Information and Network Security
6G6Z1012

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

March 14, 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 Unprotected Web Server

The current web server is serving public clients with unprotected HTTP traffic, which is easily exploitable and a very critical vulnerability when the company is dealing with financial information. Attackers can easily trick clients in a multitude of ways into sending personal information to attacker-controlled servers.

Man-in-the-middle Attack While on an unencrypted public wifi hotspot, a user may try to access the website while an attacker intercepts this unprotected traffic. The attacker could then replace the response with their own malicious server page where the user might enter personal information.

1.3 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.

1.4 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.

1.5 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 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.

This would also 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 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.

2.3 Additional Requirements

2.3.1 Authentication

Password Hash & Salt / Kerberos

2.3.2 Access Control

Access Control matrix

2.3.3 Site-to-site Connection

IPsec

2.3.4 Remote Access

IPsec / Kerberos

2.3.5 Secure Web & Email Access

SSL / TLS

2.3.6 Attack Detection / Mitigation

IDS

2.3.7 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.

2.4 Cost-effectiveness

3 Conclusion

References