IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207106 |

A Role of Modern Network Security

Tushar Narayan Patil, Sumit Shivaji Patil, Dr. Mrs. Sampada Gulavani

Department of Master of Computer Application, Bharati Vidyapeeth (Deemed to be University), Institute of Management, Kolhapur, Pune, India

ABSTRACT : Now a days security measures works more importantly towards fulfilling the cutting edge demands of today's growing industries. The need is also induced in to the areas like defense, where secure and authenticated access of resources are the key issues related to information security. Secure Network has now become a need of any organization. The security threats are increasing day by day and making high speed wired/wireless network and internet services, insecure and unreliable. There are need of different requirements to handle Wi-Fi threats and network hacking attempts. In this paper the important measures and parameters regarding large industry/organizational requirements for establishing a secure network.

KEYWORDS: Cryptography; Security Attacks; Gateways; Security Measures; WAN; Security Factors; Security Tools; Firewalls.

I. INTRODUCTION

Network security includes provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access. Network security can be defined as protection of networks and the services from unauthorized alteration, destruction, or disclosure, and provision of assurance that the network performs in critical situations and have no harmful effects for neither user nor for employee . Network security is a level of guarantee that all the machines in a network are working optimally and the users of these machines only possess the rights that were granted to them. preventing unauthorized people from acting on the system maliciously . preventing users from performing involuntary operations that are capable of harming the system .securing data by anticipating failures and guaranteeing that services are not interrupted .

II. SECURITY ATTACKS

Security attacks can be classified under the following categories:

i)Active Attacks : This type of attack requires the attacker to send data to one or both of the parties, or block the data stream in one or both directions. The attributes of active attacks are as follows,

- Modification: attacks integrity.
- Interruption: attacks availability such as denial-of-service attacks.
- Fabrication: attacks authenticity.

ii)Passive Attacks : This type of attack includes attempts to break the system by using observed data. One of the example of the passive attack is plain text attacks, where both plain text and cipher text are already known to the attacker.

The attributes of passive attacks are as follows:

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207106 |

- Traffic Analysis: Attacks confidentiality, or anonymity. It can include trace back on a network, CRT radiation.
- Interception: Attacks confidentiality such as eavesdropping, “man-in-the-middle” attacks.

III. NETWORK SECURITY MEASURES

Following measures are to be taken to secure the network :
- Employees should be cautious about physical security.
- Implementation of physical security measures like closed circuit television for entry areas and restricted zones.
- Prepare a network analyser or network monitor and use it when needed.
- When using a wireless connection, use a robust password.
- A strong firewall and proxy to be used to keep unwanted people out.
- For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
- A strong Antivirus software package and Internet Security Software package should be installed.

IV. NETWORK SECURITY TOOLS

Following tools are used to secure the network :
- Kismet – It is a powerful wireless sniffer.
- Snort- It is light-weight network intrusion detection and prevention system excels at traffic analysis and packet logging on IP networks.
- Wire shark or Ethereal -It is an open source network protocol analyzer for UNIX and Windows.
- Nessus -It is the best free network vulnerability scanner available.
- Net Cat -It is a simple utility that reads and writes data across TCP or UDP network connections.

V. BASIC NETWORK SECURITY

When connecting a matching to a network, we need to make sure no one will easily break in to it. Even if you don't think anyone will try to break into your machines - chances are that someone might try. Crackers often run network scan utilities that check a large range of IP addresses, and automatically try to find machines running servers with security holes. To protect against that, one could simply disable any unnecessary network service they are running. The attacks and the network security measures define that how using the network security tools, a better, healthy and safe network can be designed and maintained for an organization/industry.

VI. SECURITY METHODS

There are different types of security methods like cryptography and firewalls.

a. Cryptography : Cryptography relies on ciphers, which is nothing but mathematical functions used for encryption and decryption of a message . The most widely used tool for securing information and services .

b. Firewalls : A firewall is simply a group of components that collectively form a barrier between two networks. There are three basic types of firewalls:
I) Application Gateways : This software runs at the Application Layer of the ISO/OSI reference model. This is the first firewall and is some times also known as proxy gateways as shown in figure 1. These are made up of bastion hosts so they do act as a proxy server. This is the most secure, because it doesn't allow anything to pass by default, but it also need to have the programs written and turned on in order to start the traffic passing.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207106 |

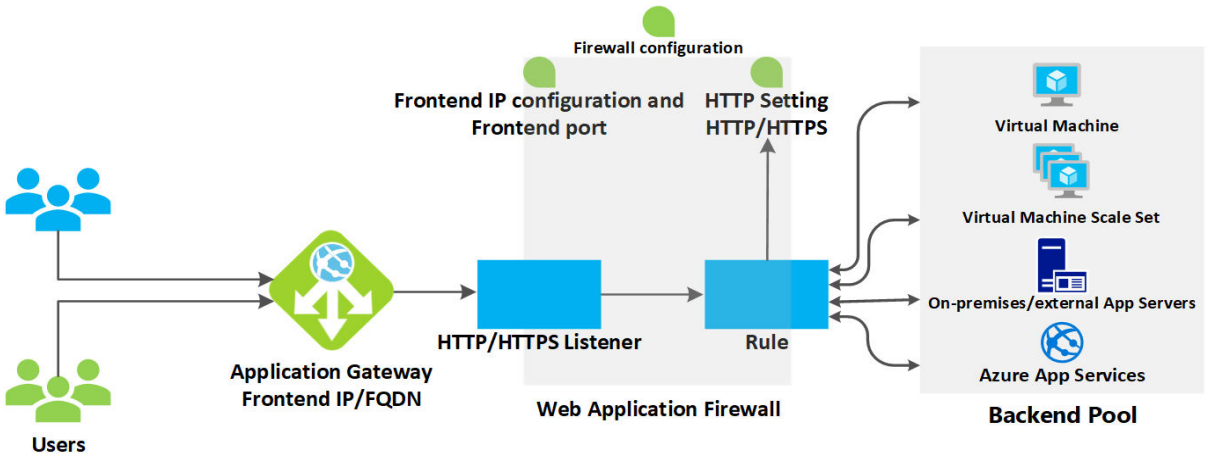

Figure 1: Application gateway

II) Packet Filtering : ACL's is a method to define what sorts of access is allowed for the outside world to have to access internal network, and vice versa. Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on. By default, a router will pass all traffic sent through it, without any restrictions as shown in figure 2. Due to low complexity and the fact that packet filtering is done with routers, which are specialized computers optimized for tasks related to networking. A packet filtering gateway is often much faster than its application layer cousins.

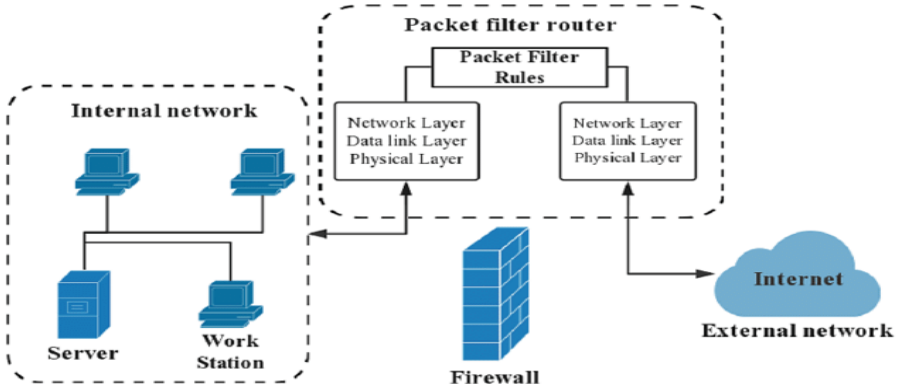

Figure 2: Packet filtering gateway

III) Hybrid Systems : In some of these systems, new connections must be authenticated and approved at the application layer. In an attempt to combine the security feature of the application layer gateways with the flexibility and speed of packet filtering, some developers have created systems that use the principles of both. Once this has been done, the remainder of the connection is passed down to the session layer, where packet filters watch the connection to ensure that only packets that are part of an ongoing (already authenticated and approved) conversation are being passed. The benefits here include providing a measure of protection against your machines that provide services to the Internet (such as a public web server), as well as provide the security of an application layer gateway to the internal network.

VII. SECURITY MANAGEMENT ISSUES

- Organizations sometimes have to deal with a number of point products in the network. Securing all of them totally while ensuring seamless functionality is one of the biggest challenges they face while planning and implementing a security blueprint.
- Adopting technologies that are easy and cost effective to deploy and manage day-to–day network security operations and troubleshoots in the long run.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207106 |

- Building and affirming high-quality resources for deployment and efficient management of network security infrastructure.
- Ensuring a fully secure networking environment without degradation in the performance of business applications.

VIII. NETWORK ATTACKS METHODS

- Eavesdropping – Interception of communications by an unauthorized party
- Data Modification – Data altering, reading from unauthorized party.
- Identity Spoofing (IP Address Spoofing) – IP address to be falsely assumed— identity spoofing and the attacker can modify, reroute, or delete your data.
- Password-Based Attacks – By gaining your access rights to a computer and network resources are determined by who you are, that is, your user name and your password. Denial-of-Service Attack – Prevents normal use of your computer or network by valid users, and it could be used for sending invalid data to application, to flood the computer, block traffic, etc.

IX. TYPES OF SECURITY

There are two types of security like WAN security and Wired equivalent privacy.

i)WAN Security : The organization need to employ something like an Up logic network security system to better automate management of this scattered computers. In organizations where there are satellite offices in various regions the task of securing the network system is even tremendous. Just imagine that one will need to fly to that place if the support if not done remotely. It's really a challenge to work with networks that span various locations.

ii)Wired Eequivalent Pprivacy (WEP) : WEP is an older network security method that is still available to support older devices, but it is no longer recommended. When you enable WEP, you set up a network security key. This key encrypts the information that one computer sends to another computer across your network. However, WEP security is relatively easy to crack.

X.NEED FOR NETWORK SECURITY

In the past, hackers were highly skilled programmers who understood the details of computer communications and how to exploit vulnerabilities. Today almost anyone can become a hacker by downloading tools from the Internet. These complicated attack tools and generally open networks have generated an increased need for network security and dynamic security policies. The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks.

XI. FUTURE WORK

Generally the network security system tools in the past were command line interface (CLI) based. In last few years that more and more computer and network administration task is done remotely through a web-based tool. Malicious code and other attacks are increasing in intensity and the damage that they cause. With little time to react, organizations have to become more proactive in their security stance.

XII. CONCLUSION

The security measures should be designed and provided in the organization. For this a company should know its need of security on the different levels of the organization and then it should be implemented for different levels. Security has become important issue for large computing organizations. There are different definitions and ideas for the security and risk measures from the perspective of different persons. Security policies should be designed first before its implementation in such a way, so that future alteration and adoption can be acceptable and easily manageable. Security policies should not be fixed rather than it should be flexible enough to fulfill the need of an organization . Also it should be capable enough to tackle future security threats while at the same time easily manageable and adoptable.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207106 |

REFERENCES

[1] Marin, G.A. (2005), "Network security basics", In security & Privacy, IEEE, Issue 6, Vol. 3, pp. 68-72, 2005.
[2] Al-Akhras, M.A., "Wireless Network Security Implementation in Universities" In Proc. of Information and Communication Technologies, 2006. ICTTA '06., Vol. 2, pp. 3192 – 3197, 2006.
[3] Farrow, R., Network Security Tools, found at http://sageweb.sage.org/pubs/whitepapers/farrow.pdf
[4] Importance of Network Security, found at
http://www.content4reprint.com/computers/security/importance-of network-security-system.htm
[5] Flauzac, O.; Nolot, F.; Rabat, C.; Steffenel, L.-A., "Grid of Security: A New Approach of the Network Security", In Proc. of Int. Conf. on Network and System Security, 2009. NSS '09, pp. 67-72, 2009.
[6] Brenton, C. and Hunt, C. (2002): Mastering Network Security, Second Edition, Wiley

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details