A SURVEY OF DIFFERENT TYPES OF NETWORK SECURITY THREATS AND ITS COUNTERMEASURES

[1]HARSHITHA B, [2]N RAMESH

M.S.Ramaiah Institute of Technology, M.S.R.I.T post, Bengaluru, Affiliated to VTU, Belgaum, Karnataka., India,
M.S.Ramaiah Institute of Technology, M.S.R.I.T post, Bengaluru., Affiliated to VTU, Belgaum, Karnataka., India,
Email: ramesh.namburi22@gmail.com, harshi.b112@gmail.com

Abstract: Today, communication had become part of Technology. Network plays a vital role in establishing a communication. A network is a collection of nodes interconnected by communication paths. Networks allow users to access remote files, databases, and can retrieve any important information either within the organization or from different organization. Networks are necessary, but still they are not considered much safe to provide security to the users because of many flaws in conventional system. Network attacks had become a curse to technology, where attacker destroy or gain illegal access to system recourses and restrict the legitimate users from accessing the information. This paper describes different types of network attacks and its countermeasures and also analysis of its severity for awareness, so that a common person can easily understand different types of network attacks in a particular scenario.

Key words: active, passive, spoofing, distributed, close-in, insider

I. INTRODUCTION

There are number of network attacks and few of them are described here, so that any person can understand and be aware of illegal access or network attacks. Even though there are defensive techniques to prevent network security threats, one cannot guarantee a secured network. In this paper network attacks are classified and described. The purpose of this survey is to highlight different types on network attacks and provide awareness to persons about network attacks and suitable countermeasures in a particular scenario. The part I of the paper describes types of network attacks, part II describers its causes and countermeasures. At the end of this paper conclusion is provided to guide contributors for the development of more security measures to prevent network attacks.

II. NETWORK ATTACKS

Network Attacks can be classified [5] as a) Passive attack b) Active attack c) Distributed attack d) Insider attack and e) Close-in attack.

Passive Attacks: This type of attack makes use of information from the system but not affect system resources. The attacker can observe the data or information transmitted between the sender and receiver. This data can include usernames, passwords and confidential e-mail messages. Passive attacks result in the disclosure of information or data files to an attacker without the knowledge of the user. Passive attack threatens the confidentiality of the system, and is difficult to detect because it gets the required information without altering the system resources. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords.

Fig 1. Passive Attack

Traffic Analysis: This is one form of passive attack, where attack takes place by observing the external characteristics of traffic. The attacker analyzes the traffic, determine the location, identify the communicating parties, and observe the length of the message being exchanged. With all these information the attacker can predict the nature of communication. All incoming and outgoing traffic are analyzed but not altered.

Active Attacks: In this type of attack, the attacker or intruder breaks into the system and alter system resources. This attack attempts to break protection features, introduce malicious code, and steal information. By doing this, the intruder can transmit the data, modify the data and also delete the information. Active attack compromises integrity or availability because it alters the operation of a system and restricts access to legitimate users. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Denial-of-Service attack (DoS): Denial-of-Service is one form of active attack where the attacker attempt to prevent legitimate users from accessing the service. There are number of ways to perform DoS attacks. The basic intention of this attack is to indefinitely interrupt services of a host connected to an internet. One common form of attack involves sending the target machine with indefinite communication request in such a way that it cannot respond to intended

traffic or respond slowly so that it becomes unavailable. This type of attacks leads to server overload i.e. server will be flooded with illegitimate request so that it fails to respond to real request. This type of attack disrupts the network components, configuration information and routing information. There are two general forms of DoS attacks: a) attack that flood services and b) attack that crash services.

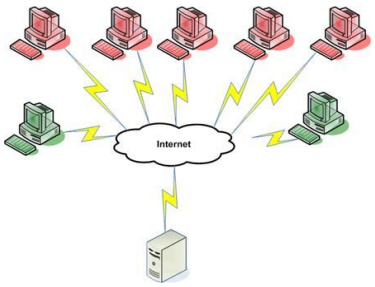

Fig 2. Denial-of- Service attack

Flood attacks include: Buffer overflow attack, ICMP flood, SYN flood.

***Buffer overflow attack*:** This is one form of DoS attack, which takes place when the buffer is overloaded with excessive traffic than intended. The purpose of this attack is to gain access to system resources and block authorized users from accessing it.

ICMP flood attack: This attack is also known as ping attack. In this form of attack, the attacker repeatedly sends large number of ping request to the entire host in a network rather than a particular machine. If there is large number of ping request, the host will not be able to receive or distinguish real request which in turn results in DoS attacks.

SYN flood attack: This is a variant of DoS attack. When the client wants to establish a TCP/IP connection with the server, an exchange of TCP/SYN and TCP/ACK packets takes place. The client sends a TCP/SYN packet to the server asking if it can connect. The server then respond to the client with TCP/SYN-ACK packet and waits for the TCP/ACK packet back from the client. In a SYN flood attack the address of the client will be forged so that when a server sends a TCP/SYN-ACK packet to the client, the client will not respond because the client does not exist. The server will be waiting for the response from the faked client. This will reduce the number of connections the server can make, which keeps legitimate users from making connections.

Spoofing: Spoofing is another type of active attack. In this type of attack, unauthorized persons pretend to be legitimate users and gain access to network and steal important information. Spoofing can take place in variety of forms. One form of spoofing is to send fake e-mails from fake address and capture login names, passwords and account information. Another form of spoofing is IP spoofing, where the IP packets are used to send the data over the network. This IP packet contains the source address and destination address. In IP spoofing, the address will be forged so that it contains different address. When the target machine receives the spoofed IP packet it sends a response back to the attacker and the attacker can gain access to restricted resources.

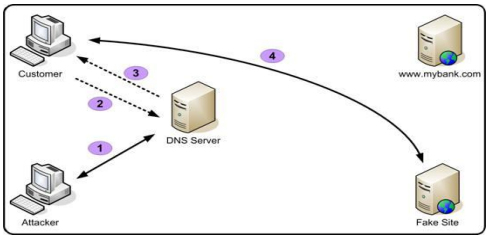

Fig 3. Spoofing attack

***Man-in-middle attack*:** As the name indicates, there will be a man in between two persons actively tracing the information and controlling the communication transparently. In this attack, the person will be unaware about the attacker and provide all information thinking that communication is going on with the original party. The attacker can then inject new information or modify the information. This allows the attacker to read, delete, modify the data, corrupt the system, inject viruses etc...

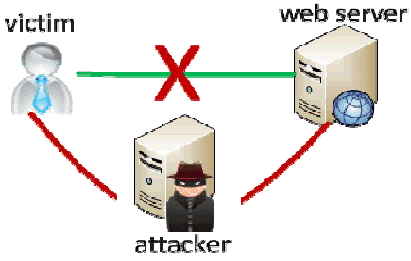

Fig 4. Man-in-middle attack

Distributed Attack: In this type of network attack, the attacker will distribute or inject the malicious code to the trusted component or software and gain unauthorized access to resources. The parties will be unaware of the attack and distribute the component or software to others. This results in a leakage of confidential information from reputed institutions and loss of data.

Distributed denial-of-Service Attack: In this attack, multiple hosts target a single system and make resources unavailable for intended users. The attacker asks all the hosts to contact a particular server or website repeatedly, by doing so there will be an increase in traffic. As a result the server or website loads slowly or sometimes makes the site completely unavailable for legitimate users. This results in loss of sensitive information for users. This type of attack can be performed by flooding the server with false traffic and making the service unavailable for intended users.

Insider Attack: In this type of attack authorized or trusted person within the organization performs the attack. This type of attack can be easily performed

when compared to other types of attacks, because the insider who will be authorized person will have knowledge about the infrastructure or architecture of the network, rules/policies the organization have adopted, or about confidential information. This type of attack is very difficult to detect, as more security policies concentrate on external attackers.

Close-in Attack: In this type of attack, the attacker attempts to physically get close to network components, data, and physical network entities in order to gain more knowledge about a network. By doing this, the attacker can modify the information, delete the data, and restrict access to legitimate users. Close contacts can be achieved either secretly or open access to the network.

Social engineering Attack: One form of close-in attack is social engineering attack, the attack is done by social interaction with the persons through e-mail or phone. The faked e-mail will be sent asking to send the bank credentials or some account information or to reset the password, the victim without knowing that it is a fake mail or phone enters all the details and using this information the attacker can gain unauthorized access to network.

III. CAUSES OF NETWORK ATTACKS AND ITS COUNTERMEASURES

Networks play a vital role in communication. In rapid growing technology, the network attacks have become a serious issue, the impact of attack had lead to huge losses for organizations,
banks, and websites. Securing the network is a challenge, many security measures have already implemented, yet the effect of attacks is unpredictable. Table 1 [6] gives the analysis of types of attacks, its causes and also highlights defensive techniques used so far in a particular network attack.

Table I. Comparison of different types of Attacks, Causes and its Countermeasures

Type of attack	Causes	Countermeasures
Traffic analysis	disclosure of important information or data files by monitoring the traffic characteristics	Encryption
Denial-of-service	slow network performance, abnormal Termination of services by sending invalid data, block traffic	external firewalls along with filters, intrusion with filters, intrusion detection system
Buffer overflow	cause system crash, bypass security service, crash operating system	perform input validation, Use of safe libraries, aware of programming languages
ICMP flood	drop connection in network, system crash	inspection and filtering of Tcp, icmp packets, firewalls, intrusion detection system
SYN flood	crash operating system, unavailability of server , Cause damage to network devices	filtering, firewalls, proxies
Spoofing	modify, delete and reroute the information	Ingress filtering, use strong authentication
Man-in-middle	read, modify and delete data, abnormal termination of application, system crash	cryptography, strong authentication, use hash function
Distributed DoS	slow network connection, unavailability of services, Network and websites	firewalls, intrusion detection and prevention system
Phishing	disclosure of username, password and confidential Information	firewalls, spam filters, anti virus, anti spyware
Sniffing	easily read, modifies and deletes data, alters Configuration information	end-to-end encryption, proper segmenting of network

CONCLUSION

Through this survey different types of network attacks and its causes are highlighted. One should be aware of network attacks and its causes and also think about how network attack can take place in a particular scenario. The user should apply appropriate security measures according to the scenario, because some of the measures are applicable at standalone system and some are applicable at online environments. The researchers and developers need to think about security measures by making use of existing countermeasures, one can think of ***developing an alarm signaling messages*** so that whenever network attack occurs, it should be able to send a message to network administrator or any user using the system either through e-mail, or SMS. From this form of alarm messages, the user can know well in advance that the attacker is attempting to gain access to network resources. From these types of alarm messages, the user can take preventive measures so that data can be secured or the loss or impact of attack may not be huge.

REFERNCES

[1] Denial of service attacks –are you vulnerable? Mr. Jitu Panesar & Mr. George Goutas.
[2] Network Security: It is a Process, not a Product. Suyog Dixit and Pankaj Kumar Jha.
[3] Modern Network Security: The Migration to Deep Packet Inspection
[4] http://technet.microsoft.com
[5] Classification of attacks. http://computernetworkingnotes.com
[6] Threats and countermeasures. http://msdn.microsoft.com

★★★