ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Study on Different Attacks on Transport, Network and Data Link Layer in TCP/IP

S.Joshna, N.Nishanth

Assistant Professor, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India

PG Scholar, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India

ABSTRACT: The representation of the network attacks generally to adopt computer networks as transportation media that to transfer the intrusion attack to the communication system itself. The individual vulnerabilities of hosts on a network can be combined by an attacker to gain access that were not be possible if the host systems were not interrelated. The TCP/IP protocol suite is exposed to various attacks which are ranging from password sniffing to denial of service. The Topological Vulnerability Analysis (TVA) extending this by searching for sequences of dependent vulnerabilities, which is distributed among various networks. It will focus mainly on network attack which are occurred around the TCP/IP (Transmission Control Protocol/Internet Protocol).

KEYWORDS: Transport layer, Network layer and Data link layer.

I.INTRODUCTION

The network security system is protective towards the website servers in various forms of attacks. By changing the network architecture many companies employ firewall and diverse policies to safeguard them. Network security plays a vital role in the part of military, government, education and business. Various forms of network attacks have been found up till now, each of them employs one or more security vulnerabilities in the TCP/IP protocol specifications. Several possible solutions to this attack have been proposed by others and some implemented. TCP/IP is the most widely used protocol suite, which was developed under the sponsorship from DRPA (Defence Advanced Research Projects Age TCP/IP defines a set of rules to allow computers to communicate over a network. It specifies how data should be formatted, addressed, shipped, routed and delivered to the right destination. There are 3 layers which are going to use in the TCP/IP model they are transport layer, network layer, data link layer.By using all those three layers various types of attacks are to be implementing. They areSYN flooding attack,Session hijacking, SSL Stripping, wormhole attack, black hole attack, Byzantine Attack, ARP spoofing, MAC flooding, DHCP attack are the attacks.

II.VARIOUS ATTACKS IN OSI LAYERS

Attacks on ad hoc networks can be categorized into two categories namely passive and active attacks. It can be active when it tries to alter system resources or affect their operation. A passive attack attempts to make use of data from the system but does notaffect system resources. The necessity of an confidentiality can be violated if it is an opponent and an attack should led to a security incident i.e. a security event that involves a security violation.

In other words, a security-relevant system event in which the system's security policy is violated. There is a way to overcome asuch problems is to use powerful encryption mechanisms to encrypt the data which is being transmitted, thereby making it difficult for eavesdroppers to obtain any useful information from the data. In order to detect various attacks, a number of countermeasures can be set up at administrative, procedural and technical levels.Computer emergency response team, information technology security check and intrusion detection system are some of the examples.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Table.1 Security attacks on Each Layer of the internet model

LAYERS	ATTACKS
Transport layer	Session hijacking, SYN flooding, SSL stripping
Network layer	Wormhole, Blackhole, Byzantine, flooding, resource consumption.
Data link layer	ARP spoofing, MAC flooding, DHCP attacks

III.TRANSPORT LAYER

The transport layer's tasks include end-to-end message transfer capabilities independent of primary network, laterally with error control, fragmentation and flow control. The transport layer uses common transport protocols to enable network communications. This may include the Transport Control Protocol (TCP) and Universal Data Protocol (UDP). The objectives of TCP-like Transport layer protocols in WSN include set up of end-to-end connection, end- to-end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection.

The purpose of Transport Layer protocols such as TCP is to provide reliable exchange of data between two endpoints equally. The word “reliable” means that a distribution endpoint make sure that the data essentially arrived at the receiving endpoint. Such a reliable service is provided by TCP (Transmission Control Protocol). Protocols such as UDP (User Datagram Protocol) in the Transport Layer take care of those needs in internet communications. Though, a WSN has a higher channel error rate when compared with wired networks.

A. *SYN Flooding Attack:*

The SYN flooding attack is a denial-of-service attack. The attacker generates a large number of half-opened TCP connections with a victim node, but never concludes the handshake to fully open the connection. There are two nodes to communicate using TCP, they should start a TCP connection using a three-way handshake. The three messages exchanged during the handshake allow both nodes to absorb that the other is ready to communicate and to agree on primary sequence numbers for the conversation. During the attack, a malicious node sends a large amount of SYN packets to a victim node, spoofing the return addresses of the SYN packets. The SYN-ACK packets are sent out from the victim right after it receives the SYN packets from the attacker and then the victim waits for the reply of ACK packet. Without receiving the ACK packets, the half-open data structure remains in the victim node.

B. *Session Hijacking:*

Session hijacking is a critical error and gives an chance to the malicious node to behave as a legitimate system. All the communications are authentic only at the beginning of session setup. The attacker may take the advantage of this and commit session hijacking attack. At first, he or she spoofs the IP address of target machine and controls the correct sequence number. After that he performs a DoS attack on the victim. As a result, the target system becomes absent for some time. Thus the attacker imitates the victim node and continues the session. Hijacking a session over UDP is the same as over TCP, except that UDP attackers not to concern about the overhead of dealing sequence numbers and other TCP mechanisms. Since UDP is connectionless, edging into a session without being detected much easier than the TCP session attacks.

C. *SSL Stripping:*

Various attacks attempt to eliminate the use of Secure Socket Layer/Transport Layer Security (SSL/TLS) overall by modifying unencrypted protocols that request the use of TLS. These attacks are known together as “SSL Stripping” (a form of the additional generic “downgrade attack”) and were first presented by Moxie Marlinspike. In the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

framework of web traffic, these attacks are only effective if the client initially contact a web server using HTTP. In SSL Strip, all the traffic flow from the victim's machine is routed through a proxy designed by the hacker and can be thought as a Man-In-the-Middle (MITM) attack. So, let us adopt that you are an attacker and able to form a linking between the victim and server. This means that all the traffic from the victim's machine will flow via your computer that serves as a proxy server and moreover the result will be in a certificate error or the encrypted traffic will be captured.

IV.NETWORK LAYER

The network layer exploits multiple common protocols to perform routing on the network. Protocols comprise of the Internet Protocol (IP), packet sniffing and DoS attacks such as ping floods and ICMP attacks. To decrease the risk of these types of attacks, routers should be hardened, packet filtering controls should be used and routing information should be controlled. A major job of the Network Layer protocols is to take care of network addressing. When a protocol in this layer collects a byte stream referred to as a datagram, it attaches a "header" with byte stream that says the protocols in the lower layers as to where accurately the data is supposed to go in the internet. Let's say that a protocol in this layer puts out a packet for forward transmission by sending it to a lower layer protocol and let's assume that a router along with the destination is unable to receive the packet because its registers are full. By attacking the routing protocols, attackers can absorb network traffic, insert themselves into the path between the source and destination, and thus regulate the network traffic flow. The attackers can create routing loops, present severe network congestion, and channel contention into certain areas.

A. *Wormhole Attack:*

In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network. This tunnel between two colluding attackers is denoted as a wormhole. Wormhole attacks are severe threats to WSN routing protocols. It could be recognized through wired link between two colluding attackers or through a single long-range wireless link. In this system of attack the attacker may form a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.The wormhole attack is mostly dangerous for many ad hoc network routing protocols. For sample, when a wormhole attack is used against an on demand routing protocol such as DSR or AODV, the attack could avoid the discovery of any routes other than the wormhole.

B. *Black HoleAttack:*

In this occurrence, an attacker uses the routing protocol to publicize itself as having the shortest path to the node whose packets wants to intercept. An attacker listen the desires for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a response that consisting of an extremely shortest route. If the malicious reply reaches the initiating node before the reply from the authentic node, a fake route gets created. Once the malicious device has been able to insert itself between the interactive nodes, it is able to do anything with the packets passing among them. It can drop the packets between them to accomplish a denial-of-service attack, or otherwise use its place on the route as the first step in a man-in-the-middle attack.

C. *Byzantine Attack:*

In this attack, a compromised middle node or a set of compromised intermediate nodes works in collusion and carries out attacks such as forming routing loops, promoting packets on non-optimal paths and selectively dropping packets. Which results in disruption or degradation of the routing services. It is hard to notice byzantine failures. The network would seem to be functioning normally in the viewpoint of the nodes, though it may actually be displaying the Byzantine behaviour.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

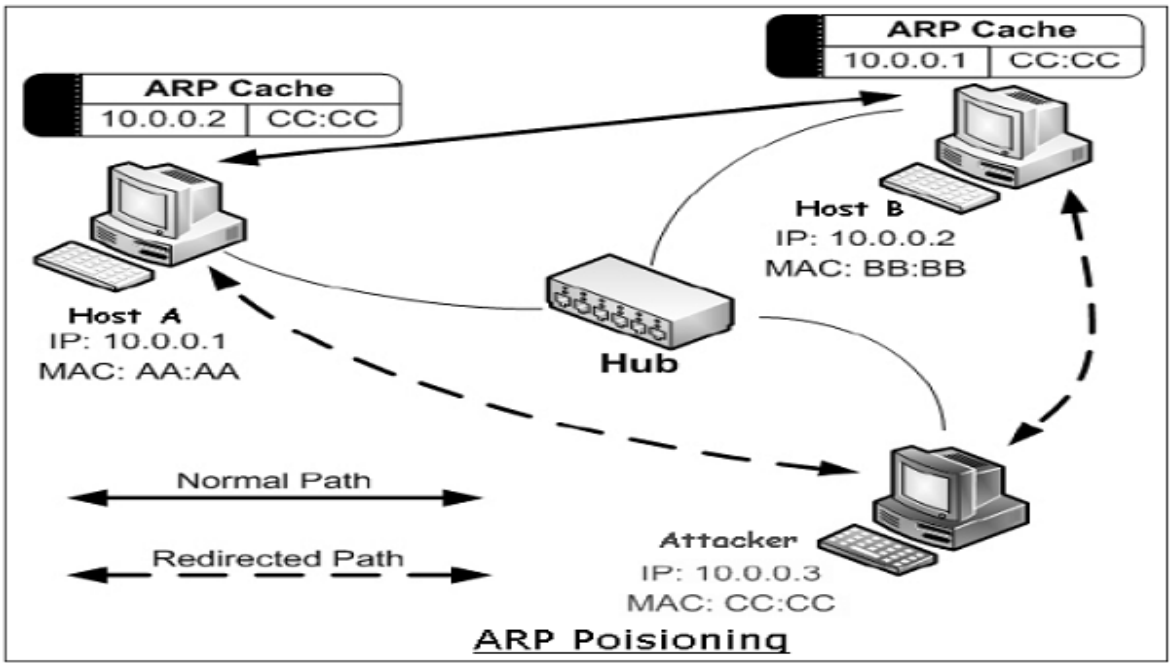
V. DATA LINK LAYER

The link layer focuses on the methods for delivering data blocks. Normally, this consist of switches utilizing protocols such as Spanning Tree Protocol (STP), which is used throughout networking for dynamic IP assignment. The Mobile Ad Hoc Network (MANET) is an open multipoint peer-to-peer network architecture. Specifically, one-hop connectivity among neighbours is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer's protocols. Perhaps the most important protocol at the Data Link Layer is the Media Access Control (MAC) protocol.

The MAC protocol provides the addressing mechanism for data packets to be routed to a particular machine in a LAN (Local Area Network). The MAC protocol also uses sub protocols, such as the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol, to decide when the machines connected to the same communication medium, such as a LAN, should communicate.Wireless medium access control (MAC) protocols have to coordinate the transmissions of the nodes on the common transmission medium.

A. *ARP Spoofing:*

The Address Resolution Protocol (ARP) translates logical Layer 3 addresses (IP Addresses) to layer 2 addresses (physical MAC addresses). When a host machine needs to find a physical Media Access Control (MAC) address for an IP address, it transmissions an ARP request. The other host that owns the IP address sends an ARP reply message with its physical address. On a switched network that relies on the physical address for delivery, clients must continue with an updated table of logical-to-physical address bindings. Each host machine on network sustains a table, called 'ARP cache'. The table holds the IP address and associated MAC addresses of other host on the network. Since ARP is a displaced protocol, every time a host gets an ARP reply from additional host, even though it has not sent an ARP request, it accepts that ARP entry and updates its ARP cache. The process of altering a target host's ARP cache with a forged entry known as ARP poisoning or ARP spoofing. ARP spoofing may allow an attacker to masquerade as legitimate host and then intercept data frames on a network, modify or stop them.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

B. *MAC Flooding:*

Denial-of-service attacks are intended to prevent a network from carrying legitimate user's data. An occurrence of this type causes a network component to stop forwarding packets to them improperly. Every switch in the Ethernet has a Content-Addressable Memory (CAM) table that stores the MAC addresses, switch port numbers, and other data. The table has a fixed size. In the MAC flooding attack, the attacker floods the switch with MAC addresses using forged ARP packets until the CAM table is full. Once CAM is flooded, the switch goes into hub-like mode and starts broadcasting the traffic that do not have CAM entry. The attacker who is on the identical network, now receives all the frames which were intended only for a specific host. Port security is a dynamic feature that can be used to limit and identify the MAC addresses of the stations that allow access to the same physical port.

C. *DHCP Attack:*

Dynamic Host Configuration Protocol (DHCP) is not a datalink protocol but solutions to DHCP attacks are also useful to link layer attacks. DHCP is used to dynamically allocate IP addresses to computers for a explicit time period. It is possible to attack DHCP servers by causing denial of service in the network or by impersonating the DHCP server. In DHCP spoofing attack, the attacker can deploy a rogue DHCP server to provide addresses to the clients. Here, the attacker can deliver the host machines with a rouge default gateway with the DHCP responses. Data frames from the host are now directed to rouge gateway where the attacker can intercept all package and reply to actual gateway or drop them. When a client without an Internet protocol (IP) address enters a network, he may choose to contact the DHCP server and request an address. If the network supports DHCP, the server will respond with an address and the lease period of time for the address. An attacker may wish to take advantage of DHCP by flooding the network with requests for addresses.

VI. CONCLUSION

This paper described the concept of OSI layers with various attacks. Security management is one of the key functional areas in open systems network management. The OSI Reference Model is used as a basis to present the security threats, security services and mechanisms which are to be managed. The model can be used to facilitate in threat identification and decision-making process by focusing on attack scenarios that illustrate vulnerable nodes, threats and shortest attack paths to the attacker's goal. The model can be used as part of risk management practices to improve security awareness through different attack scenarios and manage all system risks. Each attack is classified based on seve1ral factors, e.g. its type, likelihood of occurrence. Mainly various types of attacks starting from physical layer and data link, network layers subsequently variety of attacks at transport layer with some effective suggestions protection against those attacks.

ACKNOWLEDGENMENTS

Our sincere thanks to the experts supported this work and their valuable comments.

REFERENCES

1. Danny McPherson, BGP Security Techniques, APRICOT, 2005.
2. Hralambos Mouratidis, Paolo Giorgini, Gordon Manson, Using Security Attack scenarios to Analyse Security During Information System Design, in the 6th International Conference on Enterprise Information Systems, 2004.
3. Simon Hansman, Ray Hunt, A taxonomy of network and computer attacks, Computers & Security,DTD5, 2004.
4. L. Zhou and Z. Haas, Securing Ad Hoc Networks, IEEE Network Magazine Vol.13 No.6 (1999) pp. 24-30.
5. S. Yi, P. Naldurg, and R. Kravets, Security Aware Ad hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC, 2002.
6. Kendall, Kristopher, "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems", Masters Thesis, MIT, 1999.
7. Lippmann, R., et al., "The 1999 DARPA Off-Line Intrusion Detection Evaluation", Computer Networks 34(4) 579-595, 2000.