International Journal of Advanced Educational Research
ISSN: 2455-6157
Impact Factor: RJIF 5. 12
www.educationjournal.org
Volume 3; Issue 1; January 2018; Page No. 141-143

Network security types and problems

Dr. Pushpinder Kaur
Associate Professor, Department of History, BZSFS. Khalsa Girls College Morinda, Punjab, India

Abstract
The integration of Internet and mobile Internet, Internet of things, will promote the wide application of the Industrial Internet and other vertical internet. Smart device manufacturing, smart Internet marketing will give people work and life led to profound changes and the experience. But all walks of network security problems will become increasingly serious. Traditional networks of a variety of viruses, hackers and other threats will expand the network to the new system, they caused the damage and the impact will be more dangerous and grim. Security is an important field that consists of the provisions made in underlying computer network infrastructure, policies adopted by the network administrator to protect the network, the network-accessible resources from unauthorized access and the effectiveness of these measures combined together. Personal, government, and business applications continue to multiply on the Internet and these work-based application and services can pose security risks to individuals and to information resources of companies and governments. Information is an asset that must be protected. Network security is more challenging than ever, as today's corporate networks become increasingly complex.

Keywords: internet, network security, firewall, attacks, threats

1. Introduction

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software, and information in a network.

Network security is a challenge for network operators and internet service providers in order to prevent it from the attack of intruders. It deals with the requirements needed for a company, organization or the network administrator to help in protecting the network. Computers, networks, and the Internet affect our lives every day or we can say that we are so much dependent on them to make our life comfortable. We all are connected to the internet without any boundary, so Network Security is essential in this environment because any organizational network is accessible from any computer in the world and, therefore, potential vulnerable to threats from individuals who do not require physical access to it.

Network Security can be referred as protecting websites domains from various forms of attack. If we have the knowledge of how various attacks are executed we can protect ourselves. Security means considering vulnerabilities, threats, attacks, countermeasures, and acceptable risks. A Network were developed using different communicating devices. The Synchronous network consists of switches but do not require any security because switches do not buffer any data but a network consist of routers must be secure enough as information can be easily stolen by using malware like "Trojan Horse". The objective of network security is:

2. Security Requirements

1) **Confidentiality:** The data must be accessed and read only by the authorized individuals or parties. It is the protection of the personal information. We can compare confidentiality with privacy. Data encryption, User Ids and passwords, biometric verifications are some of the methods through which confidentiality can be protected.
2) **Integrity:** It is the assurance of not only the information can be accessed or modifies by the authorized persons only but also the data must be accurate, consistent over its entire life cycle. Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous authentication practices. Cryptography plays a very major role in ensuring the data integrity. Hashing the data you receive and comparing it with the hash of original message is another method to ensure data integrity.
3) **Availability:** Data must be available to the authorized persons at the right time. It can be ensured by rigorously maintaining all hardware, preparing hardware repairs immediately and maintaining a correctly functioning operating system environment. Regular backup must be taken, for information services that are highly critical, redundancy is appropriate method to ensure availability.
4) **Auditability:** Audit data must be recorded in such a way that all specified confidentiality and integrity requirements are met.

3. Network Security Problems

a) **Passive Attacks**: In this attack the disclosure of the confidential information or the files to an attacker without

the consent of the authorized individual or an organization. The attacker monitors for the open ports or vulnerabilities to gain the information about the target without changing it on the target machine. There are two main types of passive attacks

1. Release of Message Content
2. Traffic Analysis

b) Active Attacks: In this type of attack the hacker attempt to make changes to the data on the target machine. It can be said as the attacker can modify the stream of bits or creation of false stream of bits but the goal is same and much more of the passive attack and that is to steal the confidential information of the individual or organization and also do harm to the network or network services which they are providing. The active attacks are subdivided into different categories:

1. Replay Attack
2. Masquerade Attacks
3. Modification of Messages
4. Denial of Service (DoS)
5. Distributed Denial of Service (DDoS)

c) Insider Attack: These attacks involve someone who has authorized access to the network with either an account on the server or having a physical access to the network. He can intentionally or accidentally attack the network from some malicious or non-malicious ways. Malicious insiders intentionally eavesdrop, steal, or damage the information and they can use this information in a fraudulent manner. They can also deny access to other authorized users. In the same way attacks can be non-malicious while performing the tasks in an organization like carelessness, lack of knowledge, or intentional circumvention of security. Internal Intrusion Detection System (IDS) protect organizations against insider attacks.

d) Close-In Attack: When an individual or a group is trying to attain close proximity to networks so that, they can modify, collect the information or deny the access to the information. Close physical proximity can be achieved through secret entry into the network or an open access [7]. One of the popular close-in attacks is social engineering, where the attacker compromises the network through social interaction through an e-mail or over the phone. The attacker will apply some tricks in the conversation so that the victim can reveal the secrets of the company and he attacker could gain unauthorized access to the network or to the system.

e) Phishing Attack: It is also referred as brand spoofing or carding, the idea behind phishing is that the bait is thrown out with the hope that while most will ignore the bait, some will be tempted into biting. Phishing is a form of fraud in which the attacker tries to fetch the information such as login Ids, passwords, Credit card details etc by masquerading as a reputable entity or a person through e-mails, some communication channels or by creating fake websites which feels and look like authorized ones.

f) Password Attack: Password attacks are the classic way to gain access to a computer system to find out the password and login Id. Their goals might differ, but they all tries to crack the passwords which are stored in a network account database or a password-protected file.

4. Conclusion Categories of Network Security Threats

a. External Threats: Threats originated from individuals or groups working outside of the organizations. They do not have authorized access to any of the computer systems or the network. They contact the organizations network from the internet or from the dial-up access servers.
b. Internal Threat: A computer network or a server must be secure enough not only from the external threats but from the internal ones too. Internal threats originate from inside the organizations itself from a dissatisfied current or a former employee

5. Network Security Types

a) Firewalls: To begin planning for perimeter-oriented network-defence strategy organizations securing network by putting it behind the firewall. Securing the company's network, it's best to start on the perimeter but one must know about its perimeter, it is basically where the system interfaces with the rest of the world. Security inside the deep of an organization by installing safeguards is good idea but the biggest bang for your security buck is by building up protection along the perimeter i.e. the network's boundary: the frontier where data flows in from (and out to) other networks, including the Internet. The security at the perimeter is done with the help of the firewall that act like a checkpoint, allowing authorized data to enter unencumbered while blocking suspicious traffic.

b) Authentication: The authentication procedure is further divided into three factor authentications. The advantage of using this three factor authentication method is that it makes sure that the person who is authenticating is the authenticated person. The disadvantage of this procedure is it takes time when a person forgot the first or second factor authentication.

6. Network Security Challenges

a) Automated Assessment and Response: Automation promises- the ability to respond to threats much quicker and possibly to greater effect. In this era everyone expects high performance from their workplace networks but the technologies that make automation possible haven’t succeed the trust level yet. Security automation technologies are not granular enough to be effective in scaling to such environments. Tools are required that can be more precise about the control.

b) Software-Defined Networking (SDN): SDN is an approach to computer networking that allows network administrators to manage network services through abstraction of higher-level functionality. It has the potential to provide enterprises with the level of granular control they need in order to automate.

7. Conclusion

Network security isn’t something you either have or don’t it is a continual arms race against malicious hackers. Fortunately, as attacks become more sophisticated, so too does the technology and practices used to protect the network. One of the biggest security concerns today is the insider threat. Another major security concern is lack of consistency in

enforcing “acceptable use” policy. In current scenario there are number of ways, which guarantee for the safety and security of the network but it cannot be said they will everlasting. We have to perform regular network security testing.

8. References

1. Carle E. Landwehr, Security Issues in Networks with Internet Access, Member, IEEE.
2. Siddharth Ghansela. Network Security: Attacks, Tools and Techniques, 2013, 3(6).
3. Kartikey Agarwal. Network Security: Attacks and Defence, 2014, 1(3).
4. http://whatis.techtarget.com/definition/Confidentiality-integrityand-availability-CIA
5. http://computernetworkingnotes.com/network-security-access-listsstandards-and-extended/types-of-attack.html
6. 5 th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), Mouna Jouini
7. Eric Cole, Network Security, Bible, 2nd Edition, 2009.
8. Prakhar Golchha. A Review on Network Security Threats and Solutions. 2009; 2347:3878.
9. Inam Mohammad. A Review of types of Security Attacks and Malicious Software in Network security. Bhavya Daya, “Network Security: History, Importance, and Future”, University of Florida Department of Electrical and Computer Engineering, 2010, 4(5).