A

Seminar report

on

“Network Security”

Submitted in partial fulfillment of the requirement for the award of degree
Of Bachelor of Technology in Computer Science

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

PREFACE

I have made this report file on the topic **Network Security;** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to …………..who assisting me throughout the prepration of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

CONTENT

Introduction

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired'', an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them.

Some history of networking is included, as well as an introduction to TCP/IP and internetworking. We go on to consider risk management, network threats, firewalls, and more special-purpose secure networking devices.

This is not intended to be a ``frequently asked questions'' reference, nor is it a ``hands-on'' document describing how to accomplish specific functionality.

It is hoped that the reader will have a wider perspective on security in general, and better understand how to reduce and manage risk personally, at home, and in the workplace.

What is Network Security?

Network security is a level of guarantee that all the machines in a network are working optimally and the users of these machines only possess the rights that were granted to them.

This can include:

- preventing unauthorized people from acting on the system maliciously
- preventing users from performing involuntary operations that are capable of harming the system
- securing data by anticipating failures
- guaranteeing that services are not interrupted

History

Internet security has been an issue since the Internet rose to an international phenomenon. By 1996, the Internet already connected 13 million computers, so early security protocols were required.

These protocols required computer information to be confidential, available, and have integrity. Because the Internet made information available to everyone, people needed network security to make their information confidential. Because otherwise harmless information can expose a computer network to compromise, network security was developed to close all loops.

Basic Network Security

- When connecting a matching to a network, we need to make sure no one will easily break in to it.

- Even if you don't think anyone will try to break into your machines - chances are that someone might try.

- Crackers often run network scan utilities that check a large range of IP addresses, and automatically try to find machines running servers with security holes.

- To protect against that, one could simply disable any unnecessary network service they are running.

- First, disable all services launched via the inetd (or xinetd) daemon. Edit the file "/etc/inetd.conf" (or the files under "/etc/xinetd/"), comment out (using a leading '#') in front of all services, and save the file. Then, restart the inetd process. One way to do that:

```
killall -HUP inetd
```

Now, check that the command 'telnet 127.0.0.1' shows you a 'connection refused' error - this implies that the telnet service (if it was enabled) is now disabled.

- Next, disable any daemons started by your system, by removing the relevant links in the init directory "/etc/rc.d/rc3.d", such as sendmail, portmap and so on. Yo could also do that using a run level editor.

- Finally, you could set up firewalling rules (provided you have firewall support compiled into your kernel), and then run services behind this protection. Enable connections to services you still have running only from the IP address of '127.0.0.1' (which is a special address used internally for communications between processes running on the same machine). Info on firewall rules may be found in the firewall HOWTO.

Need for Network Security

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies.

The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks.

Because they have no Internet connectivity, networks designed in this way can be considered safe from Internet attacks. However, internal threats still exist.

There is a estimates that 60 to 80 percent of network misuse comes from inside the enterprise where the misuse has taken place.

With the development of large open networks, security threats have increased significantly in the past 20 years. Hackers have discovered more network vulnerabilities, and because you can now download applications that require little or no hacking knowledge to implement, applications intended for troubleshooting and maintaining and optimizing networks can, in the wrong hands, be used maliciously and pose severe threats.

Types

Wi-Fi Protected Access (WPA)

WPA encrypts information, and checks to make sure that the network security key has not been modified.

WPA also authenticates users to help ensure that only authorized people can access the network. There are two types of WPA authentication: **WPA** and **WPA2**.

WPA is designed to work with all wireless network adapters, but it might not work with older routers or access points.

WPA2 is more secure than WPA, but it will not work with some older network adapters.
WPA is designed to be used with an 802.1X authentication server, which distributes different keys to each user. This is referred to as WPA-Enterprise or WPA2-Enterprise.
It can also be used in a pre-shared key (**PSK**) mode, where every user is given the same password. This is referred to as **WPA-Personal** or **WPA2-Personal**.

Wired Equivalent Privacy (WEP)

WEP is an older network security method that is still available to support older devices, but it is no longer recommended.

When you enable **WEP**, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

802.1X authentication

802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks. **802.1X** uses an authentication server to validate users and provide network access. On wireless networks, **802.1X** can work with WEP or WPA keys. This type of authentication is typically used when connecting to a workplace network.

MACAdress

A Media Access Control address is a unique identifier assigned to network interfaces for communications on the physical network segment. Can be described as Ethernet hardware address (EHA), hardware address or physical address. It is assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, the card's read-only memory, or some other firmware mechanism.

The advantage to MAC filtering is that there is no attachment cost to devices that connect to the network. The policy is set on a router or switch, and the equipment attached either is permitted or it is not. The person attaching the equipment has nothing to do.

The disadvantage to MAC filtering is that it is easy to spoof due to the broadcast nature of LAN and WLAN; an advisory can sit on the wire and just listen to traffic to and from permitted MAC addresses. Then, the advisory can change his MAC address to a permitted one, and in most cases obtain access to the network.

Authentication

One-factor authentication – this is “something a user knows.” The most recognized type of one-factor authentication method is the password.

Two-factor authentication – in addition to the first factor, the second factor is “something a user has.” Examples of something a user has are a device that generates a pre-determined code, a signed digital certificate or even a bio-metric such as a fingerprint.

Three-factor authentication – in addition to the previous two factors, the third factor is “something a user is.” Examples of a third factor are all bio-metric such as the user’s voice, hand configuration, a fingerprint, a retina scan or similar.

The advantage of using a 3 factor authentication is that it's made reassuringly sure that the person who is authenticating is the person who is authenticating through multiple layers of security. The disadvantage is that there is a possibility that the person trying to authenticate loses first or the second authentication, the process can also take time.

Firewall

Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. It may be hardware or software.

The advantage of a firewall is that the user can monitor incoming and outgoing security alerts and the firewall company will record and track down an intrusion attempt depending on the severity. Some firewalls can detect viruses, worms, Trojan horses, or data collectors.

The disadvantage of firewalls is that they offer weak defense from viruses so antiviral software and an IDS (intrusion detection system) which protects against Trojans and port scans should also complement your firewall in the layering defense. A firewall protection is limited once you have an allowable connection open. This is where another program should be in place to catch Trojan horse viruses trying to enter your computer as unassuming normal traffic.

Network Attacks Methods

Whiteout implemented security measures and controls in place, your network and data might be subjected to an attack. Some attacks for instance could be passive, meaning that information is monitored; other could be active, meaning the information is varying within intent to destroy or corrupt the data or the network itself.

Likelihood your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

- Eavesdropping – Interception of communications by an unauthorized party
- Data Modification – Data altering, reading from unauthorized party
- Identity Spoofing (IP Address Spoofing) – IP address to be falsely assumed— identity spoofing and the attacker can modify, reroute, or delete your data
- Password-Based Attacks – By gaining your access rights to a computer and network resources are determined by who you are, that is, your user name and your password
- Denial-of-Service Attack – Prevents normal use of your computer or network by valid users, and it could be used for sending invalid data to application, to flood the computer, block traffic, etc.

- Man-in-the-Middle Attack – Is when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently
- Application-Layer Attack – It targets application servers by deliberately causing a fault in a server's operating system or applications and the attacker gaining the ability to bypass normal access controls

Anyhow, this is just a most commonly known network attacks methods, and indeed there plenty of more.

Advantages of Network Security

- Network Security helps in protecting personal data of clients existing on network.
- Network Security facilitates protection of information that is shared between computers on the network.
- Hacking attempts or virus / spyware attacks from the internet will not be able to harm physical computers. External possible attacks are prevented.
- Network Security provides different levels of access. If there are various computers attached to a network, there may be some computers that may have greater access to information than others.
- Private networks can be provided protection from external attacks by closing them off from internet. Network Security makes them safe from virus attacks, etc.

Problems

- Computer networks are typically a shared resource used by many applications representing different interests.
- The Internet is particularly widely shared, being used by competing businesses, mutually antagonistic governments, and opportunistic criminals.
- Unless security measures are taken, a network conversation or a distributed application may be compromised by an adversary.
- The owner of the website can be attacked as well. Some websites have been defaced; the files that make up the website content have been remotely accessed and modified without authorization.
- That is an issue of *access control: enforcing the rules* regarding who is allowed to do what. Websites have also been subject to Denial of Service (DoS) attacks, during which would-be customers are unable to access the website because it is being overwhelmed by bogus requests.
- Ensuring a degree of access is called availability.

Network Security Architecture

What & why

an organization's network infrastructure evolves over many years. Although this evolution is in direct response to the changing business needs, in many cases security has been an afterthought. Network and Systems changes, like any other change, will result in some or the other fault due to misconfigurations, deviations from industry best practices to quickly resolve irritants faced during the making the changes. All of this happens due a "for now" tactical approach to the change being implemented. Even implementing the most advanced security technologies of the day won't help if the underlying security architecture is flawed.

How?

Our systematic approach to the evaluation of the current state ensures a detailed review of the current architecture, technology & security policy of the organization, management practices and planned changes. Our highly qualified and experienced consultants will identify network and design architectural weaknesses in security, performance, scalability. Our team of security experts will recommend improvements to better align the security architecture with business objectives, your organization's security policy and industry best practices.

Some of the aspects that will be examined are:

- Review latest Threat Risk Analysis report.
- Analysis of current IT network, information flow according to business requirements and points of access to information.
- Analysis of current security controls and procedures for various security management areas.
- Analysis existing network security architecture, including topology / configuration, and security components / features.

Conclusion

That is why network security is an important field that is increasingly gaining attention as the Internet usage increases. The security threats and Internet protocols were analysed to determine the necessary security technology. However, the current development in network security is not very impressive and significant.

Therefore, researchers and scholars are rapidly evolving in developing and investigating the threats further in a future. And with this information in mind, the process can be formalized and the path becomes clearer as you delve deeper into the specifics of the security process, as well.

References

www.studymafia.org

www.google.com

www.wikipedia.com