International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

An Analysis on Network Security Measures and Tools

A.Abdulfaiza[1] ,
Assistant Professor,
Department of Computer Science and Applications ,
Sri Krishna Arts and Science College
abdulfaiza@skasc.ac.in

B.Kiruthika [2], A.Sreemathi [3], K.Shatwikha [4]
[*]Student,
Department of Computer Science and Applications ,
Sri Krishna Arts and Science College,

Kuniamuthur,Coimbatore, Tamil Nadu,India.

Abstract- Security is one of the important component in networking technology. As all the organizations prefer only secured network. The network security is more essential to areas like military, organizations, for confidential projects, etc... Initially, the Internet was designed for connectivity. But now, internet can access any information from anywhere, so the network security is more important now-a-days. Security plays a major role everywhere. There are different types of attacks in the network and the appropriate security is also being provided based on the type of attacks .Many business organizations secure themselves from attacks by using firewall and encryption mechanism. This paper explores important security measures related to different attacks, so a fully secured network can be provided in an organization.

Keywords: Cryptography, Firewall, Hybrid system, Security attacks, WAN Security.

1. INTRODUCTION

Network security is securing the networks and their services from many attacks,destruction and provision of assurance that the network performs in critical situations and have no harmful effects for user and employee[1].It also protects the network and the network accessible resources from unauthorized access. According to network security, it deals mainly about the network is secured or not.Security is not only the main aspect for the network security at each end of the communication chain. Data integrity should be maintained in the communication channel while transmitting the data. An intruder could target the communication channel, obtains, decrypts the data and inserts the false data. So securing the network is as important as securing the computers and the encrypting message must be kept private. The network security attacks, measures, tools and methods are summarized in the following paragraphs.

2. SECURITY ATTACKS

Security attack can be classified into two categories. They are passive attack and active attack. The system must be able to limit the damage occurred & recover rapidly when attack occurs.

Passive attack - When a network intruder intercepts the data travelling through the network, it is called passive attack. The example of passive attack is plain text attacks[2], where both plain text and cipher text are already known to the attacker. The unauthorized attackers listens and monitors the communication channel, it is known as passive attack. Passive attack result in the disclosure of information to an attacker without the knowledge of the user.

Active attack - When a network intruder initiates commands to disrupt the network's normal operation, it is active attack. The unauthorized attackers monitors, listens and modifies the data stream in the communication channel are known as active attack. Active attack result in the disclosure of information or modification of data.

3. NETWORK SECURITY MEASURES AND SECURITY TOOLS

Some of the network security measures that are to be taken to secure the network :

- A powerful antivirus of software collection and web security software collection should be installed[3].
- Examine a network analyzer or network monitor and use it when needed.
- Execution of physical security measures like closed circuit television for entry areas and restricted zone.
- For authentication, use correct password and change it, monthly /bi-monthly basis.
- To restrict the organization perimeter use security barriers.
- To keep unwanted people out, powerful firewall and proxy must be used.
- Use vigorous password, while using a wireless connection.
- Workers should be alert about physical security.

Some of the network security tools are:

- Kisnet - Powerful wireless sniffer.
- N-map security scanner - Free and open source utility for network exploration.
- Netcat - simple utility that reads and writes data across TCP and UDP network connections.
- Nessus - Best free network vulnerability scanner available.
- Snort - Light weight network intrusion detector.
- Wire Shark or Ethereal - Open source network protocol analyzer for UNIX and Windows.
- Back Track - Penetration tester.
- Cain and Abel - Packet sniffer & Password cracker.
- Aircrack - WEP & WPA cracker.

4. SECURITY METHODS

Cryptography and Firewall is the most widely used security methods to secure the network.

A. **Cryptography**

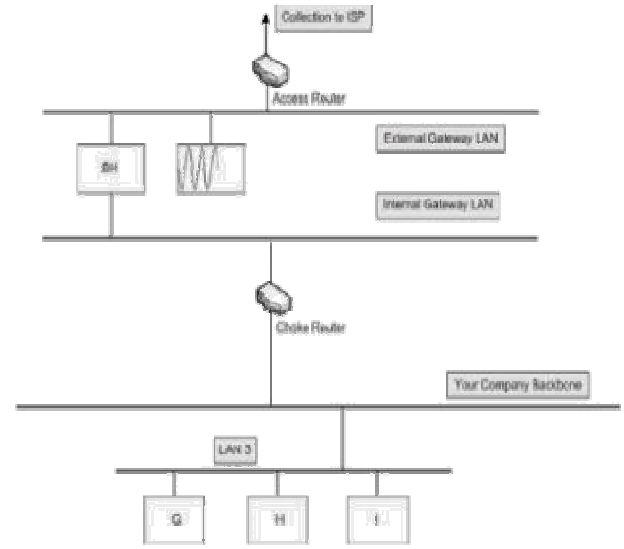
- This tool is used for securing information and service and it is the most widely used tool[4].
- Cryptography involves creating written or generated codes that allow information be kept secret.

B. Firewall

A firewall is defined as a group of components that collectively from a barrier between two networks. Firewall are basically divided into 3 types.

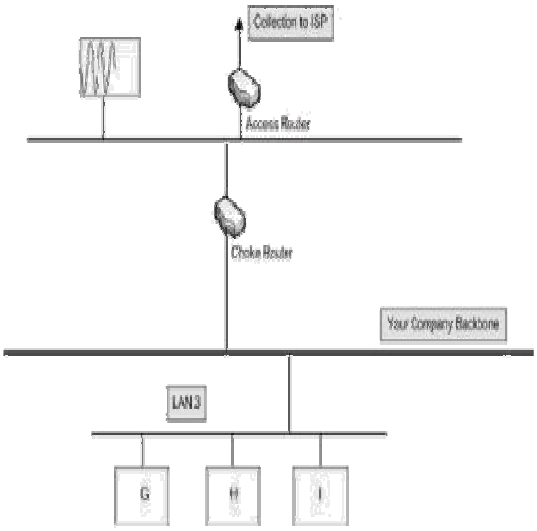
1) **Application Gateway**

Application gateway is the first firewall and it is also said to be proxy gateway. They act as proxy server and it is made up of Bastion hosts. Client behind the firewall must be classify and prioritized.It runs on a firewall system between two networks and it is an application program .It is most secure because it doesn't allow anything to pass by default.



2) **Packet Filtering**

Packet filtering is a firewall techniques used to control network access by monitoring outgoing and incoming packets. This technique have router ACLs (access control lists) turned on. ACL is a method to define what sort of access is allowed for outside world to have to access internet network and vice versa. The feature of access control is performed at a lower layer because their complex is less than application gateway. Due to lower complexity the packet filtering is done by routers which are specialized computer that are related to networking .It works on the network layer and transport layer of OSI reference or TCP and IP layer. It doesn't remember the state and hence it is called stateless firewall. A packet can differentiate the internet and internet network. Also it can be verified which network are packed came from certainly.



3) Hybrid System

Hybrid system combine elements of other types of firewall. The flexibility and speed of packet filtering is an attempt to combine the security features of the application. Some developer's have created system by using the principle of both application layer and packet filtering. In that new connection must be created and approved by a application layer .Once this process done, the remaining work of the connection is passed through the session layer. After that packet filter, watch the connection for ensure that only packet conversation has been passed.

The packet filtering and application layer proxies are used in other possible ways. It will provide a measure of protection that against to service of internet they also provide the security for application layer gateway to a web network.

5. ISSUES ON SECURITY MANAGEMENT

- Now-a-days ensuring the security strength of the organization is a big challenge. According to organization have some predefined security policies and procedures but they are not implementing. Through the use of technology we should improve these terms on people and process.
- Construct and declare high quality resources for deployment and efficient management of network security infrastructure.
- Adopting technologies are very easy and cost is effective to deploy and it will manage day to day network security operation.
- The performance of business application that are ensuring a fully secure networking environment without degradation.
- On a day to day program, business face the challenge to expand their infrastructure and increase their user group for both inside and outside of their organization. At the same time they also have to confirm the performance.
- The biggest challenge for organization have to deal with a number of product in the network. Securing all of them totally while ensuring seamless functionality they face while planning and implementing a securing blueprint.
- The implementation and conceptualization of network security is a difficult challenge. Security is mering of people, processes and technology.
- Network security is essential for all top level function also initiative and understanding purpose. Being updated is important to fragmented market is also challenge for all IT managers.

6. MWTHODS OF TECHNOLOGY

An end-to-end solution is given by leading security vendors to take care of the network security. Those solutions are the combination of hardware and software platforms. That also includes security management solution that takes care of entire security network which performs multiple functions. An integrated solution solves both the point security problem and application layer security problems.

SSL-VPN:

Secure Socket Layer is the full form of SSL. It is used to secure the data or

information or applications while transferring. VPN stands for Virtual Private Network.It is a secured network. Both SSL & VPN are safe to use for transferring data.

ASIC based appliances:

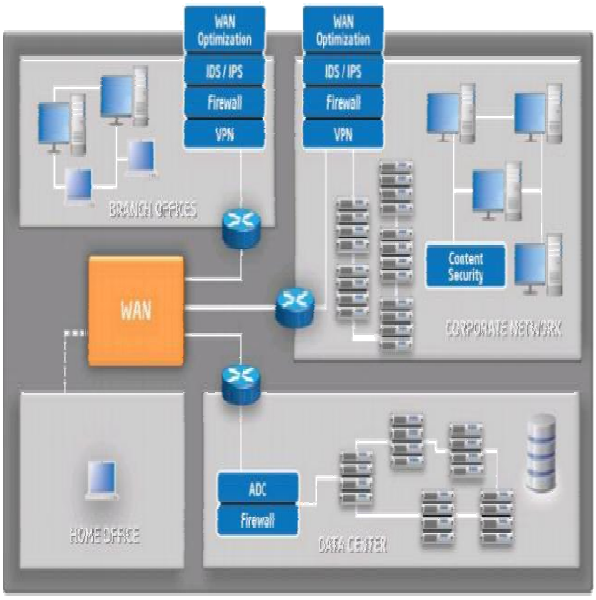
ASIC stands for Application Integrated Circuit . The standard partsofASIC are designed using microelectronics system. A silicon chip is also used for designing. It runs on open platform and it provides software based security products.

IPS & IDS:

IPS stands for Intrusion Prevention System and IDS stands for Intrusion Detection System.IPS and IDS combines to provide a tool which changes the network access control points configuration.A lot of interest from the community was received by Intrusion Prevention System.

7. WAN SECURITY

- WAN stands for Wide Area Network.
- Wide Area Network occupies a wide area that containsmultiple small networks such as LAN (Local AreaNetwork) & MAN (Metropolitan Area Network).
- Through public networks such as telephone system, computers are connected to WAN.
- Leased lines and satellites are also used to connect the computers to WAN.



8. FUTURE WORK

- The damage and intensity of attacks are more now-a-days. So the organizations must be with full security.
- Organizations must know about the future risks, threats and secure their information.
- Using CLI, the network system security tools were designed in the past.
- CLI is Command Line Interface and they were used for designing.
- In Last few years, web based tools were used for designing the tools and network tasks.
- In today's heavily inter-connected era, the network tools are more important.
- The network system security tools may be GUI or CUI based.

9. CONCLUSION

Security has become an main issue for all organizations. There are different terms and ideas for the network security & risk measures from different perspectives. The security method should be created and provided by the organization. First the company wants to know the need of security and it should be implemented. Security process should be designed before it's implementation. So the future ideas and adaptation can be approved and easily maintainable. The security system must be flexible and user friendly.

REFERENCES

[1] ImportanceofNetworkSecurity,foundathttp://www.content4reprint.com/computers/security-system.htm
[2] IntroductiontoNetworksecurity,foundathttp://www.cs.cornell.edu/Courses/cs519/2003sp/slides/15_securitybasics.pdf.
[3] FarrowR.,NetworkSecurityTools,foundathttp://sageweb.sage.org/pubs/whitepapers/farrow.pdf
[4] Stallings,W.(2006):Cryptographyand NetworkSecurity,FourthEdition,Prentice Hall.
[5] Abeginnersguidetonetworksecurity,foundathttp://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf.
[6] K.E.Hemapriya,K.Gomathy,"A survey paper of cluster based key management techniques for

secured data transmission in Manet", International Journal of Advanced Research in Computer and communication Engineering, (IJARCCE) vol 5, issue 10,october 2016.