Network security Attacks and Defences

Ranbir Singh, Deepinder Kaur
Department of Computer Science Engineering, Desh Bhagat University, Mandi Gobindgarh – 147301, Punjab, India

***Abstract*— Network security is an important aspect in every field like government offices, Educational institute and any business organization. Network security consists of the policies adopted to prevent and monitor forbidden access, misuse, modification, or denial of a computer network. Network security is very complicated subject and deal by only well trained and experienced people. However, as more and more people become wired, an increasing number of people need to understand the basics of security in a networked world. The history of the network security included introduction to the TCP/IP and interworking. Network security starts with authenticating, commonly with a username and a password. In this paper we study about various types of attacks on network security and how to handle or prevent this attack**

***Index Terms*— Denial, TCP/IP, Authenticating, attacks.**

I. INTRODUCTION

Network security refers to protecting the websites or servers from various forms of attack. Network security consists of the policies adopted to prevent and monitor forbidden access, misuse, modification, or denial of a computer network. The security of network is a big issue for security administrators because network is growing day by day. Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues [1]. Network security is very complicated subject and deal by only well trained and experienced people. Network security is important in every field of today's world such as institutes, offices, military, government, business organization and even in our daily lives. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Having the knowledge of how the attacks are executed we can better protect ourselves. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of

protecting a network resource is by assigning it a unique name and a corresponding password.

Network security has a very vast field which was developed in stages and as of today, it is still in evolutionary stage. To understand the current research being done, one must understand its background and must have knowledge of the working of the internet, its vulnerabilities and the methods which can be used to initiate attacks on the system. Internet has become more and more widespread, in today's world internet is available everywhere in our house, in our work place, mobiles, cars everything is connected to the internet and if an unauthorized person is able to get access to this network he can not only spy on us but he can easily mess up our lives.

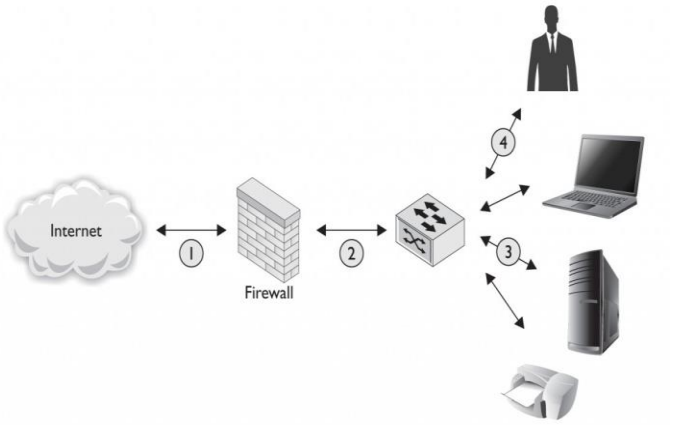

Figure 1. Network security

II. NEED OF NETWORK SECURITY

In the past, hackers were highly experienced programmers who understood the details of computer communications and how to do vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security.

The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks. Because they have no Internet connectivity,

networks designed in this way can be considered safe from Internet attacks. However, internal threats still exist. There is a estimates that 60 to 80 percent of network misuse comes from inside the enterprise where the misuse has taken place.

With the development of large open networks, security threats have increased significantly in the past 20 years. Hackers have discovered more network vulnerabilities, and because you can now download applications that require little or no hacking knowledge to implement, applications intended for troubleshooting and maintaining and optimizing networks can, in the wrong hands, be used maliciously and pose severe threats.

III. HISTORY OF NETWORK SECURITY

Recent interest in security was fueled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer related crime in U.S. history [2]. The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies [2]. Since then, information security came into the spotlight.

Public networks are being relied upon to deliver financial and personal information. Due to the evolution of information that is made available through the internet, information security is also required to evolve. Due to Kevin Mitnick's offense, companies are emphasizing security for the intellectual property. Internet has been a driving force for data security improvement.

Internet protocols in the past were not developed to secure themselves. Within the TCP/IP communication stack, security protocols are not implemented. This leaves the internet open to attacks. Modern developments in the internet architecture have made communication more secure. TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.

IV. BASIC TYPES OF ATTACKS

Here we discussed about attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. These are given below

A. PASSIVE ATTACK

A passive attack, in network security, is an attack characterized by the attacker listening in on communication. In such an attack, the hacker does not attempt to break into the system or otherwise change data. Passive attacks are very difficult to detect because they do not involve any alteration of the data. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

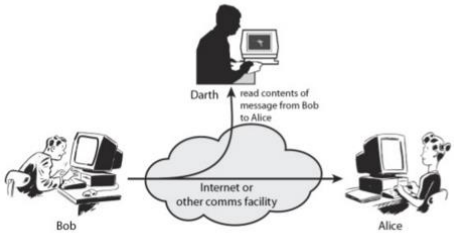

Figure 2. Passive attack

B. ACTIVE ATTACK

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through viruses, worms, or Trojan horses. Active attacks include attempts break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

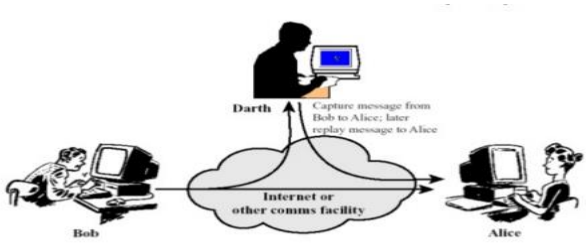

Figure 3. Active attack

C. DISTRIBUTED ATTACK

Distributed Network Attacks are often referred to as Distributed Denial of Service (DDoS) attacks. This type of attack takes advantage of the specific capacity limits that apply to any network resources – such as the infrastructure that enables a company's website. The DDoS attack will send multiple requests to the attacked web resource – with the aim of exceeding the website's capacity to handle multiple requests and prevent the website from functioning correctly. Typical targets for DDoS attacks include: Internet shopping sites, online casinos, any business or organization that depends on providing online services.

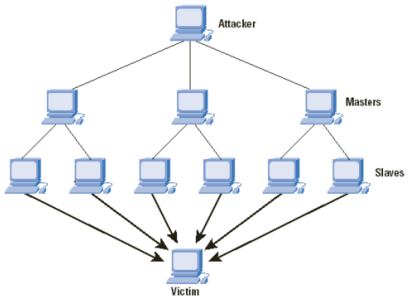

Figure 4. Distributed attack

D. INSIDE ATTACK

Insiders that perform attacks have a distinct advantage over external attackers because they have authorized system access and also may be familiar with network architecture and system policies/procedures. In addition, there may be less security against insider attacks because many organizations focus on protection from external attacks.

E. VIRUS ATTACK

A computer virus is a small program or an executable code that when executed and replicated, perform different unwanted and harmful functions for a computer and a network. Viruses can destroy your hard disks and processors, consume memory at a very large scale and destroy the overall performance of a computer or network. A Trojan is a malicious code that performs harmful actions but it cannot be replicated. Trojan can destroy systems' critical data. A computer worm is a program that replicates to all network and destroy useful data. The viruses, malware, adware and Trojan horses can be prevented if you have an updated antivirus program with the latest pattern files.

V. BASIC SECURITY TIPS

This basic Network Security useful security tips and methods to secure your network such as installing a update antivirus program, email scanning programs, network monitoring tools, internet access policy and other security prevention methods. Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers [3,4]. Network security is a very important aspect of a computer network. Minor security vulnerability can result in a heavy loss of the critical data of your server and other client computers. Keeping the computer as well as network secure, is the big responsibility of the network administrator and the security specialists. There are lot of security measures and prevention methods which I will discuss in this section. Typically a computer network can be attacked by a number of ways such as virus attacks, unauthorized access, cryptography attacks and a number of other security threats. Regularly scan all the network devices, emails, open ports, server and client computers. It's the responsibility of the network administrators to check and deploy the missing security patches in all the network computers. They should also remove the unnecessary network shares, user's accounts, wireless access points and restricts the access to the network users.

A. DOWNLOAD FILES FROM TRUSTED SITES ONLY

Many files can be downloaded from multiple locations on the Internet, but not all locations are created equal. Some are more secure than others. Ensure your users only download from trusted sites, which are often main source websites rather than file-sharing or generic websites. Also consider who in the company needs to download files and applications from a website: consider restricting this permission to only those trusted users who are required to download files as part of their day-to-day activities, and ensure that these select few are educated in how to download files safely.

B. UNDERTAKE AN AUDIT OF NETWORK SHARES

A lot of virus can spread via networks. This is commonly due to there being little or no security on network shares. Remove unnecessary shares and secure the others and their contents to limit network-aware malware from spreading.

C. CONTROL NETWORK CONNECTIONS

When computers connect to networks, they can adopt that network's security settings during that specific session. If this network is external or outside the administrator's control, the security settings may be insufficient and put the computer at risk. Consider restricting users from connecting computers to unapproved domains or networks in most instances, most users need only connect to the main corporate network.

D. TEST NEW SOFTWARE ON A VIRTUAL NETWORK BEFORE YOU USE

Although most software developers test software as much as they can, they are unlikely to have your network's exact configuration and setup. To ensure that a new installation or update does not cause any problems, test it on a virtual system and check its effects before using in to real live network.

E. DISABLE UNUSED USB PORTS

Many devices, when connected to a USB port, will be automatically detected and mounted as a drive. USB ports can also allow devices to auto run any software connected to it. Most users are unaware that even the safest and most trusted devices can potentially introduce malware into the network. To prevent any accidents, it is much safer to disable all unused ports.

VI. DEFENCE AGAINST NETWORK ATTACKS

An inherent weakness in the system may it be by design, configuration or implementation which renders it to a threat. But most of the vulnerabilities are not because of faulty design but some may be caused due to disasters both natural and made, or some maybe cause by the by same persons trying to protect the system [5].Most of the caused due to poor design, poor implementation, poor management, physical vulnerabilities, hardware and software, interception of information and human vulnerabilities. Many of the network attacks can be easily prevented by the network admin monitoring his network closely and applying the entire latest patch available from the vendor to his software. However this cannot prevent most of the attacks, to prevent them, the network requires configurations such as:

A. Configuration Management

It is as important as having a descent firewall to protect the system. As soon as a network setup is completed all its default logins, Ids, address must be changed as soon as possible as all these information is available on the internet for anyone to view. Anyone can use the default login to gain access to the network and it can put the entire network at risk. The machines inside the network must be running the running up to date copies of O and all the patches especially the security patches must be installed as soon as they are available, configuration files must not have any known security holes, all the data is backed up in a secure manner, it allows us to deal with nine out of the ten topmost attacks. Several tools are also available which allows patches to deployed simultaneously and keep things tight.

B. Firewalls

International Journal of Advance Foundation and Research in Science & Engineering (IJAFRSE) Volume 1, Issue 3, August 2014. 11 | © 2014, IJAFRSE All Rights Reserved www.ijafrse.org It is the most widely sold and available network security tool available in the market. This is the wall which stands between the local network and the internet and filters the traffic ad prevents most of the network attacks. There are three different types of firewalls depending on filtering at the IP level, Packet level or at the TCP or application level [6]. Firewalls help preventing unauthorized network traffic through an unsecured network to a private network. They can notify the user when an untrusted application is requested access to the internet. They also create a log of all the connections made to the system. These log can be very harmful in case of any hacking attempts. Firewalls only work if they are correctly configured, if somebody makes a mistake while configuring the firewall, it may allow unauthorized to enter or leave the system. It takes certain knowledge and experience to correctly configure a firewall. If the firewall goes down one cannot connect to the network as in a case of DOS attack. Firewall also reduces the speed of network performance as it examines both incoming and outgoing traffic. Firewall does not manage any internal traffic where most of the attacks come from. Many companies are under false assumptions, that by just using a firewall they are safe, but the truth is they are not, firewall can be easily be circumvented. The best thing while configuring firewall is to deny anything that is not allowed [7].

C. Encryption

Using encryption methods one can prevent hacker listening onto the data because without the right key it will just be garbage to him. Different encryption method such as using HTTPS or SHTTP during the transmission of data between the client and user, will prevent Man in the middle attack (MIM), this will also prevent any sniffing of data and thus any eavesdropping. Using VPN will encrypt all the data going through the network; it will also improve the privacy of the user. Encryption also has downsides as all the encrypted mail and web pages are allowed through firewall they can also contain malware in them. Encrypting data takes processing power from the CPU. This in turn reduces the speed at which data can be send, the stronger the encryption the more time it takes [8].

VII. CONCLUSION

There are a number of ways, which guarantee for the safety and security of your network. Perform regular network security testing. Don't provide more or unwanted access to any network user. Must have an updated antivirus program. Operating system should be regularly updated. If you have windows based operating system you can update it from the Microsoft website. Keep inventory of your network resources such as devices and software applications. Turn off your computer when you are away and don't leave your computer unattended. Put a strong network and system administrator password. Use a switched network, so that you can identify the problem very quickly.

REFERENCES

[1] Akin T.," Hardening Cisco Routers," O'Reilly & Associates, 2002.

[2] Security Overview, www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.htm

[3]Chen S., Iyer R., and Whisnant K., "Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors," In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., 2002.

[4] Kim H., "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, FEBRUARY 2004

[5] Li CHEN,Web Security : Theory And Applications,School of Software,Sun Yat-sen University, China. [6] R. K. Khalil, "A Study of Network Security Systems," IJCSNS International Journal of Computer Science and Network Security, 2010.[7] S. Alabady, "Design and Implementation of a Network Security," Technology,Vol. 1, p. 11, 2009.[8] B. Preneel, "Cryptography for Network Security," Katholieke Universiteit Leuven and IBBT, 2009.