International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 3| ISSN: 2456-3307

NS in Digitalization: Attacks and Defence

M. Soundharya[1],Mrs. E. Bhuvaneswari[2]

[1]Research Scholar, Department of Computer Science,Kamban College of Arts and Science for Women, Thiruvannamalai, Tamil Nadu, India

[2]Assistant Professor,Department of Computer Science,Kamban College of Arts and Science for Women, Thiruvannamalai, Tamil Nadu, India

bhuvaname2008@gmail.com[1],msriya333@gmail.com[2]

ABSTRACT

NS is become a gambol in our whole world. In today's world the volume of data increases every second and threats continue to transform and grow, weakening your ability to attacks. The business world is going digital as a result to bypass these things and we are adopting different methods. Network administrator has to keep track, has to update with all current advances in both the software and hardware fields to avert the user's data. Digitalization is playing an important role and integrated of digital technologies into our daily life. This paper precise similar method which are used to attack as well as various mechanisms against to defense them.

Keywords : DOS attacks, Encryption, Firewalls, Port Scanning, SHTTP, SSL, VPN

I. INTRODUCTION

Network security broach towards protect the website severs in various forms of attack. Network security has become foremost in every field of world such as military education, government, business and our day to day lives. we can better defend ourselves by keeping track of all the knowledge know how the attacks are attained. Modifying the network architecture we can avert these type of attacks, many companies employ firewall and diverse polices to safeguard them. Security network has immense field which was expanded stage and as per today's criteria. To understand the contemporary analysis being done, one should have knowledge of its background should have working in our present world internet is accessible everywhere in our house, in our work area, cars and mobiles everything is connected to the internet, if any unknown person is able to acquire access to this network they can not only spy on us but they can easily mishmash up our lives. Network comprises of routers from which information can easily be stolen by the use of malwares such as "Trojan Horses". Network security mainly focused on the data in the networks and devices which are used to the internet. A synchronous network consists of switches, since they not do buffer any of the data and they do not required to be protected. Digitalization is playing a leading role in everyone's daily life, so secure for network is the main issue to be organized. As prediction goes for the network security field, as some new trends are emanating and based on old trends such as biometric scanning while others are completely new and revolutionary. Social network sites are widely used services of day to day and it is also contain many serious shortfall, some of them do not have system of authenticating the sender as well as the receiver, during transmission as it is stored in multiple places which can be easily snatched and modified. A network contains many impuissant but most of them can be fixed by the following simple techniques. Such as updating the software,

configuring network accurately, rules for firewall, by using a good anti-virus software etc. The basic information concerned with network security which would be outlined such searching and ending impuissant, preventing network from attacks and also security measures which are currently being used. Digital India is a crusade sprint by the Indian government to make our country a digitally authorized country. This enterprise was initiated to connect people from the rural areas with high-speed internet networks to blaze any information as per their requirement. Three important segments of digital India are like erection of digital infrastructure. Digital literacy and convey digital services to an all over the country.

II. DIFFERENT TYPE OF SECURITY ATTACKS

A. Passive Attacks

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. This type of attacks incorporate the attempts to break the system using perceive data. One of the examples is plain text attack, where both the plain text are already well known to the attacker.

Properties of passive attacks are:

- **Interception:** This can be either an active or passive process.The data passing through a network can easily be snuffled and thus attacking the Confidentiality of the user, such as eavesdropping, "Man in the middle" attacks
- **Traffic analysis:** Traffic analysis is the process of interception and examine message in order to deduce information from patterns in communications. This is also a confidentiality attack. It can embrace trace back on a specific network like a CRT radiation.
-

B. Active Attacks

An active attack is a network exploit in which a hacker attempts to make changes to data on the target. In this type of attack the attacker sends data stream to one or both the groups involved or they can also be completely cut off the streams of data. It imputes are as follows:

- **Interruption:** It averts authenticated user form accessing the site. It attacks availability, such as DOS attacks.
- **Modification:** In this the data is altered mostly during the transmission. It's an integrity attacks.
- **Fabrication:** Creating spurious items on a network without genuine authorization.

C. DOS Attacks

Today a DOS attack has become a major threat for network security all over the world. They can easily be launched by any people with the basic knowledge of the network security. In a distributed denial-of-service exploit, large numbers of compromised system attack a single target. They don't require much time and planning as compared to other attacks, in short they are most cheaper and efficient method for network attacking. . They can shutdown the company network by cram-full as of with requests and thus affects network availability. With the help of network tools such as Torino, we can easily download from the internet by this any normal user can initiate an attack. DOS attacks usually works by enervate the targeted network of bandwidth, buffering of TCP connections. Application buffer, service buffer, CPU cycles, etc. DOS attacks uses many users connection to a network known as zombies, most of the time users are heedless of that their computer is infected.

D. Different Types of DOS Attacks

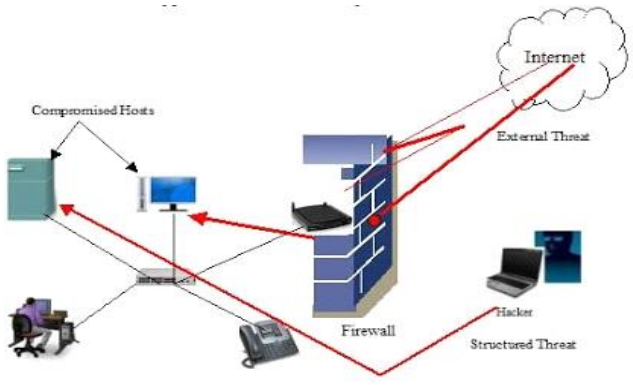
Many attacks are used to accomplish a DOS attack so as to impair service. Some of them are as follows: TCP SYN Flooding which act as whenever a client

wants to connect to the server, the client first has to sends to an SYN message to the server. Then the server responds to the client by sending a SYN-ACK message. Later the client consummates the connection by sending an ACK message. These grasp the system resources and the server has to wait till the end of the date. The person utilizing the server will never send the ACK message and will keep on sending a new connection request, until the server is overloaded and thus they cannot dispense access.

ICMP (Ping) Flood: ICMP flood overwhelms the target resources with ICMP echo request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP echo reply packets, resulting significant overall system slowdown.

UDP Flood: A UDP flood, by definition, is any DOS attack that floods a target with user datagram protocol (UDP) packets. Now many networks employ TCP and ICMP protocols to avert DOS attacks but a hacker can send large number of packages, so as UDP overloading the victim and averting any new connection.

E. Types of Network Security



III. DEFENCE AGAINST NETWORK ATTACKS

An inherent fragility in the system may be with by design, configuration or may be with implementation which contribute it to a threat. But extent of the vulnerabilities are not because of inoperative design but some may be caused due to sudden disasters both naturally and by human made or some maybe cause by the same persons trying to defend the system. Most of the Vulnerabilities are caused due to poor design, poor configuration, poor implementation, poor management, destitute physical vulnerabilities with hardware and software, information interception and human vulnerabilities. Most of the closely and applying the entire latest reinforcement available from the vendor to their software. However this cannot avert most of the attacks, to avert them each network requires configurations such as:

A. Configuration Management

The main weapon in network attack defence is tight configuration management. It is important for having a dive or slump firewall to avert the system. Anyone can use the remittance login to permit access to the network and as it can put the entire network at risk. All your configuration files in your operating systems or applications should have enough security. The machines inside the core of network must be running the run-up to update the copies of O and all the patches especially the security patches must be installed as soon as they are accessible, configuration files shall not have any known security holes, all the data is backed away in a secure manner, it allows us to allot with nine out of the ten topmost attacks. Several tools are also available which allows patches to range simultaneously and keep things tight.

B. Firewalls

Firewall is a device and/or software that stands between a local network and the internet, and filters traffic that might be harmful. It is the most extensively sold and accessible network security tool convenient in the market. This is the wall which upend between the local network and the internet, which filters the traffic ad averts most of the attacks

in the network. There are three divergent types of firewalls be contingent on filtering at the IP level, Packet level, TCP level or application level. Firewalls help in averting unauthorized network traffic through an unsecured network through a private network. They can alert the user when an untrusted application is requisite access to the internet. They also devise a log for all the connections made to the system. These logs can be very damageable in case of any attempt in hacking. If the firewall lay down, it is not able to connect through the network as in a case of DOS attack. Firewall also diminishes the speed of network performance as it investigates both incoming and outgoing traffic. Firewall does not control any sort of internal traffic where most of the attacks arrive. Many companies are under flaw assumptions that by just employing a firewall its safe, but the truth is they are not under safe condition, firewall can be easily be bypassed. The best thing while configuring firewall is to contradict anything which is not allowed.

C. Encryption

Encryption is another great weapon used in defence against network attacks. Using encryption mechanism one can avert hacker listening to the data because without the equitable key it will be debris to him. Different encryption mechanism such as HTTPS or SHTTP during the data transmission between the client and server, will avert man in the middle attack (MIM), this will also avert any disinter of data and thus any wiretap. Using VPN, which will encrypt all the data going through the network; it will also enhance the privacy of the user. Encryption also has pitfalls as all the encrypted mail and web pages are allowed through firewall they can also embrace malware in them. Encrypting data grasp processing power from the CPU. This in turn diminishes the speed at which data can be sent, as stronger the encryption it takes more time to decrypt.

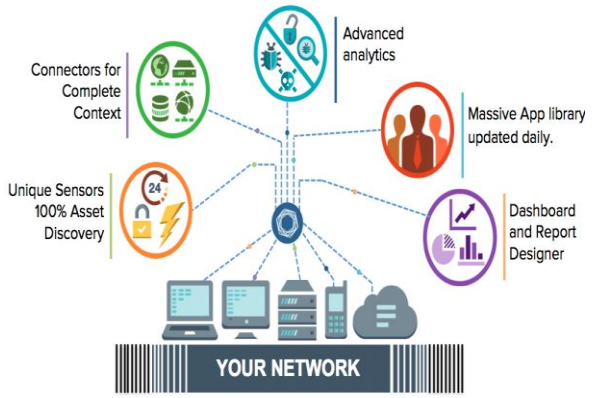
D. Defence against DOS Attacks

To avert DDoS attack many technologies have been evolved such as intrusion detection systems (IDSs), enhanced routers, firewalls etc.Thesethings which are used between the servers and the internet. They overseer incoming connections plus outgoing connections and which automatically take steps to fortify the network. They have traffic inspection access control and redundancies are built into them. IDSs have been logged into both the incoming and outgoing connections. Later these logs can be compared with the baseline traffic to recognize potential DOS attacks. If there is any unusual lofty traffic on the server it also circumspect possible ongoing DOS attack such as TCP SYN flooding. With the required configuration, the Firewalls can also use as defence against DOS attacks. Firewalls are used to allow or deny certain ports, packets, IP addresses etc. Firewalls can also accomplish real time assessment of the traffic and take the necessary steps to avert the attack. Security measures can also be deployed in routers which can generate another defence line away from the target, so even if a DOS attack arises it won't affect the internal net Service providers can also escalate the service quality of infrastructure.

E. Vulnerability Testing

A vulnerability testing is any mistakes or weakness in the system security procedures, design and implementation that may result in the violation of system's security policy. To avert any attacks on the network, one must notice any sort of open vulnerability in the network and close them; these might embrace open ports, defectiveness and outdated software with known vulnerabilities, outdated firewall regulations etc. One such method is used for port scanner which can be worn to probe a server and identify any open ports. This is used by many administrators to verify rules, policies of their servers and also can be used by attackers on a network to detect exploits. Some such tools which are obtained for free on the internet are Nmap, Super Scan. These tools are permitted to download by

everyone and each comes with a detailed respective tutorial to use them. Different types of port scans are as follows below:



IV. ENCRYPTING THE WORLD WIDE WEB (WWW)

The objectives of privacy, confidentiality and availability our communications on the web should be consistently encrypted this will reduces the number of attacks and averts anyone to view the ongoing transmissions. These can be attained by putting all together for a system of encryption and deploying a system of digital certificates which is used in our digitalization techniques. The most vital way of encryption is the SSL protocol. Network security can also be contrast to human system. The human system can be clasped as analogy, providing a preservation at each point just like a body we can greatly refine the security. Using this mechanism we can extend our resources and avert dependent on one system.

A. Secure Sockets Layer It employs both asymmetric and symmetric keys encryption which transfers data in a secure mode over a consistent network. When SSL is deployed in a browser it initiates a secure connection between the browser application and the server. It's like an encrypted subway in which the data can proceed securely. Anyone listening on the network can't decode the data passing in the subway. It yields integrity using hashing algorithms and confidentiality using encryption. The session is tackled with an asymmetric encryption. The server sends public key to the client. After the asymmetric connection both sides are switched to a symmetric connection. Asymmetric algorithms are slow and accomplish more CPU power than symmetric. While symmetric encryption, CPU load is elevated, servers can only handle a fragment of connections as compared to servers with no encryption.

B. Secure HTTP (SHTTP) It's an substitution to HTTPS, it has the same working principles as HTTPS and is plotted to secure web pages and their messages. There is a differentiation between SHTTP and SSL protocol such as SSL is a connection oriented protocol and it works on the transport level by dispensing a secure subway for transmission whereas SHTTP works on the application level and here we are encrypting each message separately, but secure subway is created. SSL can be employed for secure TCP/IP protocols like FTP but SHTTP works only on HTTP.

C. VPN Virtual Private Network (VPN) is a mechanism to carry traffic on an unsecured network. It employs a combination of encrypting, authentication and subway. VPN empowers a user to secure its privacy, as it's very difficult to detect the location of the user as the network data may be dispelled through multiple locations expand across the world before reaching its final destination.

D. E-Mail Security Both sender and the receiver of the email must be distressed about the diplomatic of the information in the mail; it has been perspective by unauthorized users, being altered in the storage or in the middle. Email can be easily be simulated therefore one must always be authenticate its source.

V. CONCLUSION

As internet has become a herculean part of our daily life, so necessitate of network security has also extended exponentially from the previous decades. As much as the users are connecting to the internet it fascinates a lot of criminals attracts. Now a day's

according to the Digital India, each and everything is connected to internet from simple grocery shopping to the defence confidentially, so as an outcome there is herculean need of security to the network. Transaction over Billions of dollars is happening every hour over the internet, at any cost this has to be protected. Even a minute unobserved vulnerability in a network can have devastating effect, if companies records are emanated, it can lay the users data such as their banking details, credit card, debit card information at threat, there are innumerable software's such as intervention in detection which have been averting these attacks, but on most of the occasion it's all because of a human oversight that these attacks transpire. Most of the attacks can be easily be averted, by re tendering many simply methods as outlined in this paper. As new and more complicated attacks prevail, researchers across the world are finding new methods to avert them. Numerous elevations are being mould in the field of network security both in the field of hardware and software, it's like a continual cat and mouse game between network security analyst and hackers/cracker, so per the requirement of internet shows no signs of diminishing it's only going to acquire much harder.

VI. REFERENCES

[1] R.E.Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.

[2] M.Kassim, "An Analysis on bandwidth Utilization and Traffic Pattern." IA CSIT Press, 2011.

[3] M.M.B.W Picoulas J, "Software Agents and Computer Network Security." Napier University, Scotland, UK.

[4] A.R.F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.