ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Network Security Attacks Solution and Analysis

Umesh B. Shingote[#1], Vaibhav P. Sawalkar[*2]

Assistant Professor, Department of Computer Science and Engineering, Mauli College of Engineering and Technology, Shegaon, Maharashtra.

Abstract— Network security is that the composition of the vital policies and managed criteria adopted by an individual for the interference of unauthorized access, modification network-accessible resources network security plays a vital role in single laptop users, numerous organizations, and business networks. With the increasing use of the web, issue of laptop security became vital half and concern. By modifying the design of designing of the web, presumably reduces the attacks across the network. The study of those attack strategies permits for the acceptable security technique to specialize in the analysis. Several organizations create additional secured from the web by coding and firewall security strategies. An "intranet" to stay connected to the web however secured from potential threats. The complete field of network security is huge and in an organic process stage. So as to know the analysis being performed these days, background of the web, its vulnerabilities, attack strategies through the web, and security technology is vital and so they're reviewed.

Keywords— Networks, Attacking methods, Network security, confidentiality, integrity.

I. INTRODUCTION

Network security permits the authentication of access to information in any type of network monitor by a selected person. Users are offer with id and word or alternative authenticating information that enables them access to info and programs among their authority. Network security is changing into of nice importance due to material possession which will be simply no heritable through the web. There are presently 2 basically different networks, information networks and synchronous network comprised of switches. The web is taken into account as a knowledge network. Since the present information network consists of computers connected routers, information is often obtained by special programs, like Trojan horses planted within the routers. The synchronous network that consists of switches doesn't buffer information and thus don't seem to be vulnerable by attackers. That's security is emphasized in information networks, like the web and alternative networks that link to the web [1, 2].

II. VARIOUS ATTACKING METHODS

Based on Confidentiality and Integrity the attacking methods are divides as follows:

A. Eavesdropping

When any unauthorized party tries to pay attention to the communication, it's referred to as eavesdropping. The contraband ability of associate listener to watch the network is usually the largest security drawback that administrator face in associate enterprise. While some secret writing services that used with supported cryptography, knowledge is browse and changed by others because it traverses the network. Passive eavesdropping is once associate trespasser solely on the network listens to the networked messages. Active eavesdropping is once the trespasser listens the networked messages and modifies the first message by inserting one thing into the communication stream. This kind of activity distorts original message. This could cause the messages being distorted. Trespasser also can copy some sensitive information like passwords [3].

B. Viruses

Viruses uses computer code programs which might self-replicate on different computers, laptops via computer networks. Virus programs are hooked up with alternative program files. Once a file is opened, the virus can activate among the system and might have an effect on alternative programs of the pc. Virus sorts may be file viruses, boot sector viruses, macro viruses or script viruses consistent with the tactic they use to infect pc [3].

ISSN: 2321-9653

C. Worms

A worm is additionally computer code programs which might self-replicate on pcs via computer networks. A worm is analogous to a pandemic as a result of their use 2 main sorts of worms, mass-mailing worms and network aware worms. Mass mailing worms use email as a method to infect alternative computers. A network-aware worm selects a target and once the worm accesses the target host, it will infect it by suggests that of a Trojan or otherwise. The most distinction between virus and worm is that worm ought not to be hooked up with alternative program files however it spreads usually via net [4]

D. Trojans

Trojan horse may be a malicious or harmful code that is contained within apparently harmless Programming or information so that it gets total management of your pc and might do something along with your pc. It will take away all information from your disc or it will run memory allocation table etc [4].

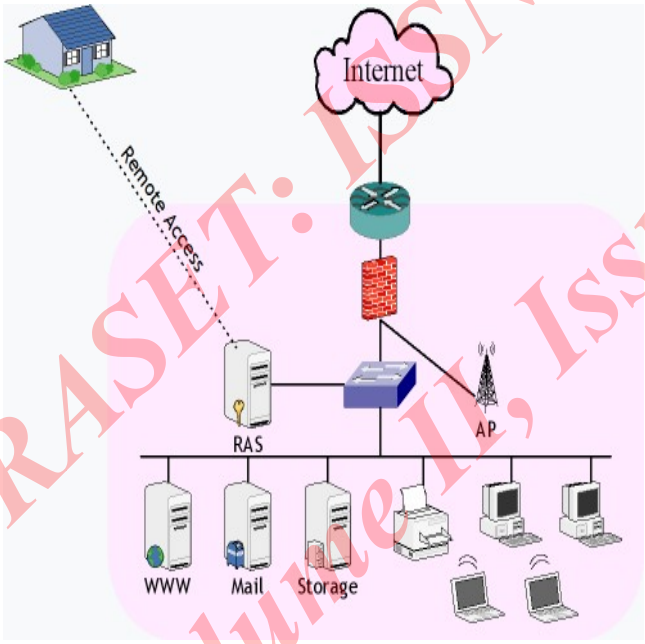

Fig1.Network Security System [13]

E. Spyware

Spyware may be a style of malware that's put in on a computer while not the information of the user so as to gather the user's non-public data. Spyware is usually hidden from the user so as to collect data concerning net interaction, keystrokes, passwords, and alternative valuable information. Spyware may also negatively have an effect on a computer's performance by putting in further computer code, redirecting browser searches, dynamic pc settings, reducing association speeds, dynamic the homepage or maybe utterly disrupting network association ability. Spyware may also be used as a sort of adware, wherever the computer code delivers uninvited pop-up ads additionally to following user behaviour. Typically, spyware is put in once a user installs a piece of free computer code that they really wished [5].

F.Phishing

Phishing is an effort to get important data or information from a personal, group, or organization. Phishing may be a technical term used for hacking personal information and this usually within the variety of e-mail messages. Phishers might tries to collect personal information, like master card numbers, on-line banking credentials, and alternative sensitive data [5].

G. Spoofing Attacks

Spoofing suggests that to do to collect the address of the pc so as to realize access to alternative computers so information and alternative secret data may be taken from those computers [5].

H. Denial of Service

Denial of service is associate attack once the system receiving too several requests cannot come communication with the requestors. The system then consumes resources anticipating the acknowledgment to complete. Eventually, the system cannot answer from now on requests rendering it while not service [5]

I. Identity Spoofing or IP Spoofing

In computer networking, the term IP address spoofing or IP spoofing refers to the creation of network protocol packets with an IP address, referred to as spoofing, with the aim of

concealing the identity of the sender or impersonating another computer system [3].

J. Packet Sniffing

It is a program which will record all network packets that travel past a given network interface, on a given pc, on a network likewise on extract sensitive data from packets [3]. Table 1. Attack Method and Security Technology [5]

Computer Security Attributes	Attack Methods	Technology For Internet Security
Confidentiality	Eavesdropping Hacking, Phishing, DOS, IP Spoofing	IDS, Firewall, Cryptographic Systems, IP Sec, SSL
Integrity	Viruses, Worm Trojans, Eaves Dropping,DOS, Ip Spoofing	IDS, Firewall, IP Sec And SSL, Anti-Malware Software
Privacy	Email Bombing, Spamming, Hacking,DOS And Cookies	IDS,Firewall, IP Sec And SSL, Anti-Malware Software
Availability	DOS,Email Bombing,Spamming,System Boot Record Infectors	IDS,Firewall, Anti-Malware Software

III.EFFECTIVE SOLUTIONS FOR NETWORK SECURITY

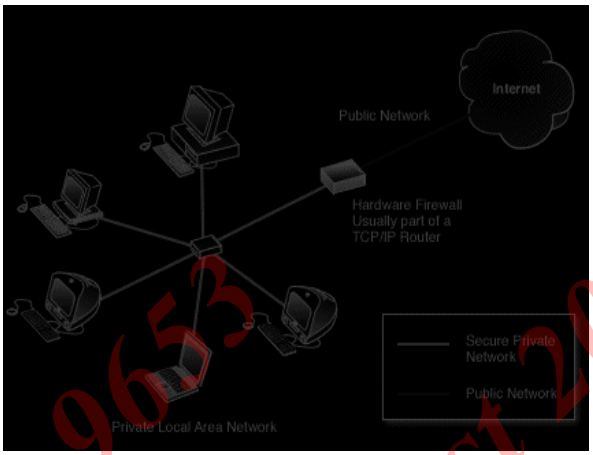

Fig 2. Computer with Hardware Firewall [12].

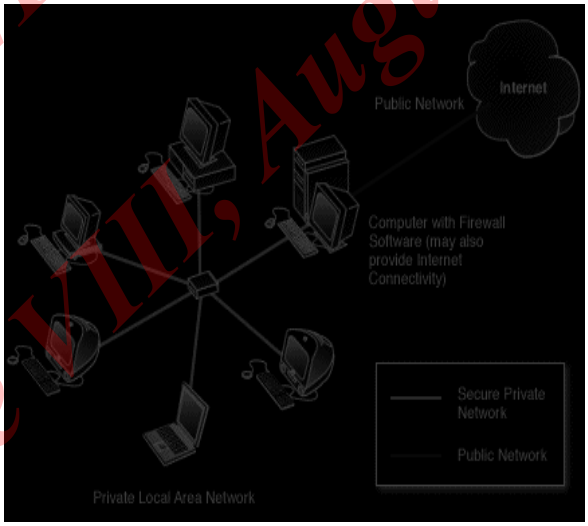

Fig 3.Computer with Software Firewall [12].

Network security can be done through hardware and software system. The software system should be perpetually updated and managed to guard you from rising threats. Web threats can still be a serious issue within the international world as long as data is accessible and transferred across the web. Completely different solutions and detection mechanisms were developed to affect these attacks.

A. Cryptography

ISSN: 2321-9653

Cryptography will be outlined because the conversion of information into a disorganized code that may be deciphered and sent across a public or non-public network. Cryptography could be a helpful and wide used tool in security engineering now a days. It concerned the utilization of codes and ciphers to misuse data into unintelligible information [9].

B. Firewall

A firewall could be a typical border management mechanism. The aim of a firewall is to dam traffic from the surface, however it might even be wont to block traffic from the within. All traffic from within to outside and contrariwise should suffer the firewall. This is often achieved by physically interference all access to the native network except via the firewall. Solely licensed traffic, as outlined by the native security policy, is going to be allowed to pass. Numerous varieties of firewalls area unit used, that implement numerous varieties of security policies a firewall is that the line psychoanalytic process against intruders. It's a system designed to forestall unauthorized access to or from a personal network. Firewalls will be enforced in each hardware and software system or a mix of each as shown in figure 2 and 3 [10].

C. Intrusion Detection Systems

Intruders are the foremost dangerous threat to network security.

There are different types of intruders as follow.

Clandestine users: These area unit users' organization's captured or gain higher-up management of the system and uses this management to evade auditing and access controls or to suppress audit assortment.

Masquerader: These area units the people organization and penetrates into the system aren't licensed to use the pc and gain access controls to take advantage of the users account.

Misfeasor: These area unit users organization access information, programs, or resources that access isn't licensed, or they're licensed to access such resources however build misuses of his or her privileges.

An intrusion detection system (ids) is an extra protection live that helps to avoid intrusions. Software system associated hardware devices will be wont to find an attack from entrant. ids product area unit won't to monitor whether or not any attack area unit there or not. Some ids systems simply monitor and provides alert signal of associate attack, whereas others try and block the attack [4].

D. Anti-Malware Software System and Scanners

Viruses, worms and Trojan horses area unit all samples of malicious software system, or malware for brief.

Special so-called associated-malware tools area unit won't to find them and cure an infected system. Completely different antivirus software system area unit out there in market like avg, avast, bit defender, macafee, trend small and lots of additional. Once you put in any of those antivirus programs and do the specified settings. It mechanically checks and blocks any malicious code once found in your laptop.

E. Secure Socket Layer (SSL)

SSL could be a suit of protocol that's wont to accomplish a decent security between application and a web site. It creates secure affiliation between internet server and web site through application so any data changed is protected. SSL is intended to create use of transmission control protocol to supply a reliable end-to-end secure service.

SSL isn't one protocol however rather it includes multiple protocols like SSL handclasp protocol, SSL modification cheerful description protocol, SSL alert protocol, SSL record protocol etc.

SSL provides authentication of shoppers to server through the utilization of certificates. Netscape and Microsoft someone browsers escort SSL.

IV.CONCLUSION

Network security is a crucial field that's more and more gaining attention because the web expands. The safety threats and web protocol were analysed to work out the required security technology. The safety technology is usually software system based mostly, however several common hardware devices area unit used. This development in network security isn't terribly spectacular.

Network security testing is mandatory for the network in use. Try to avoid unwanted access to any network user. An updated antivirus program is useful for security purposes.

Keep inventory of your network resources such as devices and software applications. Properly turn off personal computer when not in use and. Use a strong network and system administrator password. Use a switched network to identify the problem very quickly.

References

[1] Dowd, P.W. McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24- 28, Sep 1998.

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008.

[3] McClure, S., Scambray J., Kurtz, G. (2009): Hacking Exposed: Network Security Secrets & Solutions, Sixth Edition, and TMH.

[4] http://www.wikipedia.org

[5] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008 Marin,G.A., "Network security

[6] Marin,G.A., "Network security basics," Security& Privacy, IEEE , vol.3, no.6, pp.68-72,Nov.-Dec. 2005

[7] Molva, R., Institut Eurecom,"Internet Security Architecture," in Computer

[8] Networks & ISDN Systems Journal, vol. 31,pp. 787-804, April 1999.

[9] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005

[10] Murray, P., Network Security, found at http://www.pandc.org/peter/presentations/ohio-tech-2004/Ohio-tech-security-handout.pdf.

[11] "Security Overview"www.redhat.com/docs/manuals/enterprise/RHE-4 Manual/security-guide/Ch.-sgs-ov.html.

[12] Vicomsoft Ltd – Firewall Software and Internet Security, 2002.

[13] http://networkperformance.info/network-security-system.