www.oeclib.in

Seminar
On
Network security

Content

- Introduction
- What is Network Security
- History
- Basic Network Security
- Need for Network Security
- Types
- Authentication
- Network Attacks Methods
- Advantages
- Problems
- Network Security Architecture
- Conclusion

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.

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.

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.

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.

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

Types…

- **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.

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."

Three-factor authentication – in addition to the previous two factors, the third factor is "something a user is."

Network Attacks Methods

- 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.

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.

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.

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.
- 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.

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.

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 analyzed to determine the necessary security technology.
- However, the current development in network security is not very impressive and significant.

References

- www.oeclib.in
- www.google.com
- www.wikipedia.com

Thanks...!!!