Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Prevention based mechanism for attacks in Network Security

Gajanan P. Hingne[1], Umesh B. Shingote[2], Sandip S. Dabre[3]
[1]*Computer Science & Engineering, RSCE Buldhana*
[2]*Computer Science & Engineering, MGI COET,Shegaon*
[3]*Computer Science & Engineering, RSCE Buldhana*

ABSTRACT : Network Security has become vital in today's information technology era, as a result of that numerous techniques are a unit adopted to bypass it. Network administrator has to be compelled to manage with the recent advancements in each the hardware and software system fields for their betterment of the user's knowledge. This paper outlines the varied attack strategies in the field of Networking and numerous prevention mechanisms against them.

Keyword: DOS attacks, Firewalls, Encryption, Port Scanning, SSL, SHTTP, VPN.

I. INTRODUCTION

Network security refers to protective the websites domains or servers from varied types of attack. Network security is vital in each field of today's world like military, government and even in our daily lives. Having the information of however the attacks are dead we are able to higher defend ourselves. The design of the network are often changed to forestall these attacks, several firms use firewall and varied polices to safeguard themselves. Network security incorporates a terribly huge field that was developed in stages and as of now a day, it's still in biological process stage. To grasp this analysis being done, one must perceive its background and should have information of the operating of the net, its vulnerabilities and therefore the ways which may be accustomed initiate attacks on the system. web has become more and a lot of widespread, in today's world web is obtainable all over in our house, in our work place, mobiles, cars everything is connected to the net associated if an unauthorized person is in a position to induce access to the current network he can't solely spy on America however he will simply reduce to rubble our lives.

A network consists of routers from that info is often simply purloined by the utilization of malwares like a "Trojan Horses". The synchronous network incorporates switches and since they are doing not buffer any knowledge and thence aren't needed to be protected. Network security is therefore primarily targeted on the information networks and on the devices that are accustomed link to the net. As prognostication goes for the sphere of the network security it are often same that some new trends are rising some are supported previous ideas like biometric scanning whereas others are utterly new and revolutionary. Email could be a wide used service nowadays and it's additionally contain several serious flaws, there's no system of authenticating the sender as well because the recipient, it's keep in multiple places throughout transmission and may be simply intercepted and changed. SPAM are serious security threat they solely need terribly less men however have an effect on millions to billions of Email users round the world, they'll malicious link or perhaps false advertisements. A network contains several vulnerabilities however most of them will mounted by following terribly easy procedures, such as change software system and properly configuring

network and firewall rules, employing a sensible anti-virus software etc. In this report most of the fundamental info concerning network security is going to be printed such as finding and shutting vulnerabilities and preventing network attacks and additionally security measures currently being employed.

II. KINDS OF SECURITY ATTACKS

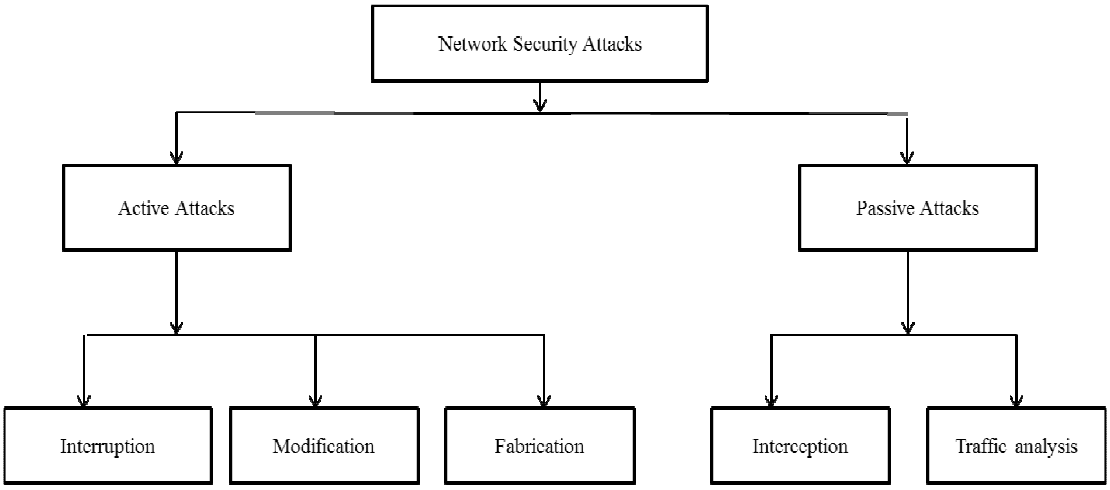

Figure 1.Network Security Attacks

A. Passive Attacks

This type of attacks includes tries to interrupt the system victimization ascertained information. One in all its example is plain text attack, wherever each the plain text and cipher text square measure already glorious to the assailant.
Properties of passive attacks square measure as follows:
Interception: the info passing through a network will be simply sniffed and so offensive the confidentiality of the user, like eavesdropping, "Man within the middle" attacks
Traffic analysis: conjointly attacks confidentiality. It will embrace trace back on a network sort of a CRT radiation.

B. Active Attacks

In this attack the assailant sends information stream to at least one or each the parties concerned or he may also utterly cut off the info stream. Its attributes square measure as follows:
Interruption: It prevents Associate in nursing genuine user type accessing the location. It attacks accessibility. Such as DOS attacks.
Modification: during this the info is changed largely throughout transmission. It attacks reliability.
Fabrication: making counterfeit things on a network while not correct permission. It attacks verification.

C. DOS Attack

DOS attacks these days became a serious threat to network security everywhere the globe. They'll be simply launched by anyone with the essential data of network security. They don't need the maximum amount time and planning as another attack, in brief they're low cost and economical methodology of offensive networks. They can closing the corporate network by overflowing it with requests and so affect accessibility of the network. With the assistance of straightforward to use network tools like Trinoo, which may be simply downloaded of the internet Associate in nursing traditional user will start an attack. DOS attacks sometimes works by exhausting the targeted network of information measure, TCP links buffer, application/service buffer, CPU cycles, etc. DOS attacks use several users connected to a network referred to as zombies most of the time users square measure unaware of that their pc is infected [8].

Kinds of DOS Attacks.

Many attacks square measure won't to perform a DOS attack thus on disable service. A number of that square measure as follows: transmission control protocol SYN Flooding. Once a consumer desires to attach to the server, the consumer 1st sends to Associate in Nursing SYN message to the server. The server then responds to the consumer by causation a SYN-ACK message to the consumer. The client completes the association by connection Associate in Attention ACK message. The association is currently established and information will be transferred simply. The matter arises once the connections stay 0.5 open and therefore the server waits for the consumer aspect to send Associate in Nursing ACK message. This takes system resources and therefore the server can wait until the expiration date. The person exploiting the server can ne'er send the ACK message and can persevere sending new association demand, until the server is overladen, so cannot give access [3].

ICMP Smurf Flooding:
ICMP package is employed to grasp whether or not the server is responding or not. The server replies with Associate in Nursing ICMP echo command. In smurf attack the offensive host forges the ICMP echo requests having victims address because the supply and therefore the broadcast address of remote networks. These computers will then remit ICMP echo reply package to supply, so congesting target's network.

UDP Flooding:
several networks currently use transmission control protocol and ICMP protocols to stop DOS attacks however a hacker will send sizable amount of packages as UDP overloading the victim and preventing any new association.

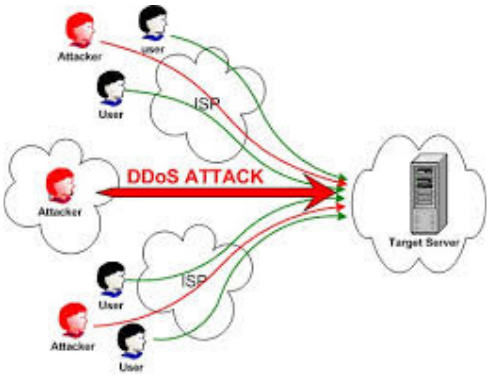

Figure 2.DoS Attacks [18]

III. PREVENTION AGAINST NETWORK ATTACKS

An inherent weakness within the system might it's advisedly, configuration or implementation that renders it to a threat. however most of the vulnerabilities aren't thanks to faulty style however some could also be caused due to disasters each natural and created, or some perhaps cause by the by same persons making an attempt to shield the system [2].Most of the Vulnerabilities caused thanks to poor style, poor implementation, poor management, physical vulnerabilities, hardware and code, interception of knowledge and human vulnerabilities. Several of the network attacks may be simply prevented by the network admin watching his network closely and applying the whole latest patch on the market from the seller to his code. However this cannot stop most of the attacks, to stop them, the network needs configurations such as:

A.Configuration Management

It is as vital as having a descent firewall to shield the system. As before long as a network setup is completed all its default logins, Ids, address should be modified as before long as doable as of these info is available on the net for anyone to look at. Anyone will use the default login to realize access to the network and it will place the entire network in danger. The machines within the network should be running the running up to this point copies of O and every one the patches particularly the protection patches should be put in as soon as they're on the market, configuration files should not have any proverbial security holes, all the information is backed up in a very secure manner, it permits America to contend with 9 out of the 10 upmost attacks. Many tools are also on the market that permits patches to deployed at the same time and keep things tight.

B. Firewalls

It is the foremost wide sold and on the market network security tool on the market within the market. This is often the wall which stands between the native network and also the net and filters the traffic ad prevents most of the network attacks. There are a unit 3 differing kinds of firewalls reckoning on filtering at the informatics level, Packet level or at the transmission control protocol or application level [11]. Firewalls facilitate preventing illegal network traffic through associate unsecured network to a personal network. They will apprize the user once associate untrusted application is requested access to the net. They conjointly produce a log of all the connections created to the system. These logs may be terribly harmful just in case of any hacking tries. Firewalls solely works if they're correctly organized, if someone makes a slip whereas configuring the firewall, it's going to enable illegal to enter or leave the system. It takes sure information and knowledge to properly configure a firewall. If the firewall goes down one cannot hook up with the network as in a very case of DOS attack. Firewall conjointly reduces the speed of network performance because it examines each Incoming and Outgoing traffic. Firewall doesn't manage any internal traffic wherever most of the attacks return from. Many companies area unit below false assumptions, that by simply employing a firewall they're safe, however the reality is that they are not, firewall may be simply be circumvented. The most effective issue whereas configuring firewall is to deny anything that's not allowed [12].

C. Encryption

Using cryptography strategies one will stop hacker listening onto the information as a result of while not the proper key it will simply be garbage to him. Different cryptography technique like victimization HTTPS or SHTTP throughout the transmission of information between the shopper and

user, can stop Man within the middle attack (MIM), this will also stop any sniffing of information and therefore any eavesdropping. Victimization VPN can inscribe all the information going through the network; it'll conjointly improve the privacy of the user. Cryptography conjointly has downsides as all the encrypted mail and websites area unit allowed through firewall they will conjointly contain malware in them. Encrypting information takes process power from the C.P.U. This successively reduces the speed at that information will be send, the stronger the cryptography the longer it takes [13].

D. prevention against DOS Attacks

To prevent DoS attack several technologies are developed like intrusion detection systems (IDSs), firewalls, and increased routers. These items area unit used between the net and servers. They monitor incoming connections similarly as outgoing connections and mechanically take steps to shield the network. They need traffic analysis, access management, redundancy designed into them [15].IDSs area unit build a log of each the incoming and outgoing connections. These logs will then be compared to baseline traffic to detect potential Dos attacks. If there's remarkably high traffic on the server it may also alert of a doable ongoing DOS attack like transmission control protocol SYN flooding [14].Firewalls may also be used as prevention against DOS attacks with the specified configuration. Firewalls may be wont to enable or deny sure packets, ports and IP addresses etc. Firewalls may also perform real time analysis of the traffic and take the required steps to stop the attack. Security measures may also use in routers which may produce another prevention line off from the target, thus though a DOS attack takes place it won't have an effect on the interior network. Service suppliers may also increase the service quality of infrastructure. Whenever a server fails a backup server will take its place, this can build result of DOS attack negligible. If the service suppliers area unit ready to distribute the significant traffic of a DOS attack over a large network quickly it may also stop DOS attacks, however this technique need laptop and network resources and that they may be terribly pricey to supply on daily basis as a result solely terribly huge corporations prefer this technique.

E. Vulnerability Testing

To prevent any attacks on the network, one should realize any open vulnerability within the network and shut them, these might embody open ports and conjointly faulty and superannuated code with proverbial vulnerabilities, outdated firewall rules etc. There are unit totally different tools on the market that permits a user to check his own network security and conjointly realize vulnerabilities in a very network [4]. One such technique is employing a port scanner which can be wont to probe a server and realize any open ports. This is often employed by several admins to verify policies of their servers and can also be employed by attackers on a network to search out exploits. A number of the tools which area unit on the market for complimentary on the net area unit Nmap, SuperScan. These tools are also downloaded by everybody and each comes with associate degree full tutorial for victimization them [16]. Differing types of port scans square measure given below.

IV. ENCRYPTING URL (WWW)

For the sake of privacy, confidentiality and availableness our communications on the online must always be encrypted this reduces the quantity of attacks and prevents anyone to look at the continued transmissions. These are often achieved by building a system of coding and using a system of digital certificates. The foremost necessary method of coding is that the SSL protocol [7].Network security may be compared to human system. The human systems are often taken as analogy, providing a

protection at every point similar to a body we are able to greatly improve the safety. Mistreatment this mechanism we are able to unfold our resources and forestall obsessed with one system [9].

A. Secure Sockets Layer

It uses each uneven and biradial keys coding transfer knowledge during a secure mode over a network. When SSL is employed during a browser it establishes a secure affiliation between the browser and also the server. It's like associate encrypted tunnel within which the information will flow firmly. Anyone listening on the network cannot decipher the information flowing within the tunnel. It provides integrity mistreatment hashing algorithms and confidentiality using coding. The session begins with associate uneven coding. The server then sends the consumer its public key. Once the uneven affiliation each the perimeter switches to a biradial affiliation. Asymmetric algorithms area unit slow and uses rather more computer hardware power than biradial ones. Even while symmetric coding, computer hardware load is high, servers will solely handle a fraction of connections as compared to servers with no coding [17].

B. Secure hypertext transfer protocol (SHTTP)

It's another to HTTPS; it's an equivalent operating as HTTPS and is intended to secure websites and their messages. There are unit variations between SHTTP and SSL protocol like SSL could be a affiliation oriented protocol and it works it transport level by providing a secure tunnel for transmission whereas SHTTP works on application level and every message is encrypted one by one, however secure tunnel is created. SSL are often used for secure TCP/IP protocols like FTP however SHTTP works solely on hypertext transfer protocol. Its use is fairly restricted as compared to HTTPS.

C. VPN

Virtual personal Network (VPN) could be thanks to transport traffic on associate unsecured network. It uses a combination of encrypting, authentication and tunneling. There are a unit many various styles of strategies of VPN however of those five area unit simply recognized. The most glorious and used protocols area unit as follows:

· Point-to-Point Tunneling Protocol (PPTP)
· Layer a pair of Tunneling Protocol (L2TP)
· Net Protocol Security (IPsec)
· SOCKS

VPN permits a user to secure it privacy as it's terribly exhausting to properly find the situation of the user because the network knowledge is also routed through multiple locations unfold across the planet before finally reaching its destination. It can also be accustomed bypass firewall and blocks of internet sites.

D. E-Mail Security

As each the sender and receiver of the e-mail one should worry regarding the sensitivity of the information within the mail, it being viewed by unauthorized users, being changed within the middle or within the storage. Emails are often simply counterfeit thus one should always certify its supply. E-mail can also be used as a delivery mechanism for viruses. Cryptography as in several different fields plays a vital role in email security [6].Emails area unit terribly unsecure. As they submit to several mail servers throughout transits they will be simply intercepted and changed. Whereas mistreatment common Email there's no method to authenticate the sender and lots of users wouldn't provide a thought to certify the e-mail received. There are a unit several standards one will opt for so as to secure his emails a number of these are: PGP, PEM, Secure useful net mail extension (MIME),

Message Security Protocol (MSP).The emails throughout their transit area unit hold on in several servers, that they submit to throughout their transit and as a result they're not truly deleted once the users delete them from their account. These copies can be simply retrieved and similarly as their contents. So there ought to be a feature to delete these copies or creating these copies secures essentially by mistreatment some sturdy coding in order that they can't be scan [10].

V. RECENT ADVANCES IN NETWORK SECURITY

Before the web became fashionable and fairly common, intrusion detection meant detection of associate unauthorized human user/person on a machine, however this definition radically modified with the appearance of Code Red worm and its variants within the year 2001. These were first generation worm they'd high unfold rats and created human countermeasures not possible. A period and an automatic system was to be developed to find and forestall more unfold of those worms. These worms generated high traffic especially on Port eighty, thus a meter approach was projected to find them. It worked for the generation wherever network infrastructure wasn't wide deployed. but they became useless within the recent years as a result of the behavior of worm is currently specific in several cases and conjointly users begin to generate high volume on their own mistreatment file sharing sites and network recreation [5]. Network security is being improved in 2 fields particularly hardware and security within the following ways:

A. Hardware Development

This field isn't developing terribly speedily as its software system counterpart however yet some superb developments area unit being created like mistreatment Biometric systems and smartcards which might drastically reduce the quantity of unauthorized access. Biometric has important use within the field of the network security, some obvious uses such a inbuilt biometric scanner hooked up to a digital computer are often used as associate authentication mechanism which might be used as a login to the system, since 2 persons cannot have the same bioscience because the each persons, it's a full proof mechanism of login [1].People tend to forget their passwords and then they keep it close to their digital computer written on a blunder or one thing else or maybe lock themselves out of their system by incorrectly coming into it too again and again. All this may be simply avoided by biometric systems as they supply user's plain proof of identity. Smartcards area unit provided by companies to its employees, they solely work after they area unit inserted within the pc and a pin issued the network Administrator is entered, since the pin issued is just four characters and numeric, users don't forget it and don't write it down.

B. Software System Developments

The software system field is incredibly wide once it involves network security. It includes firewall, antivirus, VPN, intrusion detection, and lots of rather more. The development of network security is largely still the same. Once new virus area unit found virus definitions area unit updated, it's an equivalent for firewalls instead their rules area unit updated. As a lot of and a lot of security transits to hardware like biometric. The software system should be able to use the data properly and suitably. Presently analysis is being targeted on neural networks for automatic face recognition software system. Most current algorithms need substantial process power. This power can't be on the market in tiny devices like sensors. Therefore, one should develop lightweight weight algorithms to counter this downside [1]. Antivirus works on an awfully principle, they scan a file then matches its digital signature against the glorious malwares. If the signature is match within the info it reports it, delete it or maybe clean it depending on the user's setting. This method but simple includes a Brobdingnagian downside, whenever a replacement malware is found, it takes time before the antivirus info are often updated and through this era the malware will already take complete management of the pc, disable

the antivirus or maybe hides itself from the antivirus. to stop this antivirus firms introduced a replacement system referred to as cloud scanning this way not solely can the digital signature be scanned across the info however conjointly across several computers and servers across the planet. This all happens and real time and results area unit in no time. This greatly reduces the possibility of infection from a replacement malware.

VI. Conclusion

As web has become a large a part of our existence, the requirement of network security has additionally exaggerated exponentially from the last decade. As a lot of and a lot of users hook up with the net it attracts lots of criminals. Today, everything is connected to web from straightforward searching to prevention secrets as a result there is large would like of network security. Billions of bucks of transactions happens each hour over the internet, this got to be protected in the least prices. Even a tiny low unobserved vulnerability in a very network will have disastrous have an effect on, if firms records square measure leaked, it will place the users information like their banking details and MasterCard data in danger, varied software's like intrusion detection are that prevents these attacks, however most of the time it's owing to an individual's error that these attacks occur. Most of the attacks may be simply prevented, by following several merely ways as printed during this paper. As new and a lot of refined attacks occur, researchers across the planet notice new ways to forestall them. Numerous advancements square measure being created within the field of network security each within the field of hardware and software package, it's an eternal cat and mouse game between network security analysts and loopy and as the demand of web shows no signs of decreasing it's solely getting to get lots more durable.

REFERENCES

[1]B.Daya, "Network Security: History, Importance, and Future", University of Florida Department of Electrical and Computer Engineering, 2013.
[2]Li CHEN, Web Security: Theory and Applications, School of Software, Sun Yat-sen University, China.
[3]J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.
[4]A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.
[5]S. A. Khayam, Recent Advances in Intrusion Detection, Proceedings of the 26th Annual Computer Security Applications Conference, Saint-Malo, France, pp. 224-243, 42, 2009.
[6]M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," Napier University, Scotland, UK.
[7]R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.
[8]Q. Gu, Peng Liu, "Denial of Service Attacks," Texas State University, San Marcos.
[9]M. A. Shibli, "MagicNET: Human Immune System & Network Security," IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No.1, January2009.
[10]M. Silva, "Virtual Forensics: Social Network Security Solutions," Proceedings of Student Research Day, CSIS, Pace University, 2009.
[11]R. K. Khalil, "A Study of Network Security Systems," IJCSNS International Journal of Computer Science and Network Security, 2010.
[12]S. Alabady, "Design and Implementation of a Network Security," Technology,Vol. 1, p. 11, 2009.
[13]B. Preneel, "Cryptography for Network Security," Katholieke Universiteit Leuven and IBBT, 2009.
[14]M. Kassim, "An Analysis on Bandwidth Utilization and Traffic Pattern," IACSIT Press, 2011.
[15]M. Eian, "Fragility of the Robust Security Network: 80211," Norwegian University of Science and Technology, 2011.
[16]D. Acemoglu, "Network Security and Contagion," NATIONAL BUREAU OF ECONOMIC RESEARCH, 2013.
[17] S. Shaji, "Anti Phishing Approach Using Visual Cryptography and Iris Recogn No. 3pp. 88-92, 2014.
[18] www.zerotrusion.com.

