

Assessed Coursework 1 (ACW1), Part B:

Secure Network Design

Dale Stubbs - 14024149 | Information and Network Security | 03/02/2017

Abstract and Keywords

The issue of Network Security is of paramount importance for any and all organisations, especially organisations dealing with finances. Therefore, the author provided a design for a secure network. This network not only allows the multiple branches of the organisation to communicate with each other securely but also provides the ability for employees to connect remotely via secure means. The report covers the design and justification for the choices made and covers the cost-effectiveness of the network when compared to the current network configuration. The secure network design has overcome all of the weaknesses and vulnerabilities of the old system thus creating a much more secure network the focus of which was the authentication, authorisation and access control as this was deemed the weakest part of the current network. This was achieved by using Kerberos Authentication Protocol configured using the Role-based Access Control (RBAC) model.

*Keywords – secure, network, authentication, access control, Kerberos, Role-based Access Control (RBAC).*

Contents

[1 Introduction 3](#_Toc478260494)

[2. Critical Analysis of the Current Configuration 3](#_Toc478260495)

[a. Basic ISP Router 4](#_Toc478260496)

[b. Basic Switch 4](#_Toc478260497)

[c. FTP File Transfer 4](#_Toc478260498)

[d. Firewall 4](#_Toc478260499)

[e. Unsecure Internet Connection 4](#_Toc478260500)

[3. Secure Network Design Proposal 5](#_Toc478260501)

[a. Company Requirements 5](#_Toc478260502)

[i. Kerberos 5](#_Toc478260503)

[ii. Role Based Access Control 6](#_Toc478260504)

[iii. IPsec in Tunnel Mode with Encapsulating Security Payload Service Model 6](#_Toc478260505)

[b. Network Security 6](#_Toc478260506)

[i. SSL/TLS 6](#_Toc478260507)

[ii. Firewall/DMZ 7](#_Toc478260508)

[iii. NAT 7](#_Toc478260509)

[iv. IDS 7](#_Toc478260510)

[c. Distributed Denial of Service Mitigation 8](#_Toc478260511)

[4. Conclusion 8](#_Toc478260512)

[References 9](#_Toc478260513)

# Introduction

Attacks on networks have been around since the early 1900’s with the first reported attack being made on a supposed secure wireless telegraphy technology that was exploited by Nevil Maskelyne. He interrupted a public demonstration of this technology *‘sending insulting Morse code messages through the auditoriums projector’* (New Scientist, 2017). Technology has come a long way since the days of wireless telegraphy, as has the technology for the people looking to exploit the technology, collectively known as ‘hackers’.

The current state of technology allows almost anything to be done online now and gives ‘hackers’ more opportunities to find the weaknesses in any given system, known as the ‘target’, and exploit them, often for financial gain. This is a very serious issue for company using the internet to supply customers with products of any kind. If such actions are being done on an insecure network the ‘hackers’ will find the insecurities and potentially cost the target company millions in lost revenue and custom.

A survey completed by communications and analysis firm Neustar, has revealed that in 2012 financial companies in North America had *‘a 38% increase in the number of Distributed Denial of Service (DDoS) attacks on the previous year…and…1 in 5 financial companies estimated outages would drain their revenues by $50,000 per hour’* (Neustar.biz, 2017). When combined with CNBC’s report of the largest wave of DDoS ever knocking banks *‘offline for 249 hours’*(Neustar.biz, 2017) would estimate that revenue loss could be somewhere around $12.5m. However, this does not take into account the loss of custom and brand equity that could actually become insurmountable and priceless causing the company to close down for good.

# Critical Analysis of the Current Configuration

During the analysis of the current system there were several vulnerabilities detected. Each of these vulnerabilities have different attacks that they are vulnerable to the following table gives a basic overhead of these vulnerabilities and attacks.

|  |  |
| --- | --- |
| **Vulnerability** | **Attacks** |
| Basic ISP Router | Denial of Service attacks, Packet Mistreating Attacks, Routing table poisoning. |
| Basic Switch | MAC address flooding, VLAN hopping, MAC spoofing, Address Resolution Protocol (ARP) spoofing |
| Using FTP File Transfer | Packet Capture (or Sniffing), FTP Bounce Attack, FTP Brute Force Attack, Spoof Attack, Port Stealing |
| Firewall | No firewall in branches, default passwords, outdated firewall OS, anti-spoofing controls not enabled on external interface, spoofed and fragmented traffic |
| Unsecure Internet Connection | DDoS/DoS, Eavesdropping, Data Modification, Identity Spoofing, Password Attacks, Man-in-the-middle attacks, Compromised-Key attacks, sniffer attacks, Application-Layer attacks. (Any type of network attack) |

Table 1: Vulnerabilities and Attacks

## Basic ISP Router

The router of the network is responsible for ensuring the packets are sent to the correct address either on their network or onto the next networks router. The basic router offers little protection from various attacks. Most users leave the passwords as the default password provided by the ISP on the back of the router. This creates an issue, as default router passwords are readily available via the internet. As stated in the table above there are several other forms of attacks that can happen at this level of the network and therefore a basic ISP Router will not protect a network at all.

* 1. Basic Switch

Once packet has gone through the router and the packet destination has been identified as belonging to the correct network it is then passed onto the switch. The network switch is responsible for receiving, processing and delivering the packet to the destination device. As such, it is an integral part of the network it has been deployed on. Using a basic switch offers little protection for the network and is vulnerable to the attacks mentioned in the table above.

* 1. FTP File Transfer

Using FTP to transfer files across a network is a vulnerability within itself as the file is transferred in plain text format meaning anyone with access to the network can see everything. This type of file exchange is also vulnerable to Packet Captures (aka packet sniffing), FTP Bounce Attacks, FTP Brute Force Attacks, Spoof Attacks and Port Stealing.

* 1. Firewall

There is no firewall in place at each of the branches, which is a security risk in itself. The style of firewall installed at the headquarters is insecure. Packet-Filtering firewall is independent from any applications, which means it is unable to understand the context of a communication set. This creates an easy target for any unauthorised entry into the network. If incorrectly configured then the firewall of the system will offer little protection against the attacks listed within the above table.

## Unsecure Internet Connection

The internet itself is a valuable tool for any business for communication purposes. It allows for worldwide communication to be done almost instantaneously and, as such, can allow a business to thrive and grow much more than before the internet was created. As the internet has grown, so have the abilities of hackers to penetrate networks and to intercept internet traffic and cause all sorts of problems for everyone. Using the internet without means of data encryption will leave the information being sent over the internet vulnerable to interception, modification and stealing. The table above shows all of the vulnerabilities of an unsecure connection from a network to the internet. Effectively, using an unsecure internet connection will allow hackers to breach the network and cause all sorts of problems within the network.

# Secure Network Design Proposal

## Company Requirements

The following section will cover the design of the secure network for the client. The client has specified a number of requirements that first need to be considered. These requirements are:

* Authentication
* Access Control
* Remote Access (From home) and
* Site Interconnectivity

Firstly, the client wishes to consolidate their authentication for all desktop machines across all sites. This can be achieved by deploying a Kerberos Realm across all sites.

Secondly, the client wishes to deploy an access control mechanism that would allow its employees to access the resources available in the most efficient and secure way that minimises the risk of any security breach. This can be achieved by configuring the Kerberos servers to run in a Role Based Access Control (RBAC) model.

Thirdly and fourthly, the client would like the connection between the sites to be reviewed with a view to implement a secure method of linking sites and permitting remote access to the companies’ desktops. This can be achieved by deploying IPsec within the network configured to run in tunnel mode with the Encapsulating Security Payload (ESP) sub-protocol.

### Kerberos

Kerberos is a network authentication protocol developed to provide robust authentication for servers/clients by deploying secret-key cryptography. It allows network nodes that wish to converse via non-secure means to prove their own identity to each other in a secure fashion. As this protocol uses secret-key cryptography in order to authenticate a users’ identity there is no requirement for the users’ password to be passed across the network.

The deployment of a Kerberos realm would consist of a single Authentication Server (AS) combined with a Ticket Granting Server (TGS). These two servers will be combined inside a single machine to decrease the potential cost of the network. Each of the branches would need to have an AS and a TGS installed in order to create the Kerberos Realm. This would allow all sites to communicate with each other in a secure manner as the users’ passwords are never transmitted across the network. It could also be deemed as a secure way for the remote users’ of the network to communicate from their home machines. The cost implications of this would make up the largest proportion of the cost of this system but are required to secure the network in the most efficient way.

The only shortcoming of Kerberos is that it has a single point of failure, the AS itself. If an attacker gains access to the AS and accomplishes gaining access to the information contained within the AS then the network would be deemed ‘compromised’. The simplest and most effective way to mitigate against this is to ensure that the AS itself is kept in a secure room within the branches and a log of access to the room itself is kept. Also, only allowing certain members of staff to have access to the room containing the AS will decrease the opportunity for an attacker to gain entry to the room.

### Role Based Access Control

Role based Access Control (RBAC) ensures that a user cannot access subjects and objects that they have no right to access. The users’ roles are assigned by a security administrator and the permissions contained within the roles are also assigned by the security administrator. A role is described as a *‘set of actions and responsibilities associated with a particular working activity’* (Tucker, 2014). The network users’ are also authorised to adopt roles when it is required providing a more flexible Access Control model.

### IPsec in Tunnel Mode with Encapsulating Security Payload Service Model

Internet Protocol Security (IPsec) is a secure version of the previously used Internet Protocol (IP) for sending data between users via the internet. Deploying IPsec within a network will provide increased security when sending data via the internet. It achieves this by authenticating the origin of a packet (host machine) rather than the user who sent it. When IPsec is deployed in tunnel mode, it is deployed on the network gateway meaning that the network itself would only require one machine (the router) to have IPsec installed onto it, decreasing the cost of securing the network. The Encapsulating Security Payload (ESP) model is implemented to increase the security of the data itself by way of encryption. It provides authentication of the source of the packet, data integrity through the use of encryption and confidentiality of the data contained within the packet. This is achieved due to the whole of the data packet being sent becoming the encrypted payload of a new data packet.

## Network Security

No network can be truly secure. What can be done is to make the network as secure as possible and the author believes that the following additions need to be made to the network to make it as secure as possible:

* Secure Socket Layer (SSL)/Transport Layer Security (TLS)
* Network Address Translation (NAT)
* Firewall/Demilitarised Zone (DMZ) and
* Intrusion Detection Software (IDS)

### SSL/TLS

The SSL/TLS protocol is designed to provide secure e-commerce transactions via encryption of data (credit card numbers and personal data) combined with web-server authentication. It is supported by almost all web browsers. As the company is looking to bring a few new web applications for business revolution purposes it will need to ensure that its customers are protected when using these applications and the use of SSL/TLS is required to provide this protection.

### Firewall/DMZ

The use of firewalls to create a Demilitarised Zone (DMZ) provides an additional layer of security to a company’s Local Area Network (LAN). It decreases the likelihood of an attacker gaining access to the LAN through the internet. The most secure approach to successfully implementing this is to use two firewalls to create the DMZ. The first firewall will be configured to only allow traffic that is destined to the DMZ only and the second will be configured to allow traffic from the DMZ into the LAN. The reason this is the most secure approach is because two different machines would need to be compromised by an attacker in order to gain access to the LAN.

### NAT

Network Address Translation (NAT) is another addition that can increase the security of the LAN. Using a NAT inside a network will provide a single public IP address that is visible to anyone outside the network. All of the nodes on the network are assigned private IP addresses that the internal router of the network can use to forward traffic to. As the nodes have private IP addresses they are considered to be invisible to the outside world and, as such, are no longer vulnerable to network attacks.

### IDS

Intrusion Detection Systems (IDSs) have been developed to attempt to detect unauthorised parties on the network at the earliest possible stage of an attack in order to deploy the defensive actions as early as possible to prevent/minimise the effect of the attack. This is required on a network of this type as any intruder will need to be eradicated from the network before any serious damage (breaches of confidentiality, stolen passwords, stolen credit card numbers, etc.) can occur. The chosen form of IDS would be the use of a third party open-source software called ‘Snort’. This software would be deployed on the network itself rather than on individual machines as this would provide the best form of security in the most cost-effective way.

When using all of the aforementioned security protocols combined together the author believes that the network of this company will be as secure as it possibly can be with the tools available at this time.

|  |  |
| --- | --- |
| **Vulnerability** | **Mitigation** |
| Basic ISP Router | Kerberos AS and TLS |
| Basic Switch | Kerberos AS and TLS |
| Using FTP File Transfer | IPsec in Tunnel Mode with Encapsulating Security Payload Service Model |
| Firewall | Firewall/DMZ |
| Unsecure Internet Connection | IPsec in Tunnel Mode with Encapsulating Security Payload Service Model |

Table 2: Vulnerabilities and Mitigations

## Distributed Denial of Service Mitigation

All networks are vulnerable to Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. The aim of these attacks is to render the network as unusable for legitimate users. There are multiple ways to mitigate against these types of attack that range from purchasing more bandwidth to upgrading the network hardware. In the authors opinion the best form of DDoS/DoS mitigation is to outsource it. There are multiple companies that already have the required hardware and bandwidth to deal with these forms of attacks and as such are prepared to deal with the attacks immediately and effectively.

# Conclusion

As stated earlier within this report, no network can ever be truly secure. Upon completing this report the author can conclude that the original network design (Appendix 1), although this set-up would actively connect all of the branches together effectively, lacked even the most basic of security measures in order to protect the company. The design proposed by the author not only connects the branches together but does so in a secure manner and actively protects the company from a number of different attacks. It has also been designed to provide this level of protection when using remote connectivity from outside of the network (e.g. when working from home). All of this has been designed in the most cost effective way the author could devise and, as such, meets all of the requirements outlined.

Appendices

## Appendix 1

Original Network Design



# References

New Scientist. (2017). *Dot-dash-diss: The gentleman hacker’s 1903 lulz*. [online] Available at: https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/ [Accessed 3 Feb. 2017].

Neustar.biz. (2017). *Report: 2013 Annual DDoS Attack & Impact Survey: Year-to-Year | Neustar*. [online] Available at: https://www.neustar.biz/resources/whitepapers/2012-ddos-attacks-report [Accessed 3 Feb. 2017].

Tucker, A. (2014). *Computing Handbook, Third Edition: Computer Science and Software Engineering*. 1st ed. CRC Press.