International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099

VOL 1 ISSUE 4 (2017) PAGES 16 - 20

Received: 20/05/2017. Published: 27/06/2017

ENHANCED NETWORK SECURITY SYSTEM USING FIREWALLS

P. Daniel Sundarraj,
Assistant Professor and Head,
Department of Computer Science and Apllication,
K. M. G. College of Arts and Science, Gudiyattam.

Abstract:

The Internet and computer networks are exposed to an increasing number of security threats. With new types of attacks appearing continually, developing flexible and adaptive security oriented approaches is a severe challenge. This paper discusses the security of computing systems and shows how to protect computer-related assets and resources. The paper highlights different security threats and concerns across computer networks and shows how firewalls detect these threats. At the end, different firewalls like Packet Filtering, Application Gateways and Personal Firewall are summarized and compared according to different network scenarios. The paper also proposes a new framework for the vulnerability, threat management and safeguard of network environments.

Keywords: security system, firewalls, threats, packet filtering, application gateways.

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.

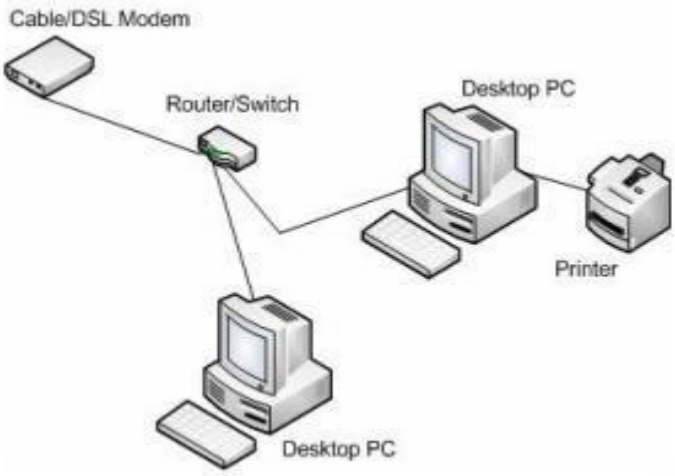

Fig.1.Basic Network Concept

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

International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099
VOL 1 ISSUE 4 (2017) PAGES 16 - 20
Received: 20/05/2017. Published: 27/06/2017

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 [2]. A network is a group of systems that are connected either using wired or wireless technology to allow sharing of resources, such as files, printers, or sharing of services, such as an Internet connection.

2. NETWORK CONCEPTS

The categories of networks are LAN, MAN and WAN. These networks are categories by their scope and geographical coverage area. 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 (MANs) is a network scattered in metropolitan cities and covers relatively smaller geographical area compare to a WAN network.

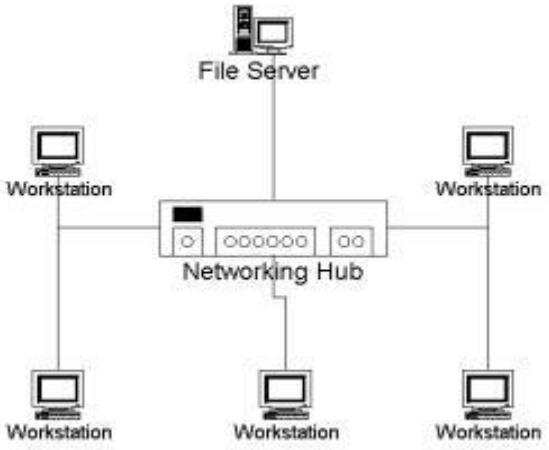

Fig.2.Local Area Network

These components form a network within an office or building. The data transfer speed can reach from 10 Mbps to 1 Gbps depending on the devices and cabling system installed. The number of nodes can vary from 100 to 1000's nodes. Ethernet LAN is the most common type of LAN network available. The smallest home LAN network can have exactly two computers and a large LAN can contain thousands of computers. LANs can be divided into logical groups called subnets. An Internet Protocol (IP) "Class A" LAN can theoretically accommodate more than 16 million devices organized into subnets. directly between systems on the network without the need of a central server and they can determine what

information or files they are willing to share with the other hosts on the network. However, Server-based networks have at least one host, which is dedicated to function as server. Client computers do not share any information with each other computers. All data is stored on the central server. Most corporate networks are based on this methodology. Within a Server-based network type, servers can play several roles.

WAN network covers long distances, and their communication facilities are provided by separate organizations. WANs differ from LAN in terms of size of network or distance and control or ownership. WANs are simply combinations of LANs, MANs and additional communications links between the LANs. WAN may belongs to a company with many offices, it may be even in different cities or countries, or it may be a cluster of independent organizations within a few miles of each other that share the network. 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.

3. NETWORK SECUIRITY TECHNIQUES

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. 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. Firewalls were invented in early 1990s. They provide a fireproof barrier between parts of the buildings, making it harder for a fire in one part of the building to spread to other parts. Similarly, a network firewall is built around a network or subnetwork to protect it from the outside. Steven and William in [11] defines firewall as a collection of components placed between an inner network and an outer network to achieve the following goals; all traffic must pass through the firewall, only traffic that is authorized by the inner network's security policy is allowed to pass, the firewall cannot be penetrated [8]. Figure-6 illustrates a firewall usually located between the external world and the internal network.

VOL 1 ISSUE 4 (2017) PAGES 16 - 20

Received: 20/05/2017. Published: 27/06/2017

4. ANALYSIS

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. he concepts of the vulnerability, threat and safeguard make up a useful technique for generating new ideas to build a framework of network security. Vulnerability is a weakness or gap in a network system that could allow security to be violated. Vulnerabilities may result from weak passwords, software bugs, a computer virus or a script code injection, no antivirus and a SQL injection. A threat is a circumstance or event that could cause harm by violating security. A threat often exploits vulnerability. A safeguard is any technique or procedure or any other measure that reduces vulnerability. A safeguard makes threats weaker or less risky. Safeguards are also called counter measures and their management is called controls.

CONCLUSION

Networking technology and applications are advancing rapidly and network security is struggling to catch up. Networking is the source of many computer security threats and it magnifiers others. Secure computing depends on the secure network and vice versa. With networking technology increasingly under attack, it’s no wonder that people are starting to take network security more seriously. In this article, we have shown some issues in network security as well as a general idea of a new framework of the vulnerability, threat and safeguard. In future work, we aim to implement this framework in the real network with different scenarios.

REFERENCES

[1] M. Abdelhaq, R. Alsaqour, M. Al-Hubaishi, T. Alahdal and M. Uddin. 2014. The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing. International Journal of Network Security. 16: 399-404.

[2] M. Uddin, A. A. Rehman, N. Uddin, J. Memon, R. Alsaqour and S. Kazi. 2013. Signature-based Multi- Layer Distributed Intrusion Detection System using Mobile Agents. International Journal of Network Security. 15: 79-87.

[3] C. Hunt. 2010. TCP/IP network administration: O'reilly.

[4] M. Uddin, R. Alsaqour and M. Abdelhaq. 2013. Intrusion Detection System to Detect DDoS Attack in Gnutella Hybrid P2P Network. Indian Journal of Science and Technology. 6: 71-83.

[5] G. Fox. 2001. Peer-to-peer networks. Computing in Science and Engineering. 3: 75-77.

[6] Z.-L. Zhang, Y. Wang, D. H. Du and D. Shu. 2000. Video staging: a proxy-server-based approach to end- to-end video delivery over wide-area networks. IEEE/ACM Transactions on Networking (TON). 8: 429-442.

International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099

VOL 1 ISSUE 4 (2017) PAGES 16 - 20

Received: 20/05/2017. Published: 27/06/2017

[7] C. Mahalakshmi and M. Ramaswamy. 2012. Data transfer strategy for multiple destination nodes in virtual private networks. Journal of Engineering & Applied Sciences. 7: 1372-1378.

[8] J.-Y. Le Boudec. 1992. The asynchronous transfer mode: a tutorial. Computer Networks and ISDN systems. 24: 279-309.

[9] J. G. Andrews, A. Ghosh and R. Muhamed. 2007. Fundamentals of WiMAX: understanding broadband wireless networking: Pearson Education.