www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 3 March 2013 Page No. 692-695

Study Of Different Attacks On Network & Transport Layer

Deepti Rajwal, Deepali Band, Prof. Atul Yadav

Department of Information Technology Rajendra Mane College of Engineering & Technology
Ambav (Devrukh)

Abstract— this paper represents Network attacks generally adopt computer networks as transportation media to convey the intrusion or even attack the communication system itself. We will put our focus mainly on the network attacks happened around the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite, which are the most widely used communication protocol and the de facto standard among the Internet society.

Keywords— TCP, Firewall, Session Hijacking, IP Spoofing, IP.

I. Introduction

The TCP/IP protocols consist of a four layer model, also known as the DARPA model. The four layer of the DARPA model are Application layer, Transport layer, Internet layer and Network Interface layer. Each layer in the DARPA model corresponds to one or more layers of the OSI model. The TCP/IP Protocol consists of four layers:

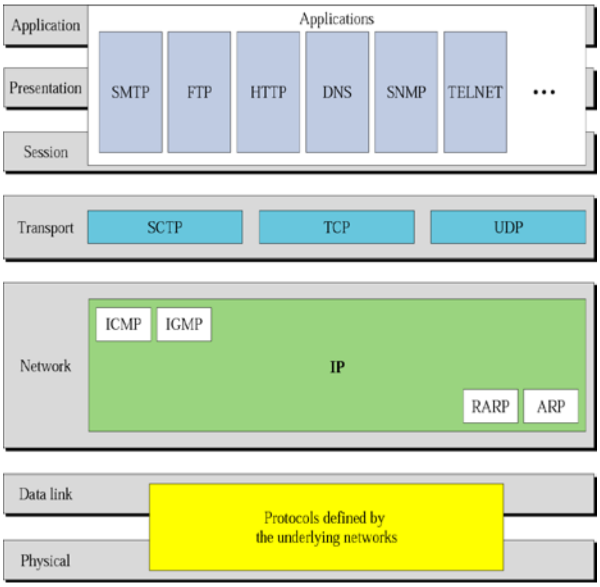

Fig. 1 TCP/IP Model

Network Interface layer: The Network interface layer is basically responsible for placing the TCP/IP packets on the network and receiving the packets from the network. The Network Interface layer encompasses the Data link layer and the Physical layer of the OSI model.

Internet layer: The Internet layer is responsible for the addressing, packaging and routing functions. The Internet layer is equivalent to the Network layer of the OSI model. The main protocols of the Internet layer are:

IP: It is a routable protocol responsible for IP addressing, routing and fragmentation.

Address resolution protocol (ARP): The ARP is responsible for the resolution of the internet layer address to the network interface layer address such as a hardware address.

Internet control message protocol (ICMP): It is mostly responsible for displaying the error messages.

Internet group management protocol (IGMP): It is responsible for the management of IP multicast group.

Transport Layer: The Transport Layer is responsible for the session and datagram services. This Transport layer is equivalent to the Transport layer of the OSI model.

Application layer: This layer is responsible for providing the ability to access the services of the other layers, and defines protocols via which the data is exchanged. The main protocols in the application layer are HTTP, FTP and SMTP.

II. Transport Layer

Here we try to explain functions and attacks of specifically on transport layer. Transport layer use two protocol TCP (Transmission Control Protocol) & UDP (User Datagram Protocol) and attacker takes help this two protocol working function for attack. TCP stands for Transmission Control Protocol. TCP/IP is a most widely used protocol suit today. This protocol is available in the Network layer of OSI model, which is responsible for the process to process delivery of the whole data will be send by the sender. This is connection oriented protocol. A connection must be established between both ends of a transmission before sending of data.

Features of TCP:

- TCP provides proper process-to-process delivery of any message from one end to other end.
- It keeps track of which segments are transmitted or received.
- The bytes of data being transferred in each connection are numbered by TCP.
- It provides Flow Control.

TCP/IP protocol suit is structured in appropriate layers. It contains total five layers and having extra Optional Layer. Each segment consists of 20 to 60 bytes of header. If the header is of 20 bytes means it doesn't contain option layer. In all five layers it has different fields, which have their own functions. Each layer is of 32-bit.i.e 4 bytes. Also known as Transfer control protocol resides in Transport layer, TCP is a connection oriented approach which means that it builds connection between the client and the server and terminates it after its work is done. TCP performs the three way handshaking method for the establishment and termination of the connection.

Three way handshaking:

For the better understanding of this topic let's take a situation where client C wish to build a connection with host H for some data transfer. Now here C will send its SYN packet along with its own initial sequence number to H, telling H that it wish to establish a connection, after receiving the request from C, H will send back the SYN packet along with an acknowledgement ACK (SYN_ACK) and its own initial sequence number, after receiving the ACK_SYN the C will send an acknowledgment ACK, and will start its data transfer.

Here the final ACK sent by the client C is the confirmation that the connection has been established. Also there are times when the Client doesn't send any packet SYN but receives SYN_ACK from H, in such cases the Client use the RST (reset) connection packet.

UDP stands for User Datagram Protocol. It is unreliable, connectionless transport layer protocol. UDP doesn't having that much of functionality as compare to the TCP/IP. But, still it is powerful and simple. If sender wants to send any small message and do not care about the more reliability, so at that time he can use the UDP, it takes very less interaction between the sender and receiver than TCP. We can use it for small applications. E.g. DNS (Domain Name System).

III. ATTACKS ON TRANSPORT LAYER

1. *SESSION HIJACKING:*

Session Hijacking is commonly known as TCP session Hijacking is a way of taking over a secure/ unsecure web user session by secretly obtaining user's session ID and pretending to be the authorized user for accessing the data.

How it works and types:

Session hijacking works by taking advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. These attacks generally fall into three categories: Man-in-the-middle (MITM), Blind Hijack, and Session Theft. In MITM attacks, an attacker intercepts all communications between two hosts. With communications between a client and server now flowing through the attacker, he or she is free to modify their content. Protocols that rely on the exchange of public keys to protect communications are often the target of these types of attacks.

In blind hijacking, an attacker injects data such as malicious commands into intercepted communications between two hosts commands like "net.exe local group administrators /add Evil Attacker". This is called blind hijacking because the attacker can only inject data into the communications stream; he or she cannot see the response to that data (such as "The command completed successfully.") Essentially, the blind hijack attacker is shooting data in the dark, but as you will see shortly, this method of hijacking is still very effective.

In a session theft attack, the attacker neither intercepts nor injects data into existing communications between two hosts. Instead, the attacker creates new sessions or uses old ones. This type of session hijacking is most common at the application level, especially Web applications. Main features are:

-URL (Uniform resource locator)

-Cookies

-Session ID

The cookies stores the previous records of the users and the URL logs can give the current visited site, a hacker take benefits from it and hacks user's session ID through it, after doing that it pretends to be the authorized user and accesses the data. A cookie usually is a piece of text sent by a server to the web client and sent back unchanged by the client, each time it access the data.

1.1 Methods used to perform session hijacking:

1.1.1IP Spoofing: It basically means taking identity of someone else to perform some task, in this the attacker pretends to be the authorized user and access some confidential information, not only this, the attacker can even send some packets with malicious content to its target machine.

1.1.2 Session Side jacking: In Session side jacking the attacker reads the network traffic between the two parties, through packet sniffing method. The packet sniffing method is nothing but unethically viewing the packet data. Usually many websites use the SSL encryption for the login purposes; this prevents the attacker from attacking those login details. But this encryption method is not continued in the rest of the page therefore allowing the attacker to attack and view the network traffic and get access to the data.

1.1.3 Session Fixation: In this method the attacker changes the session ID of the user before the user login, thereby eliminating the need to hack the session ID.

1.1.4 Cross-site Scripting: A hacker creates a hyperlink which contains malicious content. Then this hyperlink is sent to the web application, so when the targeted user clicks on that web site this infected link is generated and when the user click on this link the malicious link is generated an infects user's data.

1.2 Methods to prevent Session Hijacking:-

- Regenerating Session ID after successful Login.
- Using a long random number or characters or string as session key.
- Encryption of data passed between the parties.

2. *TCP Land Attack*

In this attack the attacker sends a SYN packet to the host server which usually has an open TCP port. Now the main question which might strike your mind is that, how the server fails to identify the attacker and provides service to it instead. Well this is because the attacker spoofs the source IP address and present itself as an authorized user.

3. *UDP Flooding Attack*

UDP is a connectionless protocol and it mainly effects the server by flooding the server machine with countless requests, this makes the machine to think that the attacker (who pretends to be the authorized user) really needs service urgently and the server machine starts providing the services to the attacker, due to this the users who actually needs the service are often overlooked.

4. *TCP & UDP Port Scanning Technique*

Here the attacker performs the port scanning of various tools of the host machine in order to find the open ports on the machine. Once these ports are identified by the attacker, it starts attacking the machine.

5. *BIND DNS*

BIND stands for 'Berkley internet name domain' it is a popular DNS server. There are times when a particular BIND DNS server doesn't have the required data in such cases it communicates with other BIND DNS server and takes the information, but in such cases it does not filter the packets received from other servers. This gives the attacker chance to send some malicious content in the network, which can cause harm to the user and to the network as well. Also there are times when the attacker itself acts as the server, which misguides the user again.

6. *Mail Transport System*

It is the most common protocol used to send the e-mails. By default the SMTP port is 25, usually this port is used by the internet connections to receive e-mails. The attacker attacks this port to retrieve the needed information, and as it is a general port the packets which enter this port are generally no filtered, this also enables the user to send some malicious content.

IV. NETWORK LAYER

The main Network protocol is Internet Protocol (IP).This is responsible for delivery of individual packets from the source to destination. IP provides unreliable and connectionless service. IP has a particular Layered structure, in which having different fields. In this each packet have its header. In IP, packets are called as Datagrams. Header is 20 to 60 bytes in length. And in data, it will contain any message. IP contains important information source IP address, destination IP address, which helps both sender as well as receiver. Because of this datagram's can't go here n there, so it helps for delivery of datagrams.

V. ATTACKS ON NETWORK LAYER

We know that network layer is very essential for sending any data. It consists of different routers and many more different devices. Network layer is responsible for delivery of each packet from source to destination. When packets travels in network, at that time there are many chances to done attack on packets, different types of attacks are done are as follows.

1. *IP Spoofing*

IP spoofing is a one type of network attack, in which attacker take an IP address of another host and using that address it communicate with targeted host. They send packet with malicious content to targeted host. And they do not get identified. But targeted host is not aware about that, so he will accept the packet and give response back. The attacker can make attack till the targeted host is in active state otherwise can't. And in IP spoofing Attacker always should know sequence number of targeted host, because whenever at starting both sender and receiver wants to establish connection at that time they have to send their initial sequence number, and then only connection will established. If attacker gets exact sequence number then he can make attack on host.

Example, If Alice and bob want to communicate with each other. And attacker wants to make attack using IP spoofing, the attacker is done that he will take IP address of that Alice and established connection with bob, after identifying correct sequence number and send message to bob. At this stage bob doesn't know that Alice is an attacker, so bob will send response back to Alice.

2. *Packet Sniffing*

Packet Sniffing basically means viewing the packet data unethically. In this type of attack, attacker attack on IP traffic which occurs in network. He captures packets from network. Data from upper layers is encapsulated into IP packets, Sometimes what happens is, more no. of packets come into network because of some problem at receiver side like receiver may not be ready or the requests wasn't processed properly etc. So, at that time in network, packet traffic occurs. So, attacker takes advantage of traffic and using different protocols like SMTP, POP3, SNMP he will do attack on packets. It makes directly attack into internal structure of protocol. For securing our data, we can't directly avoid it, but we can reduce this attack. Instead of using hubs, we can use switches.

3. *RIP Routing Attack*

RIP stands for Routing Information Protocol. When number of packets sends from source to destination at that time we use router, because router gives the shortest convenient path to reach destination. For that each and every router has their routing tables. RIP is used to distribute routing information within network such as advertising route from the local network shortest path. Original version of RIP has no built in authentication and information content in RIP packet is used without verifying it. Each router advertises their routing table after one particular time. In this, attacker make it's fake router in which he make manual table and then he can forge an RIP packet claiming that his has shortest and convenient path out of the network. So, all packets sent out from network would be then routed through that host. And that time attacker makes changes into that packet or may be dropped. After work is done by attacker using that fake router, that router get deactivated. If at that time other router wants to access that table, but actually it was not there.

4. Fragmentation Attack

Fragmentation is done for easily travel of data. If data is large so it is little bit difficult and risky to reach at destination. For that fragmentation is best option. Large amount of data is converted into small packets. And it is easily distinguish by breaking it into packets. Attacker directly attack on packets. If attacker makes changes in any one packet of data, then whole data will change. And receiver received modified wrong data. The fragment can even overlap when reassemble which further exacerbates this problem.

5. ICMP Attack

ICMP stands for Internet Control Message Protocol. It is used to send error message. If requested service is not available or that host or router could not be reached, then the ICMP does not authenticate packets. In this the attacker acts as a third party and sends fake error messages to the client, the client thinking that the message was from the host server and that the server is actually unavailable terminates the request, whereas the server still waits for the server's acknowledgment.

VI. FIREWALL

Firewall technology emerged in the late 1980s when the Internet was a new technology in terms of its global use and connectivity. Main aim of Firewall is to protect internal network. Firewall is nothing but is one software as well as hardware which act as bridge between external networks and computers. It acts as a router. It takes "good bits in and bad bits out". It has control on both incoming packets as well as outgoing packets. Firewall defines one choke point which restricts the unauthorized users from external networks. It will give access to only authorized user. Because of using Firewall we can secure our data or network. It analyses the external packets at choke point and then only it will give the access to that particular packet. In that it checks the IP addresses of the packets and what content it contains.

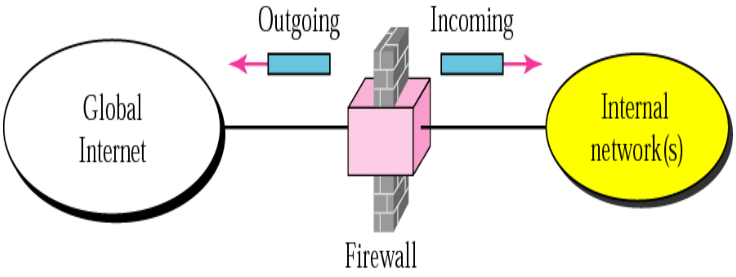

Fig.2 Firewall Design

We know firewall is essential for security purpose, but it has some limitations are as follows:

Limitation:

1. By Using firewall we can protect it from external threats but threats are available in internal network so no use of firewall.
2. Firewall can't protect against the transfer of viruses infected program or files.
3. It will not protect the attacks which are bypass from the firewall.

VII CONCLUSION

Preventing and detecting attacks that are launched over networks, and particularly over the Internet, is probably the most newsworthy aspect of security engineering. The problem is unlikely to be solved any time soon, as so many different kinds of vulnerability contribute to the attacker's toolkit. Ideally, people would run carefully written code on secure platforms; in real life, this won't always happen. In this paper we try to concentrate Transport and Network layer attack to make secure communication. We also discuss solution for attack is Firewall who monitors outsider.

REFERENCES

[1] D. E. Comer, "*Internetworking with TCP/IP: Vol. I – Principles, Protocols and Architecture*", Third Edition, Prentice Hall, 1995.

[2] Behrouz A Forouzan, "*Data Communication & Networking*", Fourth Edition, McGraw Hill Companies.

[3] Behrouz A Forouzan, "*TCP/IP Protocol Suite*", Third Edition, Tata McGraw hill.

[4] Behrouz A. Forouzan, "*Cryptography and Network Security*", Tata McGraw Hill.

[5] Mark Stamp, "*Information security Principles and Practice*" Wiley.