A REVIEW ON TECHNIQUES, TOOLS AND DEFENSE FOR NETWORK SECURITY ATTACKS AND THREATS

[1]Nega Teferra Hailu, [2]Prof. Harshal Shah
[1]Department of Computer Science & Engineering, [2]Department of Computer Science & Engineering
[1]Parul University Vadodara, Gujarat, India, [2]Parul University Vadodara, Gujarat, India

Abstract*— Thanks to technology, communication is very easy and efficient by the help of network. As a result people prefer internet communication for the fast reachability and delivery. At this time the two or more communicating parties should be consider the security of the network and know how to defeat the attacks on the network. By now, in this digital era season, there are enormous numbers of attacks are there in the internet for sniffing and spoofing. Because of several attackers are spread to assault network, keeping safe network security is the basic thing for this generation. Security becomes a very big concern when we using networks organize in an accidental or unfriendly environment. The duty of Network Security is not only keeping secure the end point of the system also it's the entire network. This review paper is tells us something how the end user is secure their system more conveniently and focus on several attacks that used by the intruders and the mechanism to defeat them. And also it focused on distinguishing mechanism for protecting network security and the obstacle that affect the network.

***Keywords*— Network Security; Attacks; Encryption; Threats; Authentication; DOS; Password; Security tools**

1. INTRODUCTION

Now a day, even if communication through network is very important thing and the fastest way of communication there were an obstacle which called an attack that made the communication is so bad [1]. So we should keep our data secure from those attacks by using the technique called Network security which refers to protecting the websites domains or servers from various forms of attack. Having knowledge of how to the attacks are transmitted over the network we can protect ourselves. Many companies used firewalls and various policies to protect themselves. Thus network security is just protecting the data and information from the attacks comes through the network.

Network Security protects and monitors unauthorized access, misuse, modification, or denial network and its accessible resources [2]. To keep safe the useful data items and the whole network it should built one specific security mechanism. As the growth of Internet and Network by this digital era, side by side there are a lot of threat and attacks are emerge quickly [3]. Thus the main thing that should be forefront for Internet and the Network is keeping them secure. The threat and the attacks are assault the poor design network, weak technology and ignorance by the users.

Securing a transmitting message during communication becomes very challenging due to increasing of threat and attacks against network security [4]. The network administrator gives an important role to checks the error in network and secure network. The simple and the most used techniques to keep safe our network resource is assigning unique name and password. Both hardware and software are needed for designing a network security.

2. ATTACKS AND THREATS

In this topic of the paper we listed the very dangerous and harmful different types of security attacks and threats over network.

Passive Attacks: - This kind of attack is working by knowing the system very well and grasps the data by interfering to the system what it wants [6]. It has the property of Intercept (sniffing data that pass through network) and Traffic Analysis (the concealment of information).

Active Attacks: - In this kind of attack the attacker modifying or totally change the data. It is characterized by Interrupt (authenticated file accessing), Modification (modifying data during transmission) and Fabrication (making imitation without correct authorization) [6].

DOS Attack: - This kind of attack is very easy to create and it's efficient to attack, thus it is a great hazard to network security. DOS assaults mostly work by draining the specific network bandwidth, buffer, CPU cycles, and network connected users [7]. There are different ways of attacks to perform DOS attack. From this: - TCP SYN Flooding, ICMP Smurf Flooding and UDP Flooding.

Security Threats: - This class of attack includes denial of service, distributed denial of service, viruses, Trojan horses, spywares, malwares, unauthorized access to the network resources and data, accidental deletion of the files and uncontrolled internet access [7].

Virus Attack: - This class of attack harms the computer and network when it is run and spread by perform different unwanted and harmful functions by replicating itself [7].

Unauthorized Access: - Getting access data items on network that is allowed only for authorized person in means of different interference [2].

Information Theft and cryptography attacks: -Losing of the very crucial information in any circumstance or accidental event.

Unauthorized application installations: -Installing and run non-licensed programs that bring computer network in to risk and danger.

Application Level Attacks: - This attack feats and uses the weakness in the application layer. E.g. web server attacks, malicious software attack and SQL injection.

Physical Layer attacks: -This attack includes Jamming (the attacker interfere network communication frequencies), Tampering or destruction (getting the access to the sensor node physically and adding some similar sensor node), Sybil Attack (network enemy introduction into a networked system).
Data Link Layer Attack: - This attack includes Collision (happened when two nodes transfer data at the same time and frequency), Exhaustion (disturbing the communication in between nodes and let push the source to retransmit), Unfairness (corrupting the performance causing other nodes to miss their transmission deadline), Interrogation (attacker sends RTS {Request-To-Send} packets to a target node by ignoring CTS {Clear-To-Send} reply packets) [3].

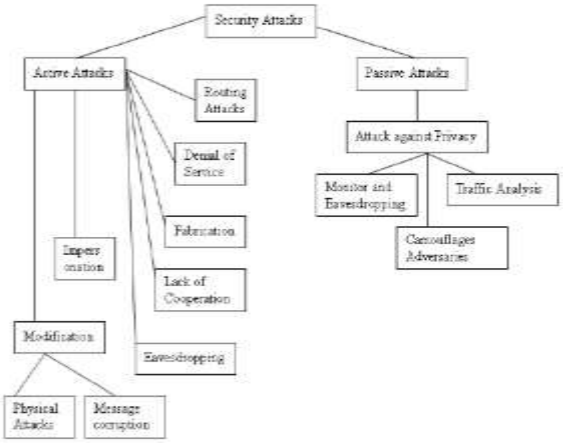

Figure 1: General Classification of Security Attacks [8]

Network Layer Attack: - In this attack the following are included. Spoofing and Altering the routing information (generating wrong messages and partition the networks into nodes), Misdirection (adding some malicious node to change the direction of the transferred messages), Internet Smurf Attack (take the address of the harmed node and broadcast echoes in the network), Sinkhole (pretending almost all the traffic towards the included node), Selective Forwarding/ Black hole Attack (add malicious node in the network that decline to forward messages and drop them), Wormhole Attack (accepts packets at one end point and underpasses them to another point in the network), Hello Flood attack (sends routing or another data with huge radio range that causes individual node thinks the opponent is its adjacent and thinks that the messages is within the radio range of the transmitter) [2].
Transport Layer Attack: - This attack includes Flooding (opponent adds new connection request until the resources go to maximum bounds), De-synchronization (interruption of communication protocol by changing the sequence number of the messages).
Weak password recovery: - Hackers or intruders are getting a way informally for finding a way of recovering of the password.
Brute force attacks: - Hackers guess the password, user name and credit card based on the owner by means of trial and error.
Insufficient authentication: - A few website did not give authentication for the users for keeping the sensitive data or information.
Shoulder surfing attacks: - Hackers collects information of the user by hiding from the by means of camera or simple physical observation [9].
Viruses, worms, and Trojan horses: - a program of computer or piece of written code that destroy or interrupt the network system
Eavesdropping:- It is spying and gathering the copies of information without getting permission to the system.
ARP spoofing: - An attack whereby an attacker or intruders sends fake message address onto a network.
Denial of service attacks: -Make the systems as busy as possible by sending trash of data for rejecting the services
Man in the middle attack: - Attacker interrupts the message as soon as it is created to transfer through network by using encryption [9].
Ping of Death: -Transferring an abnormal or otherwise malicious ping to a networked system on a computer.

3. TOOLS AND TECHNIQUES

The solution proposed for those problem listed above is the different types of defense against Network Attack. Most of the weaknesses are due to poor design, implementation, and management, physical and human exposures, hardware and software, information interception [10].
Configuration Management: - The computer contained to the network must be executing up to dates, formation files must not have any known security holes, data should be backed up.
Firewall: - A network security tool that stands between local network and internet to prevent most network attacks by filters trafficking [11]. Depend on filtering firewalls are three types that are: - IP level, Packet level and TCP or application level. It has its own limitation but is useful when it configured by denying all anything that is not allowed.
Encryption: - This method is used to transmit secure data without listening by the hacker by using scrambling with key.

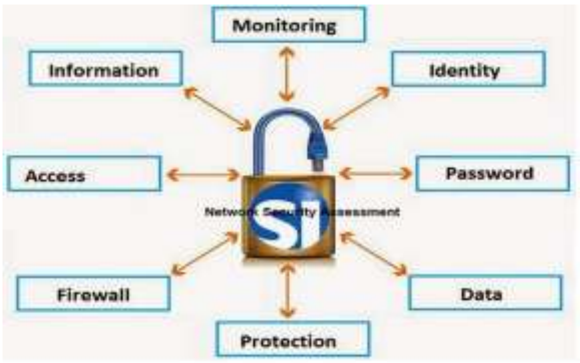

Figure 2: Network Security Solution Assessment [12]

Defense against DOS Attacks: - This method uses technologies such as, intrusion detection systems, firewalls, and enhanced routers to monitor incoming connections and outgoing connections and to protect the network by being between internet and server [13].
Vulnerability Testing: -All open ports, outdated firewall rules and faulty and outdated software should be closed [14]. It uses port scanner to differentiate the vulnerable resource over the network.
Secure Sockets Layer: - Launching a secure connection between the browser and the server.
Secure HTTP (SHTTP): -Implemented to secure web pages and their contents.
Virtual Private Network: -It is a method to pass traffic on an unsafe network.
E-Mail Security: - By using some strong encryption so that they cannot be read.
Turn off Ping Service: - Eliminating a remote user's ability to accept a response from a ping request [15].
Close unused ports: - keeping your computer secure from undesirable outside communication by the help of firewall.
Bind IP To MAC Address: - By binding IP address with the system MAC address, we can deny the out-sider.
Use Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): - Show a network or system attack by someone trying to break into or compromise a system and taking immediate action.
There are also different kinds of methods or countermeasure for the attacks especially for a layer of sensor network [16].

- ✓ Frequency hopping and code spectrum for jamming
- ✓ Tamper-proofing the physical package of node for Tampering or destruction
- ✓ Using error correcting codes for Collision
- ✓ A rate limits to the MAC admission control for Exhaustion
- ✓ Usage of small frames for Unfairness
- ✓ Anode can limit itself in accepting connection for Interrogation
- ✓ Scheduled into sleep mode for some time for Misdirection and Internet Smurf Attack
- ✓ Use Geo-Routing protocols for Sinkhole
- ✓ Design routing protocols for Wormhole
- ✓ verify the bi directionality of a link
- ✓ Under limit the number of connection for Flooding
- ✓ Authenticate the package which are communicating for De-synchronization

Some of the mechanisms are for securing network is, installing an updatable antivirus program, email scanning drivers, network checking tools, internet admission policy and other [16]. Network Administrator and security specialists are responsible for preserving the computer network safe.

4. CONCLUSION

As Internet is very important for our day to day activities we need to strengthen the security of network to safe the transmitted data over the internet. For the sake of safety and security of our network we have a lot various mechanisms we should rely on. Additionally, we should also use the network properly and use the security mechanisms listed above. If someone wants do some aspects of security to the network, the other aspect of network communication is may be affected. So we should be cautious when we implement the security for network communication.

REFERENCES

[1] Kartikey Agarwal, Dr. Sanjay Kumar Dubey, “Network Security : Attacks and Defence”, International Journal of Advance Foundation and Research in Science & Engineering, vol. 1, Issue 3, 2014

[2] Vandna, Dr. Ritu Sindhu, “Network Security: Attacks, Tools and Techniques”, International Journal of scientific research and management, Vol. 3, Issue5, 2015

[3] Mr. Prasad Mahajan, Miss Priyanka Bhute, “A Survey of Wireless Sensor Network Security”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 7, July 2015

[4] Anupriya Shrivastava, M A Rizvi, “Network Security Analysis Based on Authentication Techniques” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014,

[5] Anupriya Shrivastava, M A Rizvi, “Network Security: Attacks & Component”,International Journal of Research In Science &

Engineering,Vol. 3, Issue. 6, June 2014

[6] Casimer DeCusatis, Marcus, Anthony Sager, "Identity-based Network Security for Commercial Blockchain Services" IEEE Annual Computing and Communication Workshop and Conference, pp 474 – 477,2018

[7] Jason A. Villaluna; Febus Reidj G. Cruz,"Information security technology for computer networks through classification of cyber-attacks using soft computing algorithms", IEEE 9th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management, pp 1-6, 2017

[8] PCTECH, "Types of Security Threats and Network Attacks and their Counter Measures", Dec 2016
https://www.pctech24.com.au/blog/types-of-security-threats-and-network-attacks-and-their-counter-measures

[9] John E. Canavan,"Fundamentals of Network Security",Library of Congress Cataloging-in-Publication Data, Boston London, 2001

[10] Li CHEN,Web Security : Theory And Applications,School of Software,Sun Yat-sen University, China.

[11] R. K. Khalil, "A Study of Network Security Systems," IJCSNS International Journal of Computer Science and Network Security, 2010.

[12] SiConsult "Perimeters to Define Enterprise Network Security", Feb 2015
http://si-consult.blogspot.in/2015/02/five-perimeters-to-define-enterprise.html?spref=pi

[13] M. Eian, "Fragility of the Robust Security Network: 80211," Norwegian University of Science and Technology, 2011.

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

[15] William Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall publisher, USA, Nov 2005

[16] H. Erdem and A. Özgür, "A Review of KDD99 Dataset Usage in Intrusion Detection and Machine Learning Between 2010 and 2015," PeerJ Preprints, 1-22, Apr. 2016