International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

A Survey on Network Security Issues

Ruma Panda[1], Lavanya S[2], Monika N[3]
[1]*Assistant Professor, Dept. of Computer Science, Vemana Institute of Technology,Bengaluru*
[2,3]*Student, Dept. of Computer Science, Vemana Institute of Technology, Bengaluru*

***Abstract*--As Network security has become more popular nowadays, but establishing a network is not a major issue for network administrators but safeguarding the entire network is big issue.But today, there are various tools introduced such as firewall, net-protector etc., are available for protecting the network. Administrators are not only concentrated with the advancements fields but also focuses on the loss ofuser'sdata in a network.This paper outlines about the variousattacks andchallenges in network security.**

***Keywords*- Network, security, Attacks.**

I. INTRODUCTION

Network Security is the process of taking hardware and software obstructive measures to protect the underlying networking infrastructure from unlicensed access, misuse, malfunction thereby creating a secure platform for computers.Networks are widely being used in day to day life like business, banking, defense, social network security, DNS security etc. Network Security includes the provisions and strategiessupported by a network administrator to prevent and monitor unauthorized access, modification, or denial of a computer network and network accessible resources.

All the users who are working on the internet needs security of data but the person do not know that intruder is collecting the data. For example Assume there are two persons X and Y, here is a scenario where X &Y need to communicate with each other, but they stay away and X sends an electronic text mail without any encryption or encoding to Y, for this example let us consider that there is no security in the network. As there is a conversation between X & Y, the third person Z is on the same network as well. The data flow in the network is open to everyone, person Z can monitor the data that has been sent from person X to person Y,Z can see the content directly and make profit. If X would have an idea about how attacks are executed, then he/she might have protected the data.Many companies are using various tools like firewalls to prevent from the attack in network. Since, Network security is a huge field, it is being developed and still in evolutionary stage. There are various tools like "Egressor" from which the information can be secured. "Egress" is a tool which is intended to assist data security authority in conducting a vulnerability analysis of the network by identifying potential weakness in their network configuration. Egress tool cannot guarantee an adequate information security. This paper deliberate aboutbasic information regarding network security challenges that outlines network security attacks.

II. TYPES OF ATTACKS

In this section, we are putting forward some basic class of attacks which slows down network performance.Depending on how the attacks take places they are categories into two types:

A. Active Attacks: Active attacks are based on modification of the actual message in some manner or the creation of an incorrect message. These attacks can be easily detected because changes made to the original message, but these attacks cannot be prevented easily, they can be identified with some effort and attempts can be made to cover from them.
Active attacks can be sub divided into three categories:

1*) Masquerade attacks:* It is caused when an unauthorized entity pretends to be another entity. To understand it better lets have an example, in this example if person X and Y are legal users, the legalized communication should happen between X & Y. But here comes person Z he disguised himself as person X and communicates with Y on behalf of X. In case if Y releases his account details and password it could be accessed by Z but not X. Obviously Z going to get rich illegal.

2) Modification: As the name suggest it an alternation to original message. It results in loss of integrity.

Two types in modification attacks:

- ***Replay attacks:*** In these attacks user captures a sequence of data units and resend them.
- ***Alteration attacks:*** Alteration attacks includes some changes to the original message.

3) DoS (Denial of Service):DoS are the attacks which can make an attempt to prevent legal users from accessing some services, which they are eligible.For example: Person X is legitimate user of some abc bank where he wants to draw money, and a Person Z is not the user of the bank, but hacker who renders the network services down and blocks thenetwork. Thus the bank is unable to provide the services to the X.

B. Passive Attacks: Passive attacks are the attacks where in this attacker yield in monitoring of data transmissions. The attackers focus to obtain information that is in transit. The words passive indicates that the attacker does not attempts to perform any modification to the data. These attacks are difficult to detect because the original content is not changed. Hence, rather than detecting, preventing is better.These are classified into two categories:

- ***Releasing of message content:*** In this type of attack, unofficial data of users is released publicly over the network. In this situations data security is lost.
- ***Traffic Analysis:*** In this attack the attacker tries to find similarities betweenencoded messages and original data.

III. OTHER ATTACKS

Apart from active attacks and passive attacks we have other attacks those slowdowns the network performance, like virus, uncontrolled traffic etc. and the other different types of attacks are as follows:

1) External security threats: The most frightening attacks come from skilled sophisticated external hackers. Since an group of software application maintain open connection to IT data bases, hackers seek to control of these applications after they get inside, often by seeking application passwords set to their defaults.

2) Virus attack: A virus is harmful code that replicates by copying itself to another program. The virus needs someone to spread the infection without the permission of administrator. Due to virus attack on the hard disk of the system it destructs the data.The worm is also similar to virus. It is stand-alone programming that does not require to copy itself to a host program. Worm and virus also refer to as malware.

3) Unauthorized Access: It is an access of using the network or computer without an approval from the authorized person. It is important to scan and monitor the shared folder and resources in network and should be acquired only by authorized person.

4) Browser attacks: The most common attacks in network is browser attack. They try to trick internet user into downloading malware i.e. software which is designed to damage the computer system. Browser attacks can be protected by using encryption that secures against attackers and also look at the address bar to regulate whether the domain name in the address bar is the right place to send the password.

5) Brute force attacks: In this attack, hackers use trial and error method to decode pin number or password. It is time consuming approach because it proceeds through all possible combinations. So, to protect this kind of attacks user should keep on changing the password often by using odd combination of symbols, letter, number and cases.

6) SSL (Secure Sockets Layer) attacks:It is a type of attack, in which a sensitive information that can be accessed by attacker by means of stopping the encrypted data before it can be encrypted. Secure sockets layer construct an encoded link between a browser and website, or a mail client and mail server. SSL secures a website, which begins with HTTPS. The original SSL protocols were developed by NETSCAPE. This layer has various versions. Because of few problems in version 1.0, it was not publicly released. Then version 2.0 was out in February 1995, even this version consist of few flaws in security thereby this leads to the introduction of next version of SSL i.e., version 3.0 in 1996.PAUL KOCHER produced a complete redesign of this protocol in version 3.0."FATHER OF SSL" is Dr.TAHER ELGAMAL.As of 2014 the version 3.0 is considered insecure as it is exposed to the POODLE attack. Thereby SSL 2.0 was prohibited in 2011 and SSL 3.0 was denounced in June 2015.

7) Scans: Port scan are unfriendly searches on the internet for the on ports.so attackers can easily gain access to a computer. The attackers send a memo to a port. The reply can expose the status of a port. With the help of this status, the attackers can recognize the operating system and its vulnerabilities, this in turn help the intruder to promote a future attack.

8) Eavesdropping: Network eavesdropping is also known as network sniffing. The term eavesdrop derives from the practice of essentially standing under the eaves of a house, snooping to dialogues inside .these types of attack is dangerous because the attacker can view confidential information and encrypt and decrypt the data without the user's knowledge. Since network communication occur in a "clear text" format, which helps the attacker gaining access to information in network.

Administrators face a biggest security problem in an enterprise it is because the capacity of an eavesdropper monitoring the network. Without strong encoding of data that are based on cryptography, the information can be read by others without permission of handler.

There are two types:

- Man in the middle attack.
- Replay attack

9) Identity Spoofing (IP Address Spoofing):It is one of the most commonly used attacking methods in network. IP spoofing was used by DoS attack to overload devices and network with packets that appear to be from legal IP addresses. In this type, attacker can use a different program to construct IP packets that appear from valid address. After gaining contact to the network with a valid IP address, the intruder can delete or modify the data and also conducts various types of attack in network.

There are two different ways to surplus the target with traffic.
1. Simply flood the target with multiple spoofed addresses.
2. The other method is to spoof the target IP address and deliver packet from that addresses to many different recipients on the network. When another machine receives a packet, it will spontaneously transmit a packet to the sender in response. Since the spoofed packets seem to be sent from target ip address all replies to the spoofed packets will be sent to the target ip address.

10) Password-Based Attacks: Entree rights to a network and computer resources are determined by whom you are, that is, your user name and your password. Older application does not always safeguard uniqueness information as it is passed through the network for confirmation. This might permit an eavesdropper to gain access to the network by posing as a legal user. When an attacker finds a usable user account; the attacker has the same rights as the real user. Hence, if the user has administrator-level privileges, the invader also can create accounts for consequent access at a later time.

After gaining access to your network with a valid account, an attacker can do any of the following:

- Modify, redirect, or delete data
- Modify network and server alignments, including access controls and routing tables.
- Obtain lists of valid user and computer names and network information.

11) Data Modification: Once the communication starts between the sender and receiver, the third person in the middle of sender and receiver may read or modify the data in the packet without the knowledge of sender or receiver. For an example, if there is an online transaction, you do not want the amount transferred to be modified.

IV. CONCLUSION

Network security is the one which you either have or don't it is a frequent support fight against mischievous hackers. As the attacking to the network increases, practices and technology are used to guard the network. Most of the policies are badly printed, old-fashioned and poorly connected. As one protects their computer and message, the same way the network should also be protected. Now-a-days there exist with various technology to safeguard the network from several attacks. We have to perform regular network security testing.

REFERENCES

[1] M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.
[2] J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.
[3] A. R. F. Hamedani, "the Network Security Concerns, Tools for Testing," School of Information Science, Halmstad University, 2010.
[4] R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.
[5] Q. Gu, Peng Liu, "Denial of Service Attacks," Texas State University, San Marcos.
[6] B. Daya ,"Network Security: History, Importance, and Future,2013.
[7] Li CHEN, WebSecurity: Theory andApplications, School of Software, Sun Yat-sen University, China.
[8] S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009

