ISSN 2229-3531 (Print)
JCIT Vol. 9(5), 50-54 (2018). Periodicity-2-Monthly
ISSN 2455-9997 (Online)

JOURNAL OF COMPUTER & INFORMATION TECHNOLOGY
An International Open Free Access Peer Reviewed Research Journal of Computer Science Engineering & Information Technology
website:- www.compitjournal.org
Estd. 2010

Network Security Attacks and Defence

PRATISHTHA SAXENA[1], VIJAY TIWARI[2]

Centre For Advanced Studies, Aktu, Lucknow (India)
Corresponding Author Email: 7mcs010@gmail.Com; Vktiwari@cas.res.in
http://dx.doi.org/10.22147/jucit/090501

Acceptance Date 27th September 2018 **Online Publication Date 2nd October, 2018**

Abstract

Network security plays an important role in our today's world of internet. Now-a-days everything of our life is connected to the internet, so network security is more important. It is important in military, government, organizations, and even our daily life. So, we should have knowledge about the attacks. What types of the attacks should be happened. Having the knowledge, how the attacks are executed we can protect ourselves. Now different type of methods is adopted to bypass it. The structure of internet allowed to occur many threats itself. The entire field of network security is very huge and in changing stage. The range of the study enclose the current development in network security and attacks. This paper briefly outlines the concepts of network security, different attack methods which are used, as well as different defense mechanisms against them.

Keywords: DOS ATTACK, ENCRYPTION, FIREWALLS, PORT SCANNING, SHTTP, SSL, VPN.

Introduction

It may seem wildly to ask the question, "Why is network security important?". It has many reasons such as to protect company assets, to gain a competitive advantage, to comply with regulatory requirements and fiduciary responsibilities etc. Now a day's digitalization is playing an important role and integration of digital technologies into our daily lives. In this digital generation people becoming more active on the internet and it is growing at a high rate. In our present world internet is becoming more extensively used. Internet is accessible everywhere in our houses, organizations, military, mobiles and now in even cars also, everything is connected to the internet and if any unauthorized person or attacker is able to acquire access this network then they can not only theft our confidential data, they can have modified our data and can easily mishmash up our lives. Digitalization is playing a leading role in everyone's daily life. But along with the development in the networking several threats attacks, Trojan Horses, DOS, DDOS attack have also risen drastically. So now the main issue is to secure the network.

2. Typesof Security Attacks

2.1. Passive Attacks

In Passive Attack the attacker gathers the information but does not modified the message stream in any way and does not perform any action. These attacks are easier to realize but difficult to detect. The attacker does not make any modification or exchanged information. One of the example is plain text and in which the attacker already knows the plain text and cipher text[8].

Properties of Passive Attacks :

Interception: The data passing through a network can easily be snuffled and thus attacking the confidentiality of the user, such as eavesdropping, "man in middle" attacks.

Traffic Analysis:In this the attacker analyses the traffic.This is also a confidentiality attack.

2.2. Active Attacks :

Active Attack is one in which the attacker may transmit message and modify message in transmit or delete selected message from the wire. An attacker tries to remove or modify the messagetransmitted on the network. Active attacks are Tampering, Selective Forwarding, Sybil Attack, Jamming, Blackmail Attack, Identity Replication Attack, Spoofed Routing Information, Flooding, Wormhole attack etc.[8]

Properties of Active Attacks :

Interruption: It avoids authenticated user form accessing the website. It attacks availability, such as DOS attack.

Modification: In this the data is altered mostly during the transmission. It is an integrity attack.

Fabrication: Creating specious items on a network without original authorization. It is an authentication attack.

DOS Attack :

Denial of Service (DOS) attack is a cyber-attack. Now-a-day's DOS attack has become a crucial threat for network security cause behind it that it does not require much time and planning as compared to other attacks. It is affordable, for network attacking it has efficient method. In short, this type of attack can be launched easily. They are cheaper to execute. With the help of network tool 'Trinoo' can easily be download from internet by this anyone can execute an attack. DOS attacks usually work by exhaust the targeted network of bandwidth, application buffer, service buffer, CPU cycle etc.[9].

Different Types of DOS Attacks :

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 sourceand thus jam-packed to the victim's network. Fig 01.

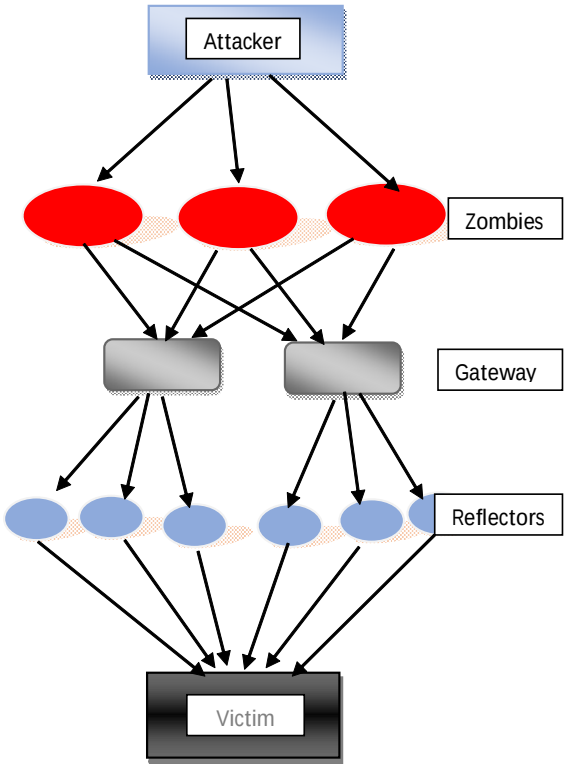

Fig 01. ICMP Smurf Flooding[6]

TCP DOS: 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[9].

UDP Flooding: Currently many networks use TCP and ICMP protocols to avoid DOS attacks but an attacker can send large number of packages, so as UDP overwhelming the victim and averting any new connection.

DDOS Attacks :

Now many attacks are based on the Distributed Denial-of-Attack (DDOS). In this, attack is executed by sending a large number of packets to a targeted network through the use of some compromised machine distributed through the internet. DDOS attack is very cheap and easier to perform. This is executed when the multiple systems on

the internet exhaust the bandwidth and resources of victim's system by sending a large number of packets. DDOS attack involved four entities attacker, agent, master control program and victim. In July 2001 some major website of United State and south Korea will also get affected by this attack.

3. Security Principle and Attack :

Three basic security principles are Confidentiality, Integrity and Availability[4].

3.1. Confidentiality :

Confidentiality mean to protect our data from unauthorized user and attackers. When an unauthorized user read or steal our data then our confidentiality break, and we loss the data confidentiality. The very important attribute is confidentiality.

Confidentiality Attack :

Passive attacks are done by the Confidentiality

3.1.1. Dumpster Diving: The attacker getssecret information from un-shared papers unloadedin office bins.

3.1.3. Wire Tapping: If the location of vicinity target network is close to the attacker. Then (s)he can tapinto network lines and pry over secret messages.

3.1.4. Packet Capture: The attacker can easily capture the data packets travelling across the network. Therefore, bysystematically intercepting a hub with which the victim is connected, or by tricking the packets to flowthrough his system by acting as a honeypot, the attacker can obtain a lot of sensitive information.

3.2. Integrity :

Integrity of data or information refers to protecting information from any unauthorized modification. When the information or data is modified in unexpected ways by the unauthorized user, then the result is known as loss of integrity. Integrity is important for critical safety and financial data used for activities such as electronic funds transfers, financial accounting.

Integrity Attacks :

Integrity attack is based on the confidentiality attack, except that the attacker does not stop after snooping, information or data, and he tries to modify the information or data.

3.2.1. Salami attack: Salami attack is a series of smaller attacks, which taken togetherengenders a devastating consequence.

3.2.2. Botnet attacks: The attacker writes a piece of software called network robot ("botnet in short") and injects into the target system. This malicious piece or code makes the whole system infected and act like a slave,thereby compromising the integrity and confidentiality of huge amounts of data.

3.2.3. Password attacks: this is done using Trojan horse, packet capture, key logger application or dictionary attacks to obtainuser credentials from the system.

4. Types of Network Security :

4.1. Security by Obscurity:It works on stealth approach. Its basic working principle is that if no one knows the system exists than it would not be attacked. The main drawback of it is that, it would not be a long-term solution and if at one time the system is discover it will be completely vulnerable[1].

4.2. The Perimeter Defence: It works in organizations. The organization harden network security by using networking tools such as behindthe firewall hide the network, separating the network from untrusted network etc. In case of inside attack this approach does nothing. Once the Perimeter Defence break, the inside system is fully vulnerable.

4.3. The Defence in Depth: It is the best way to protect the system but difficult to perform. In this approach, each system is hardened and is monitored thus acting like an island. It defends itself against the attacks.

The different types of network security are as follows Fig 02.

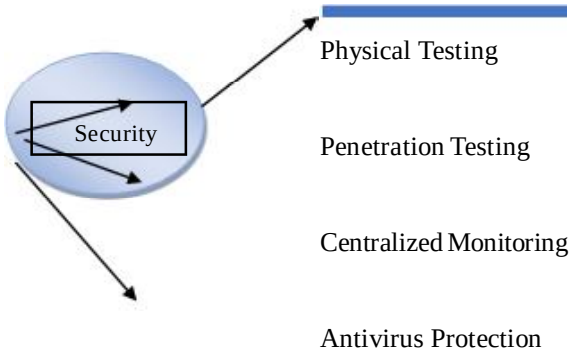

Fig: 02

5. 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 is 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:

5.1. Configuration Management :

Against network attack configuration management is a pivotal part of defence. It is important as decent firewall to defend the system. So, when the network setup is completed its default ID's, address, login must be altered as soon as possible all this information are available on the internet so anyone can view. Install the updated patches as soon as they are accessible. Configuration files shall not have any known security holes, so that all data is backed away in a secure manner. Network managers take the advantages of scanning tool such as Cyber Cop Scanner. Cyber Cop Scanner with Auto Fix knowledge 720 does vulnerability check, firewall scanning, OS detection has improved the performance. It also allows Security professional to repair security holes discovered during an audit. It has capability to test and thus information repair over 700 network protocol and application vulnerabilities.

5.2. Firewall

Firewall is the main security tool. This is the wall between local network and the Internet. This wall filters the traffic and prevent from network attacks. Most of firewall are not designed to detect and prevent a DOS attack. The software firewall can be considered a gateway that provides the only point of access between user's home network and internet. Firewall also reduces the speed of network. The firewall stops unauthorized network traffic across an unsecure network or a private network. If the firewall is configuring correctly only when it works. If firewall is not configured correctly then it may allow unauthorized users to enter. User defined security rules, on this basis firewall allow and drop the packets.Three different type of firewall's depending on filtering.

At IP level
Packet level
TCP or application level

5.3. Encryption

By encryption mechanism we prevent the data. If attacker listen the data it will just be garbage to them without the correct key because without key the encrypted date cannot be decrypt. Different encryption methods are used such as HTTPS or SHTTP during transmission of data between the client and server. It will prevent from man-in-middle attack and also prevent from any sniffing of data.

5.4. Defence Against DOS Attacks

Many technologies such as Intrusion Detection system, firewall etc. have been developed to prevent from DOS attack. They monitor the incoming-outgoing connections and analyses the traffic and access control. By these they protect the network.

Intrusion Detection System make a log file of incoming and outgoing connections and these logs can compared to baseline traffic to detect potential DOS attack. If they monitor the high rate traffic on the server it can alert of a possible ongoing DOS attack such as TCP flooding (TCP DOS attack). Firewall also protect us from DOS attack. It can be used to allow or deny certain packets, ports, IP address etc.

Security measures can also be employed in routers which can create another defence line away from the target, so even if a DOS attack takes place it won't affect the internal network. Service providers can also increase the service quality of infrastructure. Whenever a server fails a backup server can take its place, this will make effect of DOS attack negligible. If the service providers are able to distribute the heavy traffic of a DOS attack over a wide network quickly it can also prevent DOS attacks, however this method require computer and network resources and they can be very costly to provide on daily basis as a result only very big companies opt for this method[7,1].

6. Encrypting The World Wide Web :

Three basic security concepts are important Confidentiality, Integrity and availability. Our communication on the web should be consistently encrypted. The main purpose of privacy, confidentiality and availability is the information security. On the web our communication should be consistently encrypted. By this, it will reduce the number of attacks and avoid anyone to view the ongoing transmission. Through encrypting the world wide web, we can secure data (Information) over the network. We send encrypted data over the network, so it is hard for an attacker to decrypt the data. By using encryption, we can secure the data over network. The essential 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[1],[17]. Using this mechanism, we can extend us,

6.1. Secure Sockets Layer :

SSL is Standard Secure Technology which is made for establishing a secure connection between the web server

and browser. SSl create an encrypted link between the web browser and web server. It occupies both asymmetric and symmetric keys encryption which transfers data in a secure mode over a network. When SSL is deployed in a browser it initiates a secure connection between the browser and the web server. It's like an encrypted tunnel in which the data proceed securely. If Attacker listening data on the network cannot Decrypt the data, which is passing through the tunnel. It provides integrity using hashing algorithms and confidentiality usingencryption techniques.

6.2. Secure HTTP (SHTTP) :

It's a 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 differently, but secure tunnel 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[1].

Conclusion

As internet has become a herculean part of our daily life. So, network security is very important. As much the millions of the user over all the world are connecting to the internet. It attracts a lot of criminals to do cyber-attacks. Now every country forwarding their steps in the direction of Digitalization. As India starts a mission to do Digital-India. Information technologies development and Internet service become the most important aspects in the development of any nation. So cyber security has a very prominent role in the area of nation's security. In this paper we provide a detail view of network security, various attacks and the defence mechanisms against the attacks. The development in network security is not very breathtaking. Many attacks can be easily protected by the following many simple methods which is discussed in this paper.

References

1. R. E. Mahan, "Introduction to Computer & Network Security," "INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS," " Vol. *5* Issue 5, Pg.: 46-52 May 2017", Washington State University, (2000).
2. M. M. B. W. Pikoulas J, "Software Agents and Computer Network Security," "International Research Journal of Computer Science (IRJCS)," ISSN: 2393-9842 Issue 05, Volume 4" Napier University, Scotland, UK 4th may (2017).
3. 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).
4. Q. Gu, Peng Liu, "Denial of Service Attacks," International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)", Vol. *3*, Special Issue 20, April 2016, Texas State University, San Marcos.
5. A. R. F. Hamedani, "Network Security Issues, Tools for Testing," International Journal of Engineering Research & Management Technology" , Page 195 Volume *1*, Issue-5 ISSN: 2348-4039School of Information Science, Halmstad University, (2010).
6. Li CHEN, "Web Security : Theory And Applications, School of Software, Sun Yat-sen University," " China.
7. J. E. Canavan, "Fundamentals of Network Security, Artech House Telecommunications Library", International Journal of Modern Trends in Engineering and Research (IJMTER)
8. Volume 02, Issue 06, [June – 2015] ISSN (Online): 2349–9745; ISSN (Print): 2393-8161,".
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. S. Lakshminarasimman," Detecting DDoS Attacks using Decision Tree Algorithm," 2017 4th International Conference on Signal Processing, Communications and Networking (ICSCN -2017), March 16 – 18, 2017, Chennai, INDIA.
11. https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.
12. https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad.
13. https://www.digicert.com/ssl/.
14. S. Shaji, "Anti Phishing Approach Using Visual Cryptography And Iris Recognition," IJRCCT, Vol *3*. No. 3pp. 88-92, (2014).
15 https://hubpages.com/technology/Types-of-Network-Attacks.
16. KaranbirSingh ,"Distributed Defense: An Edge over Centralized Defense against DDos Attacks "Research Scholar, Dept of R.I.C, I. K. Gujral Punjab Technical University, Jalandhar, Punjab, INDIA.
17. Saba Zaidi1," USING ENCRYPTION FOR NETWORK SECURITY," Volume 02, Issue 06, [June – 2015] ISSN (Online): 2349–9745; ISSN (Print): 2393-8161.