Information and Network Security
6G6Z1012

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

March 14, 2018

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus et lectus vel magna luctus vestibulum nec ut eros. Curabitur suscipit ipsum quis ornare tincidunt. Suspendisse sodales dapibus ante ultricies sodales. Nam nisl erat, cursus at convallis ac, egestas non nisl. Phasellus faucibus efficitur feugiat. Morbi lectus purus, dictum ut velit ac, porttitor ultricies enim. Maecenas feugiat lorem eget mauris aliquet dapibus. Curabitur eros est, varius quis lacus sit amet, vehicula facilisis sem. Cras ut urna id ante ullamcorper ullamcorper.

Keywords— LAN - Local Area Network, DNS - Domain Name System

1 System Analysis (Vulnerabilities)

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 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.

1.3 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.

1.4 Unprotected Web Server

2 Design Proposal

References