School of Computing, Maths and Digital Technologies

Mark Bellingham

14032098

Network Security

2017

Contents

1 Abstract

1.1 Abstract

This report contains the proposed secure network design solution for a multinational financial company that wishes to set up new offices in Europe. It begins with an introduction of why network security is important, with relevant statistics from recent research that underline the financial and performance losses that can occur when the system is compromised.

Section 3 outlines and explains the vulnerabilities that have been identified from the brief provided, with examples of potential attacks that can and do take place on networks that are not secured properly.

Section 4 describes the recommended solution, showing how it will address the requirements of the company in a cost-effective way and prevent attacks from occurring.

The report concludes by highlighting the benefits of this design, while also acknowledging its limitations.

1.2 Keywords

Kerberos, IPSec, VPN, Role Based Access Control, Intrusion Detection System, IP tables,

2 Introduction

2.1 Why is Network Security Important?

The aim of network security is to “provide confidentiality, integrity, non-repudiation, and availability of useful data” (Wang and Kissel, 2015). In other words it should only grant access to files and services if the user has the correct permissions. The system should protect the contents of the data while it is in transmission such that it cannot be read or modified by unauthorised users. It should be able to prove the identity of a user and their actions without question. Finally it must strive to ensure that the system’s resources are fully operational at all times, even in the event of an attack. If the system does come under attack it should be able to detect such an event, block any further actions from the attacker and recover from or repair any damage.

2.2 Statistics

Some high profile attacks have hit the news in recent years. Internet service provider TalkTalk lost over 100,000 customers and suffered estimated financial losses of £60 million when they were victim to a series of hacks in 2015 (The Guardian, 2016). Yahoo had a well publicised breach which could have affected over a billion users (BBC News, 2016). Yet both of these attacks, which caused significant damage to the companies’ reputations as well as financial losses could have easily been prevented had they followed security best practises. A report commissioned on behalf of the British Government in 2016 found that 65% of large businesses suffered a breach in the previous 12 months. (Klahr, 2016).

3 Critical Analysis

3.1 Vulnerabilities in current network configuration and examples of potential attacks

Based on the scenario provided, I have identified 5 vulnerabilities that will be addressed in the final solution, and provided examples of how these vulnerabilities could be realised.

Data Centre that hosts the email, web and FTP servers

The data centre is the most important location in the whole system and represents a single point of attack for any would be intruder that could cause immense damage.

If someone managed to gain entry to this part of the system they would have complete control over the entire system including shared files, confidential emails, customer database and website – the public face of the company.

An attack here could create significant problems for the company and incur substantial losses in time and money, even if you only include the time taken for the network engineer to isolate and remove the threat.

Getting access to the data centre would enable an attacker to mount many attacks. They could steal the data from the database, files from the FTP server or private emails from the email server. The web server presents the public face of the company and an attack here could at best be an embarrassment or at worst compromise the security of the information provided through it by customers.

Another threat that this area faces is an overload of network traffic (Denial of Service attack) that could render this whole area unusable resulting in downtime for the company.

Local branches in Paris, Berlin and London

Although the local branches are using a basic router which provides some protection via Network Address Translation and a basic firewall, the employees are using advanced software such as remote desktop and FTP which introduce chinks in the armour. They would benefit greatly from a more robust system that inspects the network traffic much more thoroughly and would stop, for example, an application that has gone rogue.

An employee could install a type of malware that is not detected by the anti-virus or a new virus that has not been registered by the program if it is not kept up to date.

User authentication to all devices and servers

The scenario makes no mention of how user authentication is handled. This is an extremely important part of the system because it not only decides who has permission to be in the network but also handles which files, services and programs they are allowed to use.

Basic authentication methods are vulnerable to replay attacks. If person 1 logs in to the server providing their username and hashed password, person 2 who is eavesdropping on the network traffic can intercept this information and then use it later themselves to trick the server into believing they are person 1. This attack is prevented by adding a third component such as a session ID or timestamp, so that the authentication information is only valid for that session.

If the user does not have a strong password or authentication system set up, an attacker could guess their password. With many people choosing insecure passwords (Morgan, 2016) because they need to be easy to remember or because the IT policy dictates that they change them often. A better solution would be to connect via SSH and use private key authentication. A user's private key would be a long string of random characters making it very difficult to guess.

IP Packets

The outlined system communicates between offices using standard IP packets but the IP protocol is not, and never will be secure. It is vulnerable to IP spoofing where an attacker could hijack the IP packets and impersonate the company user, performing a man-in-the-middle attack. It could also lead to a replay attack as described in the previous paragraph. Communicating using the IP network leaves the company open to Denial of Service (DoS) attacks, where someone could flood the network with malicious packets leaving it unusable for legitimate users. One further method is by deceiving servers using the Routing Information Protocol (RIP) where someone sends out alternative routing information, which the gateways will update to without checking and then all packets between two gateways will be diverted. (Bidgoli, 2006)

This vulnerability will be addressed in Section 4 - Secure Connection.

File sharing using FTP

The company currently shares files using FTP. This traffic is not encrypted and anyone who has access to the network at any point between the user and the server will be able to read the files.

The FTP that the company is using is not encrypted. An attacker who has access to the network can snoop on the network traffic and see clearly the files that are being shared. Another vulnerability is where an attacker performs a

man in the middle attack and invisibly replaces the files with their own modified versions and the user would be unaware.

This can easily be improved by using SFTP, which is a method of transferring files over the already secure SSH. SFTP is encrypted by design and can be implemented using OpenSSH, a free open-source program for the server. One further advantage of SFTP is that it supports file attributes such as timestamps, something that is not possible using FTP. The recommendation is to use SFTP rather than its often confused with counterpart FTP/S because it uses a single data channel and is thus easier to use when accessing a server through a firewall (Mayevski, 2007).

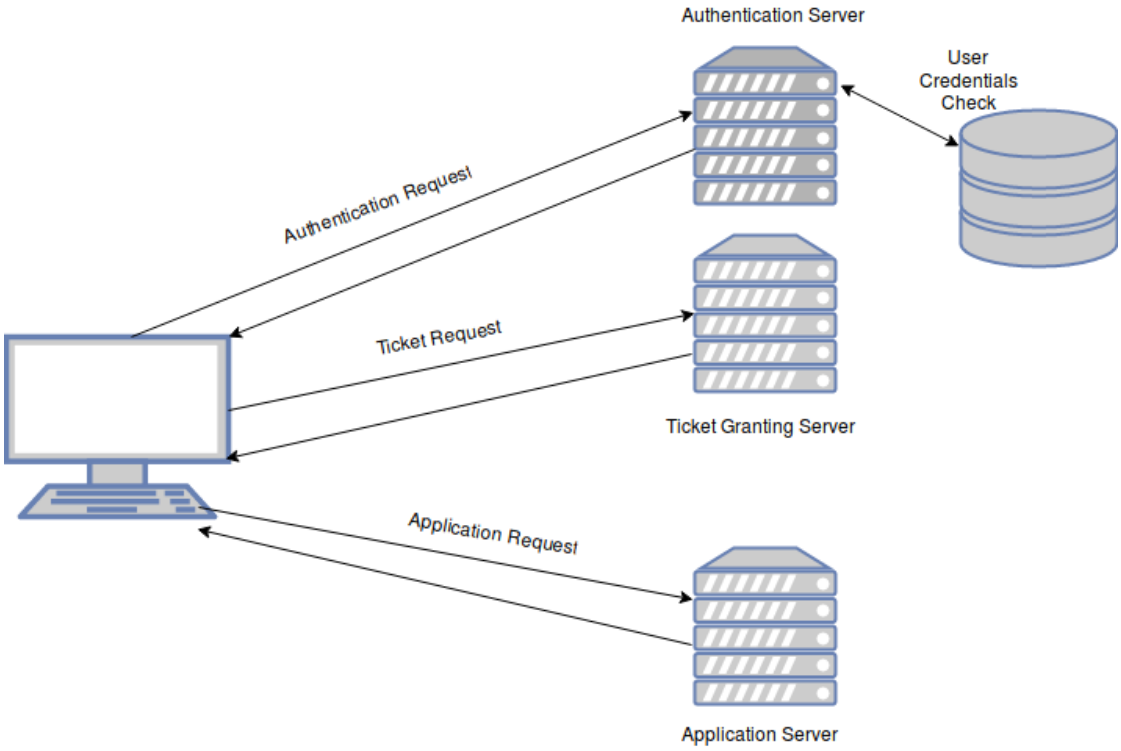
4 Secure Network Design

4.1 Authentication Requirement

The proposed network design should use the Kerberos system for authentication. Kerberos has the following benefits that would safeguard the system:

- The system is able to reliably identify the user and the user is able to reliably identify the server that they are trying to access
- The user's password is never transmitted across the network
- Users are able to access a number of different services with just a single sign on
- User does not need to do any kind of setup on their end as long as the service they are accessing is joined to the network
- Tickets expire after a certain length of time whereas SSH sessions will last until the client software has been closed
- Adding or revoking servers is controlled from a single location

The company should adopt a single realm Kerberos system because even though it has departments spread across different locations, they will all be operating under the same organisation.



Kerberos System

4.2 Access Control Requirement

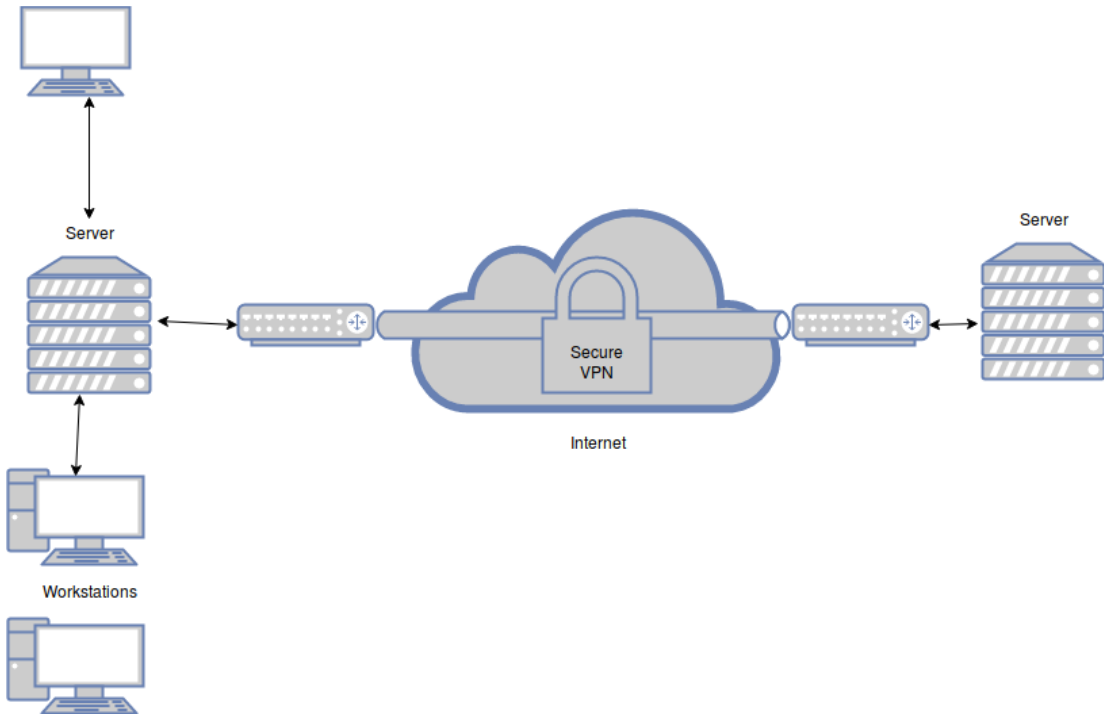
The recommended system for access control uses a Role Based Access Control system. This gives the greatest amount of flexibility while also giving the system administrators the greatest amount of control. Instead of giving individual users rights and privileges, they are assigned roles within the system according to the jobs they need to carry out. This means that whole groups of people can be assigned or denied rights within the system, increasing the system's effectiveness and the efficiency of its administrators. The table gives an overview of how this would be implemented.

Users may adopt one or more roles, files and services are assigned rights depending on who is trying to access it.

	Role 1 (basic employee)	**Role 2** (manager)	**Role 3** (CTO)
File 1	read write -	read - -	read write execute
File 2	read - -	read write -	read write execute
Service 1	- - -	read - -	read write execute
Service 2	read - execute	read - execute	read write execute

4.3 Secure Connection

The company will be transferring a lot of private and confidential information and as IP packets are not secure (explained in Section 3 – IP Packets) it is proposed that the company should use a Virtual Private Network (VPN). A VPN



VPN

enables the company to utilise the internet with a comparable level of security that they have with their internal networks. A gateway configured as VPN will put an encrypted wrapper around each of the IP packets before sending it over the internet. This wrapper is not only able to provide data payload encryption but also encrypted authentication (Whitman et al., 2012), meaning that the the company can be certain that any traffic is reaching its intended destination and cannot be intercepted along the way.

4.4 Adequate Attacks Detection

It is recommended that the company uses two different types of intrusion detection systems (IDS). A network-based IDS would provide general protection at the network boundary, by monitoring network and application protocols. A host-based IDS would provide more specialised protection for critical systems such as the servers in the data centre. The host-based IDS would monitor application activity, processes and system logs as well as the network traffic for that machine.

The IDS would use an anomaly-based detection model with a dynamic profile. This would give it the best chance of detecting both known and unknown methods of attack. Using a signature-based detection model with a static profile would only be able to detect attack types that are already known about but a high-profile company such as an international financial is likely to be a target for people developing new types of attack. An anomaly-based detection model will develop a normal profile from monitoring everyday traffic. If the traffic should deviate significantly from this it would assume that an attack is taking place and take action. This normal profile would be updated continuously as it adapts to changing patterns.

IDS is not a perfect solution, no matter which strategy is used. It will also need network forensics personnel to ensure that false alerts are kept to a minimum.

4.5 Justification of Cost Effectiveness

The proposal outlined in this document has a high level of specification, much of which can be implemented with some configuration changes and by using open-source tools that are freely available. There will be a cost of employing properly qualified network engineers who can oversee the system and react quickly to any problems. While the cost of qualified staff will not be cheap, consideration must be made to the threat level and potential for harm should an attacker manage to penetrate into the system. A large financial company would be a high value target for any would-be hacker and if they did manage to

penetrate the system they could potentially cause damage or losses costing the company many times more than the cost of security.

4.6 Efficient Solution for DDOS

The company will be able to efficiently mitigate the effects of a DDOS attack by implementing some carefully administered rules in their IP tables. They should seek to block any traffic that is not explicitly needed on their network, allowing only incoming or outgoing traffic on certain protocols or ports as required. This will reduce the number of attack vectors but the company can go further by imposing a limit on the number of connections per minute for each port that is left open. The system identifies which IP address(es) are making the very high number of connections and block them while continuing to allow traffic from other locations through.

If the company is legitimately receiving a large amount of connections from a single customer or company, they could implement a specific rule that allows this operation to go ahead.

5 Conclusion

The solution outlined in this document represents a significant improvement over the one in the initial brief. It includes reliable authentication of both the user and the servers; there is a means of controlling access to files and services for different levels of users; data is now transferred securely between the different sites; there are proposals to identify and deal with attackers trying to gain entry into the system, or trying to disrupt normal traffic from accessing the system and services; and much of these proposals can be implemented in a cost efficient way without compromising capability.

This proposal demands however, that the company employs qualified network engineers to implement and maintain the system. The protection against DDoS would not stop a determined attacker who has an army of botnet-linked computers at their disposal. And the Intrusion Detection System could potentially give false positive or false negative results if not configured and monitored correctly.

The information given in this document will go a long way towards a strong and reliable security system.

6 References

BBC News, 2016. “One billion” affected by Yahoo hack [WWW Document]. BBC News. URL http://www.bbc.co.uk/news/world-us-canada-38324527 (accessed 3.21.17).

Bidgoli, H. (Ed.), 2006. Threats, vulnerabilities, prevention, detection, and management, Handbook of information security. Wiley, Hoboken, NJ.

Klahr, R., 2016. Cyber Security Breaches Survey. University of Portsmouth.

Mayevski, E., 2007. FTPS vs. SFTP: What to Choose [WWW Document]. codeguru. URL http://www.codeguru.com/csharp/.net/net_general/internet/article.php/c14329/FTPS-vs-SFTP-What-to-Choose.htm (accessed 3.31.17).

Morgan, 2016. Worst Passwords of 2016 [WWW Document]. TeamsID. URL https://www.teamsid.com/worst-passwords-2016/ (accessed 3.27.17).

The Guardian, 2016. TalkTalk counts costs of cyber-attack | Business | The Guardian [WWW Document]. The Guardian. URL https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave (accessed 3.21.17).

Wang, J., Kissel, Z.A., 2015. Introduction to network security: theory and practice, Second edition. ed. Wiley, Singapore.

Whitman, M.E., Mattord, H.J., Green, A., 2012. Guide to Firewalls and VPNs, 3rd ed. Cengage Learning.