Attacks and Resistance of Network Security in On-Demand Application

G. Mohan Ram
Assistant Professor,
Department of CSE,
Shri Vishnu Engineering College for Women (A),
Vishnupur, West Godavari District, Bhimavaram,
Andhra Pradesh-534202.

T. Kesava
Assistant Professor,
Department of CSE,
Shri Vishnu Engineering College for Women (A),
Vishnupur, West Godavari District, Bhimavaram,
Andhra Pradesh-534202

Abstract:- Network Security has become a gambol in our real world, as each chunk of the business world are going digital, as a result to bypass these things we are adopting different technique. Network administrator has to keep track and has to update with all recent advances in both the software and hardware fields to avert the user's data. Now a day's, On Demand Application is playing an important role and integration of digital technologies into our everyday life. These paper precise different methods which are used to attack as well as different mechanisms against to defense them. In our paper , we are implementing Knowledge based Malware detection framework in network for on-Demand Application.

Key words:- Chunk, On-Demand, Network Security, Dos, Malware;

I. INTRODUCTION

Network security broach towards protecting the websites servers or domains in different forms of attack. Network security has become foremost in every field of today's world such as military, education, government, business and even in our day-to-day lives. We can better defend ourselves, by keeping track of all the knowledge about how the attacks are attained. By modifying the network architecture we can avert these kinds of attacks, many companies employ firewall and diverse polices to safeguard them. Security for the network has immense field which was expanded stage by stage and as per today's criteria, it is still in evolutionary stage. To understand the contemporary analysis being done, one should have knowledge of its background and should have working idea of the internet, its circumstances vulnerabilities and methods which are used to establish attacks on the system.

Internet has become more and more extensive, in our present world internet is accessible everywhere in our house, in our work place, mobiles, cars everything is connected to the internet and if any unauthorized person is able to acquire access to this network they can not only spy on us but they can easily mishmash up our lives.

The network comprises of routers from which information can easily be stolen by the use of malwares such as “Trojan Horses”. A synchronous network consists of switches, since they do not buffer any of the data and hence they do not required to be protected. Network security mainly focused on the data in the networks and on the devices which are used to link to the internet. Now a day, On Demand digitalization is playing a leading role in everyone’s daily life, so security for network is the main issue to be organized.

As prediction goes for the network security field it can be said, as some new trends are emanating and some are based on old trends such as biometric scanning while others are completely new and revolutionary. Social networks sites are widely used services of today and it also contain many serious shortfall, some of them do not have system of authenticating the sender as well as the recipient, during transmission as it is stored in multiple places which can be easily snatched and modified.

SPAM are serious security threats as they require very less manpower but they would affect millions to billions of social networks and website applications users throughout the world, they can malignant link or even with false advertisements. 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 and rules for firewall, by using a good anti-virus software etc.

In this report, the basic information concerned with network security which would be outlined such as finding and closing 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. The main focus of initiating this crusade is to dispense Indian citizens with electronic government services by foreshortening the paperwork. It is very constructive and coherent technique which will save time and man power to a great extent. This enterprise was initiated to connect people from the rural areas with the 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 all over the country.

II. DIFFERENT TYPES OF SECURITY ATTACKS

A. Passive Attacks:- In 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 and cipher text are already well known to the attacker.

Properties of passive attacks are: ·

Interception: 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: This is also a confidentiality attack. It can embrace trace back on a specific network like a CRT radiation.

B. Active Attacks: 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. It's an authentication attacks.

C. DOS Attack: 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. 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, 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. 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 Smurf Flooding: ICMP package is used to understand whether the server is acknowledging properly or not. The server responds with an ICMP echo command. . In smurf attack the attacking host cast the ICMP echo requests having fatality address for the source and the broadcast address of remote networks. These computers will return back ICMP echo reply package to the source, thus jam-packed victim's network. UDP Flooding: 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.

II. 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: It is important for having a dive or slump firewall to avert the system. As soon as the network setup is completes all its remittance logins, ID's, address must be altered as soon as possible if all these information are available for anyone to view on the internet. Anyone can use the remittance login to permit access to the network and as it can put the entire network at risk. 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: 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. Firewalls only exert if they are precisely configured, if somebody makes a flaw while firewall configuration, it may lead an unauthorized user to enter or exit from the system. It takes an indisputable knowledge and experience to precise configures a firewall. 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: 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. These things 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 network. Service providers can also escalate the service quality of infrastructure. Whenever a server flunks a backup server it can take its place, this will consequence the DOS attack which is negligible. If the service contributor are able to distribute the heavy traffic of a DOS attack over a wide network quickly this can also avert DOS attacks, however this method require computer and network resources, as they can be very expensive to provide on daily basis, so as a result only very big companies choose this method.

E. Vulnerability Testing: 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. There are different tools obtainable which allows a user to test their own network security and also detect vulnerabilities in a network. 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:

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.

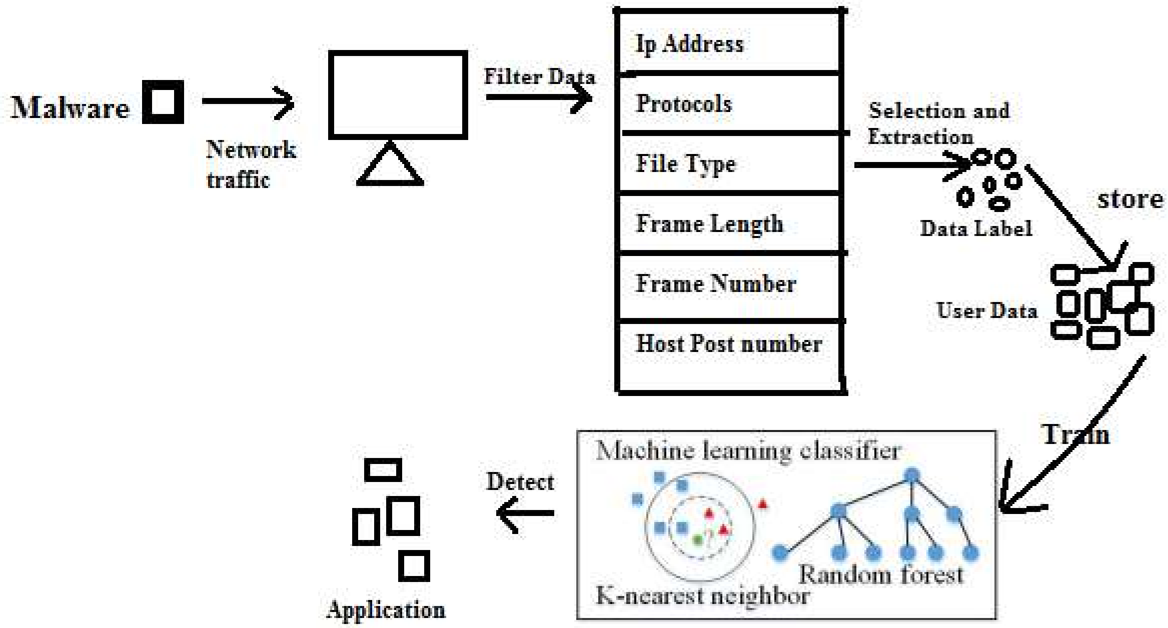
B. Secure HTTP (SHTTP): It's an substitution to HTTPS, it has the same working principles as HTTPS and is plotted to secure web pages and their messages. There is a differentiation between SHTTP and SSL protocol such as SSL is a connection oriented protocol and it works on the transport level by dispensing 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. It is fairly limited as compared to HTTPS.

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. There are different types of way of VPN but of these 5 are easily identified. The well known and deployed protocols are as follows: · Point-to-Point Tunnelling Protocol (PPTP) · Layer 2 Tunnelling Protocol (L2TP) · Internet Protocol Security (IPsec) · SOCKS 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. It also can be deployed to bypass firewall and blocks of websites.

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. E-mail can also be utilized as a delivery mechanism for viruses. Cryptography as in many other discipline plays a significant role in email security. Emails are very unsecure because as they elapse through many mail servers during transmission, they can easily be obstructed and modified. While using other simple common Email there is no procedure to authenticate the sender and many other users would not give an impression to authenticate the email received. There are so many standards one can determine in order to secure their emails some of these are: PGP, PEM, Secure multipurpose Internet mail extension (MIME), Message Security Protocol (MSP).

Knowledge Based framework Malware Detection in Network

On-Demand Application can apply knowledge based techniques to evaluate the runtime behaviors of the apps in the malware detection. In the malware detection scheme as developed, a device uses K-NN and random forest classifiers to build the malware detection model. The IoT device filters the TCP data packets and selects the data features among various network data application features including the data frame number and data length, data labels them and stores these data features in the application store. The K-NN based malware detection assigns the network traffic to the class with the largest number of objects among its K nearest neighbors. The random forest classifier builds the decision trees with the labeled network traffic to distinguish malwares. The true positive rate of the K-NN based malware detection and random forest based scheme with MalGo dataset are 99.7% and 99.9%, respectively



Proposed Framework Analysis:-

Step1:- Read Malware App

Step2:- Transfer through Network

Step3:- Filter Data

Step4:- Read Malware Meta data

Step5:- Selection and Extraction Malware app data

Step6:- Assign Data Label

Step7:- Store User Data

Step8:- Read Data Using Train Data Set

Step9:- Apply Machine Learning Classifier

Step10:- Then next K-NN process

Step11:- Detect Malware Content

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 defense confidentially, so as a 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.

REFERENCES

[1] B. Daya, "Network Security: History, Importance, and Future ,"University of Florida Department of Electrical and Computer Engineering , 2013. http://web.mit.edu/~bdaya/www/Network%20Security.pdf

[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, January 2009.

[10] M. Kassim, “An Analysis on Bandwidth Utilization and Traffic Pattern,” IA CSIT Press, 2011.

[11] M. Eian, “Fragility of the Ro bust Security Network: 80211,” Norwegian University of Science and Technology, 2011.

[12] D. Acemoglu, “Network Security And Contagion,” NATIONAL BUREAU OF ECONOMIC RESEARCH, 2013.

[13] S. Shaji, “Anti Phishing Approach Using Visual Cryptography And Iris Recognition,” IJRCCT, Vol 3. No. 3pp. 88-92, 2014.

[14] https://hubpages.com/technology/Types-of-Network-Attacks