Network Security Issues and Solutions

Mrs. Bhumika S. Zalavadia
HOD-Diploma Computer Department
Atmiya Institute of Technology and Science for Diploma Studies
Rajkot, Gujrat
bszalavadia@aits.edu.in

Abstract - Network security is now days becoming more and more important because people like to connect with each other all the time via internet. Personal computer users, employees of professional organizations, government servants, academicians, social workers, students, military peoples etc are very familiar to use network currently and all these people use the available network for most of their work. All these people keep their most important data on internet and also do the money related online transactions. The internet structure is itself such that there may be possibility of threats to occur. To secure our network we must have to know which type of security threats may occur and how? By knowing this we may able to find out security methods against these threats.

Keywords: Network Security, Threat, Virus, Attack

I. INTRODUCTION

Network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network. Today's network consists of vast number of public and private computer and other networking devices used to build this network. Networks can be private, such as within a company, college or large organization or it can be open to public access. Secure Network has now become a need of any organization. We have developed high speed wired and wireless network and internet services but because of different types of threats the entire network is becoming insecure and unreliable [1].

In all areas of life where we are using network and so there is a need to establish a secure network. Network security really means different policies implemented by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network controlled by the network administrator. In current scenario we can see that Wi-Fi networks are very common in providing wireless network access to different resources and connecting various devices wirelessly. So there is a need of different strategies to handle Wi-Fi threats and network hacking attempts [1].

II. ATTACKS AGAINST NETWORK SECURITY

We know that there are many possible security threats today those are spread over the Internet. The most common include are listed below [2].

- Viruses, worms, and Trojan horses
- Spyware and adware
- Denial of service attacks
- Data interception and theft
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Identity theft

Networks are subject to attacks from different types of malicious sources. There are two types of attacks.

A. Active attacks

In passive attacks intruder generally observers the data travelled through network and do the activities which disturb the normal behavior of network by running different commands. Some examples of active attacks are wiretapping, port scanning or idle scanning [5].

B. Passive attacks

Passive attacks have a nature of monitoring, without destroying the actual data. There are 2 types of passive attacks. In passive attacks intruder generally observers the data travelled through network by wiretapping or by another ways. He can also do port scanning to scan the entire network. Sometimes intruder do idle scanning means he just observe the network activities but do nothing. Some examples of passive attacks are

denial of service, spoofing, man in the middle, ARP poisoning, Smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, cyber attack etc.

III. NETWORK SECURITY THREATS

A. Eavesdropping

When any unauthorized party tries to listen to the communication, it is known as eavesdropping. Passive eavesdropping is when an intruder only secretly listens to the networked messages. Active eavesdropping is when the intruder listens the networked messages and modifies the original message by inserting something into the communication stream. This type of activity distorts original message. This can lead to the messages being distorted. Intruder can also copy some sensitive information like passwords [5].

B. Viruses

Viruses are software programs which can self-replicate on computers via computer networks. Virus programs are attached with other program files. Once a file is opened, the virus will activate within the system and can affect other programs of the computer. Virus types can be file viruses, boot sector viruses, macro viruses or script viruses according to the method they use to infect computer[5].

C. Worms

A worm is also software programs which can self-replicate on computers via computer networks. There are two main types of worms, mass-mailing worms and network aware worms. Mass mailing worms use email as a means to infect other computers. A network-aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise. The main difference between virus and worm is that worm does not need to be attached with other program files but it spreads generally via internet.

D. Trojans

Trojan horse is a malicious or harmful code which is contained inside apparently harmless programming or data in such a way that it gets total control of your computer and can do anything with your computer. It can remove all data from your hard disk or it can run memory allocation table etc [1].

E. Spyware

Spyware is a type of malware that is installed on a computer without the knowledge of the owner in order to collect the owner's private information. Spyware is often hidden from the user in order to gather information about internet interaction, keystrokes, passwords, and other valuable data. Spyware can also negatively affect a computer's performance by installing additional software, redirecting web browser searches, changing computer settings, reducing connection speeds, changing the homepage or even completely disrupting network connection ability. Spyware can also be used as a type of adware, where the software delivers unsolicited pop-up ads in addition to tracking user behavior. Typically, spyware is installed when a user installs a piece of free software that they actually wanted [5].

F. Phishing

Phishing is an attempt to obtain confidential information from an individual, group, or organization. Phishing is a technical term used for hacking personal data and these are generally in the form of e-mail messages. Phishers may tries to get personal data, such as credit card numbers, online banking credentials, and other sensitive information [5].

G. Spoofing Attacks

Spoofing means to try to get the address of the computer in order to gain access to other computers so that data and other secret information can be stolen from those computers [4].

H. Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

I. IP spoofing

In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system [3].

J. Packet sniffing

It is a program that can record all network packets that travel past a given network interface, on a given computer, on a network as well as to extract sensitive information from packets [3].

IV. SOLUTIONS FOR NETWORK SECURITY

Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats. Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different solutions and detection mechanisms were developed to deal with these attacks [5].

A. Cryptography

Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data [8].

B. Firewall

A firewall is a typical border control mechanism. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. All traffic from inside to outside and vice versa must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies A firewall is the front line defense mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [6].

C. Intrusion Detection Systems

Intruders are also known as hackers or crackers who are the most dangerous threat to network security. There are different types of intruders as follows.

Masquerader: These are the individuals who penetrate into the system who are not authorized to use the computer and gain access controls to exploit the users account.

Misfeasor: These are users who access data, programs, or resources for which access is not authorized, or they are authorized to access such resources but make misuses of his or her privileges.

Clandestine users: These are users who capture or gain supervisory control of the system and use this control to evade auditing and access controls or to suppress audit collection.

An Intrusion Detection System (IDS) is an additional protection measure that helps to avoid computer intrusions. Software and Hardware devices can be used to detect an attack from intruder. IDS products are used to monitor whether any attack are there or not. Some IDS systems just monitor and give alert signal of an attack, whereas others try to block the attack [4].

D. Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system. Different antivirus software are available in market like AVG, AVAST, Bitdefender, McAfee, Trend Micro and many more. Once you install any of these antivirus programs and do the required settings. It automatically checks and blocks any malicious code when found in your computer [7].

E. Secure Socket Layer (SSL)

SSL is a suit of protocol that is used to achieve a good security between web browser and a website. It creates secure connection between web server and website through web browser so that any information exchanged is protected. SSL is designed to make use of TCP to provide a reliable end-to-end secure service. SSL is not a single protocol but rather it includes multiple protocols like SSL handshake protocol, SSL change chipper spec protocol, SSL alert protocol, SSL record protocol etc.

SSL provides authentication of clients to server through the use of certificates. Netscape and Microsoft Explorer browsers come with SSL.

V. CURRENT DEVELOPMENT IN NETWORK SECURITY

Currently we are using biometric identification techniques in colleges and organizations. The biometric machines or hardware are connected with the computer so with the internet. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented [6].

A. Hardware Development

Smart cards are usually a credit-card-sized digital electronic media which stores digital information. The main idea behind smart cards is to provide undeniable proof of a user's identity. Smart cards can be used for everything from logging in to the network to providing secure Web communications and secure e-mail transactions. Smart card can be implemented with PIN number which is a personal identification number. If

your smart card is misplaced, other person can't use it because it needs your PIN number to access the resources. We are also using PIN numbers in ATM cards [6].

B. Software Developments

Wide variety of advance software is available in market to get high degree of network security including firewalls, antivirus, intrusion detection, and much more. The research focuses on development of more sophisticated software, able to deal with any type of attack in most efficient way. When new viruses come into picture, the antivirus is updated to be able to fight against those threats. This process is the same for firewalls and intrusion detection systems [6].

ACKNOWLEDGMENT

I am heartily thankful to my Principal Sir and my institute to encourage me to do this research in this area and giving me the opportunity to share this knowledge with others.

REFERENCES

[1] http://www.wikipedia.org
[2] Brenton, C. and Hunt, C. (2002): Mastering Network Security, Second Edition, Wiley
[3] Importance of Network Security, found at http://www.content4reprint.com/computers/security/importance-of-network-security-system.htm
[4] Marin, G.A. (2005), "Network security basics", In security & Privacy, IEEE, Issue 6, Vol. 3, pp. 68-72, 2005.
[5] McClure, S., Scambray J., Kurtz, G. (2009): Hacking Exposed: Network Security Secrets & Solutions, Sixth Edition, TMH.
[6] "Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.
[7] Curtin, M. "Introduction to Network Security," http://www.interhack.net/pubs/network-security.
[8] Murray, P., Network Security, found at http://www.pandc.org/peter/presentations/ohio-tech-2004/Ohio-tech-security-handout.pdf