National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Survey on Network Security

Rachana R, Vinay N
UG Scholar, KLE S. Nijalingappa College, Rajajinagar, Bangalore, Karnataka, India

ABSTRACT

Computer networks are an essential part of our life by which we can share the information through different technologies like wired or wireless networks. Nowadays wireless technologies are adopted because of its advantages and secured information transmission. This article includes definition of network, network security and their working process on information security.

Keywords : Network, DoS, Attacks, Security, Encryption

I. INTRODUCTION

Network security consists of the policies and practices adopted 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, which is controlled by the administrator. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among business, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access.

NETWORK

A network is an interconnection of autonomous computers. Two computers are said to be interconnected if they are capable of exchanging the information. Central to this definition is the fact that the computers are autonomous. This means that no computers on the network can start, stop or control another.

NETWORKING SECURITY

The networking offers endless possibilities and opportunities to every user of it, alone with convince. But this convinces endless benefits are not free from risks as there are many risks in network security. While ensuring network security, the concerns are to make sure that only legal or authorized user and programs gain access to information resources like databases.

NEED OF NETWORKING

- ✓ File sharing provides sharing and grouping of data files over the network.
- ✓ Print sharing of computer resources such as hard disk and printers etc.,
- ✓ Email tools for communication with the email address.
- ✓ Remote access able to access data and information, around the globe.
- ✓ Sharing database to multiple users at the same time by ensuring the integrity.

APPLICATIONS IN NETWORKING

• SMS(Short Message Service)

It is the transmission of short text messages to and from a mobile phone, fax machine and/or IP address. Messages must be no longer than some fixed number of alpha-numeric characters and contain no images or graphics.

• Chat

Chatting is the most fantastic thing on internet. Chatting is like a text phone. In telephone conversations, you say something, people hear it and respond , and one can hear their responses on the spot and can reply instantly.

The problems encountered under network security are as follows:

• Physical Security Holes

When individuals gain unauthorized physical access to a computer and temper with files. Hackers do it by guessing passwords of various users and then gaining access to the network systems.

• Software Security Holes

When badly written programs or 'privileged ' software are compromised into doing things that they should not be doing.

• Inconsistent Usage Holes

When a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view.

SECURITY MANAGEMENT

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. In order to minimize susceptibility to malicious attacks from external threats to the network, corporations often employ tools which carry out network security verifications.

TYPES OF NETWORK SECURITY

A. Distributed Denial of Service (DDoS)
B. Intrusion Prevention / Detection System (IPS/IDS)
C. Security Information and Event Management (SIEM)
D. Network Access Control (NAC)
E. Virtual Private Networks (VPNs)

TYPES OF ATTACKS

Network are subject to attacks from malicious sources. Attacks can be from two categories : "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.

Types of attacks include

- Passive
- Network
- Wiretapping
- Port scanner
- Idle scan
- Encryption
- Traffic analysis II.
- Virus
- Eavesdropping
- Data modification
- Denial-of-service attack
- DNS spoofing
- Man in the middle
- ARP poisoning
- VLAN hopping
- Smurf attack
- Buffer overflow
- Cyber-attack

WIRETAPPING

Wiretapping is the monitor of telephone and internet based conversations by a third party.

ENCRYPTION

The translation of data into a secret code. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it.

VIRUSES

Computer virus is a malicious program that requires a host and is designed to make a system sick, just like a real virus. Viruses can spread from computer to computer and they can replicate themselves. Some viruses are categorized as harmless pranks, while others are far more malicious.

PROTECTION METHODS

I. Authorization
It determines whether the service provider has granted access to the web service to the requestor. Authorization is performed by asking the user a legal login ID. If the user is able to provide a legal login ID, he/she is considered as authorized user.
II. Authentication
Authentication also termed as password protection as the authorized user is asked to provide a valid password and if he or she is able to do this, he or she considered to be an authentic user.
III. Encrypted Smart Cards
An encrypted smart card is a hand held smart card that can generate a token that a computer system can recognize. Every time a new and different token is generated, which even though cracked or hacked, cannot be used later.
IV. Bio Metric Systems
They form the most secure level of authorization. The Biometric systems involve some unique aspects of a person's body such as finger prints, retinal patterns, etc to establish his/her identity. V. Firewall
A system designed to prevent unauthorized access to or from a private network is called firewall. They can be implemented in both hardware and software or a combination of both.
Types of firewall techniques are:

- Packet Filter
- Application gateway
- Circuit level gateway
- Proxy server

II. CONCLUSION

Network security is an important field that is getting more and more attention as the internet expands. This field concentrates on protecting the data from the unauthorized users. This security technology consists of mostly software and even certain hardware devices too. Network security plays an important role in authorizing the users so that they can secure their data from the hacker or unauthorized users. An effective network security plan can be developed to manage the understanding of security issues, potential attackers, needed levels of security and the factors that makes the network to attack. In addition to protect the network systems from the other external threats or failures, the network security is used. It can be stated that, using Network Security data transmission can be the safer mode of transmission with very less possible interruption to the any particular system.

Cite this article as :

Rachana R, Vinay N, "A Survey on Network Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 140-142, September-October 2019. Journal URL : http://ijsrcseit.com/CSEIT194725