Different Attacks in the Network: A Review

Mohit Angurala[1], Gurinderjit Kaur[2]

[1]Assistant Professor Department of CSE, Golden College of Engineering and technology, Gurdaspur, Punjab, India
[2]Department of CSE (M. Tech Student), Golden College of Engineering and technology, Gurdaspur, Punjab, India

Abstract— *Network security is protection of the files which can be stored information in network against hacking, misuse. Network security involves the authorization or access to data which is controlled by the network administrator. Users are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Today anyone person can become a hacker which downloading tools from the internet. Nowadays security is becoming vital in case of networking because everyday a new kind of attack is generated which leads to compromise our network and have security in network is decreasing because of increase in number of attacks. In this paper we have shown the comparison between different types of attacks in a network in a tabular form.*

Keywords—**DOS, IP, Trojans, Phishing, Network**

I. INTRODUCTION

The world is becoming more interconnected with the Internet and new technology by networking. In this security issue is that which to protect data which can be stored into computer. Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access. Many network security threats today are spread over the Internet. The most common include: Viruses, worms, and Trojan horses, Eavesdropping, Data Modification, IP Spoofing, Password Based Attacks, Denial of service Attack, Man in the Middle Attack, Compromised Key Attack, Phishing, Trojans, Sniffer Attack. There are different kinds of attacks in the network security which can be discussed below.

II. ATTACKS IN NETWORK SECURITY

Two types of attacks in network security which are as following:-

1. Active Attack

In **active attack,** the attacker tries to bypass or break information into secured systems. This attack can be done through worms, Trojan horses, or Viruses. Active attacks can be included to break protection of features and to modify the information. These attacks can be involved modification of data stream or creation of a false stream. Replay of this attack which can be used to capture of data unit and retransmission for an unauthorized effect. This attack can be easy to detect because attacks can alter a data. Result of this attack is that disclosure of data files or modification of data.

Types of Active Attacks

1. 1 Denial of Service (DOS) attack

A Denial of Service (DOS) attack is aimed that to preventing authorized on the network. The Denial of Service (DOS) attack is not aimed at to collecting a data. Aimed of denial of service is that to preventing authorized, legitimate users from using computers or the network normally. Denial of Service (DOS) attack can be used to sending the invalid data to the applications or network services until the server hangs and then simply crashes a system. Denial of Service is an attack when the system is to receiving too many requests but cannot return the communication with the requestors.

1.2 IP Spoofing

IP Spoofing also known as IP address means that the address of the trusted computer is to gain the access of the other computers. The identity of the intruder is to be different by making detection which can be hidden and prevention of this attack is difficult. The intruder can be also use the valid address of the IP or to modify data. Administrators and Users can be used to protect themselves and their networks by implementing or installing the firewalls that can block the outgoing packets with the addresses of sources that can be differ from the IP addresses of the internal network or user' computer.

1.3 Man-in-the-middle attacks

Man-in-the-middle attack is the form of eavesdropping where the communication between two users is modified or monitored by unauthorized party. In the process, two original parties appear to normally communicate. Man-in-the-middle attack involves an attacker by inserting themselves which can be communicating between two parties. The attacker could also modify the messages in transit. This attack spoofs the opposite party and that parties believe and they are talking to the other expected party. Man-in-the-middle attacks are assuming your identity in order to read your message.

1.4 Masquerade

To pretend to be someone else. This could be logging in with a different user account to gain extra privileges. For example, a user of a system steals the System Administrators username and password to be able to pretend that they are them.

2. Passive Attack

A **passive attack** monitors the unencrypted traffic and then looks for clear-text passwords and other types of attacks can be used in sensitive information. Pas**sive attacks** include monitoring of unprotected communications, traffic analysis and capturing authentication information such as passwords. Result of passive attack is that to disclosure of data files or information to an attacker without the knowledge of the user. The goal of passive attack is to obtain the information that is being transmitted. Passive attack can be detect to difficult, because these type of attacks don't alter data, can be prevented, rather than detected, use of encryption.

Types of Passive Attacks

2.1 Eavesdropping

Network sniffing or network Eavesdropping is a network layer attack which consisting of capturing packets from the network which can be transmitted by other computers and reading the data content in search of sensitive information like session tokens ,passwords, or any kind of confidential information. These attacks based on cryptography without strong communication services, your data can be read by others as it traverses the network. It is referred as snooping or sniffing when attacker is eavesdropping on your communication.

2.2 Traffic Analysis

If information is encrypted, it will be more difficult to read the information being sent and received, but the attacker simply observers the information, and tries to make sense out of it; or to simply determine the identity and location of the two communicating parties.

2.3 Network Analysis

To simply monitor the transmission between two parties and to capture information that is sent and received. The attacker does not intend to interrupt the service, or cause an effect, but to only read the information.

3. Other types of attacks

3.1 Viruses

Viruses are self -replication programs that use files to infect and propagate. Once a file is opened, the virus will activate within the system. Viruses usually lead to some sort of data loss or system failure.

There are numerous methods by which a virus can get into a system:

- Through infected floppy disks
- Through an e-mail attachment infected with the virus
- Through downloading software infected with the virus

3.2 Phishing Attack

In phishing attack the hacker creates a fake web site that looks like a popular site such as the SBI bank . The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

3.3 Sniffer attacks

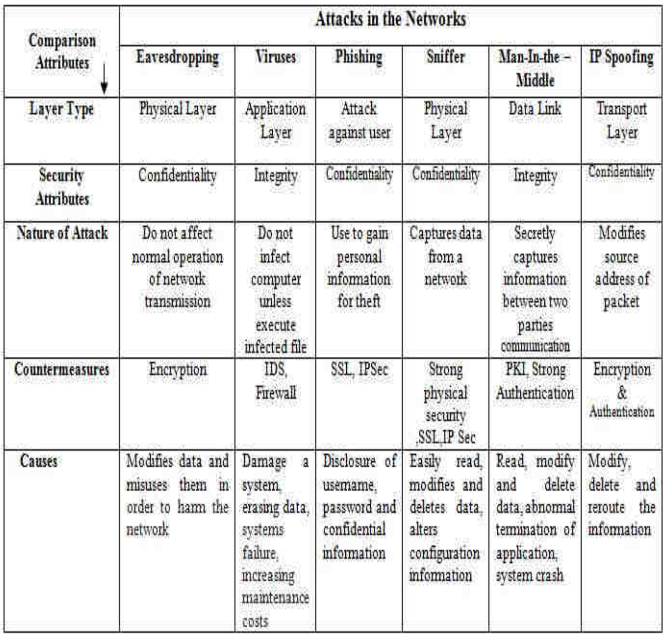
A sniffer is a device or an application that can monitor, read or capture network data exchanges and that read packets of network. A sniffer provides a full view of the data inside the packet, if the packets are not encrypted. Even encapsulated packets can be read unless and broken open then they are encrypted and the attacker does not have access to the key. A sniffer can analyze your network and gain information to cause is that to crash the system or to become corrupted. This attack

3.4 Password attacks

Aim of Password based attacks is that at guessing the password for a system until the correct password is determined. Weakness of primary security is that which can be associated with password based access control is that all security is based on the user ID and password being utilized. The information of the password is simply sent in plain text or clear – no form of encryption is utilized. Remember that network attackers can obtain password information and user ID and then pose as authorized users and attack the corporate network. The attacker has the same rights as the real user, when an attacker finds a valid user account.

We have selected following attacks and have compared the level how much harmful is that attack for our network:

III. COMPARISON TABLE



Comparison Attributes ↓	Attacks in the Networks					
	Eavesdropping	Viruses	Phishing	Sniffer	Man-In-the – Middle	IP Spoofing
Layer Type	Physical Layer	Application Layer	Attack against user	Physical Layer	Data Link	Transport Layer
Security Attributes	Confidentiality	Integrity	Confidentiality	Confidentiality	Integrity	Confidentiality
Nature of Attack	Do not affect normal operation of network transmission	Do not infect computer unless execute infected file	Use to gain personal information for theft	Captures data from a network	Secretly captures information between two parties communication	Modifies source address of packet
Countermeasures	Encryption	IDS, Firewall	SSL, IPSec	Strong physical security ,SSL,IP Sec	PKI, Strong Authentication	Encryption & Authentication
Causes	Modifies data and misuses them in order to harm the network	Damage a system, erasing data, systems failure, increasing maintenance costs	Disclosure of username, password and confidential information	Easily read, modifies and deletes data, alters configuration information	Read, modify and delete data, abnormal termination of application, system crash	Modify, delete and reroute the information

III. CONCLUSION

Network Security is the most vital and important component of information security because it is responsible for securing all the information passed through a Network computer. Overall in this paper we have given brief comparison between various kind of attacks and we have compared various types of attacks with different parameters like security attributes, causes etc.

REFERENCES

[1] D. Estrin, “Controls *for interorganization networks*” *IEEE transactions on Software Engineering*, vol. SE-13, Feb. 1987.

[2] *S. T. Walker, “Network security: The parts of sum,” Proc., 1989 IEEE Symp. On Research in Security and Privacy*, Oakland, CA, pp. 280-289, May 1989.

[3] *IEEE Journal on Selected Areas in Communications*, Special issue on Secure Communications, vol. SAC-7, May 1989.

[4] Ohta, T.; Chikaraishi, T., "Network security model," Networks, 1993. *International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', Proceedings of IEEE Singapore International Conference on, vol.2, no., pp.507-511 vol.2, 6-11 Sep 1993.*

[5] Landwehr, C.E.; Goldschlag, D.M., "*Security issues in networks with Internet access*," *Proceedings of the IEEE, vol.85, no.12, pp.2034-2051, Dec 1997*.

[6] Dowd, P.W.; McHenry, J.T., "*Network security: it's time to take it seriously*," *Computer*, vol.31, no.9, pp.24 - 28, Sep 1998.

[7] Molva, R., Institute Eurecom, “Internet Security Architecture,” *in Computer Networks & ISDN Systems Journal*, vol. 31, pp. 787-804, April 1999.

[8] Brien M. Posey, *Understanding the IPSec protocol*. Published August 24, 2000.

[9] *Intel Corporation, 2000*. IP Security: Building Block for the Trusted Virtual Network

[10] Serpanos, D.N.; Voyiatzis, A.G., "*Secure network design: A layered approach*," Autonomous Decentralized System, 2002. The 2nd International Workshop on, vol., no., pp. 95-100, 6-7 Nov. 2002

[11] Simmonds, A; Sandilands, P; van Ekert, L(2004) —*Ontology for Network Security Attacks*‖ *Lecture Notes in Computer Science* 3285 pp.317-323.

[12] Andress J., “*IPv6: the next internet protocol*,” April 2005, www.usenix.com/public actions/login/2005-04/pdfs/andress0504.pdf

[13] Marin, G.A., "Network security basics," *Security & Privacy, IEEE*, vol.3, no.6, pp. 68-72, Nov.-Dec. 2005.

[14] “Improving Security,”http://www.cert.org/tech_tips, 2006.

[15] Sotillo, S., East Carolina University, “IPv6 security issues,” August 2006,

[16] www.infosecwriters.com/text_resources/pdf/IPv6_S Sot illo.pdf.

[17] Kartalopoulos, S. V., "*Differentiating Data Security and Network Security," Communications*, 2008. ICC '08.

[18] IEEE International Conference on, pp.1469-1473, 19-23 May 2008.

[19] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, vol., no., pp.77-82, 13-15 May 2008.

[20] R. K. Khalil, “*A Study of Network Security Systems*,” IJCSNS International Journal of Computer Science and Network Security, 2010.

[21] S. Shaji, *“Anti Phishing Approach Using Visual Cryptography And Iris Recognition*,” IJRCCT, Vol 3. No. 3pp. 88-92, 2014.

[22] Mohit Angurala, “*Survey of Different Attacks on Wireless Sensor Networks-Roadmap*, “IMTC T1-CSE-ECE-099,2015