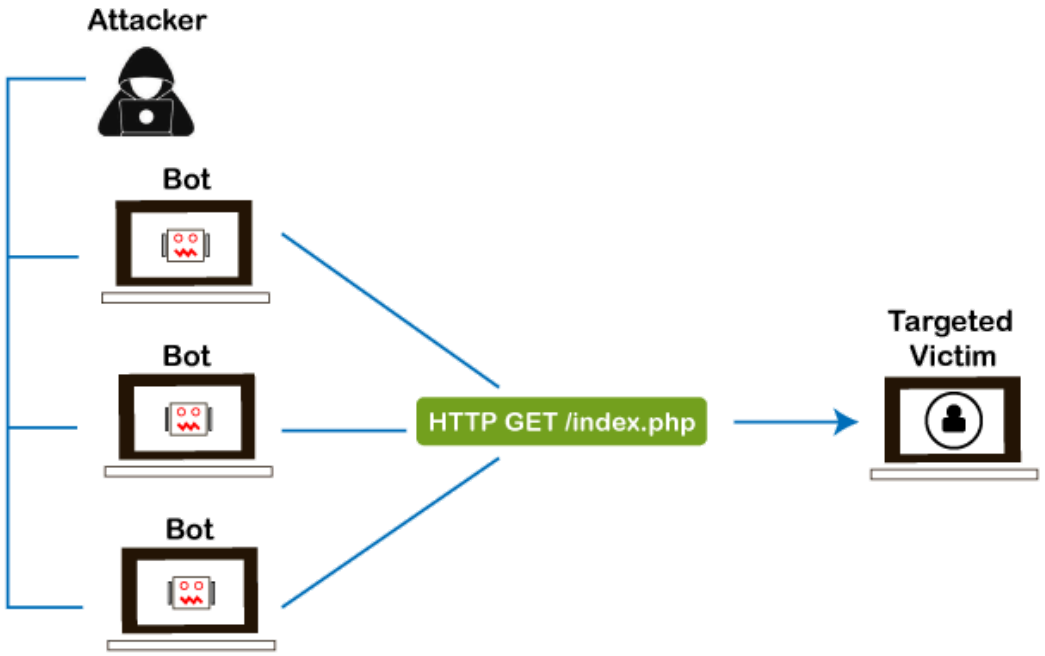
3) Describe different types of DOS attack with neat diagram

A Denial-of-Service (DoS) attack is an attack on a computer network that limits, restricts, or stops authorised users from accessing system resources.



Types of DoS attack

1. HTTP Flood
HTTP flood is similar to you hitting refresh on your browser several times. It is just that it is done at a much large scale to crash the webserver and restrict the legitimate users from reaching the webserver.

2. Ping Flood/ICMP Flood
In this attack, the target machine is sent so many ping requests that it is overwhelmed and fails to respond

3. Ping of Death
In this attack, the target machine is sent malformed packets such that the system is unable to understand and process them resulting into system crash.

4. Smurf Attack
The victim's IP address is used as the recipient for receiving respons

es from broadcast communication. The attacker then crafts a request such that all the computers in a network respond to the victim's IP address such that it is overwhelmed and crashes.

5. DNS Amplification
As you know, DNS server resolves the domain name to an IP address. The attacker crafts a DNS request (with the target's IP address) such that the DNS server responds with a large amount of data and crashes the target

6. SYN Flood
In SYN flood attacks, the attacker exploits the way a TCP connection is established. After sending the SYN packet to the target, the attacker does not respond with the ACK packet. The target keeps on waiting for the ACK until it runs out of the resources. The attacker sends multiple such SYN packets until the resources on the target are totally consumed and the target can no longer receive any SYN packets further.

7. UDP Flood
UDP flood occurs when the target receives multiple UDP packets and it needs to check if there are any UDP ports listening for UDP traffic. It wastes a lot of target resources in conducting such searches for port numbers and thus the target becomes too busy to serve any legitimate traffic thus impacting its availability.

9. Describe SNMP V3 protocol in brief?

Simple Network Management Protocol version 3 (SNMPv3) is an updated and more secure version of the SNMP protocol, which is used for managing and monitoring network devices and systems. SNMPv3 introduces several important security enhancements compared to its predecessors (SNMPv1 and SNMPv2). Here is a brief overview of SNMPv3:

Authentication:

- SNMPv3 provides authentication mechanisms to ensure the legitimacy of SNMP messages. It uses HMAC-MD5 (Message Digest 5) and HMAC-SHA (Secure Hash Algorithm) for authentication.
- Authentication helps prevent unauthorized access and tampering of SNMP messages by ensuring that the sender is who they claim to be.

Encryption (Privacy):

- SNMPv3 offers data encryption for SNMP messages, ensuring the confidentiality of the information being exchanged. It uses protocols like DES (Data Encryption Standard), 3DES, and AES (Advanced Encryption Standard) for privacy.
- Privacy mechanisms protect sensitive data from eavesdropping during transmission.

User-based Security Model (USM):

- SNMPv3 introduces the User-based Security Model, which allows for multiple users or security profiles with different access levels and authentication/privacy settings.
- Each user is associated with a security name, authentication, and privacy protocols, and access control policies.

View-Based Access Control Model (VACM):

- VACM is used in SNMPv3 to control and restrict access to SNMP-managed resources. It specifies which SNMP objects can be accessed by which users or communities.
- VACM provides fine-grained access control based on the user's security credentials.

Message Integrity:

- SNMPv3 ensures message integrity by using authentication. It calculates a message digest (hash) of the message and includes it in the SNMP packet. The recipient can then verify the digest to detect tampering.

Message Replay Protection:

- SNMPv3 includes a mechanism to protect against message replay attacks. Each SNMP message contains a timestamp, and the recipient can check whether the message is within an acceptable time window.

Notification Enhancements:

- SNMPv3 supports the sending of SNMP notifications (traps or informs) with authentication and encryption, making the notification process more secure.

Backward Compatibility:

- SNMPv3 is designed to be backward-compatible with SNMPv1 and SNMPv2c. This allows network administrators to gradually migrate to SNMPv3 while still supporting older SNMP versions.

In summary, SNMPv3 is a more secure and robust version of the SNMP protocol, addressing many of the security concerns that were present in earlier versions. It provides authentication, encryption, and access control features to ensure the confidentiality, integrity, and availability of network management data