Information and Network Security
6G6Z1012

Joshua Michael Ephraim Bridge
joshua.m.bridge@stu.mmu.ac.uk
14032908

March 20, 2018

Abstract

Keywords— LAN - *Local Area Network*, DNS - *Domain Name System*, VPN - *Virtual Private Network*, TTL - *Time To Live*

1 System Analysis (Vulnerabilities & Attacks)

1.1 Insecure IP packets

At the moment, the branches communicate to the headquarters over the internet in an insecure way. As the packets being sent over the internet are not protected, anyone could read the contents of these messages and potentially use them to attack the system. Any router or system that lies in the network path between each branch and the headquarters could intercept any message sent between them and possibly modify, remove or replay that message.

Replay Attack The current network is very suceptible to a replay attack with its user/password system. As there is no underyling security protocol to protect messages over the internet, a packet sniffer could be used to listen for a valid sign-in message and then that message could be re-sent by an attacker to gain access to the system.

1.2 Internal Access Control

A major issue with the current network layout is that all devices in each location are grouped together within the same LAN, so any computer/server can access every other computer/server. There is no access control which could prevent resources being accessed by users who should not be able to.

Internal Malicious Access Either an employee with internal network access or an outside attacker who has gained access to the network is able to access all of the resources within any location. This allows the possibility of a whole host of attacks such as offline dictionary attacks & DNS cache poisoning.

1.3 User/Password Authentication

A user/password system is unsuitable for secure authentication when connecting over the internet. Usernames and passwords for users are often very simple for the sake of being able to remember them, therefore this makes them much more suceptible to being guessed by an attacker.

Dictionary Attack If an attacker manages to get hold of the endpoint used for login, then they can start using dictionry attacks to try and guess username/password combinations. This is possible due to the lack of authentication for which devices can log in to the company system.

1.4 Insecure FTP Server

The current FTP server is serving with unprotected traffic, which is easily exploitable and a very critical vulnerability when the company is dealing with financial information.

Packet sniffing Attackers can scan network traffic to easily pick up FTP login passwords sent in plain text, furthermore they can see the files being transferred and make a copy of any file.

1.5 Unprotected DNS

The DNS server at the headquarters is currently located within the same LAN as the public facing servers and the office workstations. Therefore if any of these devices were to be compromised then the DNS server is very suceptible to being attacked.

DNS cache poisoning Due to the current network design, once an attacker has gained entry to an employee computer via either a Replay or Dictionary attack it is possible to then reach the DNS server via the LAN and poison its cache. It would therefore be possible to redirect any authentication traffic to an attacker-controlled server and collect the passwords of every user that tried to log in while the cache is poisoned.

2 Secure Network Design Proposal

In order to protect against the attacks I have identified, I suggest that the following technologies be implemented.

2.1 Attack Prevention

2.1.1 IPsec-ESP (VPN)

In order to protect against **Replay attacks**, IPsec is an ideal solution for maintaining message authenticity. When deployed in ESP mode, all devices connecting remotely to the main network has a secure connection which can not be interfered with by attackers. Finally, re-sending the same packet would not work due to the contents of the TTL header.

2.1.2 Application-level Gateway

An application-level Gateway would be an ideal solution for protecting against **Internal Malicious Access** and therefore also protecting against **DNS Cache Poisoning** & **Offline Dictionary Attacks**. If the networks witin the headquarters were split up into more logical zones seperated by firewalls, where only certain groups of users were permitted to cross these zones, then the likelihood of the latter two attacks would go down greatly. For example if an outside attacker has managed to gain access to an employee account within the network, they still will not be able to access the DNS server due to not having the correct authentication to access the server.

2.1.3 SFTP (Secure File Transfer Protocol)

To protect against **Insecure FTP packet sniffing**, a more secure file transfer protocol implementation is ideal. SFTP is an extension of SSH (Secure Shell) which allows for secure transfer of files over any network. This is relatively simple to set up and does not interfere with any firewall, as it only requires a single port (22) to work.

2.2 Additional Requirements

Below are the solutions I propose for each of the additional requirements of the company.

2.2.1 Authentication

For authenticating users, I would suggest that a more secure form of the user/password system be implemented such as password **Hash & Salt**. This would not require huge amounts of work as the user system is already there, but increasing the security of the password storage would be very useful for at least slowing offline & online dictionary attacks and making sure the passwords are not sent in plaintext over the network, which could be picked up by an attacker with a packet sniffer.

2.2.2 Access Control

Using an Access control matrix is the simplest way of increasing security within a network. At the moment there is already a user system in place; with the above improvements in security for user authentication (section 2.2.1) an access control matrix would be an ideal and efficient solution.

2.2.3 Site-to-site Connection

IPsec-ESP would provide a secure connection for both **site-to-site** and **remote access**. When deployed at the site gateway, each site could connect securely to one-another by establishing a secure tunnel where data sent between sites could not be interfered with. This same principle works for remote access - each device that will be used to connect from home could be set up with IPsec tunnel, which would again establish a secure connection to the main server.

2.2.4 Remote Access

As mentioned in sections 2.1.1 & 2.2.3, IPSec VPN is a perfect solution for implementing secure remote connection to the company network. As the same technique will be used for connecting different sites, it is more or less trivial to set this up on other computers wishing to connect from remote locations. While it would require installation on each machine wishing to connect to the network, this could be seen as a positive as it enures only trusted devices will be capable of connecting.

2.2.5 Secure Web & Email Access

In order to secure the connection between users and the Web & Email servers, installing the **SSL/TLS** protocol on each server would be the best way of securing those connections. Those protocols are designed specifically for the purpose of securing connections to online resources, and they provide protection for both confidentiality and message integrity. This does not require much upkeep, once it is in place it should work for at least a year until the certificate needs to be renewed.

2.2.6 Attack Detection / Mitigation

When trying to detect and mitigate attacks within a network, an IDS (Intrusion Detection System) is the most ideal solution. While it is not 100% effective and can produce false positives while sometimes requiring extensive monitoring, it is a lot more efficient then hiring a human being to constantly sit and monitor many different systems for signs of an intrusion.

2.2.7 DDoS Attacks

In order to protect against DDoS attacks, a **Stateful Inspection Firewall** would be ideal for filtering out requests from users which aren't trying to create a genuine session, but just to overload the servers. With a firewall like this it would greatly reduce the server load on the outbound router & web server and stop the DDoS from having a big effect on service quality. This is because the firewall would be more equipped to deal with high load without much overhead, whereas on the web server it would have to dedicate much more resources to each request/packet.

2.3 Cost-effectiveness

While my proposed solution may require a lot of initial set-up/configuration, I feel that the solutions I have suggested are used in an efficient way due to their re-use against multiple attack vectors. For example the Application-level Gateway (section 2.1.2) protects against 3 of the identified security vulnerabilities due to their cascasding nature.

3 Conclusion

References