Network Security: Root of Communication among Several Networks

Prachi Sharma[1], Sourav Kumar[2]
[1,2]Student, B. Tech, Computer Science and Engineering Department), Dronacharya Group of Institutions, Greater Noida, U.P., India

***Abstract* - As the internet evolves and computer networks become bigger and bigger, network security has become one of the most important factors for IT industry to consider. Network Security is a key to successful communication among personal computers, organizational computers or any other systems that are connected via network. Its entire field is vast and in an evolutionary stage. 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 [1].**

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 and also ensure that employees have adequate access to the network and resources to work.

This paper briefly addresses the concept of Network Security, Threats of Network Security and the Measures that can be taken or may be useful for the efficient and reliable flow of data among the various systems, connected via network [3].

***Index Terms* - Cryptography, Network Security, Network Security Policy, Prevention, Threats to Network**

I.INTRODUCTION

Nowadays, computers became an integral part of the human life. It is the fastest, reliable, easy to use and the most efficient way used by the people around the world, to communicate with their friends, other business colleagues or to learn new things, and to entertain themselves [4].

As the use of computer increases for the communication or simply the flow of data, the probability of the interrupts occurring in that flow also increases. The interrupts are basically, the security threats like phishing, identity theft, Brand theft, Hacking etc.

Network Security is fundamental defense to safeguard the collaborative enterprise. Network Security is a complex and rapidly evolving field There are three elements of the network security: -

1.Cryptography -

It is the art and science of achieving security by encoding messages/data to make them non-readable by any third party monitoring the data, except the client and the server.

Cryptography includes the two processes Encryption and Decryption.

Encryption means transforming the plain or normal text, which is send over the network, into cipher text.

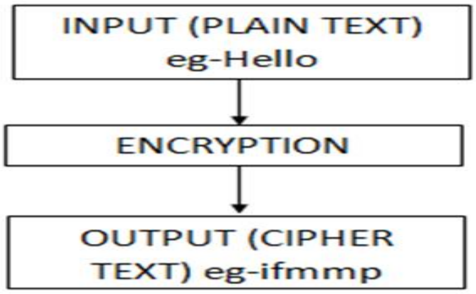

Figure 1. Encryption

Decryption is exactly opposite to the encryption. It is a transformation process of cipher text messages back to the plain text messages.

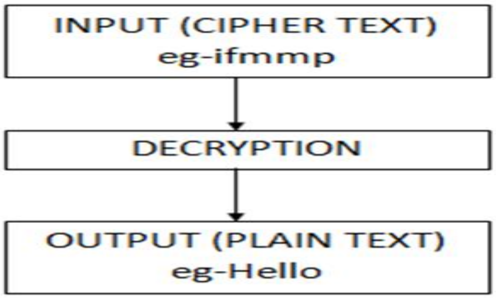

Figure 2. Decryption

Every Encryption and Decryption process has two aspects: the algorithm and the key used for the respective process.

The key is just similar to actual values required to opening specific locks. It is the key, which makes the process of cryptography secure, as the algorithm for encryption and decryption are generally known to everybody.

2. Network Protocols -

Network security protocols are primarily designed to prevent any unauthorized user, application, service or device from accessing network data. This applies to virtually all data types regardless of the network medium used.

Network security protocols define the processes and methodology to secure network data from any illegitimate attempt to review or extract the contents of data.

Some of the popular network security protocols include Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL).

3.Access Control: -

Access control is a set of controls to restrict access to certain resources. It is any mechanisms by which a system grants or revoke the right to access some data or perform some action.

Access Control system include:

1. File permissions such as create, read, edit or delete on a file server.
2. Program permissions, such as the right to execute a program o an application server
3. Data rights, such as the right to retrieve or update information in a database.

There are three types of authenticating information:

1. Something the user knows, e.g., a password, passphrase or PIN
2. Something the user has, such as smart card
3. Something the user is, such as fingerprint, verified by biometric measurement [2]

In addition, a fourth factor of authentication is now recognized: someone you know, whereby another person who knows you can provide a human element of authentication in situations where systems have been set up to allow for such scenarios.

II. COMMON THREATS

Viruses and Worms-

The virus is the program code that attaches itself to application program and when application program run, it runs along with it.

An e-mail virus is computer code sent as an e-mail note attachment which if activated, will cause some unexpected and usually harmful effect, such as destroying certain files on hard disk and causing the attachment to be re-mailed to everyone in the address book.

A micro virus is a computer virus written in the same macro language used for software application like word processors.

The worm is code that replicates itself in order to consume resources to bring it down. It exploits a weakness in an application or operating system by replicating itself.

Trapdoor-

Trapdoor is a method of gaining access to some part of system other than by the normal procedure.

Hackers who successfully penetrate a system may insert trapdoors to allow their entry at later date, even if the vulnerability that they originally exploited is closed.

It is usually inputted by the programmer and once is placed, is, an undocumented way of gaining access to operating systems, application program and online services [4].

Logic Bomb-

A logic bomb is a malware that is triggered by a response to an event, such as launching an application or when a specific data/time is reached.

The logic bomb is designed to wait until user visit a website that requires him/her to login with the credentials, such as banking site or social network.

Malware-

Malicious software (malware) is any software that gives partial to full control of computer to do whatever the malware creator wants.

The population growth of malware describes the overall change in the number of malware instances due to self-replication. Malware that does not self-replicate will always have a zero-population growth.

Hacking-

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose.

Hackers are the people who has the great knowledge about the computer system but uses this knowledge for illegal access to the personal information of the other users or collecting the system data.

Eavesdropping-

Interception of communications by an un-authorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages.

On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way [1].

Phishing –

Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or web page. Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues. Often tactics such as email spoofing are used to make emails appear to be from legitimate senders, or long complex subdomains hide the real website host.

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 [1].

Identity Theft-

This has become a major problem with people using the internet for cash transactions and banking services. In this, a criminal accesses data about a person’s bank account, credit cards, social security ,debit card and other sensitive information.

Here, the attacker does not steal anything from legitimate user, he becomes the legitimate user.

III. MEASURES TO PREVENT

Intrusion Detection System (IDS)-

It is a mechanism to detect where the intrusion occurs. It can be hardware-or-software based security service that monitors and analyses system events that may indicate a network system attack [1].

The most common classifications are network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS).

A system that monitors important operating system files is an example of HIDS, while a system that analyzes incoming network traffic is an example of NIDS.

Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system.

Firewall-

A firewall is a network security system designed to prevent unauthorized access to or from a private network.

Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.

All the traffic between the network and the Internet in either direction must pass through the firewall. The firewall decides if the traffic can be allowed to flow or whether it must be stopped from proceeding further.

Depending on the criteria used for filtering traffic, firewalls are generally classified as:

1)Packet Filter - Also known as screening router or screening filter, applies a set of rules to each packet and based on the outcome, decides to either forward or discard the packet.

Such a firewall implementation involves a router, which is configured to filter packets going in either direction.

2)Application Gateways – It is also known as Proxy server because it acts like a proxy and decides about the flow of application-level traffic.

When a client program establishes a connection to a destination service, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to communicate with the destination service.

This creates two connections, one between the client and the proxy server and the other between the proxy server and the destination.

Secure Socket Layer (SSL)-

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity [1].

Virtual Private Network (VPN)-

A VPN is a mechanism of employing encryption, authentication and integrity protection so that organization use a public network (such as the Internet) as if it is a private network.

A VPN can connect distant network of an organization or it can be allowed travelling users to remotely access a private network securely over the Internet.

Tunneling is an important concept with respect to VPNs.

Tunneling is generally done by encapsulating the private network data and protocol information within the public network transmission units so that the private the private network protocol information appears to the public network as data.

Anti-virus-

Antivirus or anti-virus software, sometimes also known as anti-malware software, is computer software used to prevent, detect and remove malicious software. Many antivirus programs include both automatic and manual scanning capabilities. The automatic scan may check files that are downloaded from the internet, discs that are inserted into the computer, and the files that are created by software installers.

The automatic scan may also scan the entire hard drive on a regular basis. The manual scan option allows the user to scan individual files or the entire system, whenever it is required.

Wi Fi Protected Access (WPA) –

WPA encrypts information and checks to make sure that the network security key has not been modified. WPA also authenticates users to help ensure that only authorized people can access the network.

There are two types of WPA authentication: -

1. WPA is designed to work with all wireless network adapters, but it might not work with older routers or access points.
2. WPA2 is more secure than WPA, but it will not work with some older network adapters.

IV. NETWORK SECURITY POLICY

A network security policy is a special kind of policy that focuses on security aspects of a computer network. Network security policies can be written in different formats and at different levels of abstraction. On the one hand, very abstract high-level policies exist which are written in natural language that express network-wide security goals [5].

On the other hand, concrete configuration of single security controls is written in a device-specific configuration language. High-level policies are easy to write and understand by humans but difficult to elaborate on machines; concrete configurations which are difficult to read and write for humans are easily interpreted by machines [5].

Policy Analysis-

Following are the three categories for analyzing the network policy-

Conflict analysis searches for possible errors within a single or a set of security policies. It searches for potential semantic errors within correlated policy rules. Conflict analysis can also be used to identify possible policy optimizations. Conflict analysis can be applied to a single policy (Intra-Policy analysis) or to set of policies of interconnected security controls (Inter-Policy analysis) [5].

Reachability analysis evaluates allowed communications within a computer network. Furthermore, it can determine if a certain host can reach a service or a set of services. In general, reachability analysis is performed online by using tools such as “ping” or “traceroute”. By using an accurate representation of the network and its security policies, reachability analysis can also be performed offline, during the design phase [5].

Policy comparison compares two or more network security policies and represents the differences between them in an intuitive way. Network security policies involved may include single concrete security control configurations, sets of configurations, and high-level policies of an entire network. One

of the best use-cases of policy comparison is to verify that a desired network security policy is implemented correctly by comparing the designed high-level policy with the concrete network configuration [5].

V. CONCLUSION

As the world is growing day by day, in the field of technical knowledge and opportunities to create something new. Communication is the most effective way to spread the ideas of growth. And for uniting the people and their ideas around the world, Network is needed but for the secure transmission of that data, Network Security is needed.

By increasing the network security, one can decrease the chances of data lost or theft, identity theft, hacking, virus attack, or any other malicious software.

As the Network security is mitigated by humans, it is also often susceptible to human mistakes. Anything from misconfigured equipment or services to unsecured usernames and passwords can pose a real threat to network security. Some default security holes of Operating Systems, network devices or TCP/IP protocols can be used by hackers to gain access to network resources.

Also, hacker tools have become more and more sophisticated, super-intelligence is no longer a requirement to hack someone’s computer or server. Of course, there are individuals that have developed sophisticated skills and know how to breach into a user’s privacy in several ways.

Thus, to prevent the system from attacks, the user should go for the network security tools like antivirus software, firewalls and so on. So that the information became accessible to the users by following the access control feature of the network security that how users and systems communicate with the other users and the systems, thus providing a secure channel for communication through the network.

REFERENCES

[1] Bhavya Daya,” Network Security: History, Importance, and Future”

[2] Sumedha et al., “Network Security Using Cryptographic Techniques” International Journal of Advanced Research in Computer Science and Software Engineering 2 (12), December - 2012, pp. 105-107

[3] Jie Shan,” Analysis and research of computer network security” J. Chem. Pharm. Res., 2014, 6(7):874-877

[4] Ailin Zeng,” Discussion and research of computer network security” J. Chem. Pharm. Res., 2014, 6(7):780-783

[5] Christian Pitscheider,” Network-Security-Policy Analysis” DEPEND 2014: The Seventh International Conference on Dependability