onto the evaluation section where the author will evaluate the results from the experiments and compare them to that investigated in chapter two to ensure the experiments were successful.

1.4.6 Chapter Six

Chapter six provides the author with a section to conclude the project, this will conclude all work and then provide a conclusion on if the project has been successful. The author will compare the work that has been done against the aim and objectives outlined at the beginning of the project to demonstrate if the project has been completed successfully.

Chapter 2 – Literature Review

2.1 Introduction

The author uses this chapter for the documentation of the research that has been conducted to enable the author to complete the project. The research covers why networks are important in any modern enterprise and what devices are used within an enterprise network. The research will then identify the latest and most common network attacks, these attacks will require the author to know solutions to enable defensive measures to be put in place to stop the attacks. The author will then identify related work, this will identify similar projects that have been conducted and relate to this project.

2.2 Enterprise Networks

[1]–[3] Enterprise networks are just like any other computer network however; they are larger than the general network. An enterprise network is essential to an enterprise as it enables access to company resources and a means of communication. This type of network is usually made up of multiple branches that communicate with each other and a central location where company data is stored. Security in an enterprise network is essential as it is part of the law to ensure that all data is both stored and transported in a secure manner. Additionally, enterprises have confidential company information stored within the network, therefore companies spend a fortune on network security.

Enterprise networks must be well planned when being designed as it is important to ensure that they are scalable if the company was to grow. If a network isn't scalable and there was an expansion, then it would require a completely new network. In enterprise networks, it is common to find the cisco hierarchal network layout as it is flexible and scalable.

2.3 Network Devices

Enterprise Networks differ from home networks as they consist of many devices. These include routers, switches, firewalls, access points, wireless controllers, servers, IP phones, and workstations. Enterprise networks must have the ability to manage traffic and forward it with a QoS, and all traffic must be forwarded in a secure manner to ensure data protection laws are complied with.

2.3.1 Routers

Routers are utilized to forward traffic between two or more networks, most commonly between a client and the service provider. Enterprise networks tend to have the use of a leased line for dedicated bandwidth to ensure the network performance is optimum. Home routers differ to enterprise routers as home routers have firewalls built-in however, enterprise networks have a separate device or software-based firewall to help secure the network. Additionally, in an enterprise network, a router is not utilized as a WAP, this is moved to access points within the network to provide better traffic management.

2.3.2 Switches

Switches are essential to enterprise networks, usually, there is a mixture of layer three switches for routing traffic and layer two switches for switching traffic within the network. Depending upon the network design sometimes layer 3 switches can be implemented instead of a router as it can handle more traffic and simplifies the network design, it can additionally be more cost-effective. Switches allow a network to be separated into multiple VLANs, these provide a smaller broadcast domain and separate network traffic. This helps to secure the network as not everyone can access all data, for example, a sales department wouldn't have access to an accounting department. Enterprise networks tend to have a three-layer design the core; this is where very high-performance switches like the Cisco 6500 series are based. The distribution layer is where again a high-performance switch is utilized like the Cisco 4500. Then the access layer tends to use lower performance switches like the Cisco 2960 & Cisco 3850. The reasoning behind this is how expensive high-performance switches are so they tend to be utilized as little as possible.

2.3.3 Firewalls

A firewall is a network device that can be used to secure a network, this is done by inspecting all network data that is being sent and received. The firewall will then allow or block traffic dependant on how its security rules are configured. Next-generation firewalls allow for additional security features and threat prevention that can detect known attacks and block them automatically. The solutions section of this chapter will cover firewalls in detail.

2.3.4 Access Points & Wireless Controllers

Access points are how wireless devices connect into the network. Enterprise networks tend to have lots of access points across each location to allow users to roam without losing connection. A wireless controller is what is utilized to manage all the access points. Trying to manage what could include hundreds of access points would be impossible however a wireless controller allows central management, status, grouping, and updates.

2.3.5 Servers & End Devices

Enterprise networks use servers to hold all the organisation's data as it allows it to easily be managed and backed up. Typically, enterprise networks will have high-performance servers that run multiple applications on each of them, the reasoning behind this is that servers are very expensive. Typical end devices in an enterprise network will include IP phones, workstations, laptops, tablets, and mobile phones. Modern-day networks must have the ability to allow connectivity and security to secure all different connections to the network. Selected users might need remote access to the network, this is when security considerations like a VPN should be used.

2.4 Network Threats

The author utilizes this chapter to analyse several common attacks being used to obtain unauthorized access to networks and systems. The research will provide the required knowledge to the author in the most recent and common attacks, this will enable the author to secure the network against several of these attacks.

2.4.1 Viruses & Worms

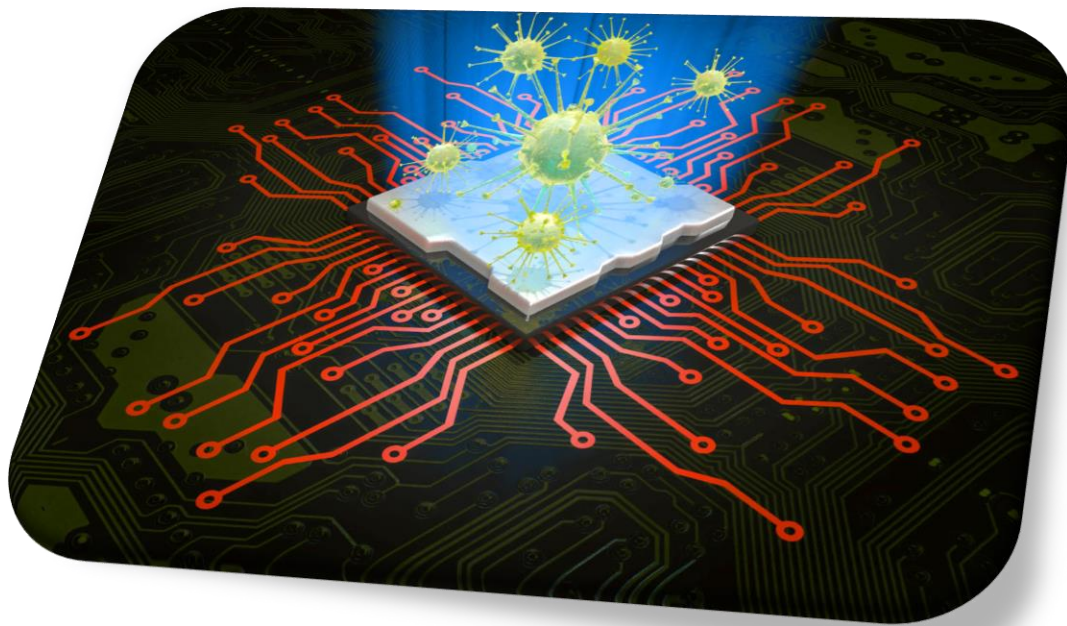


Figure 1 - Virus & Worm [4]

[5]–[7] A computer virus or worm is a piece of software that is written to infect files, documents, and systems. Once a file is infected it can be launched on a set time and date or remotely activated to perform its operations. These operations can include deletion, modifications or corruption of the files and documents. A virus can additionally give attackers loopholes into the network and allow them to remotely access the device. Once a device is infected with either a virus or worm, the infection will begin to spread across the network and infect other devices.

Solution

The solution to a virus or worm is to ensure there are anti-malware solutions installed on every device that is connected to the network. High-end firewalls can have a real-time threat detection build in; this is another point where a virus or worm can be detected before it can infect an end device. Depending on the security needs of the network high-end devices additionally can automatically rectify these issues, however, these are expensive. Both HP and Dell have devices with this capability, these devices have a system that detects system and bios changes. Once detected it will automatically reboot the device and should the bios be infected, it will install a clean version, therefore, removing the threat. Additionally, user education is the final prevention that can be used. Educating users on not opening suspicious links and files in the network can also prevent a virus or worm infecting the system.

2.4.2 Drive-by Download Attacks

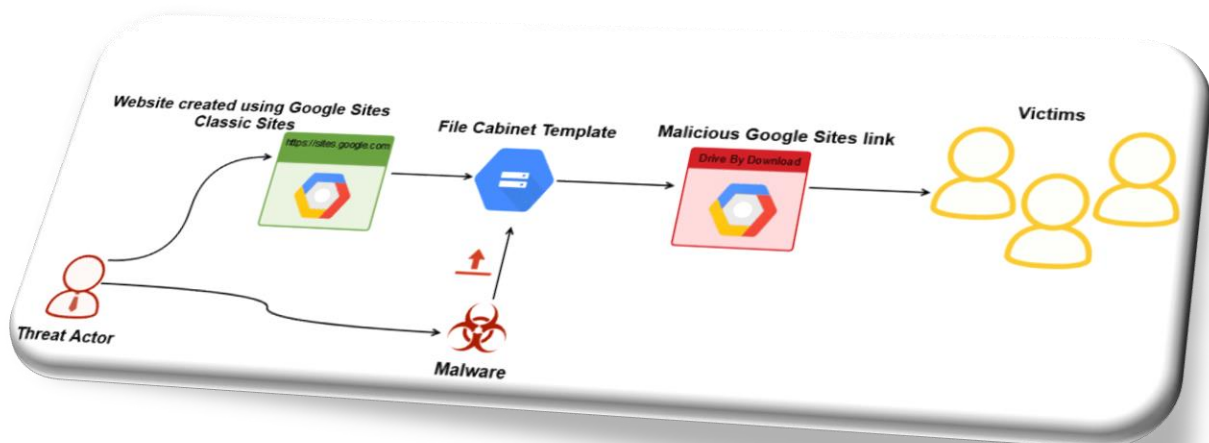


Figure 2 - Drive-by Download Attack [8]

[9]–[11] A drive-by download attack is when a user visits a website, this could be a totally legitimate website like a social media or shopping site. However, secretly the website might look exactly like the normal website, but it will be modified by attackers to secretly run code in the background of the website. This code is hard to detect as it is very simple since it has only one job to execute the installation of whatever malware the attacker has selected. Usually, the attacker will attempt to install several pieces of malware in the hope that one will not be detected by an anti-virus or anti-malware software on the system.

Solution

The solution to drive-by download attacks is to ensure that all browsers and security software are kept up to date. This will hopefully enable the browser or security solution to detect the website before it is opened. Again, high-end devices from HP like the elite and Z range have HP Sure Click, this opens an isolated browser in a virtual machine, so any web-based attack is removed when the browser is closed. User education can additionally prevent this type of attack by enabling users to have the ability to detect a website that is not legitimate. Another prevention method is to use a safe-search tool, this is designed to block websites that pose a threat before any can be opened. Finally, ad-blockers can additionally help to protect the end user from this attack, so it is recommended to install a version of this on all end devices.

2.4.3 Botnets

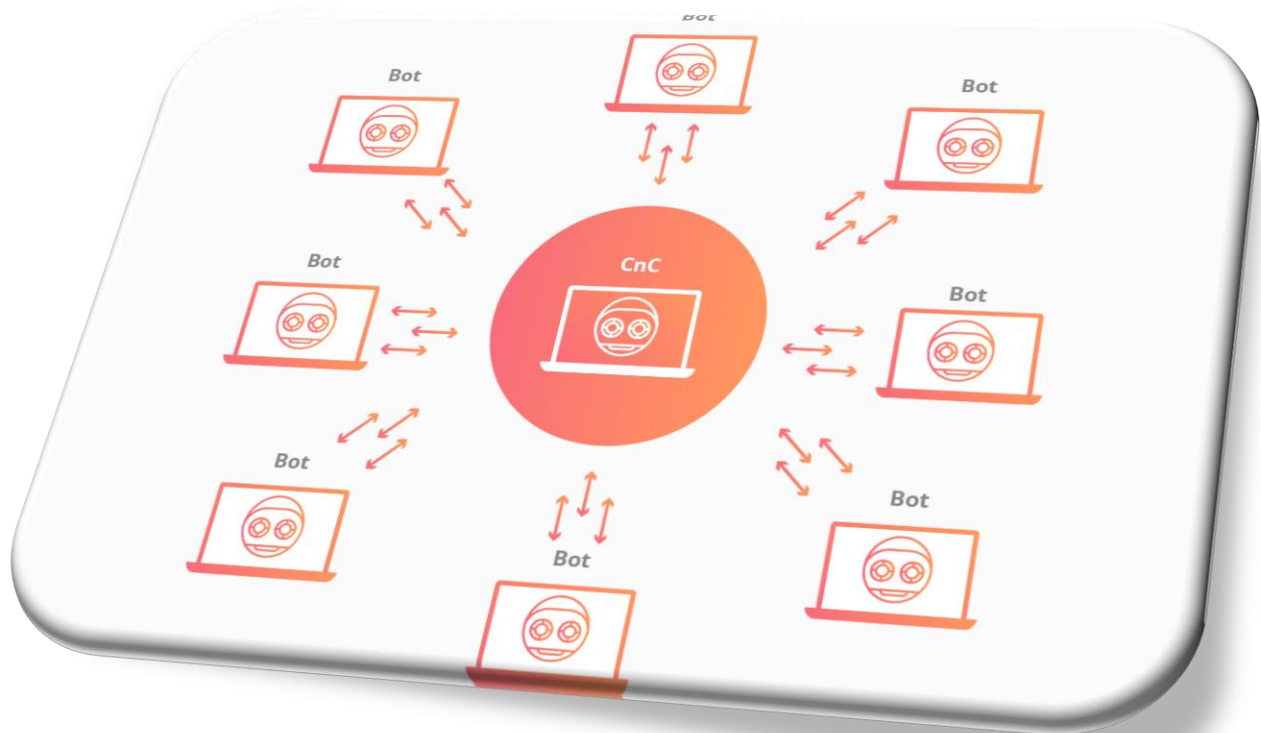


Figure 3 – Botnet [12]

[13]–[17] A botnet is a network of devices that have been compromised by an attacker. When an attacker has control of a device it is known as a zombie. An attacker then used a command and control network to use the zombies. This gives an attacker huge computing power when launching an attack. Botnets are commonly used to create a dedicated denial of service attacks. This is when a web server is overloaded with requests from zombies, this can sometimes crash the webserver and stop genuine users from accessing the website. The attacker then usually forces the website owners to pay a ransom in bitcoin to let them have access to the website again. Botnets are very powerful tools to attackers and with more devices than ever being connected to the internet, they are going to become larger and more frequent.

Solution

The first solution to a botnet is ensuring that real-time malware defence software is installed on every end device on the network. Ensuring that all software is always kept up to date is also essential to this as it fixes any loopholes that could allow attackers access to the end devices. It is essential to ensure that the internet service provider is capable of additionally detecting large volumes of traffic and blocking such attacks. This is the first line of defence sometimes preventing an attack before it hits the enterprise network. However, the network must be designed to handle a large volume of requests to prevent a botnet from taking over. A powerful firewall can additionally help detect and block some of the botnet requests, helping to reduce the risk of this type of attack.

2.4.4 Phishing Attacks

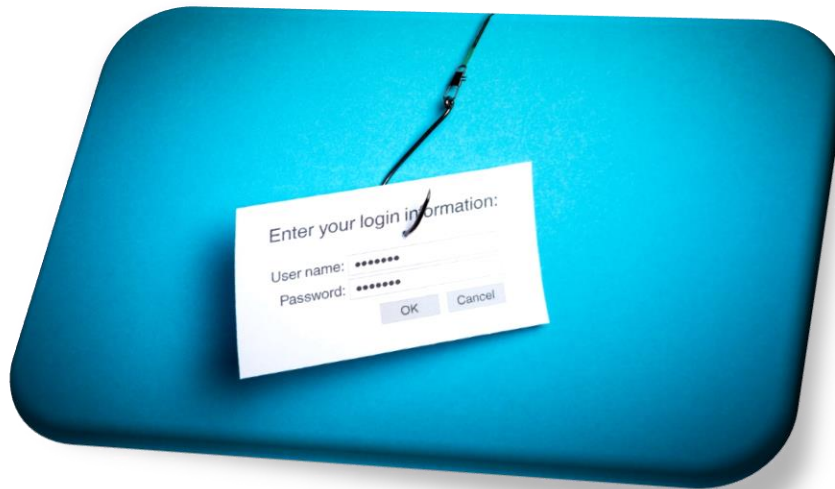


Figure 4 - Phishing Attacks [18]

[19]–[21] This type of attack uses social engineering to obtain the victim's login credentials & credit card details and other types of confidential information. This type of attack is designed to trick individuals into giving away confidential information. An example of this would be receiving an email from PayPal saying, “unauthorized changes to an account”. This would prompt a user to login to confirm the account and payment details. However, once the link in the email is clicked all the details are sent to the attacker. The victim would be unaware of the attack taking place until a bank statement arrived showing that unauthorized transactions have taken place.

Solution

The first line of defence of this type of attack is user education. This will enable end-users to be more cautious when receiving emails from well-known companies. The trick is not to click the link but go directly to the website or company themselves. However, educated users will have the ability to detect the source of the email is not PayPal when the sender's email address is paypal@gmail.com. Real-time malware detection can occasionally detect and block these links before the website launches. In enterprise networks, next-generation firewalls can additionally help prevent this type of attack.

2.4.5 Ransomware



Figure 5 – Ransomware [22]

[23]–[27] Ransomware is a piece of malware that can encrypt the end user's data stopping the organization from operating unless a ransom is paid. When an attacker requests payment it is usually done using bitcoin as it is untraceable, this is due to it being a cryptocurrency. This type of attack is on the rise due to the ability of anonymous payment methods like bitcoin, for this reason, it is one of the most feared. This type of attack has caused most organizations and individuals to lose the data stored on the systems. This attack being caused by malware means that once one network device is infected, soon the entire network will be infected, and this will stop the organization working until the ransom is paid. This type of attack is usually spread through phishing emails, as soon as the link is clicked the entire network is encrypted.

Solution

The first line of defence for this type of attack is a real-time anti-malware software, additionally, all updates and patches need to be constantly kept up to date to prevent this type of attack. Educating users to recognize phishing attacks can additionally help prevent this type of attack before it happens. The major solution to a ransomware attack is to ensure all the organization's data is backed up in multiple secure locations, this will ensure that even if some data is encrypted it can all be restored. This will ensure that the organization can recover and be operational again with minimal disruption.

2.4.6 VLAN Hopping Attack

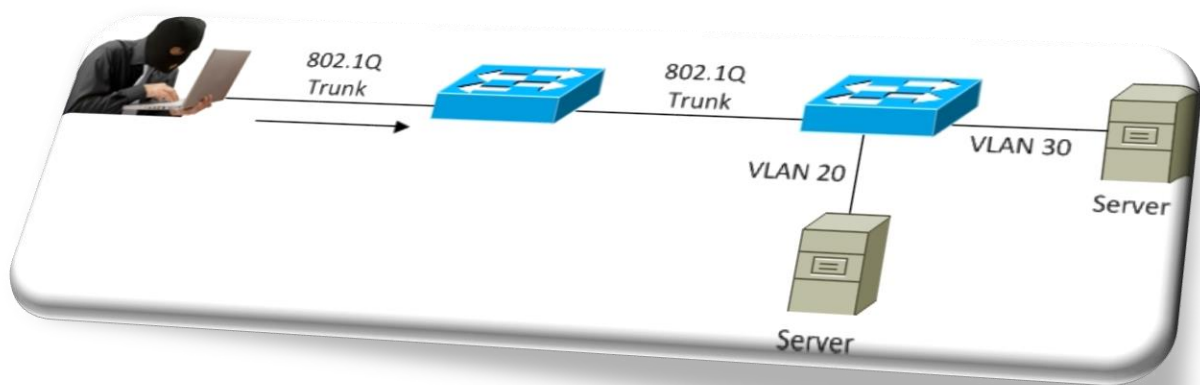


Figure 6 - VLAN Hopping Attack [28]

A VLAN hopping attack is conducted using the dynamic trunking protocol. This is what is used to negotiate a link between the two devices, this is known as a trunk. This enables easier configuration of switches within the network, however, it provides an attacker with an easy method for attacking the network and obtaining access to multiple virtual local area networks with the possibility to access sensitive data. The attacker must spoof the attacking device like the switch, this utilizes the 802.1Q encapsulation. This changes the attacker's link from access mode to a trunk connection, allowing access to all networks attached to the switch.

Solution

The solution to a virtual local area network hopping attack has been developed by cisco. The defence for this attack is to ensure that dynamic modes at the interface level are not enabled and the port mode is configured during the network configuration, instead set the links to either switchport mode access or switchport mode trunk. This means that detailed planning before the development of a network can completely avoid this type of attack.

2.5 Network Defences & Countermeasures

The author utilizes this part of the report to investigate several countermeasures that could be utilized to minimize the risk of attacks on the network. The report will explain what each solution can help prevent and explain how it will benefit the network that is being designed and implemented.

2.5.1 Firewall

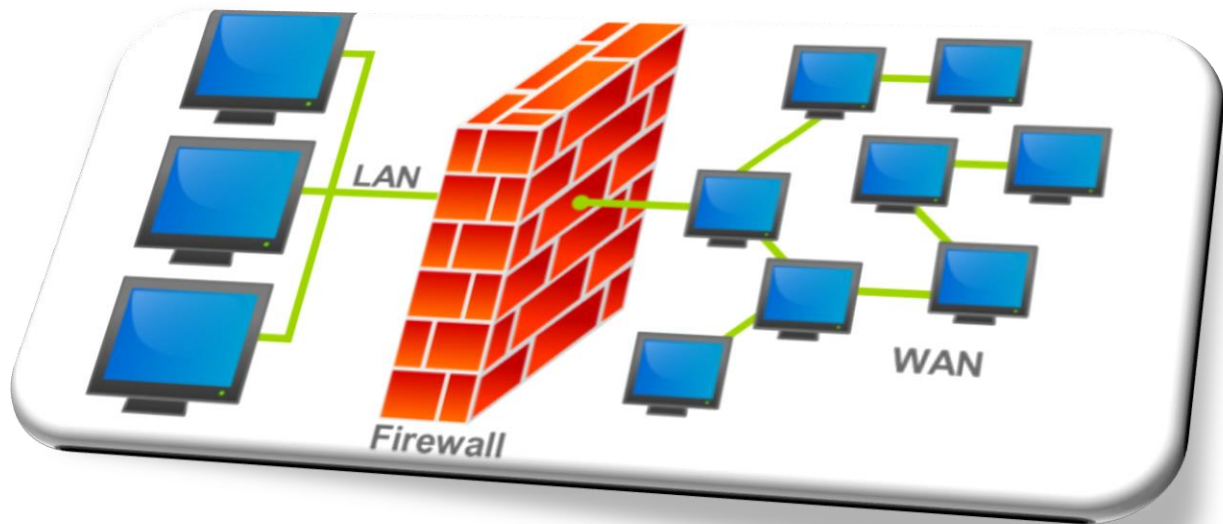


Figure 7 – Firewall [29]

[30]–[33] A firewall is a very common security implementation in a network. Enterprise networks tend to have next-generation firewalls to help protect the organization's data from attackers. A firewall can be a physical stand-alone device or a virtual device, either of these does the same job however performance can differ depending on the type of firewall selected. There are usually two locations in a network that a firewall will be positioned. The first location is between the ISP and the network, this is used to filter external traffic coming into the network. The second location is between the network and sensitive data stored on the servers; this is to ensure only people with authorization access to the correct resources. A firewall is a list of rules that allow or deny inbound or outbound traffic. It is important to test a rule when it is implemented to ensure it allows or blocks the connection as expected.

Firewalls are designed for different solutions, these are packet filtering, stateful inspection, application layer, and next generation. Packet filtering firewalls monitor packets entering and exiting the network this is done on source & destination IP address, ports, and protocols. Stateful inspection firewalls can additionally analyse the packets history table and allow or block the connection based on this. Application firewalls can additionally analyse the application layer, for example, FTP, SNMP, etc and allow or block connections based on this. Next-generation firewalls can additionally perform deep packet inspection and inspect it against a list of known threats and protect the network from new threats. This type of firewall was able to defend against the WannaCry ransomware attack in May 2017. However, the more features on a firewall can dramatically increase the purchase cost.

2.5.2 Intrusion Prevention System

[34]–[37] Intrusion prevention system is a security mechanism that can protect the network from attackers. An intrusion prevention system will use deep packet inspection to monitor the network, this will enable the system to detect anomalies within the network. If an event is detected, then it will record all related information and alert the network administrators. The intrusion prevention system can also take preventative measures to automatically prevent attacks, this could include closing ports or blocking selected access points. This is essential in an enterprise network since it would not be possible for an individual to monitor the whole network. Once the intrusion prevention system identifies an attack it will block the attacker's IP address, reconfigure the firewall and remove all malicious content added by the attacker.

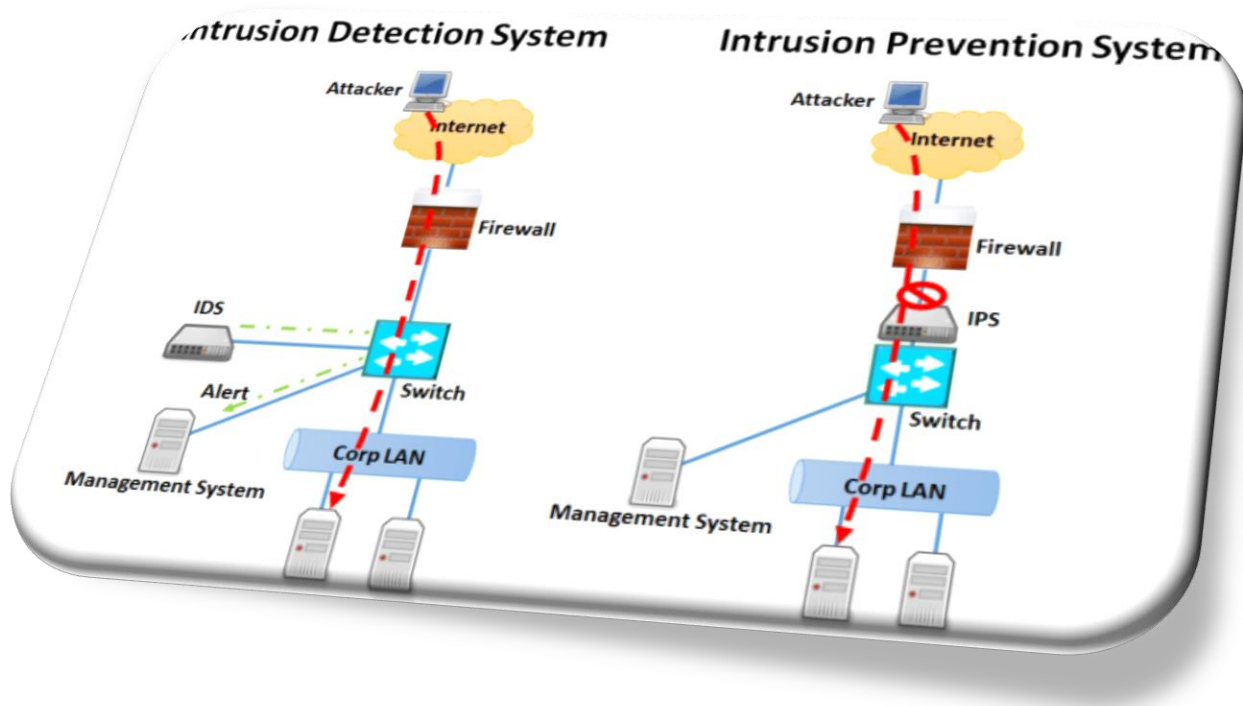


Figure 8 - Intrusion Prevention & Detection Systems [38]

2.5.3 Intrusion Detection System

[39]–[43] There are several types of an intrusion detection system, these are signature-based network-based, host-based, and anomaly-based intrusion detection systems. A network intrusion detection system is implemented at the entrance and exit points of the network, this enables the stem to monitor all traffic travelling from and to the network. A host intrusion detection system gets installed on all end devices within the network. This can be the first line of defence if the attack is launched from the host device additionally, it can be a last line of defence if an attacker gets past the network intrusion detection system. A signature-based intrusion detection system tracks all network packets to compare them to a database of known threats. An anomaly-based intrusion detection system is utilized to monitor performance, protocols & ports looking for changes. Once a change has been detected this type of detection system alerts the network administrator. This allows the network administrator to investigate the change and possibly prevent the attack.

2.5.4 Encryption



Figure 9 – Encryption [44]

[45]–[48] Encryption is the process of taking plain text and encrypting it using an encryption algorithm. Data is encrypted using an encryption key, once encrypted the data is changed into ciphertext that is only viewable with the decryption key. There are several encryption algorithms types however, the most commonly used are asymmetric and symmetric. Asymmetric encryption algorithms use two different keys, these are known as a public key and a private key. The public key that is used to encrypt the data is shared across the internet however, the private key is required to perform the decryption process is kept private. The Rivest-Shamir-Adleman also additionally known as RSA is a popular asymmetric algorithm. Symmetric encryption algorithms are generally faster at encrypting data as they use the same key for both encryption and decryption. However, the recipient must have the key from the sender before the data can be decrypted. The advanced encryption standard, sometimes known as AES is a popular symmetric encryption algorithm.

The strongest encryption algorithms are currently Triple data encryption standard, Rivest-Shamir-Adleman, Blowfish, Twofish, and Advanced encryption standard. Data encryption is essential for organizations due to data protection laws and to ensure company and client data is safe from attackers. This is one of the reasons why in enterprise networks all sensitive data is encrypted as it is stored. This prepares the data for transmission should the data ever need to be sent, ensuring data confidentiality. Encryption can additionally be used when using a virtual private network, this allows a secure connection over the internet further increasing data confidentiality.

2.5.5 Virtual Private Network

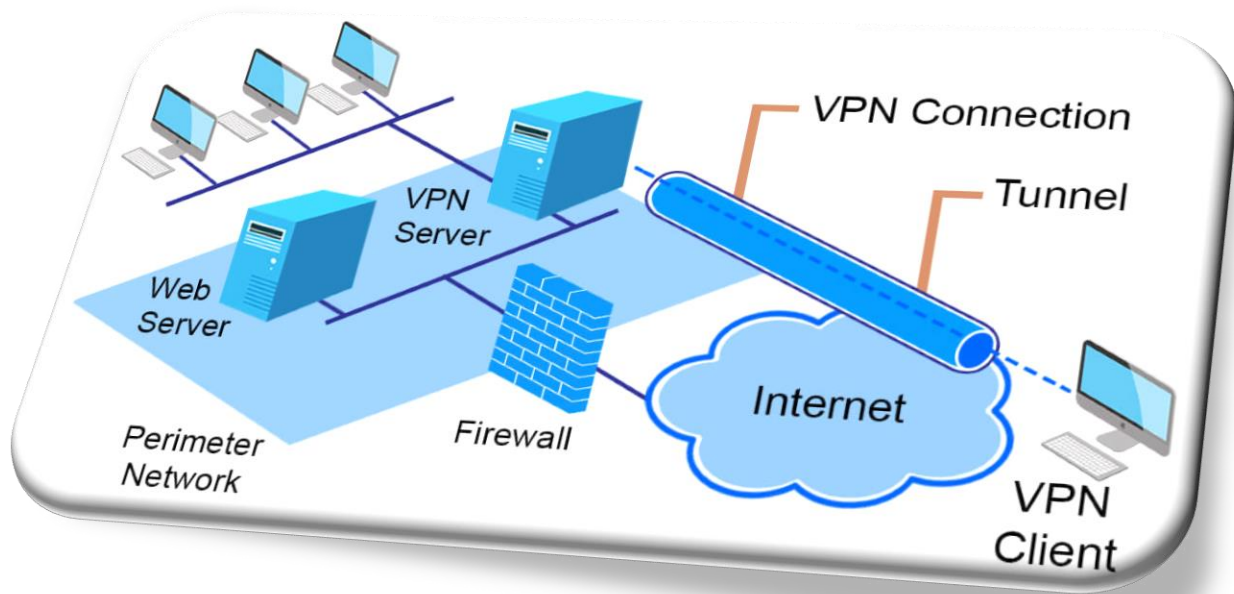


Figure 10 - Virtual Private Network [49]

[50]–[53] A virtual private network is an essential security mechanism within an enterprise network, due to its ability to encrypt what would be insecure communication over the internet. A VPN establishes an encrypted tunnel that encrypts all data sent over the internet from the client to destination. All network traffic that travels across this tunnel is encrypted therefore protected from unauthorized access. Virtual private networks allow employees a secure method to connect to the enterprise network and its resources from anywhere in the world. However, usually, the end device needs to have the VPN client software to have the ability to connect to the network. Virtual private networks use several different protocols to create the encrypted tunnel, these are Layer 2 tunnelling protocol, Transport layer security (TLS), Point to point tunnelling protocol (PPTP), OpenVPN, Secure Socket Layer (SSL), and IP Security (IPsec).

There are several types of VPN these are site-to-site, remote access, mobile and hardware virtual private networks. A site-to-site VPN is created when a gateway device like a firewall connects the entire network in one location to another location over a VPN. It is common for IP Security to be the selected protocol for a site-to-site VPN. A remote-access VPN forces a user to communicate with a network gateway like a firewall to provide the end device access to the network. However, the end device must authenticate itself before network access is obtained. A remote-access VPN uses SSL or IPsec as a protocol to create the tunnel between the client and destination. A mobile VPN client is not given a physical IP address however, it is provided with a logical IP address that is always used by the device to connect to the VPN. A hardware VPN provides enhanced security to a software-based VPN. However, this requires additional hardware meaning increased implementation costs. Therefore, this type of VPN is more commonly found in large enterprise networks.

2.5.6 Anti-Virus & Anti-Malware



Figure 11 - Anti-Virus & Anti-Malware [54]

[55], [56] Anti-virus software was created to protect devices from viruses and worms. This software is designed to perform checks on files and check them against a list of known viruses and worms. If a file is detected to have a virus then the software will automatically quarantine the threat, this will stop the virus from harming the system and allow the end-user the option to repair or delete the infected file. However, nowadays this alone is not enough it is essential to have real-time based threat detection. This gives the anti-virus the ability to monitor device performance and programs looking for abnormal behaviour. If a virus is detected the software will automatically quarantine the threat, additionally the software will alert the end-user.

[57], [58] Anti-Malware is a software that can additionally detect viruses, spyware, rootkits, and adware. Signature-based detection uses a list of known malware threats to check against if malware is detected it is automatically quarantined for removal by the end-user. Behavioural-based detection monitors the device performance and processes, to detect unauthorized actions or abnormal behaviour that can be caused by malware. Again, should a threat be detected it will be automatically quarantined for the user to remove the threat. Sandboxing offers an isolated environment to run applications that are not listed in the known application database. This provides a secure environment for software to be monitored in, should a threat be detected the session will terminate and the new application will be blocked on the end device.

2.5.7 Physical Security

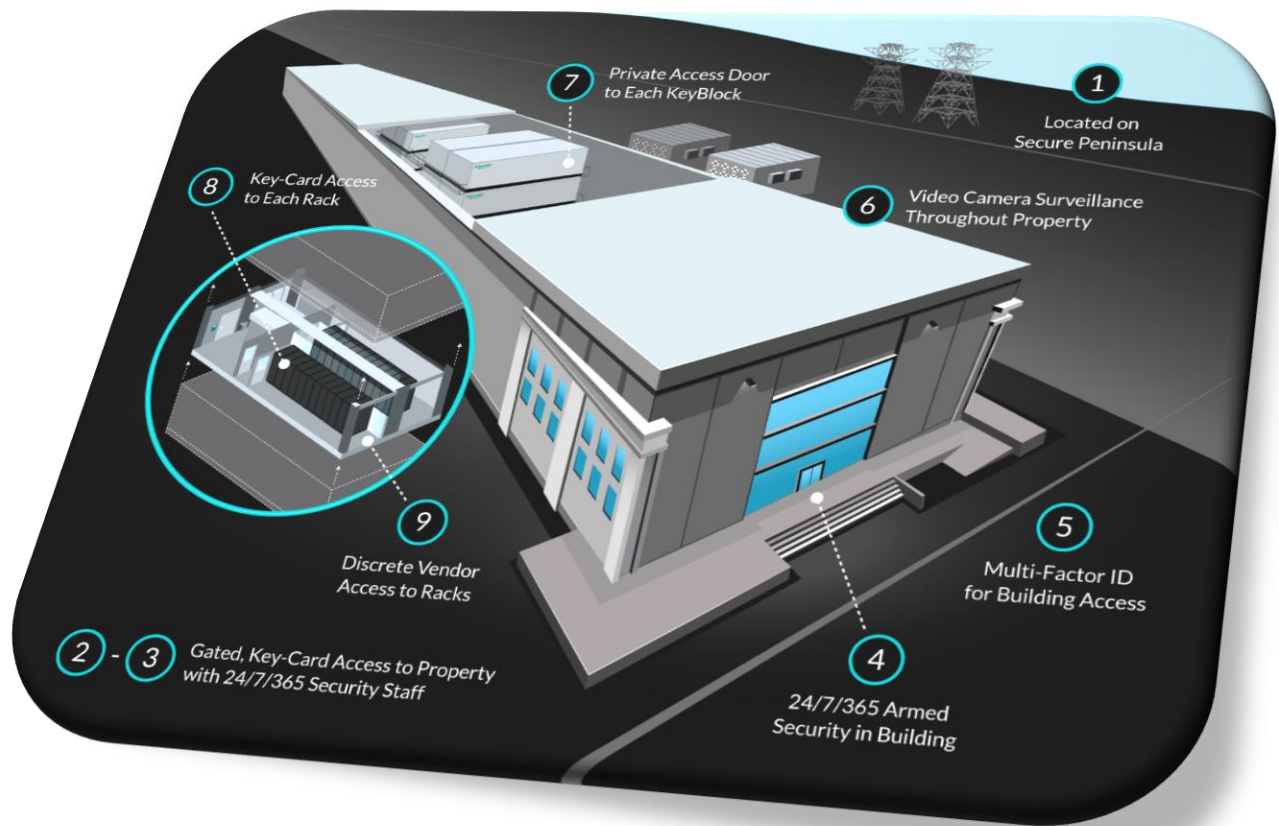


Figure 12 - Physical Security [59]

Physical network security is essential to an enterprise network as a physical attack on the network could cause catastrophic damage. However, this is usually one of the most common vulnerabilities within a network as it is so easily overlooked. Companies spend thousands on the state of the art security devices, however, commonly leave windows and doors open for an attacker to walk in and obtain easy access to the network. This is the reason why a multi-layered approach is essential to the security of the network. The first defence is a perimeter fencing; this simply provides an obstacle for an attacker to overcome. The second defence is gated access with constant security staff to ensure only authorized individuals obtain access to the building via a key-card access system.

The third defence depending upon threat level and company size is armed security guards within the building. The fourth defence is multi-factor authentication systems for building access with additional security systems for restricted zones. The fifth defence is to ensure the segmentation of the servers, this prevents access to the entire network resources from one location. The sixth defence is closed-circuit television systems (CCTV). This should be monitored continuously looking for unauthorized access. Finally, each server rack should have a different access card, code or physical lock to limit what an attacker could do should an attack happen.

2.5.9 Email Security



Figure 13 - Email Security [60]

[61]–[63] Email is one of the most common communication methods within organizations, it allows for communication with both internal staff and external clients, suppliers, etc. However, email is not secure as it is designed to be accessed by anyone. In enterprise networks, it is important to ensure that email encryption is always used. Email encryption is the process of encrypting messages at the source and decrypting messages at the destination. This ensures that emails are kept confidential and secure. Emails are a common path used by attackers to obtain unauthorized access to the enterprise network and company information. Email is commonly attacked using several different methods, the most common are spam, phishing attacks, malware, and targeted attacks.

It is recommended that organizations have an email security policy in place. This provides staff with a clear policy that must always be followed, it is common to find things like the removal of executable software in an email policy to protect the network. It is important to ensure that there is a secure email gateway that processes all inbound and outbound email traffic, this ensures no threats are allowed in through the email. Additionally, an email encryption solution should be implemented to ensure that all confidential data is protected before being sent across the internet. It does this by scanning all emails for sensitive data if found it automatically encrypts the email being sent to prevent attackers from reading the email.

2.5.10 VLAN Segmentation

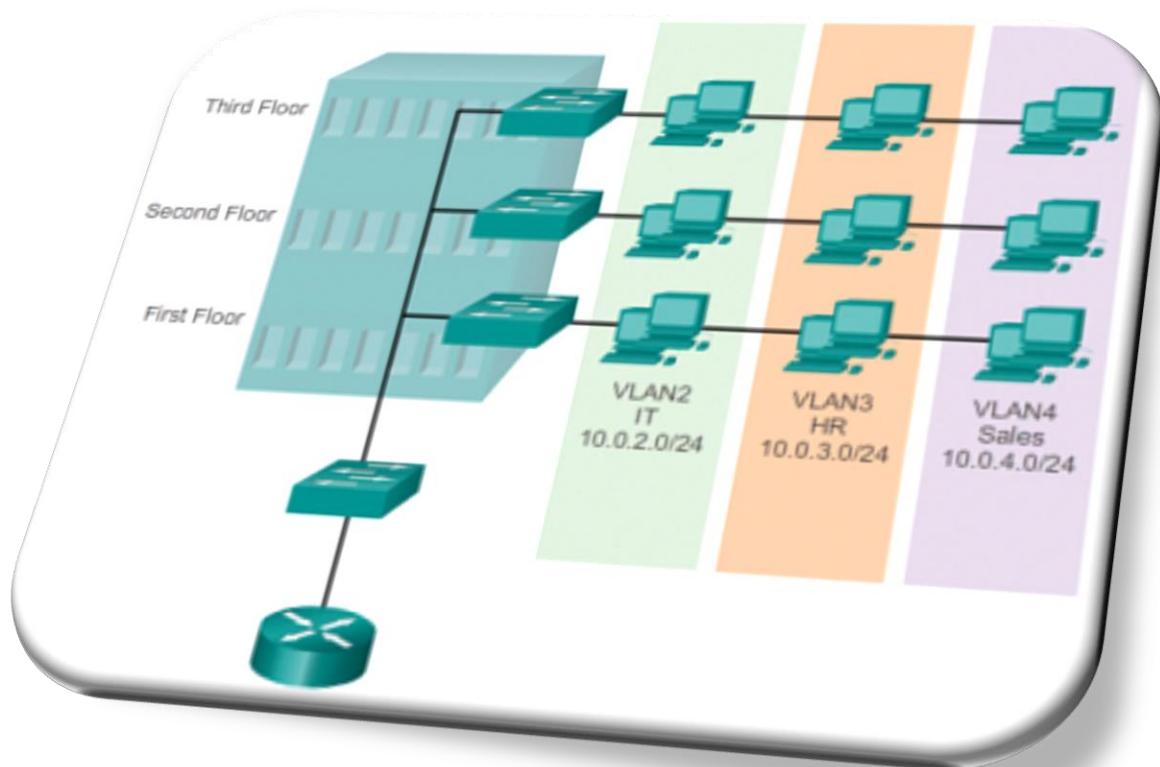


Figure 14 - VLAN Segmentation [64]

[65], [66] An enterprise network is a large network with a large amount of traffic however, implementing VLAN segmentation allows the network to be broken up into smaller broadcast domains. This is useful in reducing unnecessary traffic within the network. When a device in a VLAN broadcasts a frame, it is only sent to all the same VLAN devices, not the entire network. Security is also increased when VLANS are implemented within the network, due to the fact only devices within the same VLAN can access traffic & resources this reduces the risk of an attacker accessing confidential information. There are several additional benefits of using VLAN segmentation within the network. The first benefit is the ability to easily implement quality of service into the network, this ensures that performance is maintained for the end-users.

There can be a reduction of implementation due to the ability to utilize bandwidth more efficiently, therefore, allowing slightly lower performance devices to be used without a loss of performance. A network with VLANS is additionally easier for the network management team to manage, as devices are grouped into VLANS it means access control & security parameters can be configured on a grouped basis. A network should have an isolated management VLAN, this should have ACLs to prevent unauthorized access. If the network uses a native VLAN then it should differ to the management VLAN so no one without authorization can obtain access to management VLAN.

2.5.11 Wireless Security

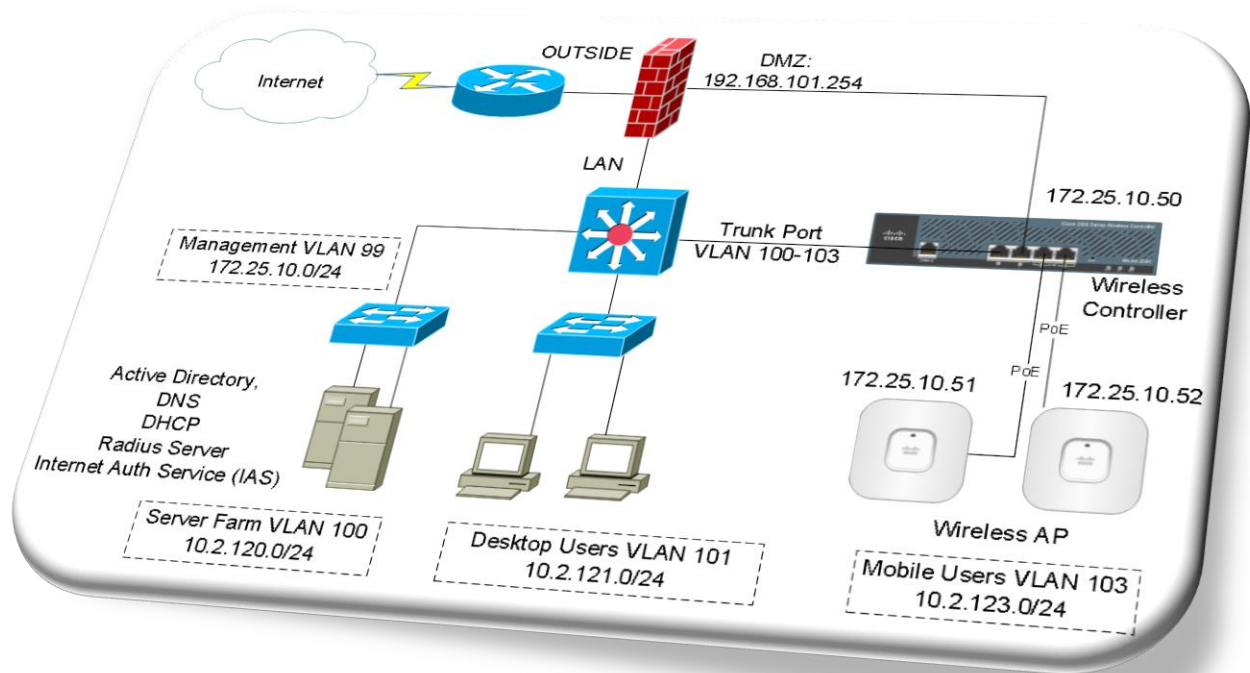


Figure 15 - Wireless Security [67]

[68]–[71] In wireless networks security can be a problem since wireless networks not requiring physical access to the network. This is the reason why it is important to ensure that all wireless traffic is encrypted, ensuring that if an attacker accessed the network the data is still secure and not compromised. In a home-based network then WPA2 is commonly used however mac authentication can additionally provide a second measure to protect the network. A guest network can provide an additional security measure as it removes the risk of a guest accessing confidential information. Enterprise networks have more confidential data stored so require additional security parameters.

Enterprise wireless security is usually done using a RADIUS Server. A RADIUS server moves the authentication from the access point to a dedicated server, the servers have access to a central database that is used to authenticate both the user and device before providing access to the network. A RADIUS server reduces the risk of unauthorized access over a wireless communication method; however, it does not remove the risk entirely. A wireless LAN controller can provide an additional security measure by enabling authentication and monitoring of the network access points. This enables the management team to detect a rogue access point and act before it can be used for unauthorized access. Newer high-performance access points are now being designed with wireless intrusion prevention therefore, providing additional security implementations to ensure wireless communications are secured from attackers.

2.5.12 Access Control



Figure 16 - Access Control [72]

[73]–[76] Access control is the process of limiting what user's resources users can view, modify and delete. It is an important part of network security due to the reduction of risk if any employee or attacker wanted to harm the network, this would be the first line of defence. Access control is both preventing physical access to the network, and logical access limits what resources can be accessed by users. Access control uses passwords, biometrics and security tokens to perform authorization and authentication of users, this ensures it is as difficult as possible should an attacker want to obtain access to the network. Access control is difficult to implement in a network as all users require different privilege levels therefore, it is important to create groups for different departments as this makes it easier to modify permissions.

There are several methods of access control these are mandatory access control (MAC) in this type of access control the resources are classified into different levels, it becomes the job of the operating system to then grant or deny permission to resources. Discretionary access control (DAC), is the process of creating a policy that is used to grant or deny access to the resources. Role-based access control (RBAC), is used to provide restrictions based on groups with a set of functions for example students, lectures. Rule-based access control, this is the process of the administrators granting or denying permission based on location or time. It is common to find that more than a single access control measure is put into place therefore, minimizing the risk of an attack on the organization.

2.5.13 Data Loss Prevention



Figure 17 - Data Loss Prevention [77]

[78]–[80] Data loss prevention is a system that is incorporated into enterprise networks, it has the role of ensuring that sensitive data is not able to be sent outside the network. Dependant on the risk of sensitive data, data loss prevention can be a single or several pieces of software to stop sensitive data being sent. The software allows the organization to configure the rules to create the perfect data loss prevention solution. The law is constantly becoming stricter with newer stricter data protection and privacy laws, meaning organizations must comply to abide by the law. Therefore, data loss prevention solutions are becoming more essential to an enterprise network than ever.

Data loss prevention solutions are used to monitor all traffic and scan it for sensitive data, newer solutions can filter the traffic while the packets are travelling within the network. This solution is essential to one major threat an internal attack, it is common for this to be overlooked by an organization. However, this solution stops sensitive data being forwarded over email or preventing backup to a cloud storage provider like Google drive or dropbox. The software would be denied permission and the attempt would be logged, this can prevent accidental leaks and malicious attacks on the organisation's data and ensure compliance of laws.

2.6 Related Work

The paper “Design and Develop Hands-on Cyber-Security Curriculum and Laboratory” by Dongqing Yang [81], outlines several objectives, firstly to design and implement a virtual enterprise network, performing penetration testing, network hardening, and auditing. The first objective is the development of a virtual enterprise network to be used within a laboratory environment. There are three network zones protected by a firewall with different security levels, inside most secure, DMZ second most secure and outside least secure. The network simulates an attacker attacking over the internet using Kali Linux to attack the internal network where devices like VoIP, servers, routers, and switches are targeted. The report then moves into the penetration testing section where the author outlines several different attacks that can be conducted including firewall evasion, password cracking, wireless cracking, hacking cisco routers. The paper then moves onto network hardening to prevent the attack from being used to obtain unauthorized access and concludes on network auditing. This paper is related to this project due to both being based upon building enterprise networks. Additionally, both this paper and the project relate as both conduct penetration testing and implement solutions to the network to secure the vulnerabilities identified.

2.7 Conclusion

In conclusion, this chapter has provided the author with background research that is required to complete this project. The author has covered several topics that are essential to this paper however, the most essential are the network threats and network defence and countermeasures. The author has additionally found the related work section very helpful in providing information related to a similar project, this has enabled some of the tools and ideas to be utilized within this project. Overall this chapter has been very successful in providing the author with the required background knowledge. The following chapter is on research methodology, this chapter will provide the author with a methodology that can be followed to allow a successful outcome from the project.

Chapter 3 – Research Methodology

3.1 Introduction

The author will discuss several different research methodologies that need to be used to allow the author to complete the project. The next part of the report will be used to give the author a method to evaluate the project to ensure all aims and objectives are met.

3.2 Research Overview

The author utilizes this chapter to provide a guide for completing the project. There are several sections that are essential to the successful outcome of this project. These are several sections that have to be related to the project to enable the research methodology to be created. The figure of the research onion below provides the author different methodologies that can be used, this chapter will be used to document what method has been selected and how it is the most appropriate for this project.

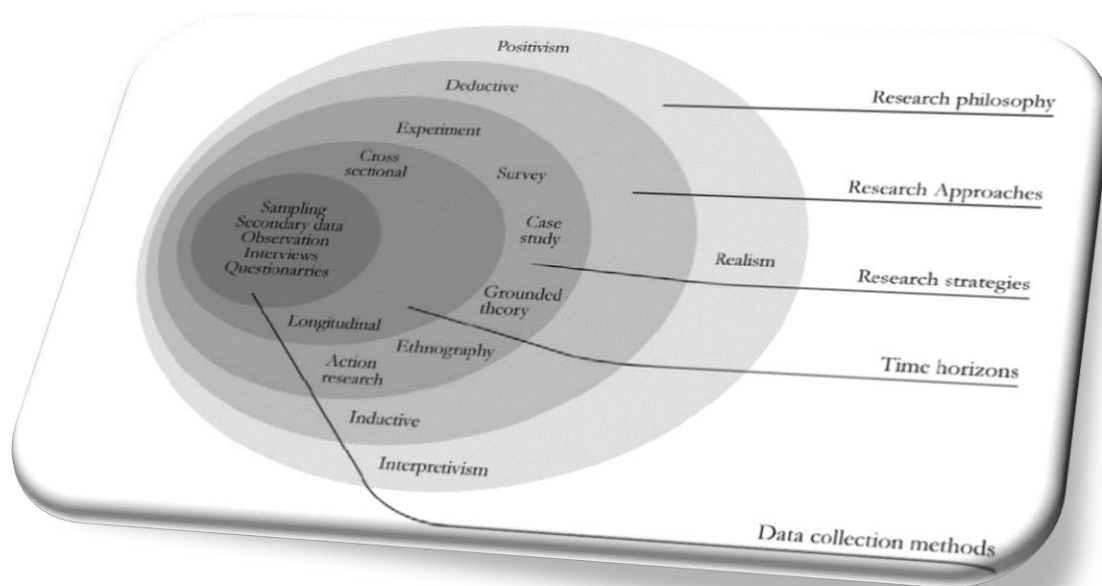


Figure 18 - Research Onion [82]

3.2.1 Research Philosophy

The research onion has several possible philosophies choices to be used during the project however, positivism has been chosen for the research philosophy. The reasoning for this choice is the project is based on experiments. Positivism research philosophy can be used when research is based on scientific evidence. Experiments are classified as scientific evidence and this is the reasoning why this research philosophy has been chosen.

3.2.2 Research Approach

The author has chosen deductive as the research approach as is the best approach when a theory is being tested. The author believes that enterprise networks have lots of vulnerabilities, the author aims to provide evidence of this theory during the experimentation. The author will then provide solutions that have been gathered during the research section of the project.

3.2.3 Research Strategies

There are several different research strategies within the research onion that could be used for the project however, the experimental strategy has been identified as the most appropriate for this project. The author selected this as within this strategy there is a minimum of one variable that can be changed to conduct the experiment and record the findings. During the testing of the enterprise network, the author will carry out several attacks, the different attacks are the variable that is changeable. This allows the findings from the different attacks to be documented; to enable a comparison of the findings of the attacks to be compared to that of the research identified to understand if the attacks are successful.

3.2.4 Time Horizons

There is an option between longitudinal and cross-sectional identified within the research onion. The author has decided to use a cross-sectional as a time horizon. The author has selected this as cross-sectional is when a single task is conducted at a time, during the testing of the enterprise network the author will conduct a single attack at a time. This will ensure that each attack is conducted properly and highlight issues that need to be rectified to secure the network.

3.2.5 Data Collection Methods

This section of the chapter identifies the different data collection methods that will be utilized within the project. The author has identified two data collection methods for the project these are secondary data and observation. The author selected observation as when the attacks are performed against the enterprise network the author will need to observe and document the results. Secondary data has been chosen by the author as there is a need to conduct a comparison between the observations within the experiments and secondary data identified in the research. The author will have the ability to compare results and findings with related projects identified within the related work. Table 1 below is used to identify how the several chapters within the project relate to the research onion.

Component	Research Approach
Chapter 1 – Introduction	Deductive – This is used when a theory is already made that enterprise networks are insecure
Chapter 2 – Literature Review	Qualitative Research – Understanding enterprise network design and network threats & solutions Action Research – Understanding findings identified within the research
Chapter 3 – Research Methodology	Action Research – Understanding findings identified within the research
Chapter 4 – Design & Implementation	Action Research – Understanding findings identified within the research Experiment – changing the variable to gather the findings from the experiment
Chapter 5 – Evaluation	Qualitative Research – Gathering the results Action Research – Understanding findings identified within the research Triangulation – Comparing findings with similar experiments to ensure results are correct
Chapter 6 – Conclusion	Action Research – Understanding findings
Chapter 7 – Reflection	Triangulation – Comparing findings with similar experiments to ensure results are correct

Table 1 - Data Collection Methods

3.3 Research Deliverables

The author conducted research to enable the author to understand enterprise network design and current network threats and solutions. The research enables an enterprise-class network to be implemented by the author. It will also enable the author to obtain more accurate results from experiments on network security. The research will additionally support the results and findings by proving solutions to attacks that are successful on the network, this will enable the author to implement solutions to prevent the attack harming the network in the future.

3.4 Triangulation

This project is essentially conducted in three different sections research, implementation and experiments. Triangulation will help the implementation section of this project by ensuring that the network is built correctly, this will be done by comparing the network to that of previous implementations identified within the research. Triangulation will support the experimentation section of this project by enabling the author to compare the findings of the experiment with related work to ensure experiments are successful. This will enable the author to ensure that the results and findings are accurate.

3.5 Conclusion

In conclusion, this chapter has provided the author with a plan of how the project can be conducted to obtain a successful outcome. This has been based on the research onion however, it has been a detailed plan of how each section of the onion can support the project. The most important section of this chapter has been triangulation, the reasoning for this is that it everything that is completed is verified against research to ensure that it is completed correctly. This chapter will guide the author throughout the remainder of the project until completion. The following chapter is on design and implementation, this chapter will cover the design and implementation of an enterprise-class network. This will provide a testbed for the experiments to be carried out in chapter five.

Chapter 4 – Design & Implementation

4.1 Introduction

There are two different sections to this chapter, the first is the design and the second is the implementation. The design process is where the network plan is essentially created. This will include different network devices and end devices. There will additionally be security implementations made onto the devices to help secure the enterprise-class network. Upon completion of the enterprise-class network, the author will have the ability to identify weaknesses. The author can then implement solutions during the implementation of the report. The implementation part of the report will be to construct the outlined design in the first part of this chapter; this might be slightly different due to the possibility of limitations with devices. The final part will be the documentation of the implementation that has been completed for this project.

4.2 Problem Formulation

Building a secure enterprise-class network is the main aim of the project. The first stage is to construct the network, this will include a large volume of cisco networking devices including routers, switches, and wireless access points. The network will additionally include a variety of end devices that are typically found within an enterprise network. The initial design of the network will not include any major security implementations to allow testing to be conducted in chapter five, this is where solutions will additionally be implemented to secure the network from identified threats. The main tool during the penetration testing will be Kali Linux however several additional tools will be utilized to test the vulnerabilities within the network. The completion of this will ensure that the project outcome is successful.

4.3 Design

There are several considerations that must be made before designing a network. In an enterprise network there must be a design that allows for the future growth of the network, otherwise, if more devices were required a totally new network would be needed. The next consideration is the devices that are required as part of an enterprise-class network, this will additionally include how the network will communicate with different devices whether it be a wireless or wired connection. The next consideration is what software will be required on the end devices for the network and organization to operate effectively. The final consideration will be on network addressing and designing a network scheme that can fit the current network and allow for future expansion of the enterprise network.

The table below shows the IP addressing scheme that is going to be used within the network. The network will use the 10.10.0.0 for the networking IP addressing scheme. The table additionally shows the different VLANs that will exist within the network. This allows traffic to be separated to enhance network security and minimize the risk of an attack on the network.

VLAN NAME	VLAN NUMBER	NETWORK ADDRESS
Servers 1	Vlan 20	10.10.20.0
Servers 2	Vlan 30	10.10.30.0
Staff	Vlan 40	10.10.40.0
Guest	Vlan 50	10.10.50.0
Management	Vlan 99	10.10.99.0

Table 2 - IP Addressing

The table below will be used for a list of devices that will be used within the network. This may differ when the physical network is created due to limitations however, it outlines what the author aims to implement within the network. The author wanted a minimum of 30 networking devices within the network. The network is designed to meet this requirement and provide room for future expansion should it be required in the future.

Device	Quantity
Cisco Router	1
Cisco Adaptive Security Appliance	1
Cisco Layer 3 Switch	8
Cisco Layer 2 Switch	20
Access Points	1
Servers	2
Workstation	21

Table 3 - Device List

The figure that can be seen below is a blueprint of the network, this is used to demonstrate how the network should be physically connected. It additionally provides a physical view of the network to support the author when building the network. The network may differ to this plan due to the possibility of limitations however, this is roughly how the author would like the network to be. This network will have over 30 networking devices, allowing the author to meet the requirement of the network being classified as an enterprise network.

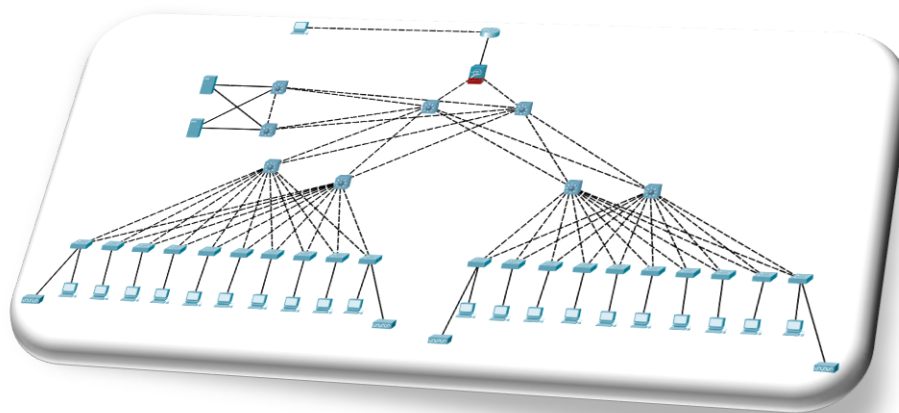


Figure 19 - Network Blueprint

4.4 Implementation

The author uses this section to document the implementation of the project. This will cover the required configurations for different devices within the network to enable communication between devices. This will additionally document software that is being. This enables the author to complete vulnerability testing to identify security weakness in the next chapter. The author will then implement solutions to reduce the risk of the network being attacked using the vulnerabilities that are discovered. The network that has been designed will be implemented on physical devices in a lab environment and on Cisco packet tracer.

4.4.1 Core Switch Configuration

The network designed includes two core switches these are the main devices of the network; in this network design, everything is routed between the core. There are two core switches to provide redundancy to the most critical section of the network. The core switches are where the VLAN information is stored and these two devices are configured as servers, all other switches are clients within the network. The author has additionally configured hot standby routing protocol on the core switches, figure 20 provides verification of the VLANs created and hot standby routing protocol has been implemented. The network uses a native VLAN trunk to communicate this is VLAN 99. In an enterprise network, the core layer usually uses high-end Cisco 6500 series switches. However, due to limitations, the core switches in the physical network are Cisco 3560 series switches, in the network simulation the Cisco 3650 series switches are used

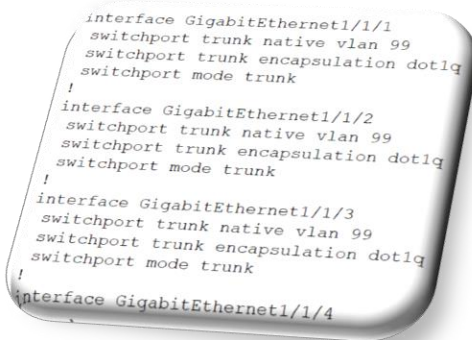


```
interface Vlan20
mac-address 0030.a36d.c701
ip address 10.10.20.2 255.255.255.0
standby 20 ip 10.10.20.1
standby 20 priority 105
standby 20 preempt
!
interface Vlan30
mac-address 0030.a36d.c702
ip address 10.10.30.2 255.255.255.0
standby 30 ip 10.10.30.1
standby 30 priority 105
standby 30 preempt
!
interface Vlan40
mac-address 0030.a36d.c703
ip address 10.10.40.2 255.255.255.0
ip helper-address 10.10.20.4
standby 40 ip 10.10.40.1
standby 40 priority 105
standby 40 preempt
!
interface Vlan50
mac-address 0030.a36d.c704
ip address 10.10.50.2 255.255.255.0
ip helper-address 10.10.20.4
standby 50 ip 10.10.50.1
standby 50 priority 105
standby 50 preempt
!
interface Vlan99
mac-address 0030.a36d.c705
ip address 10.10.99.2 255.255.255.0
ip helper-address 10.10.20.4
standby 99 ip 10.10.99.1
standby 99 priority 105
standby 99 preempt
```

Figure 20 – Core Switch Configuration

4.4.2 Distribution Switch Configuration

The distribution switches are used within the network to distribute the traffic between the core switches and access switches. Figure 21 below, shows that ports connected to either the core or access layer switches are trunking the native VLAN 99. Enterprise distribution switches are typically Cisco 4500 switches. However, due to limitations, the switches in the physical network are Cisco 3560 series, in the network simulation the Cisco 3650 series are used.

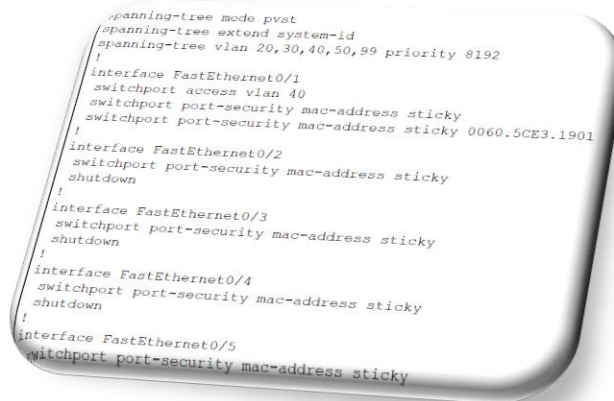


```
interface GigabitEthernet1/1
switchport trunk native vlan 99
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/2
switchport trunk native vlan 99
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/3
switchport trunk native vlan 99
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/4
```

Figure 21 – Distribution Switch Configuration

4.4.3 Access Layer Switches

The access switches are used within the network to provide access to the network, the access switches are connected to the end devices. The research conducted for the project pointed out that port security should be enabled. Figure 22 shows that the author has implemented switchport port-security with mac address sticky. This means that once a device is connected to the port the switch will save the mac address and only this device will have access to the network. If another device connects that will have a different mac address the port will shut down. The network administrator will then have to log in and shut the port down and enable the port again before it will allow access to the stored mac address device. In an enterprise network, Cisco 2960 series switches are typically used; both the physical and simulation implementations utilize these switches.



```

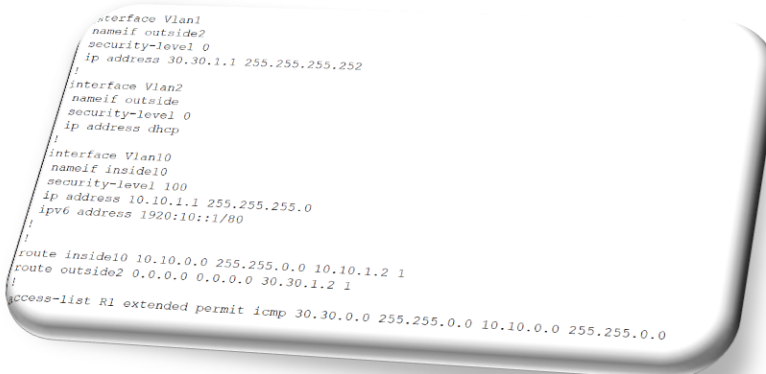
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 20,30,40,50,99 priority 8192
!
interface FastEthernet0/1
switchport access vlan 40
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0060.5CE3.1901
!
interface FastEthernet0/2
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/3
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/4
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/5
switchport port-security mac-address sticky

```

Figure 22 – Access Switch Configuration

4.4.4 Adaptive Security Appliance

The Cisco Adaptive Security Appliance is the firewall that is used between the network and the router. The aim of this is to block external traffic entering the network and allow internal communications outside the network. Figure 23 shows that the outside interface VLAN 1 has a security level of 0, and the inside VLAN 10 has a security level 100. However, there is an access list to allow remote access with a VPN through the network 30.30.0.0. In an enterprise network, it is essential to allow some employees remote access to company resources. This firewall in an enterprise network would be the Cisco Firepower 4100 series however due to limitations both the physical and simulated networks use the Cisco 5505 firewall.



```

interface Vlan1
nameif outside2
security-level 0
ip address 30.30.1.1 255.255.255.252
!
interface Vlan2
nameif outside
security-level 0
ip address dhcp
!
interface Vlan10
nameif inside10
security-level 100
ip address 10.10.1.1 255.255.255.0
ipv6 address 1920:10::1/80
!
route inside10 10.10.0.0 255.255.0.0 10.10.1.2 1
route outside2 0.0.0.0 0.0.0.0 30.30.1.2 1
!
access-list R1 extended permit icmp 30.30.0.0 255.255.0.0 10.10.0.0 255.255.0.0

```

Figure 23 – Adaptive Security Appliance Configuration

4.4.4 Wireless Access Point

The wireless access point that is being used for the network is an EnGenius wireless router. It is used to provide wireless communications for both staff and guests. Typically, in most networks more communications are wireless however, in an enterprise network there are more wired connections. The configuration of the router is on the IP address 192.168.0.1, the username and password are admin. Figure 24 shows the wireless network details, it shows that there are two different SSID's used within the network STAFF-Wi-Fi and GUEST-Wi-Fi.

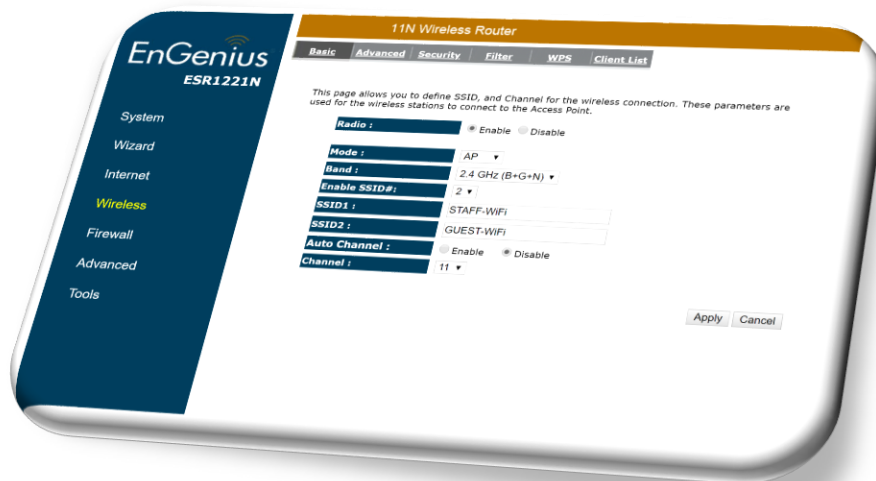


Figure 24 – Wireless Access Point (1)

Figure 25 below is used to provide evidence that the network is secured using a WPA2(AES) password. This means that the network can only be accessed by users with the password helping to protect the network from wireless attacks. The password or pre-shared key has been configured to adminadmin. The pre-shared key is the same for both networks attached to the access point.

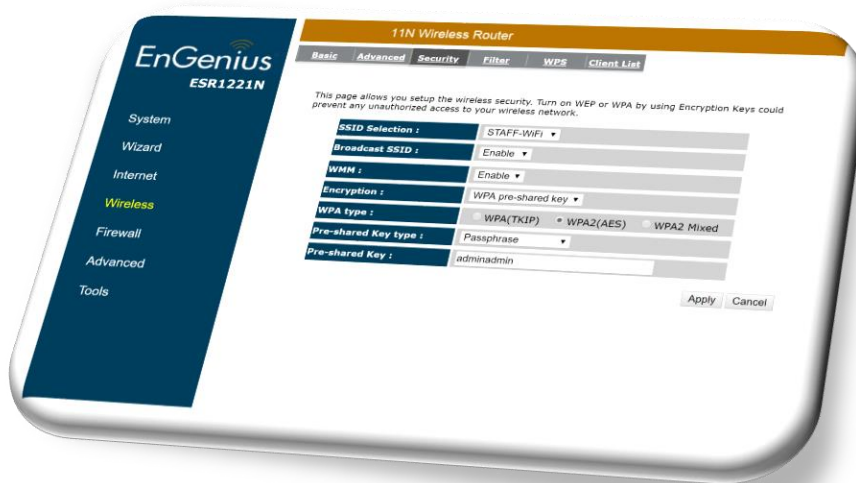


Figure 25 – Wireless Access Point (2)

4.4.5 Virtual Private Network

The implementation includes a VPN for remote access on the remote desktop. This VPN is created on the enterprise network to allow the staff remote access to company resources. Figure 26 shows an ipconfig command without the VPN and with the VPN. This figure provides evidence that the VPN has been implemented and communications to the network over the internet are using an encrypted IPsec tunnel. This ensures that traffic is kept hidden and attackers cannot access any data communications between the remote device and the network.



Figure 26 – Virtual Private Network

4.5 Conclusion

Chapter four has been very helpful in providing the author with the experience of both designing and implementing an enterprise-class network. There are some security considerations that have been implemented to protect the network however, no major security implementations have been made to allow the experimentation to test the network vulnerabilities in chapter five. Overall the author found this chapter very useful within the project as it provides a platform for the experiments to be conducted within. The next chapter is results and findings, this will discuss what experiments will be carried out and if the experiments were successful.

Chapter 5 – Results and Findings

5.1 Introduction

The author will use chapter five to document the results and findings from the implementation and experiments that will be done to have a successful outcome for the project. The experiments that are going to be conducted, if successful there will additionally be solutions provided to prevent the attack being used to obtain unauthorized access to the enterprise network. This chapter will cover several different attacks that are commonly used by attackers to attack networks.

5.2 Vlan Hopping Attack

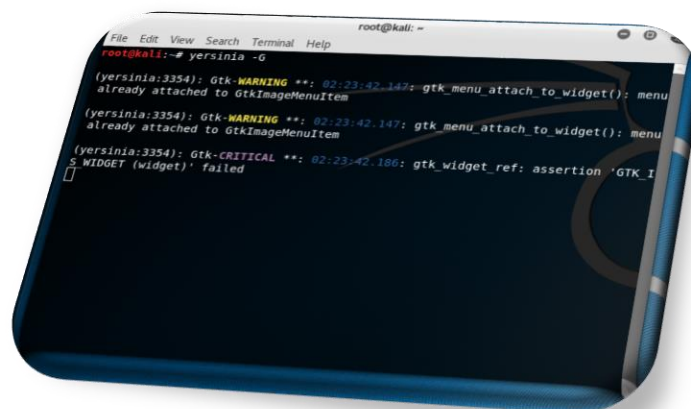
The network that the author has designed and implemented uses several VLANS these are servers 1, servers 2, staff, guest and management. The implementation of VLANS helps protect the network ensuring an attacker would have access to a limited single, for example, a guest would not have access to the staff VLAN unless the traffic is routed through the layer three switches. All-access switches have access to a single VLAN either staff or guest access. This attack will investigate if the network is susceptible to switch spoofing. This will be conducted by the attacker being connected to access switch 1 and connected to switchport f0/24. The attacker will have access to the guest VLAN 50. The switch configuration can be seen in figure 27 below, verify that the port is set to access the guest VLAN.



```
interface FastEthernet0/23
switchport port-security mac-address sticky
shutdown
interface FastEthernet0/24
switchport access vlan 50
switchport port-security mac-address sticky
interface GigabitEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
```

Figure 27 - Vlan Hopping Attack (1)

The attacking device was then connected to switchport f0/24. The attack is conducted within Kali Linux through software called Yersinia. The first stage was to launch a root terminal and type the command yersinia -G, this is shown in figure 28 below.



```
root@kali: ~
root@kali:~# yersinia -G
(yersinia:3354): Gtk-WARNING **: 02:23:42.142: gtk_menu_attach_to_widget(): menu
already attached to GtkImageMenuItem
(yersinia:3354): Gtk-WARNING **: 02:23:42.147: gtk_menu_attach_to_widget(): menu
already attached to GtkImageMenuItem
(yersinia:3354): Gtk-CRITICAL **: 02:23:42.186: gtk_widget_ref: assertion 'GTK_I
S_WIDGET (widget)' failed
```

Figure 28 - Vlan Hopping Attack (2)

When Yersinia launches, it gives you the options on what to do with it, the first stage is to click choose attack, this enables the attacker to choose what interface to launch the attack from. The interface that was selected was ethernet. This then launches the attack options that can be seen in figure 29 below.



Figure 29 - Vlan Hopping Attack (3)

The next stage is to select the type of attack that is being conducted, in this case, it is a dynamic trunking protocol attack, so DTP is clicked. This launches the window that can be seen in figure 30. The final stage of this attack is to choose to send a DTP packet or enable trunking, for this attack enable trunking was selected then click ok.



Figure 30 - Vlan Hopping Attack (4)

Figure 31 below shows that the attack has been launched successfully and the switchport has changed from switchport access VLAN 50 to switchport mode trunk. This now gives the attacker access to the entire network and allows for further attacks to be conducted by the attacker.

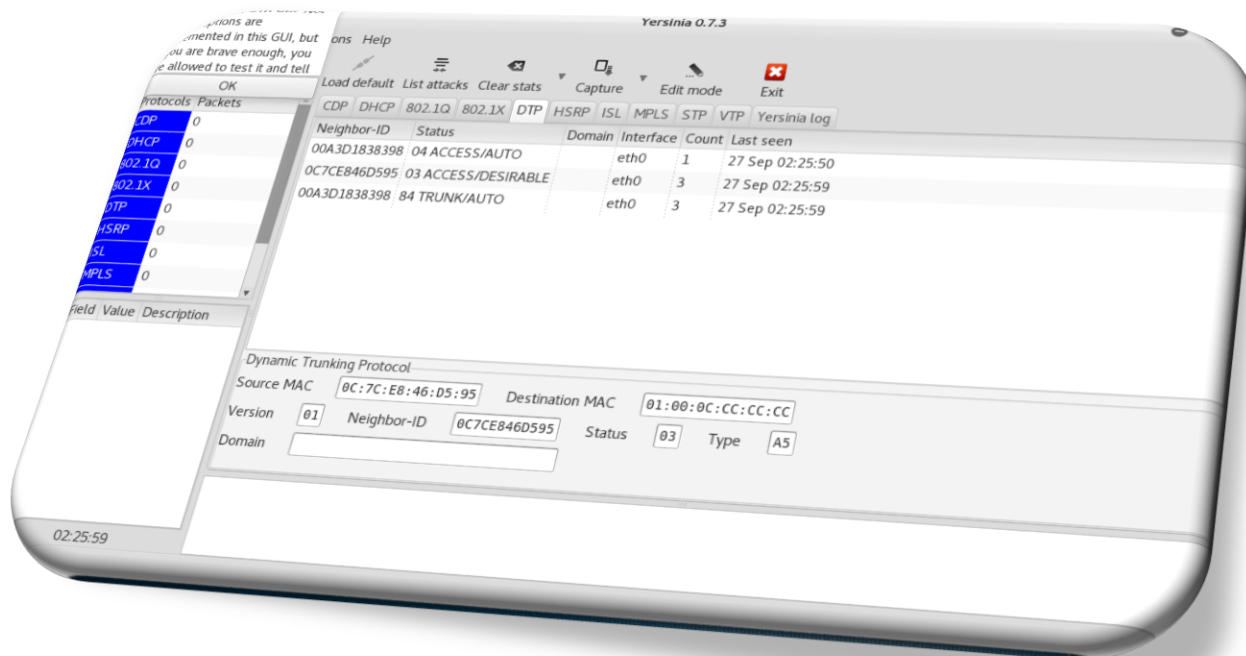


Figure 31 - Vlan Hopping Attack (5)

Figure 32 below shows the status of switchport f0/24 before the attack and the trunked interfaces. It then shows the attack has been conducted and the status of switchport f0/24 has changed to trunk. This shows that the attack has been conducted successfully and the results are as expected from earlier research in chapter 2.

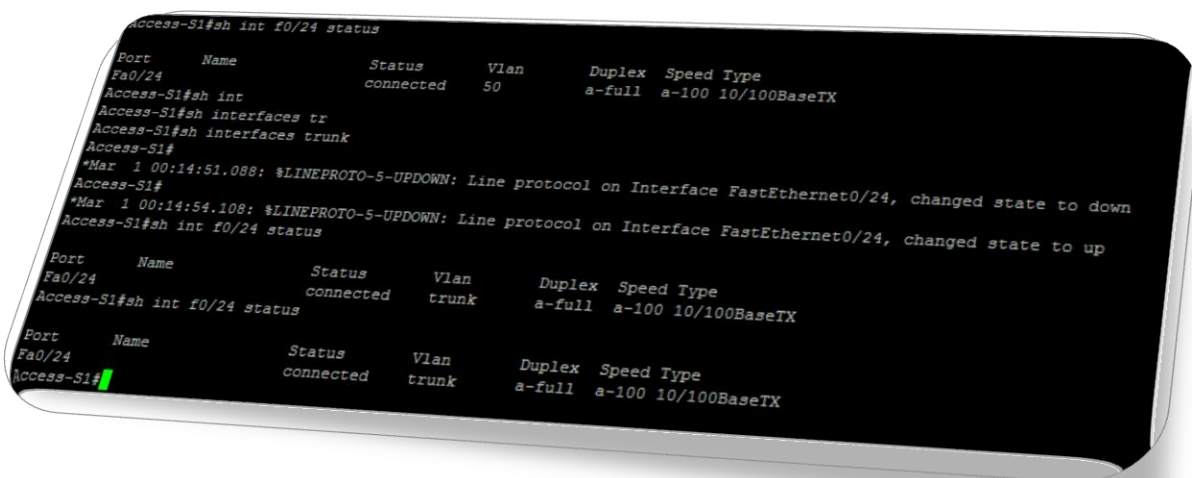


Figure 32 - Vlan Hopping Attack (6)

The next step was a solution to this type of attack, this was identified within the research and literature section of the document to be to set the state of the switch by entering switchport mode access, this ensures that the switchport is only able to access one single VLAN in access mode. Figure 33 below is used to verify the configuration has been updated before the attack is conducted to ensure the network is safe from this type of attack.

```
interface FastEthernet0/24
switchport access vlan 50
switchport mode access
switchport port-security mac-address sticky
!
interface GigabitEthernet0/1
switchport trunk native vlan 99
switchport mode trunk
```

Figure 33 - Vlan Hopping Attack (7)

Figure 34 below shows that the attack has been run again, however, the switchport status has stayed at access/desirable. This shows that the attack has not been successful therefore providing clear evidence that the network is protected from this vulnerability.



Figure 34 - Vlan Hopping Attack (8)

5.3 Wi-Fi Password Cracking

The first step of this attack is to start the wireless card. This is done by opening a terminal window, then typing `airmon-ng start wlan0`. Figure 35 below shows the command and demonstrates the output given once the command has been entered.

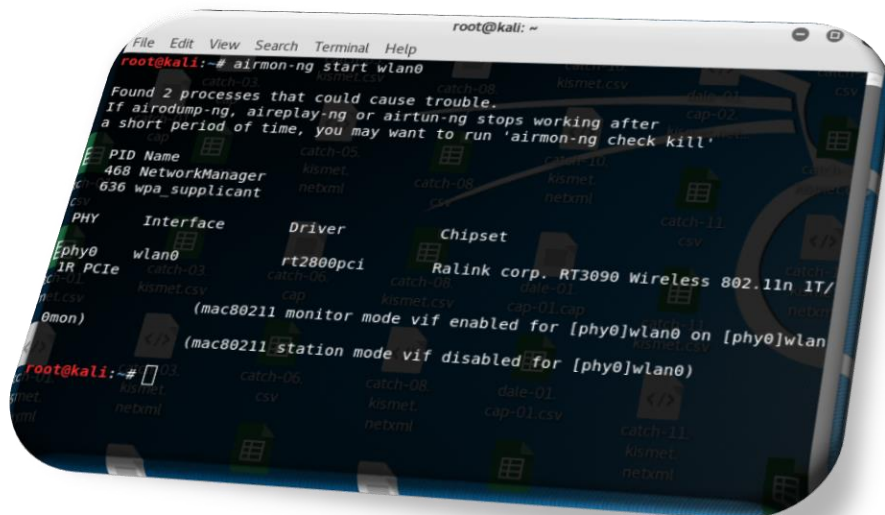


Figure 35 – Wi-Fi Password Crack (1)

Monitoring mode must now be enabled, this is turned on by entering the command `airodump-ng wlan0mon`. This will then scan for all wireless networks in the area, this allows for the staff network to be located that is at the top of the list in figure 36. It is important to make a note of the BSSID of the network being 88:DC:96:03:E4:20. The next stage is to only monitor the staff network, this is done by typing `airodump-ng -c 11 -b 88:DC:96:03:E4:20 -w test wlan0mon`.



Figure 36 – Wi-Fi Password Crack (2)

Figure 37 shows two windows, the left window shows the network is being scanned and once traffic is monitored on the target network the attack is ready for the next stage. This can be seen in the right window. A new terminal is opened and the command `aireplay-ng -0 0 -a 88:DC:96:03:E4:20 wlan0mon`. This then forces the device to reconnect and gives a WPA handshake as can be seen in the top right of the left window.



Figure 37 – Wi-Fi Password Crack (3)

The final step is to use aircrack-ng to attempt to crack the password. This is done by typing `aircrack-ng -w root/Desktop/fasttrack.txt root/Desktop/test-01.cap`. This is telling the software to test the wordlist `fasttrack.txt` against the `test-01.cap` handshake capture file. Figure 38 demonstrates the window that launches after this command has been entered. The software will then test the password list until all passwords have been tested if the password is found it will show key found [adminadmin] as in figure 38. This demonstrates that the attack has been successful and found the password to the wireless network. The solution to this type of attack is to first always use complex passwords of more than 8 characters, including a mixture of different cases, symbols, and numbers.

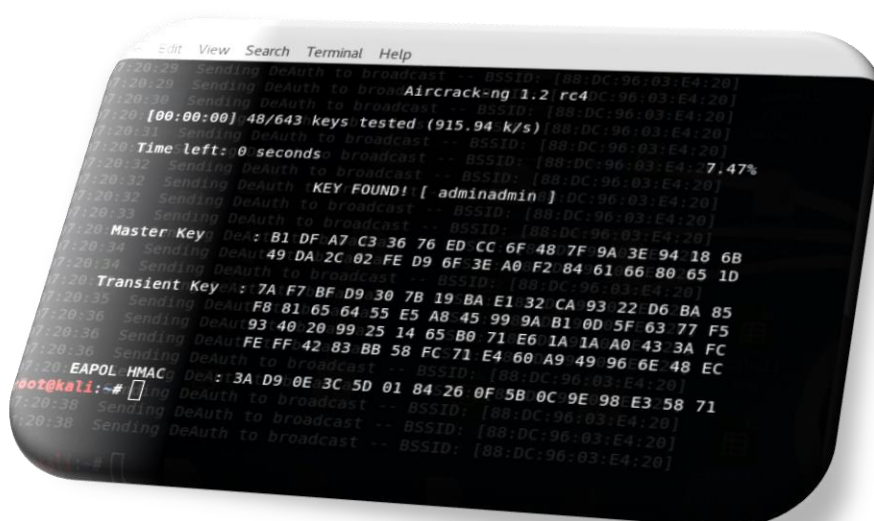


Figure 38 – Wi-Fi Password Crack (4)

The solution that has been implemented within the network is what would typically be used within an enterprise environment. This is to ensure that wireless access points are authenticated using a wireless local area controller. The controller then uses WPA2 authentication, but this is done through a radius server as can be seen in figure 39.



Figure 39 – Wi-Fi Password Crack (5)

Figure 40 below demonstrates the radius server that has been implemented to secure the network from password cracking. The radius server is then used by the access points to authenticate users. It allows users to have a unique username and password to further secure the network, these users can be added or removed easily to ensure that access is only granted to the users that require it. However, it is still important to ensure that complex passwords are used. These implementations ensure that the network has been secured from this type of attack in the future.



Figure 40 – Wi-Fi Password Crack (6)

5.4 **Conclusion**

Overall the author believes that this chapter has been successful, the attacks that have been conducted have outlined vulnerabilities that existed within the network. The author has identified solutions to each of these attacks and implemented them within the network to prevent the attacks from happening in the future. The next chapter is a conclusion and recommendations, this is where the author will conclude the project and outline recommendations for future research.

Chapter 6 – Conclusion & Recommendations

6.1 Introduction

This chapter will be used to give an overview of the work that has been completed for this project. The author will summarize the project, then move onto a conclusion to conclude the work that has been completed. The conclusion will discuss if the project is successful in meeting the requirements outlined by the author in chapter one. This chapter will then move onto recommendations for future research. The author will have the ability to determine what could be further investigated in the future to obtain better results and findings from the project.

6.2 Summary

This project is to design and implement a secure enterprise network. Chapter two was used to document the research that was conducted to provide the knowledge required to complete this project. The next chapter was then used to investigate how the research onion relates to this project. The research onion provided the author with the structure that was followed to enable a successful outcome from this project. The fourth chapter was the design and implementation section of the project. It was important to ensure that the network design met the requirements. The chapter provided the author with a testbed to conduct the attacks in chapter five. Chapter five is the most essential section of the project. This is where the experiments were carried out. The VLAN hopping attack was the attack that the author found most interesting. These attacks highlighted major security vulnerabilities that the author implemented solutions to prevent these types of attacks in the future.

6.3 Conclusion

This section of the document will investigate the aim and objectives outlined at the beginning of this project and see how each one has been met. This will allow the author to have a definitive conclusion of the outcome of the project. The aim of this project is to design and implement an enterprise-class network with a minimum of 30 networking devices. This will enable the author to conduct experiments, to investigate weaknesses within the network allowing solutions to be implemented to secure the network. The objectives of this project are to investigate enterprise-class networks and vulnerabilities to implement solutions to prevent these attacks from happening on the network.

- Research enterprise-class networks
- Research networking devices
- Investigate several vulnerabilities and solutions to be used for the project
- Plan and implement an enterprise-class network that consisting of more than 30 networking devices
- Conduct experiments and configure solutions to secure the network

The author used chapter two to document the research that has been conducted for this project. This included research on the following topics enterprise-class networks, networking devices, network threats, and network defences and countermeasures. This allowed the author to successfully achieve three of the objectives in this chapter. Chapter three used the research onion to outline a methodology that could be used to allow the author to complete this project. The author found the methodology to be helpful in providing a structure for the project to be completed with.

Chapter four was used to complete the design and implementation section of the report. This enabled the author to have an enterprise-class network build to continue onto chapter five. Chapter four met the fourth objective by having more than 30 devices within the network that was designed and implemented. Chapter five was used for the results and findings section of the document. This section of the report was used to document each of the experiments that were conducted within the project. The author then documented solutions to the attacks and implemented them within the network to prevent these attacks from being used against the network in the future. This enabled the author to meet the last objective that was outlined at the beginning of the project. Overall the author believes that the aim and objectives have been met within the project. This gives the author confirmation that the project was successful as all aims and objectives set out have been met.

6.4 Recommendations for Future Research

This project has outlined several areas for future research. The first area that the author feels there could be improvements made is understanding Kali Linux. If the author had a better understanding of the Linux operating system there may have been possibilities to further improve the attacks that were conducted within the project. Therefore, the author has chosen this as the first area for future research. The next area for future research is to conduct further attacks against the network, this will outline further vulnerabilities within the security of the network and enable the author to better protect the network. However, threats are advancing daily and becoming more sophisticated so a network will never be 100% secure. This is why it is important to try and prevent as many threats as possible.

Chapter 7 – Reflections

7.1 Introduction

This chapter will be used to discuss how the project was completed. This chapter will investigate both the positive and negative aspects of the project and conclude. The positives of the project will investigate what went well within the project and investigate why it went well. Additionally, the negatives of the project will be investigated. This will investigate what wasn't as successful and why it wasn't. The conclusion will then conclude on the outcome of the project.

7.2 Positives

The author found the related work section of the project very helpful in the completion of this project. This section of the report was used to document the related work that was required as background information to enable the author to understand each section of the project. The author found the third chapter to be very useful in providing a clear and detailed methodology that was followed to allow the project to be completed successfully. However, this had to be used in conjunction with the Gantt chart to ensure that everything was completed on schedule.

This brings the author to the next positive aspect of the project is time management. The Gantt chart enabled the author to understand what needed to be done and when it had to be completed to allow the project to be finished on time. The last positive aspect of the project was the design and implementation section of the project. The author feels like this was a very successful part of the project by meeting the aim and objective set out at the beginning of this project.

7.3 Negatives

The author found that the understanding of Kali Linux operating system was the first negative. Unfortunately, the author had only limited knowledge of the operating system. Therefore, if further research was conducted on Kali Linux the author believes the experiments that were completed could have been enhanced. The author feels that this would have improved the project outcome. The final negative of this project was not being able to attend project meetings due to other commitments. The author feels that with additional guidance and supports the outcome would have been improved.

7.4 Objectives

The author outlined several objectives at the start of this project. This section of the report will investigate how each of these was completed during the project. The first objective was "Research enterprise-class networks", chapter two section two was used to investigate what enterprise networks are and what they are used for. The next objective was "Research networking devices", chapter two section three was used to investigate different networking devices. The next objective was "Investigate several vulnerabilities and solutions to be used for the project", this was achieved in chapter two section four where network threats and solutions were investigated.

The next objective was "Design and implement an enterprise-class network that consists of more than 30 networking devices", this was met in chapter four where a network consisting of more than 30 networking devices was both designed and implemented. The final objective was "conduct the penetration testing and implement solutions to secure the network", this was completed in chapter five and solution have been implemented within the physical and virtual networks.

7.5 **Conclusion**

The author feels that the project has been completed to a successful outcome, the reasoning behind this decision is the fact that both the aim and objectives set out in chapter one of the project have all been successfully met. However, the author does feel that the project could have been improved by improving the authors understanding of Kali Linux and conducting additional attacks. Additionally, the quality of the project could have been improved by being able to attend project meetings.

References

- [1] A. Aguilar-Gonzalez, J. A. Nolasco-Flores, C. Vargas-Rosales, and R. Bustos, "Characterisation, design and simulation of an efficient peer-to-peer content distribution system for enterprise networks," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 122–137, 2017.
- [2] A. M. Shabalin and E. A. Kaliberda, "The organization of arrangements set to ensure enterprise IPV6 network secure work by modern switching equipment tools (using the example of a network attack on a default gateway)," in *11th International IEEE Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines", Dynamics 2017 - Proceedings*, 2017, vol. 2017-Novem, pp. 1–8.
- [3] N. Vignesh, R. Lohith, S. Arun Kumar, H. Dagale, and K. Sangeeta, "An IOT based network management system for enterprise network," in *Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017*, 2018, pp. 1089–1093.
- [4] "cso_computer_infection_spreading_virus_worm_by_juan_fernando_velez_melguizo_gettyimages-1082271852_2400x1600-100807410-large.jpg (1200×800)." [Online]. Available: https://images.idgesg.net/images/article/2019/08/cso_computer_infection_spreading_virus_worm_by_juan_fernando_velez_melguizo_gettyimages-1082271852_2400x1600-100807410-large.jpg. [Accessed: 23-Sep-2019].
- [5] H. A. Khan, A. Syed, A. Mohammad, and M. N. Halgamuge, "Computer virus and protection methods using lab analysis," in *2017 IEEE 2nd International Conference on Big Data Analysis, ICBDA 2017*, 2017, pp. 882–886.
- [6] Z. J. Jia, Y. Y. Yang, and N. Guo, "Research on computer virus source modeling with immune characteristics," in *Proceedings of the 29th Chinese Control and Decision Conference, CCDC 2017*, 2017, pp. 4616–4619.
- [7] 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 *Proceedings of 2018 15th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2018*, 2018, vol. 2018-Janua, pp. 415–421.
- [8] "Picture2.png (974×370)." [Online]. Available: <https://securityledger.com/wp-content/uploads/2019/04/Picture2.png>. [Accessed: 23-Sep-2019].
- [9] B. Chen and Y. Shi, "Malicious Hidden Redirect Attack Web Page Detection Based on CSS Features," in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, 2019, pp. 1155–1159.
- [10] H. Kikuchi, H. Matsumoto, and H. Ishii, "Automated Detection of Drive-By Download Attack," in *Proceedings - 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2015*, 2015, pp. 511–515.
- [11] A. K. Sood and S. Zeadally, "Drive-By Download Attacks: A Comparative Study," *IT Prof.*, vol. 18, no. 5, pp. 18–25, Sep. 2016.
- [12] "ddos-botnet-star-network-topology.png (1400×934)." [Online]. Available: <https://www.cloudflare.com/img/learning/ddos/what-is-a-ddos-botnet/ddos-botnet-star-network-topology.png>. [Accessed: 23-Sep-2019].
- [13] G. Vormayr, T. Zseby, and J. Fabini, "Botnet Communication Patterns," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2768–2796, 2017.
- [14] B. Alothman and P. Rattadilok, "Towards using transfer learning for Botnet Detection," in *2017 12th International Conference for Internet Technology and Secured Transactions, ICITST 2017*, 2018, pp. 281–282.

- [15] S. C. Chen, Y. R. Chen, and W. G. Tzeng, "Effective Botnet Detection Through Neural Networks on Convolutional Features," in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 2018, pp. 372–378.
- [16] H. Dhayal and J. Kumar, "Botnet and P2P Botnet Detection Strategies: A Review," in *Proceedings of the 2018 IEEE International Conference on Communication and Signal Processing, ICCSP 2018*, 2018, pp. 1077–1082.
- [17] K. Alieyan, M. Anbar, A. ALmomani, R. Abdullah, and M. Alauthman, "Botnets Detecting Attack Based on DNS Features," in *ACIT 2018 - 19th International Arab Conference on Information Technology*, 2019, pp. 1–4.
- [18] "iStock-184016998.jpg (1254×837)." [Online]. Available: <https://s27942.pcdn.co/wp-content/uploads/2018/10/iStock-184016998.jpg>. [Accessed: 23-Sep-2019].
- [19] M. Baykara and Z. Z. Gürel, "Detection of phishing attacks," in *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, 2018, vol. 2018-Janua, pp. 1–5.
- [20] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 2017, pp. 537–540.
- [21] T. Churi, P. Sawardekar, A. Pardeshi, and P. Vartak, "A secured methodology for anti-phishing," in *Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017*, 2018, vol. 2018-Janua, pp. 1–4.
- [22] "RTX35YNS-1024x765.jpg (1024×765)." [Online]. Available: <https://d3i6fh83elv35t.cloudfront.net/newshour/app/uploads/2017/05/RTX35YNS-1024x765.jpg>. [Accessed: 23-Sep-2019].
- [23] R. Agrawal, J. W. Stokes, K. Selvaraj, and M. Marinescu, "Attention in Recurrent Neural Networks for Ransomware Detection," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2019, vol. 2019-May, pp. 3222–3226.
- [24] I. Kara and M. Aydos, "Static and Dynamic Analysis of Third Generation Cerber Ransomware," in *International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, IBIGDELFT 2018 - Proceedings*, 2019, pp. 12–17.
- [25] S. Saxena and H. K. Soni, "Strategies for ransomware removal and prevention," in *Proceedings of the 4th IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB 2018*, 2018, pp. 1–4.
- [26] B. Lokuketagoda, M. P. Weerakoon, U. M. Kuruppu, A. N. Senarathne, and K. Yapa Abeywardena, "R - Killer: An email based ransomware protection tool," in *13th International Conference on Computer Science and Education, ICCSE 2018*, 2018, pp. 735–741.
- [27] A. Chuquilla, T. Guarda, and G. Ninahualpa Quina, "Ransomware - WannaCry Security is everyone's," in *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 2019, pp. 1–4.
- [28] "4.jpg (670×212)." [Online]. Available: <https://s8185.pcdn.co/wp-content/uploads/2013/10/4.jpg>. [Accessed: 23-Sep-2019].
- [29] "firewall-diagram.png (650×300)." [Online]. Available: <https://www.howtogeek.com/wp-content/uploads/2013/04/firewall-diagram.png>. [Accessed: 23-Sep-2019].
- [30] H. M. T. Al-Hilfi, B. A. Salih, and I. Marghescu, "Design of secured WLAN by using

- ‘packet filtering firewall,’” in *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, 2018, vol. 2018-Janua, pp. 1857–1862.
- [31] S. Lin, D. Zhang, Y. Fu, and S. Wang, “A design of the ethernet firewall based on FPGA,” in *Proceedings - 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics, CISP-BMEI 2017*, 2018, vol. 2018-Janua, pp. 1–5.
- [32] N. Gupta, V. Naik, and S. Sengupta, “A firewall for Internet of Things,” in *2017 9th International Conference on Communication Systems and Networks, COMSNETS 2017*, 2017, pp. 411–412.
- [33] K. Neupane, R. Haddad, and L. Chen, “Next Generation Firewall for Network Security: A Survey,” in *Conference Proceedings - IEEE SOUTHEASTCON*, 2018, vol. 2018-April, pp. 1–6.
- [34] P. R. Chandre, P. N. Mahalle, and G. R. Shinde, “Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification,” in *Proceedings - 2018 IEEE Global Conference on Wireless Computing and Networking, GCWCN 2018*, 2019, pp. 135–140.
- [35] A. Pomsathit, “Performance analysis of intrusion prevention system on cyber security for voice over Internet protocol (VoIP),” in *11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, 2016, pp. 5–5.
- [36] B. Siregar, R. F. Dwiputra Purba, Seniman, and F. Fahmi, “Intrusion Prevention System Against Denial of Service Attacks Using Genetic Algorithm,” in *2018 IEEE International Conference on Communication, Networks and Satellite, Comnetsat 2018 - Proceedings*, 2019, pp. 55–59.
- [37] S. Ravji and M. Ali, “Integrated Intrusion Detection and Prevention System with Honeypot in Cloud Computing,” in *Proceedings - 2018 International Conference on Computing, Electronics and Communications Engineering, iCCECE 2018*, 2019, pp. 95–100.
- [38] “img_59420b2523f30.png (640×379).” [Online]. Available: https://i1.wp.com/www.bansalonsecurity.com/wp-content/uploads/2017/11/img_59420b2523f30.png?resize=640%2C379&ssl=1. [Accessed: 23-Sep-2019].
- [39] R. Samrin and D. Vasumathi, “Review on anomaly based network intrusion detection system,” in *International Conference on Electrical, Electronics, Communication Computer Technologies and Optimization Techniques, ICEECCOT 2017*, 2018, vol. 2018-Janua, pp. 141–147.
- [40] M. E. Pamukov and V. K. Poulkov, “Multiple negative selection algorithm: Improving detection error rates in IoT intrusion detection systems,” in *Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017*, 2017, vol. 1, pp. 543–547.
- [41] A. Garg and P. Maheshwari, “A hybrid intrusion detection system: A review,” in *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016*, 2016, pp. 1–5.
- [42] A. Warzynski and G. Kolaczek, “Intrusion detection systems vulnerability on adversarial examples,” in *2018 IEEE (SMC) International Conference on Innovations in Intelligent Systems and Applications, INISTA 2018*, 2018, pp. 1–4.
- [43] A. Borkar, A. Donode, and A. Kumari, “A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS),” in *Proceedings of the International Conference on Inventive Computing and Informatics, ICICI 2017*, 2018,

- pp. 949–953.
- [44] “free-encryption.jpg (700×479).” [Online]. Available: <http://documents.trendmicro.com/images/TEEx/articles/free-encryption.jpg>. [Accessed: 23-Sep-2019].
 - [45] S. A. Khan, R. K. Aggarwal, and S. Kulkarni, “Encryption Schemes of Cloud Computing: A Review,” in *2019 5th International Conference on Advanced Computing and Communication Systems, ICACCS 2019*, 2019, pp. 23–26.
 - [46] B. Daddala, H. Wang, and A. Y. Javaid, “Design and implementation of a customized encryption algorithm for authentication and secure communication between devices,” in *Proceedings of the IEEE National Aerospace Electronics Conference, NAECON*, 2018, vol. 2017-June, pp. 258–262.
 - [47] K. Huang, R. Tso, and Y. C. Chen, “One-time-commutative public key encryption,” in *Proceedings of Computing Conference 2017*, 2018, vol. 2018-Janua, pp. 814–818.
 - [48] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, “Comprehensive study of symmetric key and asymmetric key encryption algorithms,” in *Proceedings of 2017 International Conference on Engineering and Technology, ICET 2017*, 2018, vol. 2018-Janua, pp. 1–7.
 - [49] “How-VPN-Work.jpg (1140×600).” [Online]. Available: <https://www.allbestvpn.com/wp-content/uploads/2019/02/How-VPN-Work.jpg>. [Accessed: 23-Sep-2019].
 - [50] D. Deshmukh and B. Iyer, “Design of IPsec virtual private network for remote access,” in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2017*, 2017, vol. 2017-Janua, pp. 716–719.
 - [51] G. Lopez and E. Grampin, “Scalability testing of legacy MPLS-based Virtual Private Networks,” in *2017 IEEE URUCON, URUCON 2017*, 2017, vol. 2017-Decem, pp. 1–4.
 - [52] T. Lackorzynski, S. Kopsell, and T. Strufe, “A Comparative Study on Virtual Private Networks for Future Industrial Communication Systems,” in *2019 15th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2019, pp. 1–8.
 - [53] P. Majumdar, A. Pandey, S. K. Khatri, R. Jain, R. Majumdar, and V. P. Mishra, “Combination of Virtual Private Network and Wireless Sensor Network: Protection Against the Interference Problem of IOT,” in *2019 Advances in Science and Engineering Technology International Conferences, ASET 2019*, 2019, pp. 1–6.
 - [54] “150886501059ef73f2ea4109.97677128.jpg (1633×918).” [Online]. Available: <http://vestnikkavkaza.net/upload2/2017-10-24/150886501059ef73f2ea4109.97677128.jpg>. [Accessed: 23-Sep-2019].
 - [55] I. Martin, J. A. Hernandez, and S. De Los Santos, “SignatureMiner: A fast anti-virus signature intelligence tool,” in *2018 IEEE Conference on Communications and Network Security, CNS 2018*, 2018, pp. 1–2.
 - [56] D. Xu, X. Xu, C. Yang, and W. Gui, “SIVR spreading model with anti-virus factor in complex networks,” in *Proceedings of the 28th Chinese Control and Decision Conference, CCDC 2016*, 2016, pp. 101–106.
 - [57] S. Talukder, S. Roy, and T. Al Mahmud, “An Approach for An Distributed Anti-Malware System Based on Blockchain Technology,” in *2019 11th International Conference on Communication Systems and Networks, COMSNETS 2019*, 2019, pp. 1–6.
 - [58] Z. Fang, J. Wang, B. Li, S. Wu, Y. Zhou, and H. Huang, “Evading Anti-Malware Engines with Deep Reinforcement Learning,” *IEEE Access*, vol. 7, pp. 48867–48879, 2019.
 - [59] “diagram-security.jpg (1318×1000).” [Online]. Available: <http://www.keystonenap.com/wp-content/uploads/2014/11/diagram-security.jpg>.

- [Accessed: 23-Sep-2019].
- [60] "email-security-xs.jpg (1000×750)." [Online]. Available: <https://www.welivesecurity.com/wp-content/uploads/2019/01/email-security-xs.jpg>. [Accessed: 23-Sep-2019].
- [61] T. Li, A. Mehta, and P. Yang, "Security Analysis of Email Systems," in *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, 2017, pp. 91–96.
- [62] Y. G. Zeng, "Identifying email threats using predictive analysis," in *2017 International Conference on Cyber Security And Protection Of Digital Services, Cyber Security 2017*, 2017, pp. 1–2.
- [63] K. Om, "Secure email gateway," in *2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, ICSTM 2017 - Proceedings*, 2017, pp. 49–53.
- [64] "03fig01.jpg (360×279)." [Online]. Available: http://ptgmedia.pearsoncmg.com/images/chap3_9781587133183/elementLinks/03fig01.jpg. [Accessed: 23-Sep-2019].
- [65] M. B. Lehocine and M. Batouche, "Flexibility of managing VLAN filtering and segmentation in SDN networks," in *2017 International Symposium on Networks, Computers and Communications, ISNCC 2017*, 2017, pp. 1–6.
- [66] S. Jeuk, G. Salgueiro, F. Baker, and S. Zhou, "Network segmentation in the cloud a novel architecture based on UCC and IID," in *2015 IEEE 4th International Conference on Cloud Networking, CloudNet 2015*, 2015, pp. 58–63.
- [67] "Cisco-wireless-controller-1.png (1111×674)." [Online]. Available: <https://www.speaknetworks.com/wp-content/uploads/2015/07/Cisco-wireless-controller-1.png>. [Accessed: 23-Sep-2019].
- [68] B. Jay White, P. Manager, and W.-F. Solutions, "TECHNOLOGY FEATURE » Internet of Things (IoT)," 2017.
- [69] L. J. Chen, D. X. Chen, L. Xie, and J. N. Cao, "Evolution of wireless sensor network," in *IEEE Wireless Communications and Networking Conference, WCNC*, 2007, pp. 3005–3009.
- [70] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep-2016.
- [71] A. Kavianpour and M. C. Anderson, "An Overview of Wireless Network Security," in *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, 2017, pp. 306–309.
- [72] "access-control-access-granted.jpg (1000×667)." [Online]. Available: <https://www.tedsystems.com/wp-content/uploads/2019/03/access-control-access-granted.jpg>. [Accessed: 23-Sep-2019].
- [73] J. H. Huh *et al.*, "Next-Generation Access Control for Distributed Control Systems," *IEEE Internet Comput.*, vol. 20, no. 5, pp. 28–37, Sep. 2016.
- [74] J. Wei, G. Yang, and Y. Mu, "Comments on 'Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks,'" *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, pp. 3097–3099, Apr-2016.
- [75] A. Sunaina and R. Poojary, "Breakthrough in access control technology," in *2017 International Conference on Electrical and Computing Technologies and Applications, ICECTA 2017*, 2018, vol. 2018-Janua, pp. 1–4.
- [76] F. Xu, C. Qiu, A. Guo, and C. Zhao, "Access control for software-defined heterogeneous

- wireless access network,” in *2016 16th International Symposium on Communications and Information Technologies, ISCIT 2016*, 2016, pp. 520–524.
- [77] “MFA.png (500×500).” [Online]. Available: <https://velvot.com/demo/wp-content/uploads/2018/07/MFA.png>. [Accessed: 23-Sep-2019].
- [78] D. Gugelmann, P. Studerus, V. Lenders, and B. Ager, “Can Content-Based Data Loss Prevention Solutions Prevent Data Leakage in Web Traffic?,” *IEEE Security and Privacy*, vol. 13, no. 4, pp. 52–59, Jul-2015.
- [79] A. Boranbayev, M. Mazhitov, and Z. Kakhanov, “Implementation of security systems for prevention of Loss of Information at Organizations of Higher Education,” in *Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015*, 2015, pp. 802–804.
- [80] E. Costante, D. Fauri, S. Etalle, J. Den Hartog, and N. Zannone, “A Hybrid Framework for Data Loss Prevention and Detection,” in *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*, 2016, pp. 324–333.
- [81] D. Yuan, “Design and develop hands on cyber-security curriculum and laboratory,” in *Proceedings of Computing Conference 2017*, 2018, vol. 2018-Janua, pp. 1176–1179.
- [82] “The-research-process-onion-Saunders-et-al-2003-p-83.png (850×500).” [Online]. Available: https://www.researchgate.net/profile/Jenifer_Piesse/publication/227224340/figure/fig7/AS:393626166284292@1470859199160/The-research-process-onion-Saunders-et-al-2003-p-83.png. [Accessed: 23-Sep-2019].

Appendices

Figure 41 demonstrates the original Gantt chart used within the project proposal the finish date was the 21 august 2019 however, figure 42 below demonstrates that the project was finished on the 20 September 2019. This shows that the authors original Gantt chart was not really accurate with the timings required to complete each section of the report.

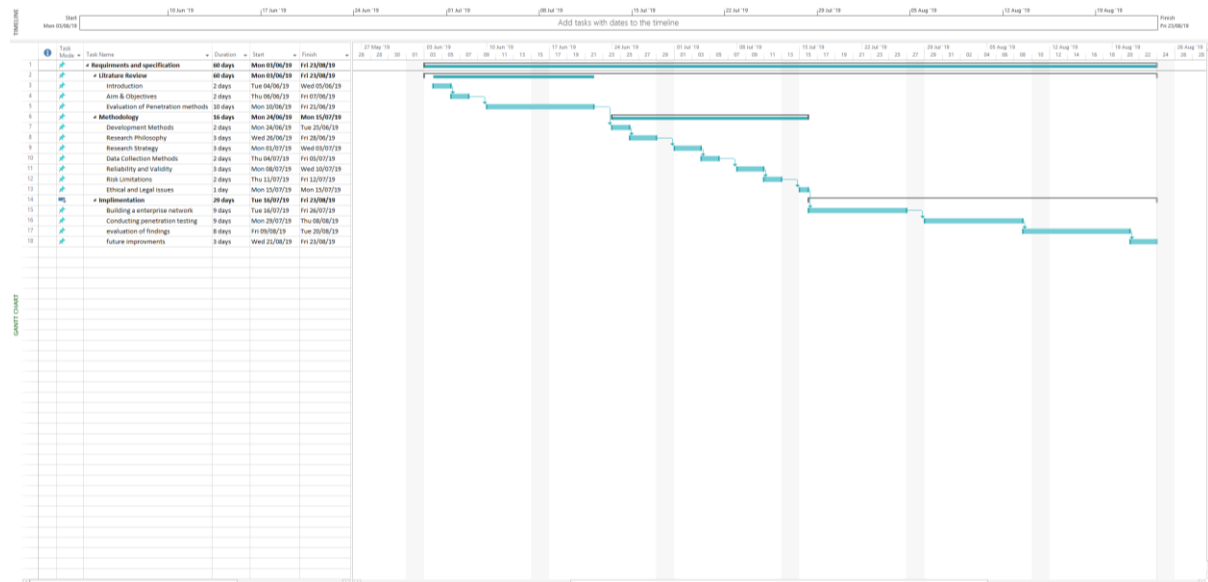


Figure 41 –Gantt Chart (1)

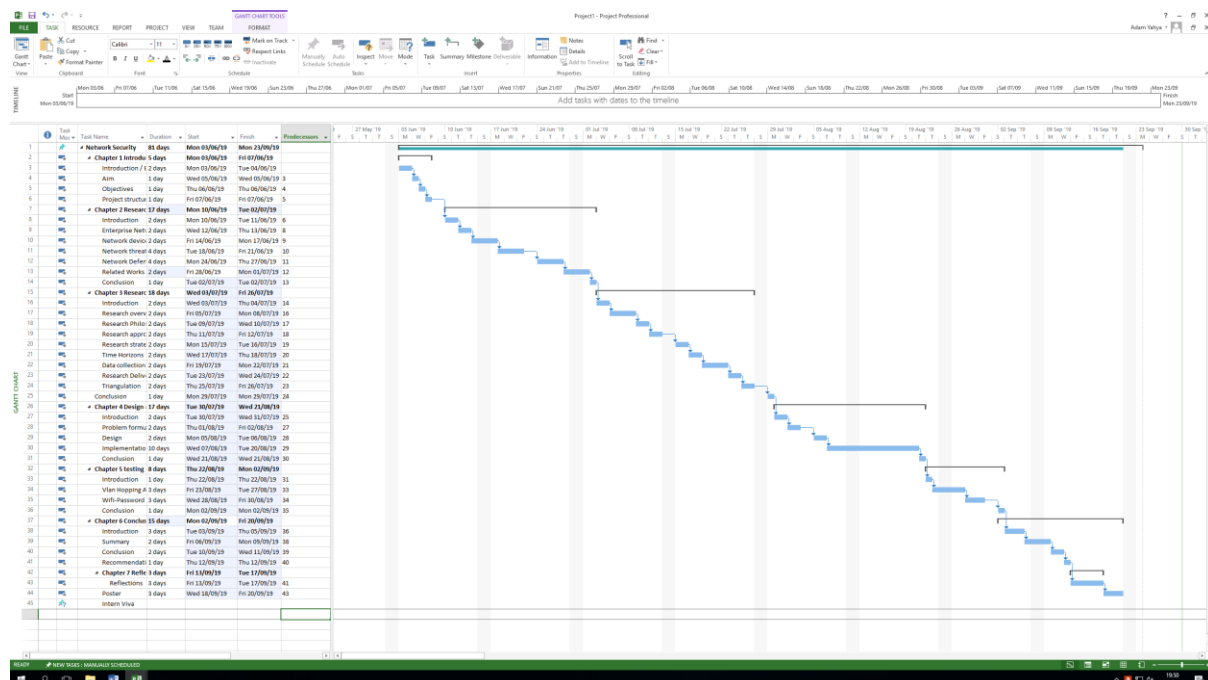


Figure 42 –Gantt Chart (2)