Networking & Network Security

Miss. Leena R Bhitre

Research Student (YCMOU)

Plot no 10, Vasundhara Colony, Nandanvan Colony, Aurangabad- 431002, M.S

Abstract

Network Security is the difficulty subject, only well-trained and experienced experts can tackle this problem. This article deals with what is known as network and its security. It explains the reasons of security failure, requirements for security that will help us to understand some of the risks and how to overcome them.

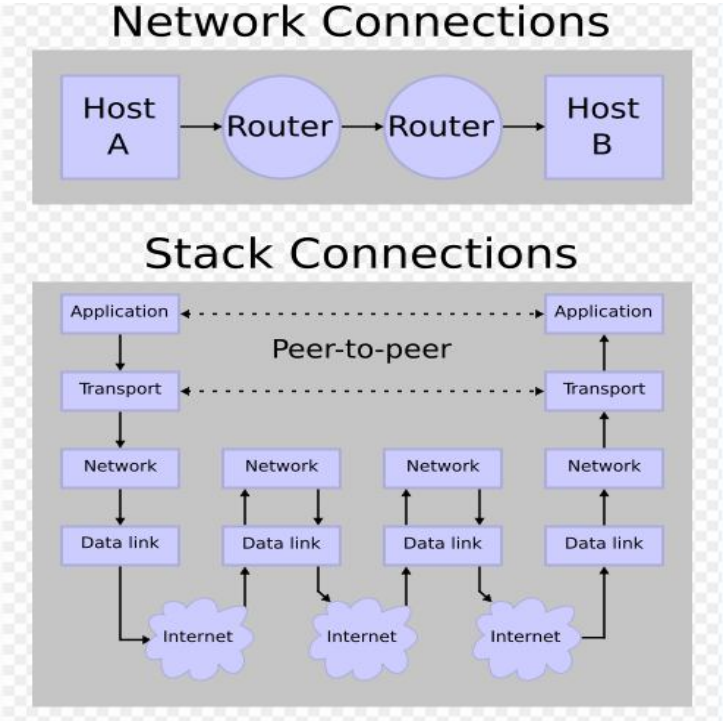
Introduction

To understand network security basic knowledge of computer networks is required. In this paper we have tried to cover some of the fundamentals of networking and how they can be solved by taking some precautions. Why does network security fails, what are it requirements, about attackers and so on.

What is Network?

Network is generally an interconnection of various groups or systems where information is shared between these system or group. This is done with the help of computer network system. Computer Network may be classified by what is called the network layer at which they operate according to basic reference models

1. The four-layer Internet Protocol Suite model
2. The seven-layer Open Systems Interconnection (OSI) reference model



Reprint requests: Miss. Leena R Bhitre
Plot no 10, Vasundhara Colony, Nandanvan colony,
Aurangabad- 431002 (M.S)
Tel:-9420317643, Email-rlrb@rediffmail.com

Seven Layer Open Systems Interconnection

OSI Model			
	Data unit	**Layer**	**Function**
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Interhost communication
	Segment	4. Transport	End-to-end connections and reliability (TCP)
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing (IP)
	Frame	2. Data link	Physical addressing (MAC & LLC)
	Bit	1. Physical	Media, signal and binary transmission

What is Internet?

Internet is the world's largest network of Networks. a worldwide network of computers that allows the "sharing" or "networking" of information at remote sites from other academic institutions, research institutes, private companies, government agencies, and individuals.

Why Does Network Security Fail?

Network security fails in several common areas.

Human Factors

Users, developers, managers and administrators are all very common sources of network security failure. People introduce vulnerabilities to network security is by creating weak passwords. Also physical security and social security where peoples often leave their door open or unlock. Exploiting the basic trust, trust , fears, and ego of humans is an incredibly powerful way to break into a network.

Policy Factors

Draconian, Vague, Provide no compliance guidelines, Outdate, Not enforced or poorly enforced and not read.

Misconfiguration

Administrators and developers are bound to make configuration and other types of mistakes that can easily lead to security vulnerabilities and ultimately to the compromise of an organization's information.

Poor assumptions

Making poor, misguided or unjustified assumptions is the root cause of many security vulnerabilities. Administrators can make poor assumptions about user behavior, about how technology works, or about whether tasks have been completed. It takes only one small oversight resulting from an unjustified assumption for an attacker to compromise a network or application. Preventing administrators and developers from making unjustified assumptions is one of the single biggest ways you can improve security.

Ignorance

Closely associated with making poor assumptions is ignorance. Often administrators and developers simply are not aware of the consequences of their actions of the threats that attackers pose to their network or application. Network management might also be the source of ignorance regarding how to properly secure information assets or what the threats to information assets are.

Failure to stay up-to-date

The security of a network is only as good as its last update.Remember, security is dynamic-it is not fixed state. Consequently. You must be vigilant about both securing information assets and maintaining the security of those assets. Certainly this is no more evident than with security patching for operating systems and applications. There is in effect a race between

administrators and attackers each time a security patch is released.

Requirement for Network Security

Confidentiality - Protection from disclosure to unauthorized persons

Integrity Maintaining data consistency

Authentication- Assurance of identity of person or originator of data

Non-repudiation- Originator of communications can't deny it later

Availability- Legitimate users have access when they need it

Access control- Unauthorized users are kept out

• User authentication used for access control purposes

• Non-repudiation combined with authentication

Security Threats

Information disclosure/information leakage

Integrity violation

Masquerading

Denial of service

Illegitimate use

Generic threat: Backdoors, Trojan horses, insider attacks

Most Internet security problems are access control or

authentication ones

• Denial of service is also popular, but mostly an annoyance

Attack Types

Passive attack can only observe communications or data

Active attack can actively modify communications or data

• Often difficult to perform, but very powerful

– Mail forgery/modification

– TCP/IP spoofing/session hijacking

Security Services

From the OSI definition:

- Access control: Protects against unauthorized use
- Authentication: Provides assurance of someone's identity
- Confidentiality: Protects against disclosure to unauthorized identities
- Integrity: Protects from unauthorized data alteration
- Non-repudiation: Protects against originator of communications later denying it

Security Mechanisms

- Encryption is used to provide confidentiality, can provide authentication and integrity protection
- Digital signatures are used to provide authentication, integrity protection, and non-repudiation
- Checksums/hash algorithms are used to provide integrity protection, can provide authentication

Conclusion

From the about discussion it is clear that Network Security is a complicated task and it needs to train peoples in respect to overcome the problems regarding network security. Also peoples should be aware of new change taking place in same aspects.

References

- Kevin Lam, David LeBlanc and Ben Smith (2004) Assessing Network Security, Prentice-Hall of India Pvt.Ltd. New Delhi.pp 5-13.
- Sanjay Pahuja (2005) The Complete Reference Data Communication & Computer Networks, Standard publishers distributors. Delhi. Matt Curtin (March 1997) Introduction to Network Security