International Journal of Emerging Trends in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 3, Issue 2 (March-April 2016), PP.54-58

Accomplishment of Security Techniques In Network System: A Study

Mrs. Ruma Rahul Kapre
(Department Of Computer Science, Dharampeth M. P. Deo Memorial Science College/RTMNU, India)

Abstract :- :- Network security involves of the necessities and policies clinch by a network administrator. Misuse, modification, unauthorized access, refutation of a network of computer and network-accessible resources are prevent and supervise by network administrator. Network security provides permission of access to data in a network. Users are allotted an ID and password and also other authenticated information that permits them access to information and programs within their authority. Network security deals with day to day transaction and communication in the field of business, government places, and social sites and even for individuals publically and also privately. Networks can be private, such as within a company, and others which might be open to public access. by assigning a irreplaceable name and password to network resource, can be protected. In this research paper researcher discuss on different security issues and techniques which will help to advance the security in various era.

Keywords: - Firewall with types, Network security techniques, Security issues.

I. INTRODUCTION

Network

A group of interconnected computers and peripherals that is capable of sharing software and hardware resources amongst many users'. Network computer devices that originate, route and release the data are called network nodes. Nodes consists of personal computers, phones, servers as well as networking hardware. The devices are supposed to be in network, when one device is able to interchange information with the other device, whether or not they have a uninterrupted connection to each other.

Computer networks vary in various places like in the transmission media used to convey the signals, the communications protocols to organize network traffic, its size, topology and organizational set on.

Security

Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper exposé thereby creating a safe platform for computers ,users and programs to perform their permitted critical function within a secure environment. Network security is typically detained by a network administrator or system administrator. A network security system normally depend on on layers of protection and consists of several mechanisms including networking monitoring and security software in addition to hardware and applications. All components are well organized to increase the overall security of the computer network. Network security starts with authenticating, usually with a username and a password.

II. SECURITY TECHNIQUES

- Hashing
- Symmetric Key Cryptography
- Diffie-Hellman Key Exchange
- Public Key Cryptography

2.1) Hashing: -

In hashing technique the hash value is used when user has sent request to another user. During this process, a value is generated from the string of text. The generated value is called hash value. By applying this technique on the text, the hash is significantly reduced than the text itself. The adoption of using a formula for generation of hash value will not be same for the various texts.

The Hash plays a important key role in security systems where they're used to confirm that transferring text/message have not been obstruct. The sender creates a hash of the message, encrypts it, and sends it with the message itself. The receiver then decrypts the message and generates another hash from the received message. The values are always associated which are created by sender and receiver. The probability of getting safe and secure messages will increase if both the values are equal.

2.2) Symmetric Key Cryptography:-

The algorithms which are use for cryptography that utilizes the same cryptographic keys for encryption of plaintext and decryption of symbols text. These keys are use for the simple transformation of data which are identical. To sustain private information link these keys are characterized a shared secret between two or more parties. Symmetric-key systems are modest and quicker but their main flaws is that the two parties must give-and-take the key in a secure way. Public-key encryption escape this problem because the public key can be dispersed in a non-secure way, and the private key is never diffused. Some time Symmetric-key cryptography is also called secret-key cryptography. The most potently used symmetric-key system is the Data Encryption Standard (DES).

2.3) Diffie-Hellman Key Exchange:-

The scheme was first issued by Whitfield Diffie and Martin Hellman in 1976. Diffie–Hellman key exchange (D–H) is a specific technique of securely swapping cryptographic keys over a public channel and was one of the first public-key protocols. The Diffie–Hellman key exchange method allows two parties that have no earlier knowledge of each other tomutually create a shared secret key over an insecure channel. For encryption of successive communication using a symmetric key cipher, this key will be used.The scheme is also used to secure a variety of Internet services. Although Diffie–Hellman key agreement is a non-authenticated protocol, it provides the basis for a variety of authenticated protocols, and is used to run perfect forward privacy in Transport Layer.

2.4) Public Key Cryptography:-

Public-key cryptography finds purpose in center of the discipline information security. Information security (IS) is concerned with all aspects of securing electronic information assets against security threats. Public-key cryptography is used as a mode of assuring the privacy, authenticity and non-reputability of electronic communications and data storage.A cryptographic system that uses two keys - a public key recognized to everyone and a private or secret key acknowledged only to the recipient of the message. The Public Key System associates the public and private key in such a way that the message will be encrypted by the public key only and decrypted by the corresponding private key only. Likewise, it is almost impossible to presume private key if you know the public key.

III. Firewall

Firewalls are used to avoid unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. To avoid unauthorized access to or from private network ,a firewall system is designed. Incoming and outgoing messages of the intranet pass through the firewall, which examines each

message and blocks those that do not meet the precise security criteria. Following section discuss few firewall techniques to prevent unauthorized access.

3.1) Common Firewall Techniques

Most of the home and corporate networks are protected by firewalls technique. The information which comes through the internet gets filtered by a firewall program or device to your network or computer system. There are quite a few types of firewall techniques that will avoid potentially harmful information from getting through.

3.1.1) Packet Filter

Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

3.1.2) Application Gateway

Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.

3.1.3) Circuit-level Gateway

Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

3.1.4) Proxy Server

Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

IV. TYPES OF ATTACKS

Malevolent sources are forcefully attacks the networks. Attacks can be of two categories: "Passive" when network intruder to catch data roaming through the network, and "Active" in which an impostor initiates commands to interrupt the network's normal operation.

Types of attacks include:

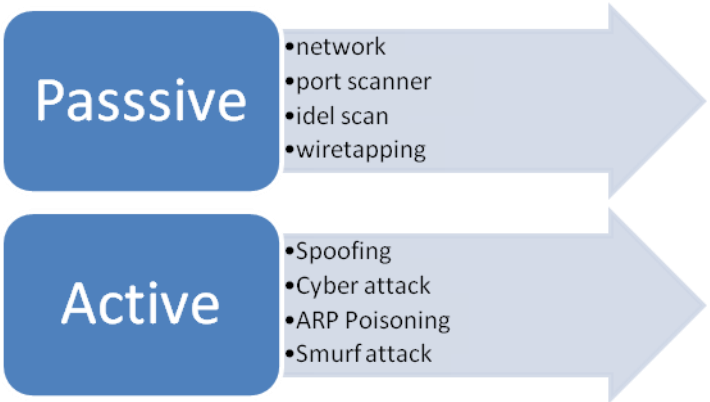

fig: types of attacks

These security techniques will help to improve data reliability, security, authenticity and availability. We will focus on these issues:

Availability

For any information system to aid its purpose, the information must be available when it is required. Computing system will help in saving and processing the information. For successful execution of any computing system it required the security controls, communication channels which always work correctly. To increase the Availability of the systems the necessity is that the objective of the system should remain available all times. During the process of system upgradation the accessibility of the service should not hamper because of power outages, hardware failures, and system upgrades. Ensuring availability also encompasses precluding denial-of-service attacks, such as a flood of incoming messages to the target system fundamentally imposing it to shut down.

Security

The technology which is applicable for gaining any security is Network security. A computer is an electronic device with a processor and some memory. Such electronic devices can group from non-networked standalone devices such as calculators and other ubiquitous devices. With the help of these devices computing can be done via use of mobile phones. IT security experts are almost always found in any chief creativity due to the nature and assessment of the data within larger businesses. They are liable for trying all of the technology within the company safe from malicious cyber-attacks that often try to break into critical secluded information or to increase the control of the internal systems.

Authenticity

Authentication is the technique which emphasis on authenticating a uniqueness. There are different types of information that can be used for authentication. Things such as a PIN, password, a magnetic swipe card, biometrics, palm prints, fingerprints, voice prints and retina (eye) scans. Strong authentication involves providing more than one type of authentication information (two-factor authentication). Today the most public form of identification is the username on computer system. and the most shared practice of authentication is the password. Usernames and passwords are fulfilling their purpose. But now in the current trends, they are no longer acceptable. Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

Reliability

The term "reliable" is a synonym for assured. Reliability is the assets of leading to consistent intended behavior and results. Reliability is also well-defined as the assets of trustworthiness. Data are often considered reliable when they are exact and defined, and when they can be replicated. Computer security objective is to hold protected information and assets from theft, venality, or natural disaster. This allows the information and property to remain accessible and dynamic to it's imagine users. The mechanism by which delicate and valuable information protected is nothing but the Computer Security. With the help of security techniques the services are protected from publication, tampering or breakdown by unauthorized activities or untrustworthy individuals and unplanned events. A "reliable" service is one that inform the user if delivery miscarries, while an "unreliable" one does not inform the user if delivery fails.

Reliable protocols typically sustain more overhead than unreliable protocols, and as a result, functions more slowly and with less scalability. A reliable protocol delivers reliability properties with respect to the release of data to the intended recipients.

V. Conclusion

Now a day's security is big issue. To make a glance on this issue , In this paper the researcher discussed some security techniques like hashing, Symmetric key Cryptography, Diffie-Hellman Key Exchange, Public Key Cryptography. There are different ways to provide the security by using authentication and authorization

techniques. Employing these techniques in network systems will really help to achieve the various parameters like reliability, availability, security and flexibility of the data. According to this, the work that needs to be done, and the necessity & concerns needs to be addressed. The researcher also talks out types of attack in this paper. The work is not limited and we will not provide full security to network and hence there is future scope of security issue.

REFERENCES

1) R. K. Khalil, "A Study of Network Security Systems," IJCSNS International Journal of Computer Science and Network Security, 2010.
2) S. Alabady, "Design and Implementation of a Network Security," Technology,Vol. 1, p. 11, 2009.
3) B. Preneel, "Cryptography for Network Security," Katholieke Universiteit Leuven and IBBT, 2009.
4) Simmonds, A; Sandilands, P; van Ekert, L (2004) Ontologyfor Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.
5) Curtin,M."IntroductiontoNetworkSecurity,"http://www.interhack.net/pubs/network-security
6) M. Frantzen, F. Kerschbaum, E. Schultz, and S. Fahmy, "A framework for understanding vulnerabilities in firewalls using a dataflow modelof firewall internals,"Computers and Security, vol. 20, no. 3, pp. 263–270, May 2001
7) Li Tao. Introduction to network security. Beijing: Electronic Industry Press. 2003,107-111