HIGH SPEED NETWORK (IT-316)

Under supervision of

Mrs. Anamika Chauhan

Submitted by

Varun Kumar 2K19 / IT / 140

Department of Information Technology, DTU

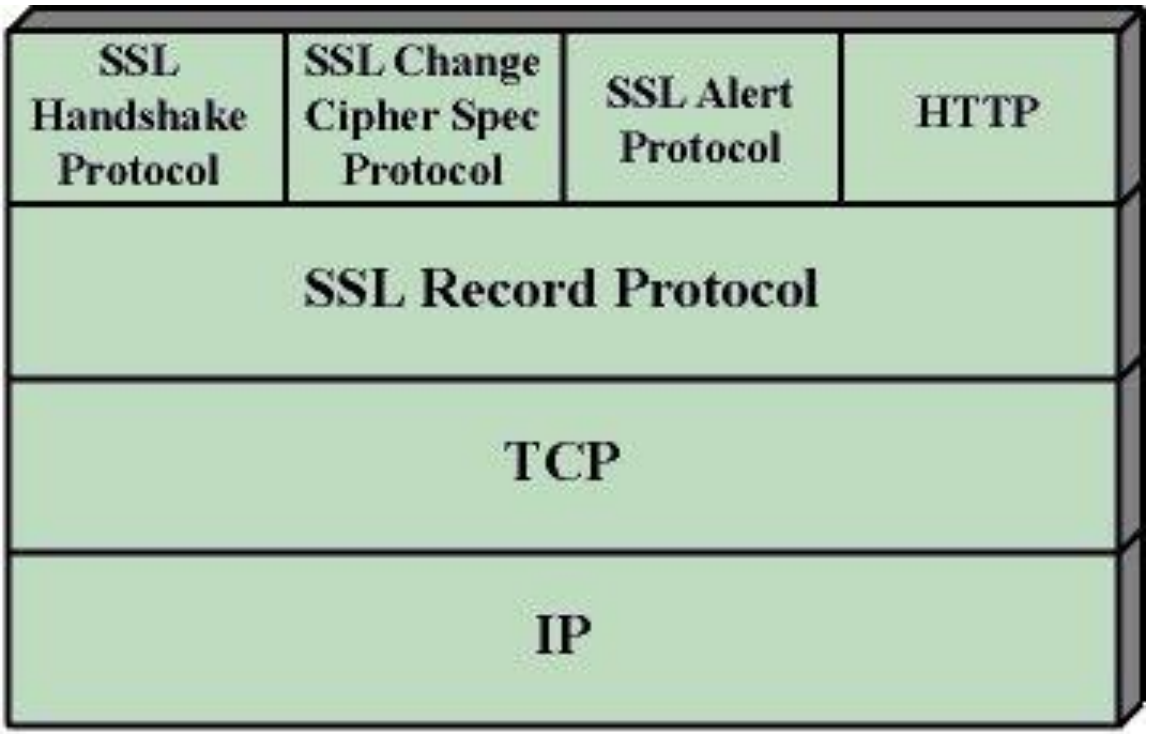
Secure Socket Layer (SSL)

Secure Socket Layer (SSL) delivers data protection between a browser and a server. SSL encipher the link between a server & a browser that guarantees that all data exchanged between them is kept secret and secure.

Secure Socket Layer Protocols:

- SSL record protocol
- Change the cipher spec protocol
- Handshake Protocol
- Alert protocol

SSL Protocol Stack:

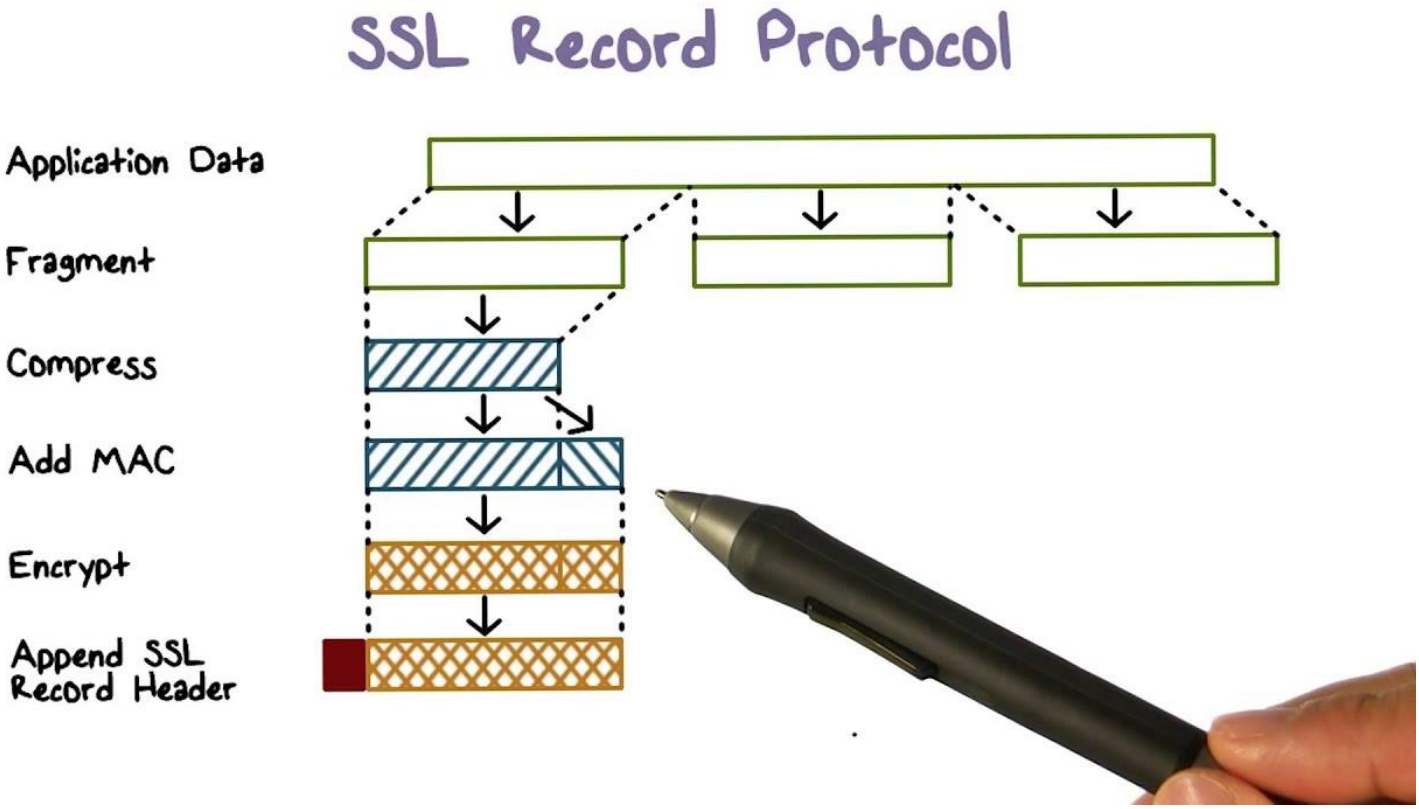


SSL Record Protocol:

SSL Record delivers 2 services to SSL connection

- Confidentiality
- The Integrity of the Message

In the SSL Record Protocol application data is split into parts. The parts are pressed & enciphered with MAC (Message Verification Code) created by algorithms such as SHA (Secure Hash Protocol) and MD5 (Message Digest) added. After that data encryption is done and the final SSL header is added to the data.



Handshake Protocol:

Handshake Protocol is used to set up sessions. This protocol allows the client and server to certify each other by sending a series of messages. The handshake protocol uses four stages to complete its cycle.

- ➔ **Step 1:** In Step 1 both the Client and the Server dispatch hello packets to each other. In this IP session, the cipher suite version and protocol are exchanged for safety reasons.
- ➔ **Step 2:** Server transmits its certificate and Server Exchange Server. The server finishes phase 2 by transmitting a Server-hello-end packet.
- ➔ **Step 3:** In this Phase, the Client answers to the server by transmitting its certificate and the client exchange key.
- ➔ **Step 4:** A change in the cipher suite has taken place again after the end of this Protocol.

Change-cipher Protocol:

This protocol utilizes an SSL record protocol. Until the Handshake Protocol is terminated, the output of the SSL record will be in standby mode. After the handshake protocol, the standby mode is swapped to the current state.

The cipher switch protocol has a single message that is of 1 byte & can only contain single value. The objective of this protocol is to permit the status awaiting to be copied to the current state.

Alert Protocol:

This protocol is used to transmit SSL-associated warnings to peer individuals. Every message in this protocol has 2 bytes.

Level **(1 BYTE)**	**Alert** **(1 BYTE)**

The standard is segregated into two parts:

Warning (level = 1) : This Notice has no impact on the link between the transmitter & the receiver. Some of these are:

- Wrong certificate : If the certificate received is damaged.
- Outdated Certificate : If the certificate expires.
- Unknown Certificate : When an unambiguous problem occurred in processing the certificate, making it inappropriate.
- Missing certificate : If the suitable certificate isn't accessible/available.
- Turn off notification: Notify that the sender will no longer transmit messages over the network.

Fatal Error (level = 2) : This Notice terminates the link between the sender & the receiver. The 2nd byte in this protocol defines the error. Some of these are:

- Failure to HandShake: If the sender is incapable of bargaining for a satisfactory set of security para meters when taking into account the available options .
- Poor MAC record: When wrong MAC is accepted.
- Decompression failure: If the degradation function receives the incorrect input.
- Illegal para meters: If the field is out of range or does not match other fields.
- Unexpected message: If the wrong message is acquired.

Essential Features of SSL

1. This is a two-layer protocol.
2. The upper hand of this approach is that the service may be fitted to the particular needs of a provided application.
3. SSL is intended to use TCP to provide trustworthy end-to-end security service.
4. Secured Socket Layer was established by Netscape.

Transport Layer Security (TLS)

Transport Layer Securities (TLS) is aimed to offer safety on the transport layer. TLS is derivatived from a security protocol known as Secure Socket Layer (SSL). TLS guarantees that no outside member can listen or disrupt any message.

There are a few advantages of TLS:

- **Encryption**: TLS / SSL can help safeguard data transmitted using encryption.
- **Flexibility of algorithm**: TLS / SSL offers the functions of certification methods, encryption & hashing algorithms used during secure sessions.
- **Easy to Deploy**: Many TLS / SSL applications temporarily on the server 2003 operating system.
- **Interaction**: TLS / SSL works with various web browsers, including Microsoft Internet Explorer as well as many applications.
- **Easy to Use**: Because we use TLS / SSL under the application layer, many of its functions are hidden to consumers.

TLS Working :

The client connects to the server (using TCP), the client will be something. Client submits specification number:

1. SSL / TLS version.
2. which cipher suits the compression method he wants to use.

The server inspects which variant of SSL / TLS is endorsed by both sides, selects the cipher suite in one of the client options (if it supports one) & selects the compression method. After this fundamental setup is done, the server issues its certificate. This certificate should be entrusted by the client himself or his client. After validating the certificate & validating the identity of the server (not the man in the middle), the key is changed. This can be a public key, "PreMasterSecret" or just whatever dependent on the cipher suite.

Both server and client can now calculate symmetrical encryption keys. The handshake is completed and the two hosts can safely communicate.The TCP connection on both sides will allow the connection to be terminated incorrectly. Connectivity can not be jeopardized by this, it is simply broken.

Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) , a mechanism that makes it possible to create voice calls through broadband internet connections rather than conventional phone lines. Some VoIP services let you contact other VoIP customers, whereas others let you call anyone. They may or may not have a telephone number, which may include local, long-distance, mobile, and global lines. Some VoIP services require you to only use a computer or a specialized VoIP phone, while others enable you to use a normal phone attached to a VoIP adapter.

This network is created through VoIP, which allows users to make communications and conduct web meetings using laptops, smartphones, and other portable devices.

Several common characteristics include:

video calls;
voicemail;
audio calls;
instant messaging;
team chats;
email;
SMS texts;
mobile and desktop apps; and

How VoIP / Internet Voice Works -
Voice over IP (VoIP) services convert speech to digital signals. When a standard phone number is called, the signal is transformed to a regular cell service, or analogue signal, prior to hitting the transmitting end. You may use VoIP to make direct calls to a laptop using a special VoIP phone or a regular phone connected to a special adapter. Hot wireless hotspots in places such as hotels, hospitals, cafes, and so on allow users to access the internet and maybe utilize the wireless VoIP service.

VoIP services translate a person's speech from sound to digital information, which is then transferred across Ethernet or Wi-Fi to some other user — or group of users. VoIP will employ codecs to do this.
Codecs are hardware or software-based compression and decompression processes for massive volumes of VoIP data. When compression is applied, voice quality may degrade, but bandwidth needs are reduced. Equipment manufacturers will also use proprietary codecs.

Encapsulating audio into data packets, transferring the packets across an IP network, and encapsulating the packets back into audio at the other end of the connection are all steps in the process of sending data to other users. To

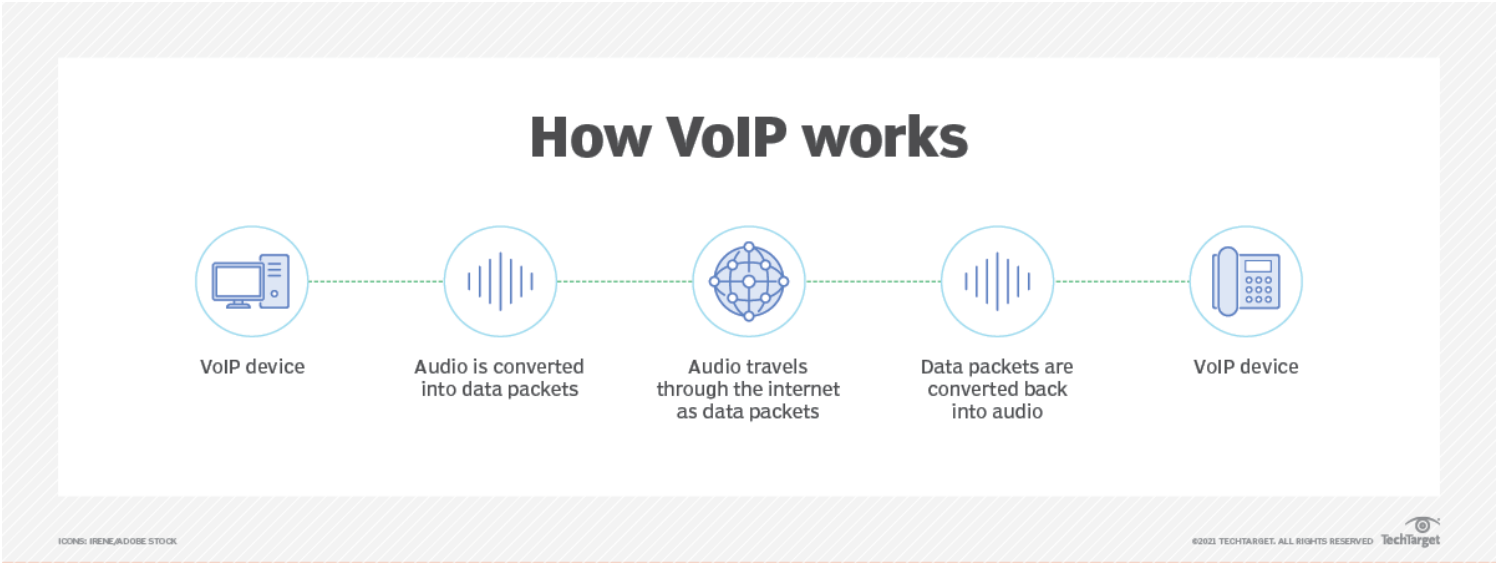
provide acceptable speech quality, business or private networks often utilize quality of service (QoS) to prioritize voice traffic over non-latency-sensitive applications.

An IP PBX to manage user telephone numbers, devices, features, and clients; gateways to connect networks and provide failover or local survivability in the event of a network outage; and session border controllers to provide security, call policy management, and network connections are also common components of a typical VoIP system.

Location-tracking databases for E911 (enhanced 911) call routing and management platforms can also be included in a VoIP system. Call performance information can be collected for reactive and proactive voice-quality control.

VoIP decreases network infrastructure costs by removing circuit-switched networks for voice and enables carriers to provide voice services across Broadband and private networks. This should also allow businesses to run a single phone and data network.

VoIP also benefits from the robustness of IP-based networks by allowing for quick failover, outage recovery, and redundant communications between endpoints and networks.



Required Resources -

A cable modem or high-speed services such as a local area network are required for a high-speed internet connection. A computer, adapter, or special phone is necessary. Some VOA services only work with your computer

or a specific VOA phone. Some apps allow you to utilize a traditional phone connected to a VoI adapter. Certain software and inexpensive microphones are necessary if you use your computer. VoI phones connect straight to your broadband and operate just as well as a typical phone call. If you have a phone with a VOIP adaptor, you may dial as usual, and your service provider can also give you a dial tone.

Benefits of VoIP -

1. **Lower cost** Price is lower than typical phone bills.
2. **Higher-quality sound.** With uncompressed data, audio is less muffled or fuzzy.
3. **Access for remote workers**. Good for employees who work remotely as they have a number of options to call into meetings or communicate to other teammates.
4. **Added features**. These features include call recording, queues, custom caller ID or voicemail to email.
5. **Low international rates**. When a landline makes an international call, the call is routed over a wired connection. VoIP does not require a wired line and makes calls via the internet, thus it is classified as normal traffic and is less expensive.

VoIP inefficiency -

1. Some VoIP services may not function during power outages, and the service provider may not offer backup power.
2. Not all VoIP services are directly connected to emergency services with emergency numbers.
3. VoI providers may or may not offer reference services.

Denial of Service DDoS attack

Consider a situation in which you browse several websites and one of them appears to be slow. You blame their servers for improving their durability, since they may experience a high volume of user traffic on their site. The majority of the sites have previously considered this topic. They might be the victims of a DDoS attack, also known as a Distributed Denial of Service attack.

In a DDOS attack, an attacker attempts to render a certain service unavailable by directing continuous and massive traffic from several storage systems. Due to the high volume of traffic, network resources are used to provide applications for these rogue terminal programmes, preventing genuine users from accessing the resources.

Types of DDoS attacks -

DDoS attacks can be divided into three main categories:

1. **Application Layout Attack -**

   This attack focuses on the assault on layer 7 of the SI model, where web pages are produced to reply to a request initiated by the end user. Applying does not need a large amount of time for the client and may quickly generate several requests on the server. On the other hand, responding to a request takes an enormous toll on the server since it has to create all the pages, compile any queries, and upload the results from the website upon request.

   Examples: HTTP Flood Attack and Attack on DNS Services.

2. **Protocol Attack -**

   They are also known as state attacks. This attack is based on the vulnerability of the protocol stack's layer 3 and layer 4. These types of attacks make advantage of resources such as servers, firewalls, and loading bays.

   Examples: SYN Flood and Ping of Death.

3. **Volumetric Attack -**

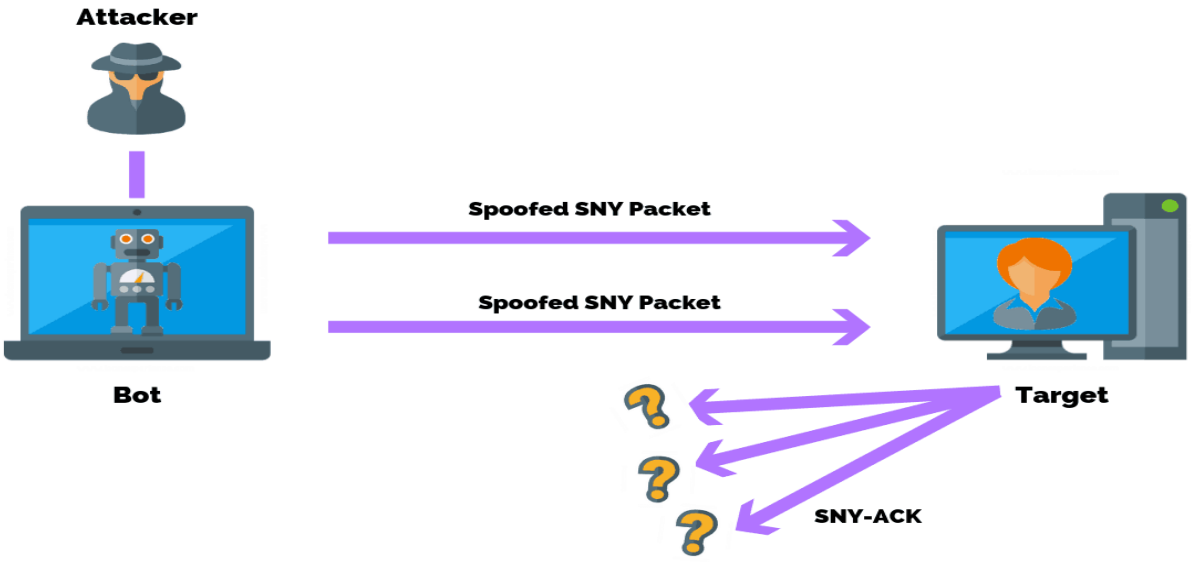
Volumetric ttack focuses on exploiting network bandwidth and saturating it with a boost or botnet to prevent its availability to users. It is simple to do simply directing large amounts of traffic to a certain server.

Examples: NTP Expansion, DNS Expansion, UDP Flood Attack and TCP Flood Attack.

Common DDoS attacks -

- ### SYN Flood Attack -

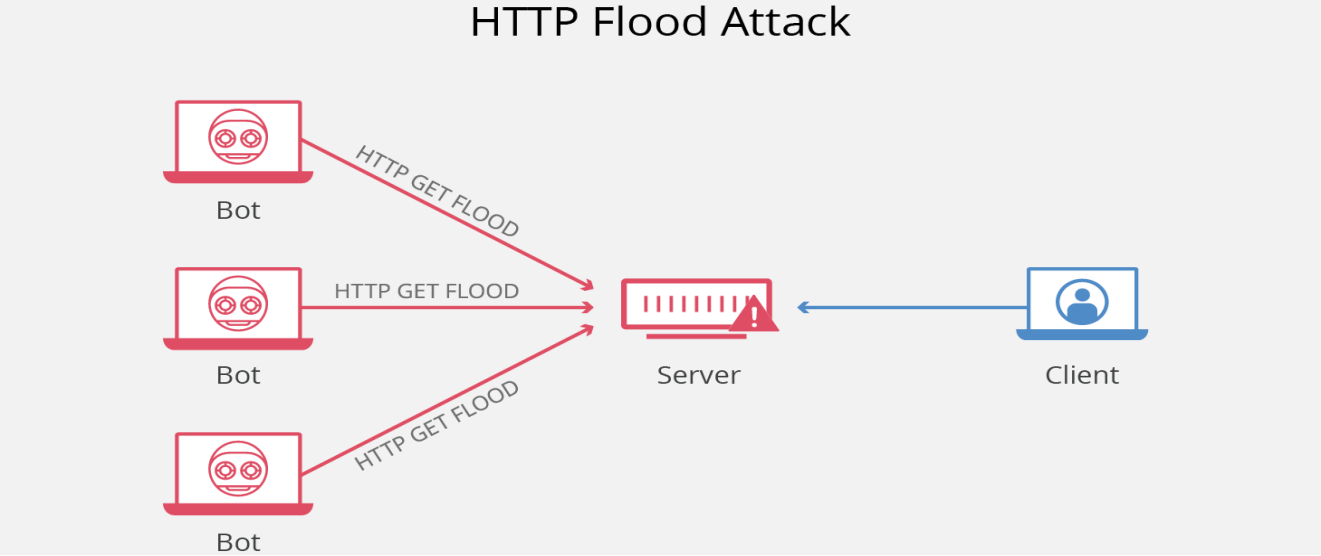
  The Flood SYN attack operates in the same way: the naughty child rings the doorbell (begs) and runs away. An old man came in and opened the door without seeing anyone (no answer). Finally, after such common situations, an adult grows tired and does not respond to real people. SYN ttack employs T Handshake by sending SYN messages with a malicious I address. The victim's server is still responding, but it is not receiving the most recent information.



- **HTTP flood attack –**

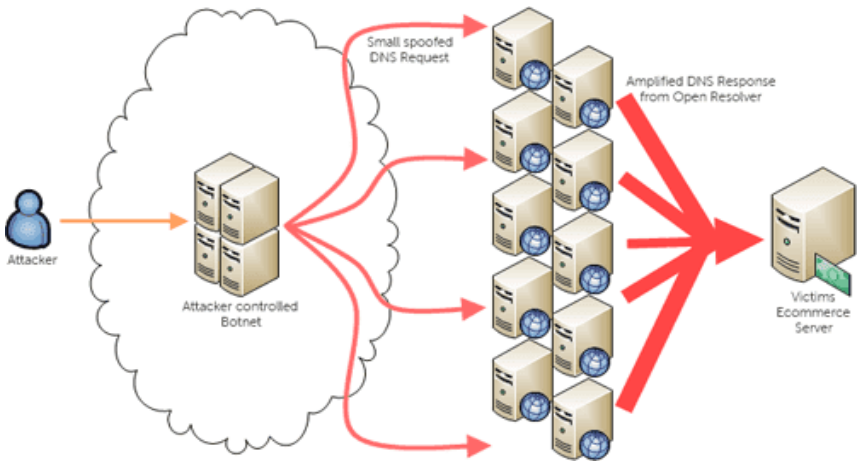
  Multiple HTTP requests were sent against the targeted server at the same time during the HTTP Flood attack. This causes the network's network resources to be depleted and so fails to satisfy the

needs of real users. HTTP Flood attacks come in two varieties: HTTP GET attacks and HTTP POST attacks.



- **DNS amplification –**

  Assume you phone a Pizza Hut and ask them to call you back on a number and give you all the pizza combinations they have. As a result, the large output is created with a tiny input. However, the number you gave them is not yours. Similarly, DNS mplification works by asking a DNS server from a corrupted IP address and organizing your request so that the DNS server responds with large volumes of data to the target victim.



DDoS mitigation -

DDoS assaults are more difficult to prevent than DDoS attacks because traffic arrives from various sources and it is difficult to separate malicious strangers from non-malicious hosts. Some of the mitigating strategies that can be implemented include:

- **Blackhole Route -**

  Network traffic is targeted at a 'black hole' in blackhole routing. In this case, both brutal traffic and non-violent traffic are lost in the black hole. This bargaining action is important when the server is attacked by DDOS and all traffic is moved to maintain the network.

- **Rate Limiting -**

  Reducing the rate entails controlling the amount of traffic transmitted or received by the network interface. It's great for slowing down site scrapers and brute-force intrusion attempts. However, merely restricting the size is insufficient to avoid integrated DDoS assaults.

- **Blacklisting / Whitelisting -**

  Blacklisting is a method of blocking IP addresses, URLs, domain names, and so on that are included in the list, as well as allowing traffic from all other sources. Whitelisting, on the other hand, refers to the process of approving all I addresses, URLs, domain names, and so on stated in the list while refusing all other resources access to network resources.