International Journal of Optimal Research in Science and Technology (IJORST)
Volume 5, Issue, April 2021

Analysis of Network Security Issue and Its Attack and Defense

Ganesh M Dahane

***Abstract*-Network Security has become very important in today's world, as a result of which various methods are adopted to bypass it. Network administrators need to keep up with the recent advancements in both the hardware and software fields to prevent their as well as the user's data. Network security gradually attracts people's attention. This paper briefly introduces the concept of network security and need of network security also the various attack methods which are used, as well as various defence mechanism against them.**

***Keywords*- Network security, network security factor, security hazards, DOS attacks, Firewalls, Encryption, Port Scanning, SSL, SHTTP, VPN.**

I. INTRODUCTION.

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security refers to protecting the websites domains or servers from various forms of attack. Network security is important in every field of today's world such as military, government and even in our daily lives. Having the knowledge of how the attacks are executed we can better protect ourselves. Computer network security is fundamentally network information security. It refers to the network system that we use to preserve and flow information and data which may otherwise be exposed to accidental or deliberate damage, leaks or changes. Generally speaking, network security is inextricably related to the confidentiality integrity, authenticity and reliability of network. Its control technologies and concepts are necessary to analyse.to protect our network we need to establish a security analysis model based on researches of network security to make sure computer network work safely.as a result computer network security problem occurred very frequently in fast few year. Hence it make it very urgent to build network security model. A network consists of routers from which information can be easily stolen by the use of malwares such as a "Trojan Horses" Network security is thus mainly focused on the data networks and on the devices which are used to link to the internet. As forecasting goes for the field of the network security it can be said that some new trends are emerging some are based on old ideas such as biometric scanning while others are completely new and revolutionary. Email is a widely used service today and it is also contain many serious flaws, there is no system of Authenticating the sender as well as the recipient, it is stored in multiple places during transmission and can be easily intercepted and changed. SPAM are serious security threat they only require very less manpower but affect millions to billions of Email users around the world, they can malicious link or even false advertisements. A network contains many vulnerabilities but most of them can fixed by following very simple procedures, such as updating software and correctly configuring network and firewall rules, using a good anti-virus software etc.

II. NEED FOR NETWORK SECURITY

The network model today need security against attacker and hackers. Network security includes two basic securities.

1. Security of data information-to protect the information to unauthorized access and loss.
2. Computer security-to protect data from security. Here network security means not only means security in a single network rather in any network or network of network.

III. NETWORK SECURITY HAZARDS

A. Passive attacks

A passive attacks monitors unencrypted traffic and look for clear text password and sensitive information that can be used in other types of attacks. Passive attack include-

- Traffic analysis.
- Monitoring of unprotected communication.
- Decrypting weekly encrypted traffic.
- Capturing authenticating information such as password.

B. Active attacks

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to 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 or modification of data.

C. Password attack

An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters.

D. Buffer overflow

A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

E. DOS Attack

DOS attacks today have become a major threat to network security all over the world. They can be easily launched by anyone with the basic knowledge of network security. They don't require as much time and planning as some other attacks, in short they are cheap and efficient method of attacking networks. They can shutdown the company network by overflowing it with requests and thus affects availability of the network. With the help of easy to use network tools such as Torino, which can be easily downloaded of the internet any normal user can initiate an attack. DOS attacks usually works by exhausting the targeted network of bandwidth, TCP connections buffer, application/service buffer, CPU cycles, etc. DOS attacks use many users connected to a network known as zombies most of the time users are unaware of that their computer is infected.

IV. NATURE OF SECURITY HAZARDS

Security of computer network is needed to fulfil users' requirements of computer network's integrity and confidentiality. With different computer usage, the need of computer security nature could be divided into different risk levels based on the use, in order to protect the security of computer network and analyse specific security feature based on specific requirements

V. 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. Most of the Vulnerabilities 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:

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.

A. 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.

VI. ENCRYPTING THE WORLD WIDE WEB (WWW)

For the sake of privacy, confidentiality and availability our communications on the web should always be encrypted this reduces the number of attacks and prevents anyone to view the ongoing transmissions. These can be achieved by putting together a system of encryption and employing a system of digital certificates. The most important way of encryption is the SSL protocol. Network security can also be compared to human system. The human system can be taken as analogy, providing a protection at each point just like a body we can greatly improve the security. Using this mechanism we can spread our resources and prevent dependent on one system.

A. VPN Virtual Private Network (VPN)

It is a way to transport traffic on an unsecured network. It uses a combination of encrypting, authentication and tunnelling. There are many different types of methods of VPN but of these 5 are easily recognized.The most known and used protocols are as follows:

-Point-to-Point Tunnelling Protocol (PPTP)

- Layer 2 Tunnelling Protocol (L2TP)
- Internet Protocol Security (IPsec)
- SOCKS

B. Secure HTTP (SHTTP)

It's an alternative to HTTPS, it has the same working as HTTPS and is designed to secure web pages and their messages. There are differences between SHTTP and SSL protocol such as SSl is a connection oriented protocol and it works it transport level by providing a secure tunnel for transmission whereas SHTTP works on application level and each message is encrypted separately, but secure tunnel is created. SSL can be used for secure TCP/IP protocols like FTP but SHTTP works only on HTTP. Its use is fairly limited as compared to HTTPS.

C. E-Mail Security

As both the sender and receiver of the email one must be concerned about the sensitivity of the information in the mail, it being viewed by unauthorised users, being modified in the middle or in the storage. Email can be easily counterfeit therefore one must always authenticate its source. E-mail can also be used as a delivery mechanism for viruses. Cryptography as in many other fields' plays a crucial role in email security [6].Emails are very unsecure. As they pass through many mail servers during transits they can be easily intercepted and modified. While using common Email there is no process to authenticate the sender and many users would not give a thought to authenticate the email received. There are many standards one can choose in order to secure his emails some of these are: PGP, PEM, Secure multipurpose Internet mail extension (MIME), Message Security Protocol (MSP).

CONCLUSION

Since internet has become an integral part of our daily lives, the need for network security has increased manifolds in the last decade. As more and more users connect to the internet it attracts a lot of criminals. Nowadays, everything is connected to the internet and so, even a small threat to the network's security could pose a big problem for the users. Today, everything is connected to internet from simple shopping to defence secrets as a result there is huge need of network security. Billions of dollars of transactions happens every hour over the internet, this need to be protected at all costs. Even a small unnoticed vulnerability in a network can have disastrous affect, if companies records are leaked, it can put the users data such as their banking details and credit card information at risk, numerous software's such as intrusion detection have been which prevents these attacks, but most of the time it's because of a human error that these attacks occur. Most of the attacks can be easily prevented, by following many simply methods as outlined in this paper.

REFERENCES

[1] -R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.
[2] Q. Gu, Peng Liu, "Denial of Service Attacks," Texas State University, San Marcos.
[3] -B. Daya ,"Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013.
[4] -Ailin Zeng, "Discussion and Research of Network Security", China, 2014.
[5] -R. K. Khalil, "A Study of Network Security Systems," IJCSNS Internatio nal Journal of Computer Science and Network Security, 2010
[6] -https://en.wikipedia.org/wiki/Network_security#Types_of_Attacks.

AUTHOR'S PROFILE

Ganesh Dahane received his Bachelor of Engineering (B.E) degree in Information Technology in 2006 from Dr. vithalrao vikhe patil college of engineering Ahmednagar, India. He has around three and half year industrial working experience. He received Master of Technology (M.Tech) degree in CSE from LNCT Indore. His area of research is Data structure.