Experiment 4

Name	Ameya S. Daddikar
College I.D.	161070015
Course	Btech. Computer Engineering

Aim

To study TCP/IP vulnerabilities, attacks and defence mechanism.

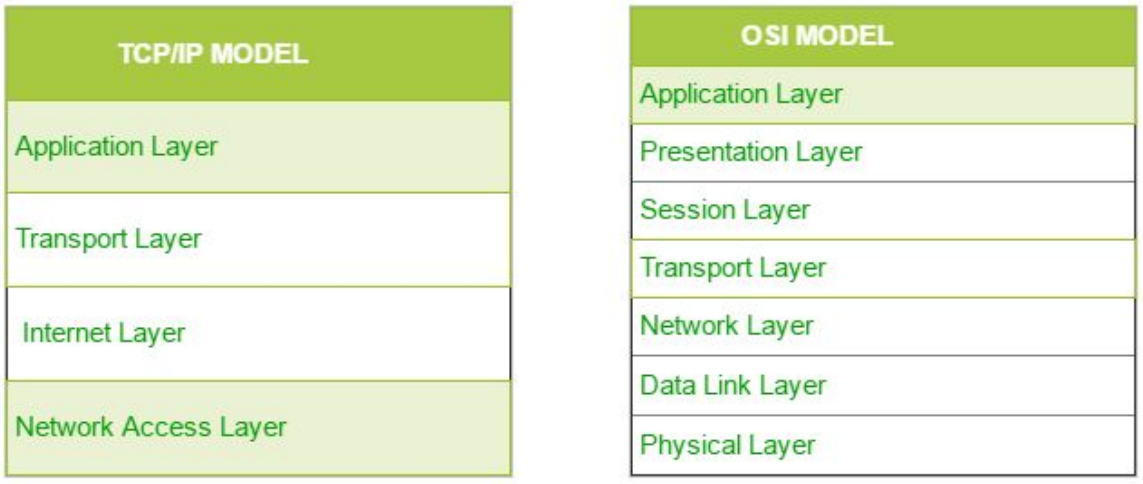
Theory

The TCP/ IP model

The OSI Model is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

- Process/Application Layer
- Host-to-Host/Transport Layer
- Internet Layer
- Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



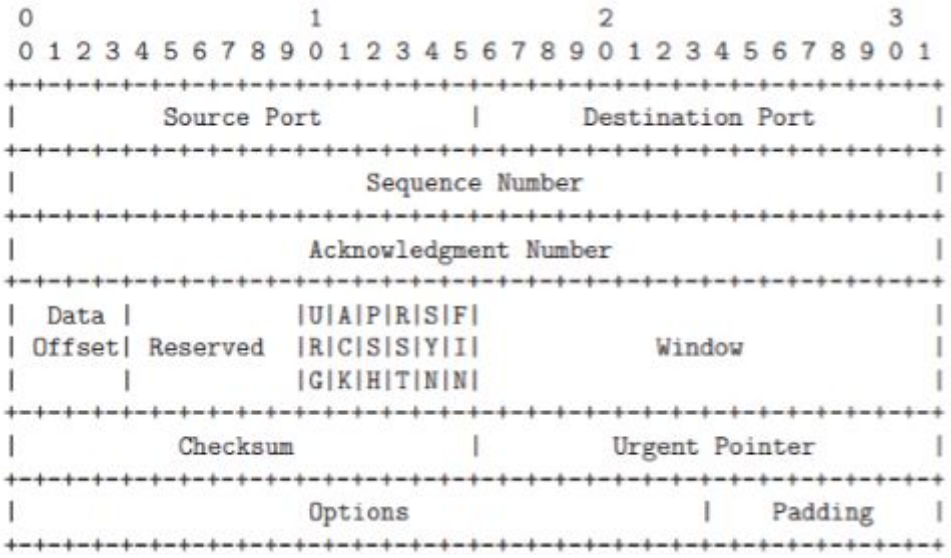
The Transport Layer

Through handshaking and acknowledgments, TCP provides a reliable communication link between two hosts on the internet. When we say that a TCP connection is reliable, we mean that the sender's TCP always knows whether or not a packet reached the receiver's TCP.

If the sender's TCP does not receive an acknowledgment that its packet had reached the destination, the sender's TCP simply re-sends the packet. Additionally, certain data integrity checks on the transmitted packets are carried out at the receiver to ensure that the receiver's TCP accepts only error-free packets.

A TCP connection is full-duplex, meaning that a TCP connection simultaneously supports two byte-streams, one for each direction of a communication link.
TCP includes both a flow control mechanism and a congestion control mechanism.
Flow control means that the receiver's TCP is able to control the size of the segment dispatched by the sender's TCP.This the receiver's TCP accomplishes by putting to use the Window field of an acknowledgment packet.

Congestion control means that the sender's TCP varies the rate at which it places the packets on the wire on the basis of the traffic congestion on the route between the sender and the receiver. The sender TCP can measure traffic congestion by measuring the rate at which the ICMP source-quench messages are received from the routers



IP Protocol

The Internet Protocol (or IP as it generally known), is the network layer of the Internet. IP provides a connection-less service.

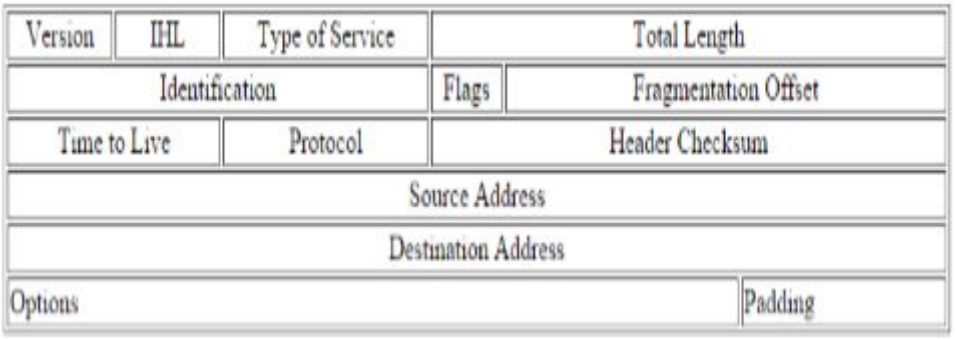
The job of IP is to route and send a packet to the packet's destination. IP provides no guarantee whatsoever, for the packets it tries to deliver.

The IP packets are usually termed datagrams. The datagrams go through a series of routers before they reach the destination.

At each node that the datagram passes through, the node determines the next hop for the datagram and routes it to the next hop.

Since the network is dynamic, it is possible that two datagrams from the same source take different paths to make it to the destination. Since the network has variable delays, it is not guaranteed that the datagrams will be received in sequence. IP only tries for a best-effort delivery.

It does not take care of lost packets; this is left to the higher layer protocols. There is no state maintained between two datagrams; in other words, IP is connection-less.



TCP/ IP Vulnerabilities

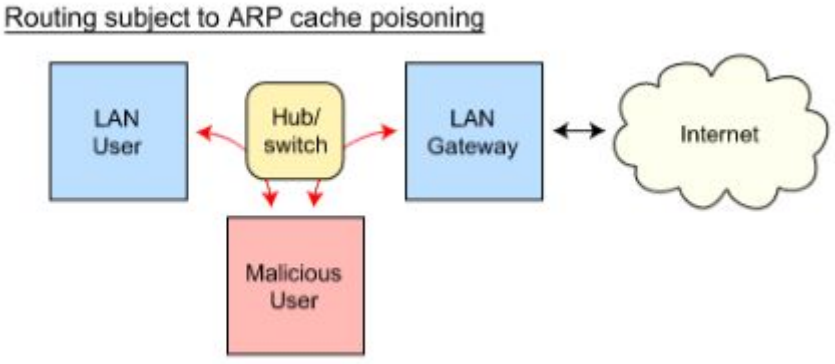
ARP Spoofing

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network.

This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.

Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.

ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.



Port scanning

Port Scanning is one of the most popular techniques attackers use to discover services that they can exploit to break into systems.

All systems that are connected to a LAN or the Internet via a modem run services that listen to well-known and not so well-known ports.

By port scanning, the attacker can find the following information about the targeted systems: what services are running, what users own those services, whether anonymous logins are supported, and whether certain network services require authentication.

Port scanning is accomplished by sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can be probed for further weaknesses.

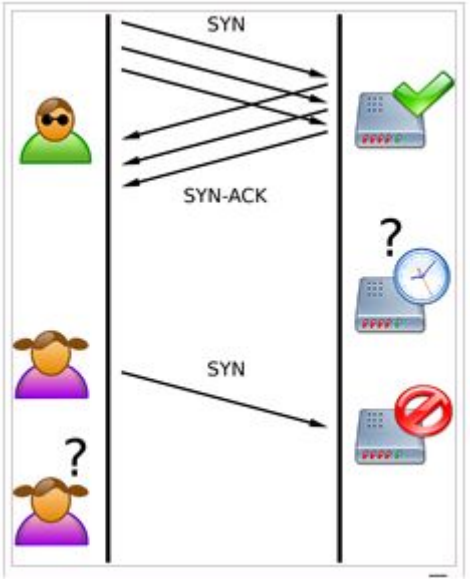
Port scanners are important to network security technicians because they can reveal possible security vulnerabilities on the targeted system.
Port Scan Techniques

- Address Resolution Protocol (ARP)
- TCP connect
- TCP SYN
- TCP FIN

TCP syn flood attack

TCP SYN flood is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.



The malicious client either does not send the expected ACK, or—if the IP address is spoofed—never receives the SYN-ACK in the first place. Either way, the server under attack will wait for acknowledgement of its SYN-ACK packet for some time.

During this time, the server cannot close down the connection by sending an RST packet, and the connection stays open.

Before the connection can time out, another SYN packet will arrive. This leaves an increasingly large number of connections half-open – and indeed SYN Food attacks are also referred to as “half-open” attacks.

Eventually, as the server’s connection overflow tables fill, service to legitimate clients will be denied, and the server may even malfunction or crash.

The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Alice, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

IP spoofing

IP address spoofing is one of the most frequently used spoofing attack methods. In an IP address spoofing attack, an attacker sends IP packets from a false (or “spoofed”) source address in order to disguise itself.

Denial-of-service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses.

IP spoofing is the action of masking a computer IP address so that it looks like it is authentic.

During this masking process, the fake IP address sends what appears to be a malevolent message coupled with an IP address that appears to be authentic and trusted.

In IP spoofing, IP headers are masked through a form of Transmission Control Protocol (TCP) in which spoofers discover and then manipulate vital information contained in the IP header such as IP address and source and destination information.

Types of spoofing attacks:

- Non-Blind Spoofing
- Blind Spoofing
- Man In the Middle Attack
- Denial of Service Attack
- DNS Spoofing

Defense Mechanisms

Some simple prevention mechanisms like password protecting the system to avoid unauthorized use have become widely popular.

1 Firewalls - Firewalls are systems designed to prevent unauthorized access to or from a network. A firewall is a dedicated appliance or software running on a system which inspects network traffic passing through it and denies or permits passage based on a set of rules. Firewalls can be implemented in both hardware and software or a combination of both. Firewalls can be of the following types:- Packet filter:- It inspects each packet entering or leaving the network and rejects or accepts based on defined rules. It is effective and transparent but difficult to configure. IP spoofing can be easily done for packet filter firewalls. Application Gateway:- Decision to allow or disallow depends upon specific application for e.g. ftp, Telnet etc. It is very effective but imposes performance degradation. Circuit-level Gateway:- It applies security mechanism when a TCP or UDP connection is established. After the connection establishment no further checking is done and packets could flow between hosts. Proxy server:- It sits between the client and server. A client requires some services such as a file, connection web page or other resources available on a different server. The proxy server validates the request with its filter rules and after the request is validated by the filter, the proxy provides the resources by connecting to the relevant servers and requesting services on behalf of clients. Some of the commonly used firewalls are :- Netfilter: It is an open source, firewall written in C that supports different IPV4 protocols and can be used with command line interface [10]. IPFilter: is an open source firewall that supports both IPv4 and IPv6. It works on different types of operating systems like AIX, BSD/OS, and some other flavours of BSD and Solaris.

2. A virtual private network (VPN) – A VPN is a private network that uses a public network such as internet to connect remote sites or users together. Instead of using a dedicated, real world connection such as leased line VPN uses “virtual” connections routed through the internet from the company’s private network to the remote site. It is implemented as an additional logical layer on top of an existing larger network.

3. Authentication - Computer Security authentication means verifying the identity of a user logging onto a network. Authentication is the process of determining whether the person is genuinely the person whose identity he or she is claiming to be. In other words authentication is the process of verification of the identity of a user.

4. Intrusion Detection System (IDS) – An intrusion detection system is a software / hardware designed to detect some unwanted attempts to access, manipulate and/or disable computer system. These attempts are generally generated from a network such as internet. It monitors network and/or system activities for malicious activities or policy violations. It is the process of monitoring the events occurring in a system or networks

5. Intrusion Prevention System (IPS) An Intrusion Prevention System (IPS) uses rule based detection technique for detecting malicious traffic and preventing attacks. IPS is the advancement of intrusion detection system IDS.

6. Some popular IDS being used are :- Snort: It is an open source IDS that works on application layer and network layer. It can detect and prevent different attacks like buffer overflow, denial of service attack, port scan, SMB probes and some other attacks.

7. Some commonly used mitigating techniques against IP Spoofing include use of encrypted session in router, using Access Control List for applying the security policies, application of defence mechanisms of upper layers.

8 Counteracting Ping of Death Attack – Techniques like changing the LAN IP address, use of filtering devices such as routers and dedicated firewall to drop all incoming (ICMP) packets are commonly used to defend against such attacks.

9. Mitigating Smurf Attack – For countering a smurf the commonly used techniques include “state-full” inspection at firewall and to deny external ICMP traffic access to the internal network.

10. Countermeasures for Long File or User Name Attacks – Such attacks can be countered by configuring the network filtering device to automatically drop the traffic which contains file names and usernames that are more than 255 characters long.

11. SYN Attack Countermeasures - Identifying the source IP Addresses of the attack packets and then using a firewall or router to block all traffic from this source.

Conclusion

Thus we studied the mechanism and vulnerabilities of the TCP/ IP architecture.