# NETWORK SECURITY:

- FIREWALLS: It can be compared with a security guard standing at the entrance of a minister's home. He keeps an eye on everyone and physically checks every person who wishes to enter the house. It won't allow a person to enter if he/she is carrying a harmful object like a knife, gun etc. Similarly, even if the person doesn't possess any banned object but appears suspicious, the guard can still prevent that person's entry.
- The firewall acts as a guard. It guards a corporate network acting as a shield between the inside network and the outside world. All the traffic in either direction must pass through the firewall. It then decides whether the traffic is allowed to flow or not. The firewall can be implemented as hardware and software, or a combination of both.

- **Packet Filters –**
  It works in the **network layer** of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to ‘discard all packets’ or to ‘accept all packets’.

**Security threats** to Packet Filters:

1. **IP address Spoofing:**
   In this kind of attack, an intruder from the outside tries to send a packet towards the internal corporate network with the source IP address set equal to one of the IP address of internal users.

2. **Source Routing Attacks:**
   In this kind of attack, the attacker specifies the route to be taken by the packet with a hope to fool the firewall.

3. **Tiny Fragment Attacks:**

   Many times, the size of the IP packet is greater than the maximum size allowed by the underlying network such as Ethernet, Token Ring etc. In such cases, the packet needs to be fragmented, so that it can be carried further. The attacker uses this characteristic of TCP/IP protocol. In this kind of attack, the attacker intentionally creates fragments of the original packet and send it to fool the firewall.

2. **Application Gateways –**

   It is also known as **Proxy server**. It works as follows:

   1. **Step-1:** User contacts the application gateway using a TCP/IP application such as HTTP.
   2. **Step-2:** The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.
   3. **Step-3:** After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

3. **Stateful Inspection Firewalls –**
   It is also known as 'Dynamic Packet Filters'. It keeps track of the state of active connections and uses this information to decide which packets to allow through it, i.e., it adapts itself to the current exchange of information, unlike the normal packet filters/stateless packet filters, which have hardcoded routing rules.
4. **Circuit-Level Gateways –**
   It works at the **session layer** of the OSI Model. It is the advanced variation of *Application Gateway*. It acts as a virtual connection between the remote host and the internal users by creating a new connection between itself and the remote host. It also changes the source IP address in the packet and puts its own address at the place of source IP address of the packet from end users. This way, the IP addresses of the internal users are hidden and secured from the outside world.

# stateful vs stateless firewalls

**STATELESS Firewalls (packet filters)**

Stateless firewalls watch network traffic and restrict or block packets based on source and destination addresses or other static values. A stateless firewall filter, also known as an access control list (ACL), does not statefully inspect traffic. Instead, it evaluates packet contents statically and does not keep track of the state of network connections.

*Purpose of Stateless Firewall Filters*

The basic purpose of a stateless firewall filter is to enhance security through the use of packet filtering. Packet filtering enables you to inspect the components of incoming or outgoing packets and then perform the actions you specify on packets that match the criteria you specify. The typical use of a stateless firewall filter is to protect the Routing Engine processes and resources from malicious or untrusted packets.

## STATEFUL Firewall

Stateful firewalls can watch traffic streams from end to end. They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledge or established). It can tell if the MTU has changed and whether packets have fragmented. etc.

Stateless firewalls are typically faster and perform better under heavier traffic loads. Stateful firewalls are better at identifying unauthorized and forged communications.

# IDS

- Intrusion Detection System (IDS)
- An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching.
- Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

**Classification of Intrusion Detection System:**

IDS is basically classified into 2 types:

1. **Network Intrusion Detection System (NIDS):**
   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnetts to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

2. **Host Intrusion Detection System (HIDS):**
   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. Anexample of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

**Detection Method of IDS:**

1. **Signature-based Method:**
   Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.
2. **Anomaly-based Method:**
   Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

- **Comparison of IDS with Firewalls:**
  IDS and firewall both are related to the network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it don’t signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

# Intrusion Prevention System (IPS)

- Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

**Classification of Intrusion Prevention System (IPS):**

Intrusion Prevention System (IPS) is classified into 4 types:

1. **Network-based intrusion prevention system (NIPS):**
   It monitors the entire network for suspicious traffic by analyzing protocol activity.
2. **Wireless intrusion prevention system (WIPS):**
   It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
3. **Network behavior analysis (NBA):**
   It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.
4. **Host-based intrusion prevention system (HIPS):**
   It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

## Detection Method of Intrusion Prevention System (IPS):

1. **Signature-based detection:**
   Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.
2. **Statistical anomaly-based detection:**
   Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.

**Comparison of IPS with IDS:**

The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

# Tcp stack:

# 1.Network interface layer

| NO. | PROTOCOL | ATTACK | TOOLS FOR ATTACK | DEFENCE MECHANISM |
|---|---|---|---|---|
| 1. | ARP | CACHE POISONING,ARP SPOOFING | ARP0c, Dsniff arpspoof, smit | ARP MONITORING AT SWITCHES TOOL:ARPWATCH |
| | | MAC FLOODING | ARPoison, Parasite | Source IP address filteration for network administration. |
| | | MAN IN THE MIDDLE | arpspoof, Parasite | Monitoring at network gateways and firewalls |
| | | | | |
| | | | | |

- The ARP Spoofing is an attack where the attacker sends falsified ARP Messages (Address Resolution Protocol) so that the attackers MAC address will be linked with the IP address of a legitimated user in the network.
- ARP poisoning is an attack that is accomplished using the technique of ARP spoofing.
- ARP spoofing is a technique that allows an attacker to craft a "fake" ARP packet that looks like it came from a different source, or has a fake MAC address in it.
- An attacker uses the process of ARP spoofing to "poison" a victim's ARP table, so that it contains incorrect or altered IP-to-MAC address mappings for various attacks, such as a man-in-the-middle attack.

- The MAC Flooding is an attacking method intended to compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table. This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch. This table allows the switches to direct the data out of the ports where the recipient is located
- As we've already seen, the hubs broadcast the data to the entire network allowing the data to reach all hosts on the network but switches send the data to the specific machine(s) which the data is intended to be sent. This goal is achieved by the use of MAC tables The aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.
- MAC Address Table is full and it is unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like a broadcasting.
- As the attacker is a part of the network, the attacker will also get the data packets intended for the victim machine. So that the attacker will be able to steal sensitive data from the communication of the victim and other computers. Usually a packet analyzer is used to capture these sensitive data.
- After launching a MAC Flood attack successfully, the attacker can also follow up with an ARP spoofing attack. This will help the attacker retaining access to the privileged data even after the attacked switches recover from the MAC Flooding attack.

# 2.Network layer

| NO. | PROTOCOL | ATTACK | TOOLS FOR ATTACK | DEFENCE MECHANISM |
|---|---|---|---|---|
| 1. | IP | DOS | HPING,NEMESIS,NETDUDE | PERFORMING MONITORING OF TCP SESSIONS USING NETWORK BASED IDS |
| | | IP SPOOFING | APSEND,AICMPSEND, ETTERCAP | NIDS,HIDS |
| | | TEARDROP | HPING,NEMESIS | NIDS,HIDS |
| | | SOURCE ROUTING | WINDDUMP,SNORT | DENY SOURCE ROUTING AT GATEWAYS AND FIREWALLS |
| 2. | ICMP | PING OF DEATH | HPING,NEMESIS,NETDUDE | IMPLEMENT STATEFULL FIREWALLING.MONITOR NETWORK TRAFFIC USING NIDS AND HYBRID IDS |
| | | SMURF | WIRESHARK,SNIFFT,DSNIFF | RESTRICTION OF SPECIFIC ICMP MSGS. FIREWALLS AND IDS |
| | | ICMP FLOOD | WIRESHARK,SNIFFT,DSNIFF | RESTRICTION OF SPECIFIC ICMP MSGS. FIREWALLS AND IDS |

- A **teardrop attack** is a denial-of-service (DoS) **attack** that involves sending fragmented packets to a target machine. Since the machine receiving such packets cannot reassemble them due to a bug in TCP/IP fragmentation reassembly, the packets overlap one another, crashing the target network device.

# ping of death

- On the Internet, ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. One of the features of TCP/IP is fragmentation; it allows a single IP packet to be broken down into smaller segments. In 1996, attackers began to take advantage of that feature when they found that a packet broken down into fragments could add up to more than the allowed 65,536 bytes. Many operating systems didn't know what to do when they received an oversized packet, so they froze, crashed, or rebooted.

✔SMURF ATTACK:The **Smurf attack** is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

- The fix is two-fold:

- Configure individual hosts and routers to not respond to ICMP requests or broadcasts; or
- Configure routers to not forward packets directed to broadcast addresses.

Source routing:

Source routing is a specific routing process where senders can specify the route that data packets take through a network. This allows for troubleshooting and various transmission goals. Source routing is an alternative to traditional routing where packets just move through a network based on their destination.

Source routing is also known as path addressing.

An ICMP Flood attack - the sending of an abnormally large number of ICMP packets of any type (especially network latency testing "ping" packets) - can overwhelm a target server that attempts to process every incoming ICMP request, and this can result in a denial-of-service condition for the target server.

# 3.TRANSPORT LAYER

| NO. | PROTOCOL | ATTACK | TOOLS FOR ATTACK | DEFENCE MECHANISM |
|---|---|---|---|---|
| 1. | TCP | TOO BIG FRAGMENT | BUBONIC,TARGA3 | PACKET FILTER FIREWALL |
| | | CONNECTION HIJACKING/BLIND ATTACK | HUNT,JUGGERNAUT, TSIGHT | NIDS,HIDS,STATEFUL FIREWALLING |
| | | TCP RESET | HPING2,NEMESIS,SCAPY | NIDS,HIDS,STATEFUL FIREWALLING |
| | | LAND | BUBONIC,TARGA3 | PACKET FILTER FIREWALL |
| | | SYN FLOOD | HPING2,NEMESIS,SCAPY | PACKET FILTER FIREWALL |

# TCP Reset Attacks

This attack is fairly simple to understand once the above attack is clear to you. In this attack :

- Once the attacker is able to hijack a TCP session (as told above), this attack can be launched.
- The attacker sends packets with RST Flag ON to both A and B or any one of the host.
- Since both A and B do not know that an attacker has sent these packets so they treat these packets normally.
- Since they are reset packets so connection between A and B is terminated.

So we can see that TCP reset attacks are aimed to terminate a valid TCP connection between two hosts.

- A LAND Attack is a Denial of Service (DoS) attack in which, the attacker sets the source and destination information of a TCP segment to be the same. A vulnerable machine will crash or freeze due to the packet being repeatedly processed by the TCP stack.

| NO. | PROTOCOL | ATTACK | TOOLS FOR ATTACK | DEFENCE MECHANISM |
|---|---|---|---|---|
| 1. | UDP | UDP FLOOD | TRINOO | PACKET FILTER FIREWALL |
| | | FRAGGLE | NEMESIS,ETHERAL, SNIFFIT,Dsniff | NIDS,HIDS,STATEFUL FIREWALLING |
| | | | | |
| | | | | |
| | | | | |

A UDP flood is a type of denial-of-service attack in which a large number of User Datagram Protocol (UDP) packets are sent to a targeted server with the aim of overwhelming that device's ability to process and respond. The firewall protecting the targeted server can also become exhausted as a result of UDP flooding, resulting in a denial-of-service to legitimate traffic.

- A **Fraggle Attack** is a denial-of-service (DoS) **attack** that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. It is very similar to a Smurf **Attack**, which uses spoofed ICMP traffic rather than UDP traffic to achieve the same goal.

# 4:APPLICATION LAYER

| NO. | PROTOCOL | ATTACK | TOOLS FOR ATTACK | DEFENCE MECHANISM |
|---|---|---|---|---|
| 1. | HTTP | SLOWLORIS | WEBSPY,WEBSNIFF | INGRESS FILTERING |
| | | HTTP FLOOD | JUGGERNAUT | FIREWALL ,HIDS,NIDS |
| | | HTTP SESSION HIJACKING | BUGBEAR,GONERWORM,MELISSA | ANTISPAM,ANTIVIRUS,URL AND CONTENT FILTERING |
| 2. | DNS | DNS AMPLIFICATION ATTACK | WEBMITM,JUGGERNAUT | FIREWALL,HIDS,NIDS |
| | | | | |

**ingress filtering:**

In computer networking, **ingress filtering** is a technique used to ensure that incoming packets are actually from the networks from which they claim to originate. This can be used as a countermeasure against various spoofing attacks where the attacker's packets contain fake IP addresses to make it difficult to find the source of the attack.

- Slowloris is an attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target. This type of attack requires minimal bandwidth to launch and only impacts the target web server, leaving other services and ports unaffected.

## Mitigating the Slowloris attack:

While there are no reliable configurations of the affected web servers that will prevent the Slowloris attack, there are ways to mitigate or reduce the impact of such an attack. In general, these involve increasing the maximum number of clients the server will allow, limiting the number of connections a single IP address is allowed to make, imposing restrictions on the minimum transfer speed a connection is allowed to have, and restricting the length of time a client is allowed to stay connected.

- In an HTTP flood, the HTTP clients such as web browser interact with an application or server to send HTTP requests. The request can be either “GET” or “POST”. The aim of the attack is when to compel the server to allocate as many resources as possible to serving the attack, thus denying legitimate users access to the server's resources.
- OR
- A HTTP flood attack is a type of volumetric distributed denial-of-service (DDoS) attack designed to overwhelm a targeted server with HTTP requests. Once the target has been saturated with requests and is unable to respond to normal traffic, denial-of-service will occur for additional requests from actual users.

### GET flood

The GET request is used to retrieve static content like images. Typically this induces relatively low load on the server per request.

### POST flood

POST requests are more likely to require the server to perform some kind of processing, such as looking up items in a database. Therefore, HTTP POST flood attacks typically impose higher load on the server per request.

## Methods of mitigation

As HTTP flood attacks use standard URL requests hence it is quite challenging to differentiate from valid traffic. One of the most effective mitigation methods is the combination of traffic profiling methods that mainly includes identification of IP reputation, tracking abnormal actions and employing progressive sanctuary challenges.

- **session  Hijacking**
- Using a packet sniffer (a tool for detecting the presence and movement of data packets), an attacker may capture data packets and gain full access to an HTTP session. If there’s weak authentication between a web server and its clients, the attacker may assume full control of the client’s rights, switching the communication to one directly between them and the targeted server.

- DNS amplification, like other amplification attacks, is a type of reflection attack. In this case, the reflection is achieved by eliciting a response from  DNS resolvers to a spoofed IP address.
- During a DNS amplification attack, the perpetrator sends out a DNS query with a forged IP address (the victim's) to an open DNS resolver, prompting it to reply back to that address with a DNS response. With numerous fake queries being sent out, and with several DNS resolvers replying back simultaneously, the victim's network can easily be overwhelmed by the sheer number of DNS responses.

a **reflection attack** is a method of attacking a challenge-response authentication system that uses the same protocol in both directions. That is, the same challenge-response protocol is used by each side to authenticate the other side. The essential idea of the attack is to trick the target into providing the answer to its own challenge.[1]

The general attack outline is as follows:

1. The attacker initiates a connection to a target.
2. The target attempts to authenticate the attacker by sending it a challenge.
3. The attacker opens another connection to the target, and sends the target this challenge as its own.
4. The target responds to the challenge.
5. The attacker sends that response back to the target on the original connection.

If the authentication protocol is not carefully designed, the target will accept that response as valid, thereby leaving the attacker with one fully authenticated channel connection (the other one is simply abandoned).

# Tcp vulnerabilities and attacks

- **IP and Source Routing**
- When information is broken up into packets, the IP source generates a listing of the routes that packets must take to reach their intended destination. This listing may in turn be used by the recipient to send information back to the sender.
- Unfortunately, at this stage attackers can also gain access to the source path, and modify the options in the route for a data packet. In what's known as a source route attack, an attacker may also be at liberty to read the data packets, potentially gaining access to confidential information, financial details. This risk may be offset to some extent by dropping or forwarding any data packets which carry the source route option.

# TCP and Reassembly

- Data packets reaching their destination may arrive in a logical sequence, or out of order. In some cases, they may not arrive at all. At the data's origin point, it's the job of the Transmission Control Protocol or TCP to break the information into packets, which it then assigns numbers to for reassembly at the destination point.

# Predicting TCP Sequences

- With some diligent application of the right kind of algorithms, it’s possible for an attacker to guess the sequence of numbers that TCP assigns to a stream of data packets. Knowing the next number in a transmission sequence, an attacker may potentially “step in” to an ongoing communication and pose as the originator of the message.
- TCP sequence numbers are typically increased by a constant amount each second, and by half of that number each time a connection begins. So one way of guarding against the prediction of the next number in a sequence by an attacker who may have gained access to a server through apparently legitimate means is to generate a random increment for the initial sequence number.

- **TCP Blind Spoofing**
- Here, an attacker is able to guess both the sequence number of an ongoing communication session and its port number. They are then in a position to carry out an injection attack, inserting corrupted or fraudulent data into the stream – or worse, malicious code or malware.

- **SYN Flooding**
- Remember those SYN and ACK segments needed to establish a TCP connection? Under the protocol rules, a client or server receiving these requests is required to respond to them, to keep the communication going. This requirement is the basis of a SYN flooding attack, whereby multiple SYN packets are spoofed using a bogus source address, then sent to a targeted server.
- Under compulsion to respond, the server will send out SYN-ACK packets to an address that doesn’t exist, creating a flood of half-opened sessions awaiting replies that will never come. During this time, no fresh connections will be allowed by the server, and connection requests from legitimate users will be ignored – a Denial of Service or DoS scenario.

- **Man-in-the-Middle Attacks**
- In an unsecured communication, data may pass between sender and receiver as “clear text” – unprotected and unencrypted information which may include user credentials and passwords. By spoofing an IP address, and attacker may intercept an ongoing transmission and become the man (or woman, or bot) in the middle of a communication, steering valuable data towards themselves – or misinformation and malware toward the recipient.

- PUSH + ACK  ATTACK
- tcp connection hijacking

# Defence:

- Packet filtering firewall
- Nids
- Better seq nos

# Router attacks

- DDOS

✔ PING OF DEATH
✔ SMURF ATTACK
✔ PING FLOOD ATTACK
✔ ARP POISONING

- MITM

- ATTCAKS ON BGP
- ATTACKS ON OSPF

✔ HELLO PACKETS DROPPED
✔ MAX SEQUENCE ATTACK
✔ UNKNOWN LOGINS

# Router attacks

- DDOS

✔PING OF DEATH:Ping of death is also known as "long ICMP.“

On the Internet, ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. One of the features of TCP/IP is fragmentation; it allows a single IP packet to be broken down into smaller segments. In 1996, attackers began to take advantage of that feature when they found that a packet broken down into fragments could add up to more than the allowed 65,536 bytes. Many operating systems didn't know what to do when they received an oversized packet, so they froze, crashed, or rebooted.

To avoid Ping of Death attacks and its variants, many sites block ICMP ping messages altogether at their firewalls.

✔SMURF ATTACK:The **Smurf attack** is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

- The fix is two-fold:

- Configure individual hosts and routers to not respond to ICMP requests or broadcasts; or
- Configure routers to not forward packets directed to broadcast addresses.

✔PING FLOOD ATTACK:The DDoS form of a Ping (ICMP) Flood can be broken down into 2 repeating steps:

- The attacker sends many ICMP echo request packets to the targeted server using multiple devices.
- The targeted server then sends an ICMP echo reply packet to each requesting device’s IP address as a response.

✔ARP POISONING:ARP poisoning is an attack that is accomplished using the technique of ARP spoofing.

- ARP spoofing is a technique that allows an attacker to craft a "fake" ARP packet that looks like it came from a different source, or has a fake MAC address in it.
- An attacker uses the process of ARP spoofing to "poison" a victim's ARP table, so that it contains incorrect or altered IP-to-MAC address mappings for various attacks, such as a man-in-the-middle attack.

- MITM

- ATTCAKS ON BGP:

✔Tcp reset ..due to which bgp has to do a lot of processing over many routers when any route goes down.

- ATTACKS ON OSPF

✔HELLO PACKETS DROPPED

✔MAX SEQUENCE ATTACK

✔UNKNOWN LOGINS