ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 7, September 2012

Survey on Network Security, Threats & Firewalls

Mr. Sachin Taluja[1], Prof. Rajeshwar Lal Dua[2]

[1]M.Tech Scholar, Department of Electronics & Communication Engineering, Jaipur National University, Jaipur

[2]HOD, Electronics & Communication Engineering, Jaipur National University, Jaipur.

ABSTRACT-
Network security is an important task that must be seriously considered when designing a network. It defined as the policies and procedures followed by a network administrator to protect the network devices from threats and simultaneously, the unauthorized users must be prevented from accessing the network. As the numbers of attacks are increasing day by day, it is necessary to explore the information regarding new attacks and take appropriate steps to safeguard the network from malicious attacks .This could be done with the help of firewalls that secure the network from the malicious attacks. Firewalls are nothing but are network devices that enforce an organizations security policy. Since their development, various methods have been used to implement firewalls. These methods filter network traffic at one or more of the seven layers of the ISO network model, most commonly at the application, transport, network, and data-link levels. Newer methods, which have not yet been widely adopted, include protocol normalization and distributed firewalls. Our main objective is to enhance the security in a network by performing various tasks in the network security process using firewalls. Here we discuss various type of network threats in network security approaches and their solution by the use of different firewalls phenomena.

Keywords- Network Security, Network Threats, firewalls, Traffic.

I. INTRODUCTION

Network Security is important in any environment. As large information is available on the network and it is possible to share this data through it, it should be secure. People and organizations have been protecting their data from harmful activities using different rules that identify and block such things. However current and future threats require development of more adaptive defensive tool. Attack is an assault on system security that derives from an intelligent threat. It can be mainly classified as Active attacks and Passive attacks. Active attacks are in the nature of eavesdropping on, or monitoring of, transmissions while passive attacks involves some modification of the data stream or creation of false stream.To avoid these types of attacks, we need to improve the network safety-defense mechanism of Firewalls. In a network security policy, the main points to be considered are firewall .Network firewall is a system which limits network access to and from a network. It is usually positioned between a trusted, protected private network and an untrusted, public network. Firewall allows only approved traffic in and out according to a thought-out plan (firewall policy). In its work firewall minimizes security threats which range from curious prowlers to well-organized, technically knowledgeable intruders that could gain access to private information or interfere with user’s legitimate use of system.[1-3]

II. NETWORK SECURITY

Network security covers a variety of computer networks, both 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. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done.

In modern computer networks, following important security features should be included:

(a) User and data authentication

In accessing a network, a user provides user name and password to proof acceptance to use the network. This is known as authentication

(b) Data integrity

When data is in transit through the network, the data should be void of any manipulation by intruders or hackers that may tamper the original nature of the information. Data integrity can be performed by hashing the data sent using MD5 (message digest 5) or SHA-1 or SHA- 2 (secure hash) algorithm. When a hash message arrive its destination, a hash of the data is computed and checked against hash sent by the source computer. If the two hashes match, data integrity has been maintained if not data is rejected for reason of modification in transit. With hashing enforce on data, it is difficult to modify data in transit without detection. SHA- 2 is the most secured and recommended because it is difficult to attend two messages
that hash to same hash value.

(c) Confidentiality

When data travels across the network, it should be obscured to those who it not intended for. To achieve this, the data is encrypted symmetrically or asymmetrically. Symmetrical encryption uses shared sacred key to encrypt and decrypt data. A long and complex key renders a more secure encryption. 3DES (Data encryption standard) or AES (advanced encryption standard) algorithm could be used for symmetrical encryption. Asymmetrical encryption uses two separate keys, one for encryption and the other for decryption. The public key is used for data encryption and private key for data decryption. Asymmetrical encryption is reserved only for the authentication purpose because it demands a lot of computing power compare to it symmetric counterpart. An example of asymmetric encryption algorithm is RSA (Rivest, Shamir and Adleman).

(d) Availability

The organization network and services should always be available to authorize persons when ever needed. This means 24 hours of a day and 7 days a week; if not, these will cause tremendous lose of human productivity and financial lose to the company. Network availability should be accomplished such that the total down time percentage for the entire year should be less than 1%. Denial of service attack (DOS) could be launch to deny availability to network resources. DOS mitigation techniques should be put in place to thwart attackers .Now morden security systems consist of combined application of security mechanisms on three different ISO/OSI reference model layers:

(1) Application level security (end-to-end security) based on strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens (e.g. smart cards) – internal network attacks protection.
(2) Transport level security based on establishment of a cryptographic tunnel (symmetric cryptography) between network nodes and strong node authentication procedure – external network attacks protection.
(3) Network IP level security providing bulk security mechanisms on network level between network nodes – external network attacks protection.

These layers are projected in a way that vulnerability of one layer could not compromise the other layers and thus the whole system is not vulnerable.[4-6].

III. THREAT TO NETWORK SECURITY

There is various type of network threats discussed below

(a) Adware

It is software that displays advertisements on your computer.Adware, or advertising-supported software, displays advertising banners or pop-ups on your computer when you use the application. Adware can slow down your PC. It can also slow down your internet connection by downloading advertisements.

(b) Backdoor Trojans

A backdoor Trojan allows someone to take control of another user's computer via the internet without their permission. it may pose as legitimate software, just as other Trojan horse programs do, so that users run it. Alternatively as is now increasingly common users may allow Trojans onto their computer by following a link in spam mail.

(c) Bluejacking

Bluejacking is sending anonymous, unwanted messages to other users with Bluetooth-enabled mobile phones or laptops.Bluejacking depends on the ability of Bluetooth phones to detect and contact other Bluetooth devices nearby. The Bluejacker uses a feature originally intended for exchanging contact details or "electronic business cards".

(d) Bluesnarfing

Bluesnarfing is the theft of data from a Bluetooth phone.Like

Bluejacking, Bluesnarfing depends on the ability of Bluetooth-enabled devices to detect and contact others nearby.In theory, a Bluetooth user running the right software on their laptop can discover a nearby phone, connect to it without your confirmation, and download your phonebook,pictures of contacts and calendar.Your mobile phone's serial number can also be downloaded and used to clone the phone.

(e) Boot Sector Viruses

Boot sector viruses spread by modifying the program that enables your computer to start up.When you switch on a computer, the hardware looks for the boot sector program which is usually on the hard disk, but can be on a floppy disk or CD and runs it. This program then loads the rest of the operating system into memory.A boot sector virus replaces the original boot sector with its own, modified version (and usually hides the original somewhere else on the hard disk).

(f) Browser Hijackers

Browser hijackers change the default home and search pages in your internet browser.Some websites run a script that changes the settings in your browser without your permission. This hijacker can add shortcuts to your "Favorites" folder or, more seriously,can change the page that is first displayed when you open the browser.You may find that you cannot change your browser's start page back to your chosen site.

(g) Chain Letters

An electronic chain letter is an email that urges you to forward copies to other people. Chain letters, like virus hoaxes, depend on you, rather than on computer code, to propagate themselves. The main types are
Hoaxes about terrorist attacks, premium-rate phone line scams, thefts from ATMs and so forth. False claims that companies are offering free flights, free mobile phones, or cash rewards if you forward email. ¦Messages, which purport to be from agencies like the CIA and FBI, warning about dangerous criminals in your area.

(h) Cookies

Cookies are files on your computer that enable websites to remember your details.When you visit a website, it can place a file called a cookie on your computer. This enables the website to remember your details and track your visits. Cookies are small text files and cannot harm your data. However, they can compromise your confidentiality. Cookies can be stored on your computer without your knowledge or consent, and they contain information about you in a form you can't access easily.

(i) Denial of Service attack (DoS)

Denial-of-service (DoS) attack prevents users from accessing a computer or website.In a DoS attack, a hacker attempts to overload or shut down a computer, so that legitimate users can no longer access it. Typical DoS attacks target web servers and aim to make websites unavailable. The most common type of DoS attack involves sending more traffic to a computer than it can handle.

(j) Document Viruses

Document or "macro" viruses take advantage of macros – commands that are embedded in files and run automatically.Many applications, such as word processing and spreadsheet programs, use macros.A macro virus is a macro program that can copy itself and spread from one file to another. If you open a file that contains a macro virus, the virus copies itself into theapplication's startup files. The computer is now infected

(k) Email Viruses

Many of the most prolific viruses distribute themselves automatically by email.Typically, email-aware viruses depend on the user double-clicking on an attachment.This runs the malicious code, which will then mail itself to other people from that computer. The etsky virus, for example, searches the computer for files that may contain email addresses, and then uses the email client on your computer to send itself to those addresses.

(l) Internet Worms

Worms are programs that create copies of themselves and spread via internet connections. Worms differ from computer viruses because they can propagate themselves, rather than using a carrier program or file. They simply create exact copies of themselves and use communication between computers to spread. A worm can have malicious effects. For example, it may use affected computers to deluge websites with requests or data, causing them to crash (a "denial-of-service" attack). Alternatively, it can encrypt a user's files and make them unusable. In either case, companies can be blackmailed.

(m) Mousetrapping

Mousetrapping prevents you from leaving a website.If you are redirected to a bogus website, you may find that you cannot quit with the back or close buttons. In some cases, entering a new web address does not enable you to escape either. The site that mousetraps you will either not allow you to visit another address, or will open another browser window displaying the same site. Some mousetraps let you quit after a number of attempts, but others do not.

(n) Obfuscated spam

Obfuscated spam is email that has been disguised in an attempt to fool anti-spam software.Spammers are constantly trying to find ways to modify or conceal their messages so that your anti-spam software can't read them, but you can.

(o) Page-jacking

Page-jacking is the use of replicas of reputable web pages to catch users and redirect them to other websites. Scammers copy pages from an established website and put them on a new site that appears to be legitimate. They register this new site with major search engines, so that users doing a search find and follow links to it. When the user arrives at the website,they are automatically redirected to a different site that displays advertising or offers of different services. They may also find that they cannot escape from the site without restarting their computer (just like mousetrapping).

(p) Parasitic viruses

Parasitic viruses, also known as file viruses, spread by attaching themselves to programs.When you start a program infected with a parasitic virus, the virus code is run. To hide itself, the virus then passes control back to the original program.The operating system on your computer sees the virus as part of the program you were trying to run and gives it the same rights. These rights allow the virus to copy itself,install itself in memory or make changes on your computer.

(q) Pharming

Pharming redirects you from a legitimate website to a bogus copy, allowing criminals to steal the information you enter.Pharming exploits the way that website addresses are composed.

(r) Phishing

Phishing is the use of bogus emails and websites to trick you into supplying confidential or personal information.Typically, you receive an email that appears to come from a reputable organization,such as a bank. The email includes what appears to be a link to the organization's website. However, if you follow the link, you are connected to a replica of the website.Any details you enter, such as account numbers, PINs or passwords, can be stolen and used by the hackers who created the bogus site. These are fews among the Network Threats [7].

IV. FIREWALL

Firewalls are essential aspects of all networks. However they are complex and if not correctly configured and managed may result in security breaches.These Firewalls are the first front line defense mechanism against network attacks.In any network environment network Security is an essential aspect of network configuration and management. However, a network will typically consist of many different user applications all of which represent potential security breaches. Furthermore there are numerous protocols such as Packet assembler/disassembler (PAD), Internet Control Message Protocol (ICMP) and Simple Network Management Protocol (SNMP) that are enabled by default and must be explicitly disabled. Whilst other protocols such as HTTP and HTTPs must be allowed but restricted using access control lists. It is essential therefore to disable a potentially wide range of services and devices interfaces that are not being used but selectively restrict other protocols with an appropriate firewall configuration. After identifying potential security breaches a router must be configured by means of a firewall [8].

Firewall is one of the most widely used solutions for the Internet world. All traffic inside to outside and vice versa, must pass through the firewall. Different types of firewalls have different types of rules and security policies. The authorized traffic will be sent based only on local policies. The firewall itself is protected, i.e.; it uses a trusted hardware and operating system. Generally, firewalls are of three types.

(a) Circuit level firewalls
(b) Application level firewalls
(c) Packet filtering firewalls

(a) Circuit Level firewalls

For certain applications the circuit level gateway can be either a stand-alone system or a specialized function performed by an application level gateway. End-to-End TCP connections in a circuit level gateway are not permitted but instead of that, the gateway creates two TCP connections, one between the gateway and the TCP user on an inner host and the other between the gateway and the TCP user on the outside host. When the TCP connection is established the gateway exchanges the TCP segments without examining the content. The security functions only determine which connections are to be allowed [18]. The behaviour of the Circuit level firewall for establishing the connection between the inner and outer host is shown in the Figure 1.

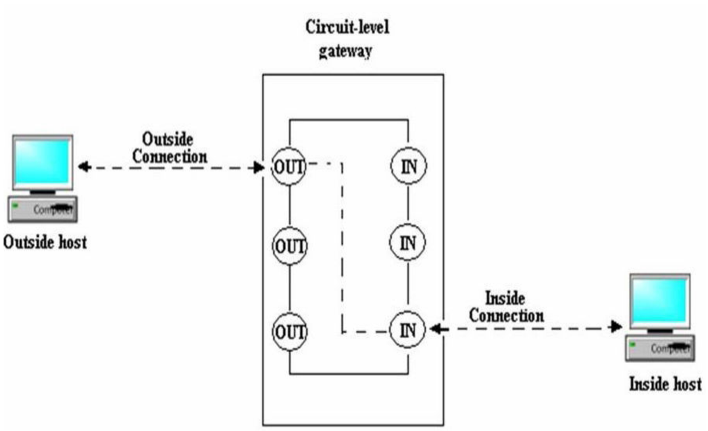

Figure 1: Circuit level gateway

(b) Application level firewalls

An Application level gateway which is also called a proxy server, acts as a relay of application-level traffic. A user can contact the gateway by using a TCP/IP application and then the gateway asks about the remote host which is to be accessed. Then in response the user must give a valid user ID and authentication details, then the gateway contacts the application on the remote host and exchange the TCP segments application data between the two end points. However, to perform these things the gateway must implement the proxy code. We can configure the gateway to support only the particular features of an application.The behaviour of Application level firewall in connecting the two ends is shown in Figure 2.

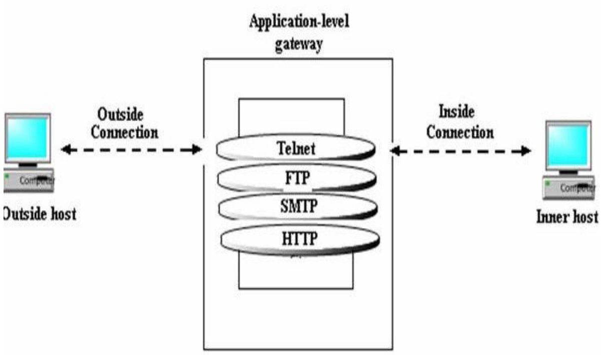

Figure 2: Application level gateway

(c) Packet filtering firewalls

The packet filtering is done based on the set of rules configured on a packet filter router. The packet is forwarded or discarded based on the configurations done. There are two default policies involved in forwarding or discarding the packet, they are

- **Default:** Discard (Which doesn't match the set of rules)
- **Default:** Forward (Which matches with at least any one of the rules)

If a packet matches with at least any one of the rules, then one of the default actions takes place i.e., it is forwarded, and if it doesn't match with any of the set of rules, then the other default action takes place i.e., discards the packet. The block diagram of a Packet filtering router is shown in Figure 3.

The packet filtering is done based on information in the network packet.

- **Source IP address:** The IP address from where the packet is originated.
- **Destination IP address:** The IP address to which it wishes to send.
- **Transport-level address of source and destination:** The applications like SNMP or telnet which are defined by the transport level port (TCP or UDP)
- **IP protocol field:** Transport protocol is defined.
- **Interface:** From which interface of a router the packet is originated and to which interface of a router the packet is destined to be sent [2][9].

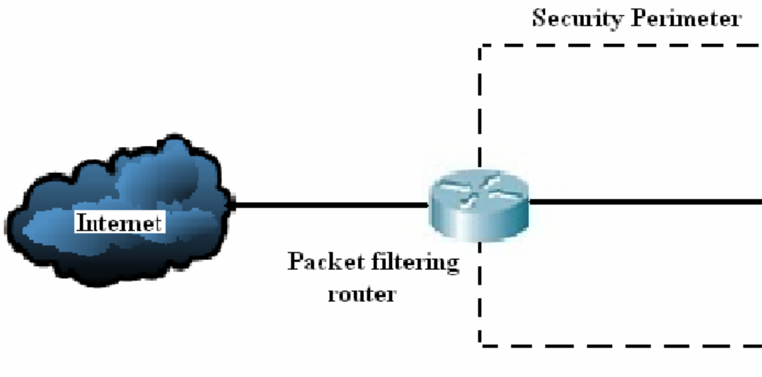

Figure 3: Packet filtering firewall

V. CONCLUSION

In this paper, different mechanism in the modern computer network security concept,threats to the network and their solution by using of firewall are surveyed.. It is concluded that only network security architecture by using firewalls are protect internal and external attacks in modern computer networks. Also, the most frequently used security mechanisms on the application, transport and network layers are analyzed to conclude that more than one layer should be covered by the appropriate security mechanisms in order to achieve high quality protection of the system beside of various type of network threats are used by hackers . The survey is done regarding analysis of network security concept, various challenges in form of network threats used by hackers and appropriate security mechanisms with potential vulnerabilities by means of using different type of firewalls. Hence we can say that appropriate security mechanism by using firewalls can be applied in such a way that defense capability of network against network threats, can enhanced, so that network is more secure against network threats.

References

[1] Ashvini Vyavhare, Varsharani Bhosale, Mrunal Sawant, Fazila Girkar, “Co-operative Wireless Intrusion Detection System Using MIBs From SNMP” in International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012 DOI : 10.5121/ijnsa.2012.4211 147

[2]Technical report, IDE1202, February 2012 , “Enhancing Network Security in Linux Environment” Master Thesis in Computer Network Engineering by Ali Mohammed, Sachin Sama and Majeed Mohammed at School of Information Science, Computer and Electrical Engineering Halmstad University Box 823, S-301 18 Halmstad, Sweden February 2012[2][9]

[3] Tihomir Katić,Predrag Pale “Optimization of Firewall Rules” Faculty of Electrical Engineering and Computing University of Zagreb Unska 3, HR – 10000 Zagreb, Croatia

[4]Network security From Wikipedia, the free encyclopedia

[5] Mbah Gipson Mbah thesis “Network Security- Securing Network Equipment And Network Users’ Environment” SAVONIA UNIVERSITY OF APPLIED SCIENCES Final project 23 August 2010.

[6] Rajeshwari Goudar, Pournima More, “Multilayer Security Mechanism in Computer Networks,” in Computer Engineering and Intelligent Systems www.iiste.org ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online) Vol 3, No.2, 2012.

[7]http://www.whatsthelatest.net/news/types-computer-security-threats-cybercrime/ About Portfolio Links Contact Search HomeNews Computer Software Internet MobileHealth Funny How To Home ? News ? 21 Types of Computer Security Threats 21 Types of Computer Security Threats February 21, 2010

[8] S P Maj, W Makasiranondh, D Veal, “An Evaluation of Firewall Configuration Methods” in IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.8, August 2010 ,Manuscript received August 5, 2010,Manuscript revised August 20, 2010.

Authors

Sachin Taluja-
M.Tech Scholar atJaipur National University, Jaipur. He received B.E. from M.D.University Rohtak, Haryana in Electronics and Communication. He has over 5 years of Industrial experience in the Field of Computers. His Area of interest includes Network Security, Artificial intelligence, Communication system, Computer architecture, Wireless Communications, Digital Communications, fiber optics, Nano Technology. He has attended various workshops on different domains of computers.

Prof. Rajeshwar Lal Dua-
A Fellow Life Member of IETE and also a Life member of I.V.S & I.P.A, former “Scientist F” of the Central Electronics Engineering Research Institute (CEERI), Pilani has been one of the most well-known scientists in India in the field of Vacuum Electronic Devices for over three and half decades. His professional achievements span a wide area of vacuum microwave devices ranging from crossed-field and linear-beam devices to present-day gyrotrons. He was awarded a degree of M.Sc (Physics) and M.Sc Tech (Electronics)from BITS Pilani. He started his professional carrier in1966 at Central Electronics Engineering Research Institute (CEERI), Pilani. During this period he designed and developed a specific high power Magnetron for defence and batch produced about 100 tubes for their use. Trained the Engineers of Industries with know how transfer for further production of the same. In 1979 he visited department of Electrical and Electronics Engineering at the University of Sheffield (UK) in the capacity of independent research worker, and Engineering Department of Cambridge University Cambridge (UK) as a visiting scientist. After having an experience of about 38 years in area of research and development in Microwave field with several papers and a patent to his credit. In 2003 retired as scientist from CEERI, PILANI & shifted to Jaipur and joined the profession of teaching. From last eight years he is working as professor and head of electronics department in various engineering colleges. At present he is working as head and Professor in the department of Electronics and communication engineering at JNU, Jaipur. He has guided several thesis of M.tech .of many Universities.