International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 3, September - November, 2017 | Pages 18-22

ENHANCED NETWORK SECURITY SYSTEM USING FIREWALLS

R. Ganeshan
Assistant Professor, Dept of CSE, St. Joseph College of Engineering Sriperumbudur, India
Dr. Paul Rodrigues
Professor, Dept of CSE, Indra Gandhi College of Engineering and Technology Chengalpattu, India.

Abstract:
Network security consists of the provisions and policies embraced by a network administrator to preclude and monitored 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 network administrator. 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. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. In this research paper researcher discuss on different security issues and techniques which will help to improve the security in various era of the world.
Keywords: Administrator, Network Resource, Network Security.

1. INTRODUCTION

In the last few years, the Internet has experienced an explosive growth. Along with the widespread evolution of new emerging services, the quantity and impact of attacks have been continuously increasing [1]. Defense system and network monitoring has become an essential component of the computer security to predict and prevent attacks. With the thriving technology and the great increase in the usage of computer networks, the risk of having these network to be under attacks have been increased. We interact with network every day and perform banking transaction, surfing Internet, buy online goods and pay it using online transaction. Life without networks would be considerably less convenient and many activities would be impossible. Threats to computer security are computer crimes, including viruses, electronic break-ins, and natural and other hazard. Security measures consist of encryption, restricting access, anticipating disasters and making backup copies. Keeping information private depends on keeping computer systems safe from criminals, natural hazard and other threats. Computer crime is an illegal action which the perpetrator uses special knowledge of computer technology. Number of techniques have been created and designed to help in detecting and/or preventing

such attacks. As networks become more common, several security issues and challenges are becoming more apparent. Some standard technologies currently used on the Internet are not secure. Awareness is the key if we want to further secure networks from infiltration. From the normal user's perspective, a network is sometimes designed in such a way that it looks like two end points with a single connection in the middle. Although this perspective view is functionally correct but sometimes it ignores the complex design, such as implementation and management of the network concept. The categories of networks are LAN, MAN and WAN. These networks are categories by their scope and geographical coverage area.

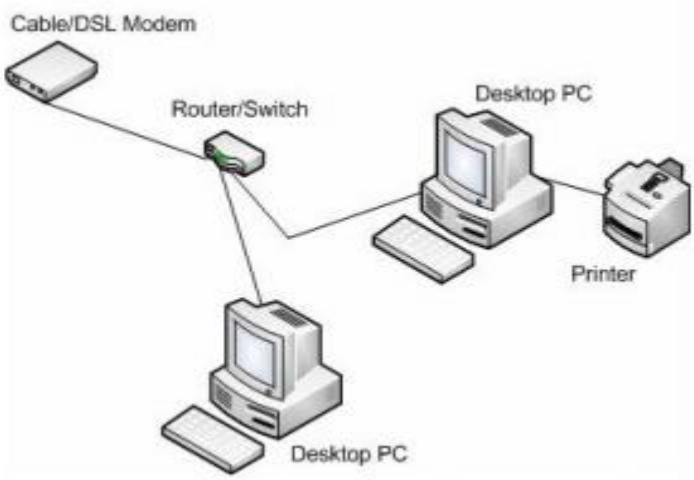

Fig.1.Basic Network

The networks are continuously experiencing staggering and scaling growth as users demands increase. More people use the Internet to get connected to others and find and share information and other resources. Different types of networks are differentiated based on their size (in terms of the number of machines), their data transfer speed and their reach. Local Area Network (LANs) is a smaller network compared with Wide Area Network (WANs), which is simply a combination of multiple LAN networks. Metropolitan Area Network.

2. RELATED WORK

Nowadays with the spreading of the Internet and online procedures requesting a secure channel, it has become an inevitable requirement to provide the network security. There are various threat sources including software bugs mostly as the operating systems and software used becomes more functional and larger in size. Intruders who do not have rights to access these data can steal valuable and private information belonging to network users. As network become more common, several security issues are becoming more apparent. Some antivirus and security network technology are not secure. A National Research Council report warned in 1991 that "emerging trend, point to growth in both level and the sophistication of threats. There is reason to believe that we are at a discontinuity: with respect to computer security, the past is not a significant predictor of the future". Events since 1991 have validated this belief. Implications of security challenges are always discussed nowadays. Since networks are carrying and holding

information of all types around the world, it is exceedingly attracting the targets to attack and take away important data and other resources. Networks bring more resources within the reach of more potential attackers. Like threats to computing systems, threats to networks can compromise confidentiality and integrity of devices and data stored.

There are different motivations why the attackers always attack and want to harm networks in a computing environment. A clever attacker investigates and plans before acting. Information is the attacker's greatest weapon. Insiders may collect the system information that they are authorized and provide to intruders. In order to obtain passwords or other secrets, outside intruders use social engineering and other tricks to attack networks and steal important information. Besides that, an easy way to gather network information is to use port scan, a program for a particular IP address, that reports which port respond to messages and which of several known vulnerabilities seem to be present.

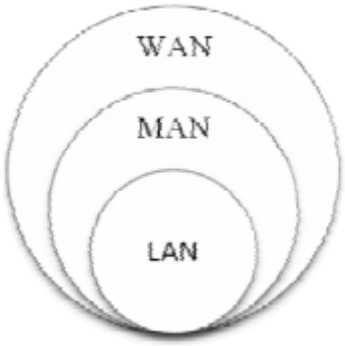

Fig.2.Types of Network

Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate use in managing networks, but it also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

3. PROPOSED SYSTEM

A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Personal Firewall works in the application layer of firewall. Personal firewall runs on a workstation to block unwanted traffic, usually from the network. It can complement the work of a conventional firewall by screening the kind of data a single host will accept, or it can compensate for the lack of a regular firewall as cable or modem connection. It is difficult to separate entirely advances in firewall technology from the commercial products that implement them. There is a large market for commercial firewall products, which has driven many crucial recent developments. At the same time, without direct inspection of the source code, it can be quite difficult. Commercial implementations of personal firewall include Norton Firewall from Symantec, Kaspersky Internet Security, Lavasoft Personal Firewall and MCAfee Personal Firewall. This framework of the vulnerability, threat and safeguard are useful to security analyzing, and

evaluating for deciding, which safeguards mechanisms to apply and use. Therefore, there is a relationship between framework elements as shown in Figure-7 below, which we represent vulnerability as V, threat as T and safeguard as S. Meanwhile, the proposed framework presents itself as the box which inside the box are computing system (V) with its procedures and controls (S). In contrast, outside the box is the threats (T), including the authorized users. In addition, a circle represents active events in the framework. This scenario describe how does framework behaves to save our system as we consider that safeguard S1 guards against the threat T1 which attempt to attack vulnerability V1 and also S2 guards against T2 which attempt to attackV2. Finally, S3 and S4 represented by the curved boundary, guards against any others threats that exploiting any of the vulnerabilities of the proposed framework. 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 secrecy, 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 is that the public and private keys are associated in such a manner that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Likewise, it is virtually impossible to deduce the private key if you know the public key.

4. ANALYSIS

Information Technology security is data security applied to technology (most often some form of computer system). It is sensible to note that a computer does not inevitably mean a home desktop. A computer is any device with a processor and some memory. Such devices can array from non-networked standalone devices as simple as calculators, to networked mobile computing strategies such as smartphones and tablet computers. IT security experts are almost always found in any chief enterprise/establishment due to the nature and assessment of the data within larger businesses.

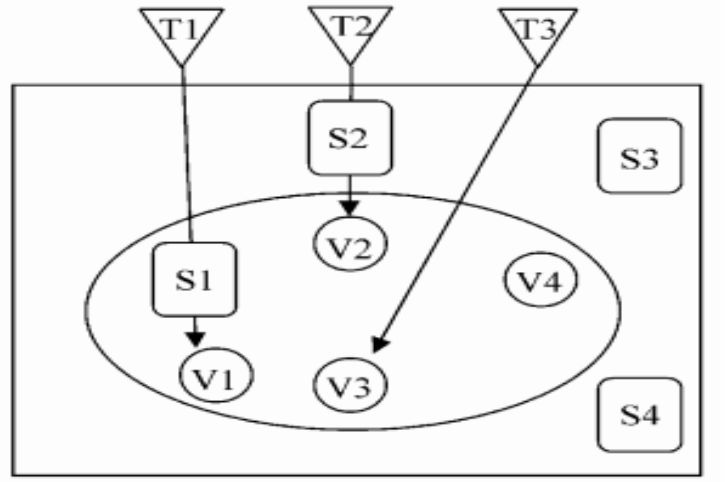

Fig.3.Frame Work

They are liable for keeping all of the technology within the company safe from malicious cyber-attacks that often attempt to breach into critical secluded information or gain control of the internal systems. The objective of computer security embraces protection of information and property from theft, venality, or natural disaster, while allowing the information and property to remain accessible and dynamic to its envisioned users. The term computer system security means the collective processes and mechanisms by which subtle and valuable information and services are protected from publication, tampering or breakdown by unauthorized activities or untrustworthy individuals and unplanned events. Other possibilities embrace using both packet filtering and application layer proxies. The benefits here embrace providing a measure of protection against machines that provide services to the Internet (such as a public web server), as well as deliver the security of an application layer gateway to the internal network. Using this method, in order to get to services on the internal network, an attacker will have to break through the access router, the bastion host, and the choke router.

CONCLUSION

The security issues in networked systems as described in this paper identify some of the work that needs to be done, and the necessity & concerns needs to be addressed. Several countries dependent on some of the IT based infrastructure could face serious national consequences resulting from their vulnerabilities. The changing technologies and the changing threats is complicating our understanding of the threats and how to deal with them. Due to the complexities among networks internationally, any increases in network security must involve the dedicated efforts of as many nations as possible. A great deal of understanding can be accomplished through such mechanisms, but not without taking note of their earlier troubles.

REFERENCES

1. "Google Query Serving Architecture" at National Conference by NACC(National assessment and Accreditation Counci"Intrusion Controls in Computer "Networks: How Effective are they and what a computer engineer can do?" at National Conference.
2. Brush, C, Surcharge for Insecurity, Information Security Magazine.
3. M.Bellare, S.Thomson, Key-versatile signatures and applications: RKA, KDM and Joint Enc/Sig. Advances in Cryptology - Euro crypt.
4. American Bar Association. International Cyber-crime Project of the ABA Privacy and computer crime.
5. Council of Europe, Convention on Cyber-crime- Explanatory Report.
6. Stallings, William, Network security essentials, Pearson Education Asia.