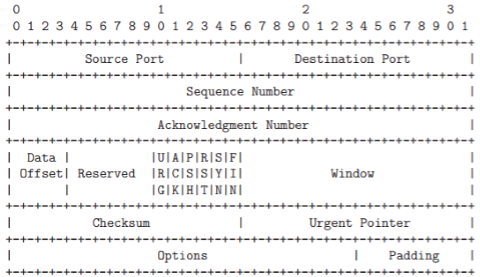
**Q . List and explain different TCP/IP vulnerabilities?**

**TCP/IP**

* We now live in a world in which the acronyms TCP and IP have become almost as commonly familiar as the other computer related words like bits, bytes, megabytes, etc
* IP stands for the Internet Protocol that deals with routing packets of data from one computer to another or from one router to another.
* On the other hand, TCP, which stands for Transmission Control Protocol, deals with ensuring that the data packets are delivered in a reliable manner from one computer to another. You could say that TCP sits on top of IP.
* A less reliable version of TCP is UDP (User Datagram Protocol). Despite the pejorative sense associated with the phrase “less reliable”, UDP is extremely important to the working of the internet
* The different communication and application protocols that regulate how computers work together are commonly visualized as belonging to a layered organization of protocols that is referred to as the TCP/IP protocol stack.

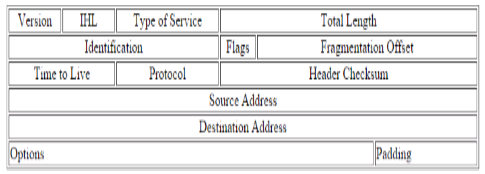
**The Transport Layer**

* 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**

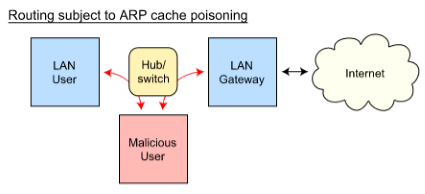
* The Internet Protocol (or IP as it generally known), is the network layer of the Internet. IP provides a connection-less service.
* The job of IP is to route and send a packet to the packet's destination. IP provides no guarantee whatsoever, for the packets it tries to deliver.
* The IP packets are 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.



**Following are the vulnerabilities in TCP/IP**

**1. 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.



**1. ARP Spoofing attack:**

* The effects of ARP spoofing attacks can have serious implications for enterprises.
* In their most basic application, ARP spoofing attacks are used to steal sensitive information. Beyond this, ARP spoofing attacks are often used to facilitate other attacks such as:

**1. Denial-of-service attacks:**

DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target’s MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target’s MAC address, overloading the target with traffic.

**2. Session hijacking:**

Session hijacking attacks can use ARP spoofing to steal session IDs, granting attacker’s access to private systems and data.

**3. Man-in-the-middle attacks:**

MITM attacks can rely onARP spoofing to intercept and modify traffic between victims.

**2. 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**

1.1 **Address Resolution Protocol (ARP)**

* + ARP scans discover active devices on the local network segment by sending a series of ARP broadcasts and incrementing the value for the target IP address field in each broadcast packet.
  + This type of scan will have every IP device on the network respond with its own IP address in response. This scan will effectively map out an entire network.

**1.2 TCP connect**

* + The Vanilla TCP connect scan is the most basic scanning technique.
  + The scan uses the connect system call of an operating system on a target system to open a connection to every port that is open.
  + The scan is extremely noisy and easily detectable. The targeted system logs will show connection requests and error messages for the services that accepted the connections.

**1.3 TCP SYN**

* + The TCP SYN (Half Open) scans are called half open because the attacking system doesn’t close the open connections.
  + The attacking scanner will send a SYN packet to the target and wait for a response. If the port is open, the target will send a SYN|ACK.
  + If the port is closed, the target will send an RST.
  + This type of scan is difficult to detect. The target system is in charge of closing the open connections and the target, most likely, will not have the proper logging set up to detect this type of scan.

**1.4 TCP FIN**

* + The TCP FIN scan has the ability to pass undetected through most firewalls, packet filters, and scan detection programs.
  + The attacking system sends FIN packets to the targeted system. The closed ports will respond with an RST. The open ports will ignore the packets. The attacking system will take note of which ports it received an RST on and report on the ports that did not respond with an RST.

**3. TCP syn flood attack**

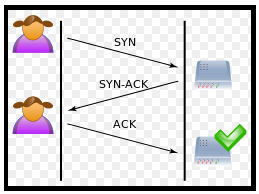
* TCP SYN flood is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.
* Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

**Attack description**

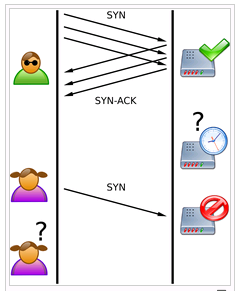
* When a client and server establish a normal TCP “three-way handshake,” the exchange looks like this:

1. Client requests connection by sending SYN (synchronize) message to the server.
2. Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client.
3. Client responds with an ACK (acknowledge) message, and the connection is established.

* In a SYN flood attack, the attacker sends repeated SYN packets to every port on the targeted server, often using a fake IP address.
* The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.
* 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.



A normal connection between a user (Alice) and a server. The three-way handshake is correctly performed.



SYN Flood. 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.

**4. 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

* This type of attack takes place when the attacker is on the same subnet as the victim. The sequence and acknowledgement numbers can be sniffed, eliminating the potential difficulty of calculating them accurately.
* The biggest threat of spoofing in this instance would be session hijacking. This is accomplished by corrupting the data stream of an established connection, then re-establishing it based on correct sequence and acknowledgement numbers with the attack machine.
* Using this technique, an attacker could effectively bypass any authentication measures taken place to build the connection.

**Blind Spoofing**

* This is a more sophisticated attack, because the sequence and acknowledgement numbers are unreachable.
* In order to circumvent this, several packets are sent to the target machine in order to sample sequence numbers. While not the case today, machines in the past used basic techniques for generating sequence numbers.
* It was relatively easy to discover the exact formula by studying packets and TCP sessions. Today, most OSs implement random sequence number generation, making it difficult to predict them accurately.
* If, however, the sequence number was compromised, data could be sent to the target. Several years ago, many machines used host-based authentication services (i.e. Rlogin). A properly crafted attack could add the requisite data to a system (i.e. a new user account), blindly, enabling full access for the attacker who was impersonating a trusted host.

**Man In the Middle Attack**

* Both types of spoofing are forms of a common security violation known as a man in the middle (MITM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties.
* The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient.
* In this way, an attacker can fool a victim into disclosing confidential information by “spoofing” the identity of the original sender, who is presumably trusted by the recipient.

**Denial of Service Attack**

* IP spoofing is almost always used in what is currently one of the most difficult attacks to defend against – denial of service attacks, or DoS.
* Since crackers are concerned only with consuming bandwidth and resources, they need not worry about properly completing handshakes and transactions.
* Rather, they wish to flood the victim with as many packets as possible in a short amount of time. In order to prolong the effectiveness of the attack, they spoof source IP addresses to make tracing and stopping the DoS as difficult as possible.
* When multiple compromised hosts are participating in the attack, all sending spoofed traffic, it is very challenging to quickly block traffic.

**5. DNS Spoofing**

* The Domain Name System (DNS) is a system that associates domain names with IP addresses.
* Devices that connect to the internet or other private networks rely on the DNS for resolving URLs, email addresses and other human-readable domain names into their corresponding IP addresses.
* In a DNS server spoofing attack, a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address.
* In many cases, the new IP address will be for a server that is actually controlled by the attacker and contains files infected with malware. DNS server spoofing attacks are often used to spread computer worms and viruses.

**Q. What is cryptography and types of cryptography?**

**Cryptography** is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

* **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
* **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
* **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.
* **Non-repudiation** refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

There are two main requirements for cryptography:

1. It should be computationally infeasible to derive the plaintext from the ciphertext without knowledge of the decryption key.
2. It should be computationally infeasible to derive the ciphertext from the plaintext without knowledge of the encryption key.

Consider two parties Alice and Bob. Now, Alice wants to send a message m to Bob over a secure channel.  
So, what happens is as follows.  
The sender’s message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of receival, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.

Alice (Sender) Bob (Receiver)

C = E (m, k) ----> m = D (C, k)

Here, C refers to the Ciphertext while E and D are the Encryption and Decryption algorithms respectively.

Let’s consider the case of Caesar Cipher or Shift Cipher as an example.  
As the name suggests, in Caesar Cipher each character in a word is replaced by another character under some defined rules. Thus, if A is replaced by D, B by E and so on. Then, each character in the word would be shifted by a position of 3. For example:

Plaintext : Geeksforgeeks

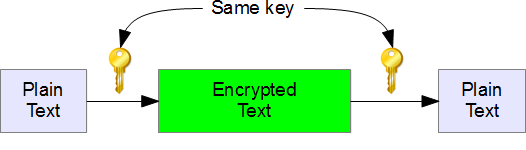
Ciphertext : Jhhnvirujhhnv

There are three types of cryptography techniques :

* Secret key Cryptography
* Public key cryptography
* Hash Functions

### **1. Secret Key Cryptography**

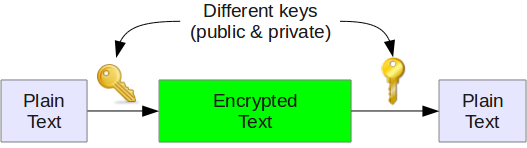
This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption.



The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

### **2. Public Key Cryptography**

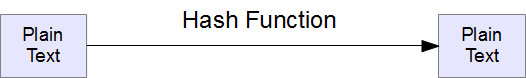
This type of cryptography technique involves two key crypto system in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption.



In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob’s public key and Bob can decrypt the message with its private key.

This is what we use when we setup [public key authentication in openssh](https://www.thegeekstuff.com/2008/11/3-steps-to-perform-ssh-login-without-password-using-ssh-keygen-ssh-copy-id/) to login from one server to another server in the backend without having to enter the password.

### **3. Hash Functions**



This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered,compromised or affected by virus.