Types of DDoS attacks

Distributed Denial of Service (DDoS) attacks involve overwhelming a target's network, service, or website with a flood of internet traffic, rendering it unavailable to legitimate users. There are several types of DDoS attacks, each targeting different components of a network or application. Here's a breakdown of the main types:

1. Volume-Based Attacks

These attacks aim to saturate the bandwidth of the target site or network.

- **UDP Flood**: In a UDP (User Datagram Protocol) flood, large volumes of UDP packets are sent to random ports on a target, overwhelming its ability to respond, leading to a crash or denial of service.
- **ICMP Flood (Ping Flood)**: Attackers send a high volume of ICMP Echo Request (ping) packets to the target, overwhelming its ability to process the incoming and outgoing traffic.
- **Amplification Attacks**: Attackers use a small amount of traffic that gets amplified by intermediary servers (like DNS servers) to generate a massive amount of traffic aimed at the target. Examples include DNS amplification and NTP amplification attacks.

2. Protocol Attacks

These attacks consume resources at the network, transport, and session layers.

- **SYN Flood**: In a SYN flood, the attacker sends a large number of TCP/SYN packets, often with spoofed sender addresses. The server allocates resources for each incoming SYN packet but does not receive the expected ACK response, causing resource exhaustion.
- **ACK Flood**: Similar to SYN floods, ACK floods target the acknowledgment phase of the TCP handshake, overwhelming the target's ability to process TCP packets.
- **Ping of Death**: Attackers send malformed or oversized packets to a target, which can cause the system to crash or become unresponsive.

3. Application Layer Attacks

These attacks target the application layer, aiming to exhaust server resources or disrupt application-specific functionality.

- **HTTP Flood**: The attacker sends numerous HTTP requests (GET or POST) to the target web server, overwhelming it and causing it to become unresponsive.
- **Slowloris**: This attack method involves sending partial HTTP requests to the target server, keeping many connections open and incomplete. The server is kept busy waiting for the completion of these requests, preventing it from processing legitimate ones.
- **DNS Query Flood**: Attackers flood the DNS server with a large number of requests, exhausting its resources and making it unable to respond to legitimate queries.

4. Fragmentation Attacks

These attacks involve sending fragmented packets that require the target to reassemble them, consuming excessive resources.

- **IP Fragmentation Attack**: Attackers send fragmented packets, which require the target to reassemble them. If the reassembly buffer is overwhelmed, it can lead to service disruption.
- **Teardrop Attack**: In this type of attack, fragmented packets with overlapping payloads are sent to the target, causing it to crash or become unstable due to its inability to reassemble the packets correctly.

5. Multi-Vector Attacks

- **Combination Attacks**: These attacks combine multiple types of DDoS methods, such as combining volume-based, protocol, and application layer attacks simultaneously. Multi-vector attacks are particularly challenging because they target different layers of the network stack, making them harder to mitigate.

6. Botnet-Based Attacks

- **Botnet DDoS**: Attackers use a network of compromised devices (botnets) to launch a DDoS attack. The sheer scale of the attack makes it difficult to defend against. Botnets can be used to carry out any of the above types of attacks on a massive scale.

7. Connection Flood Attacks

- **TCP Connection Exhaustion (Sockstress)**: Attackers maintain open TCP connections to exhaust server resources, leading to a denial of service.

8. Application Exploit Attacks

- **Zero-Day DDoS Attacks**: These attacks exploit previously unknown vulnerabilities in applications or protocols to cause a denial of service.

9. IoT-Based Attacks

- **Mirai and Similar Botnets**: Attackers exploit vulnerabilities in Internet of Things (IoT) devices to build massive botnets capable of launching devastating DDoS attacks.

Mitigation Techniques

- **Traffic Filtering**: Use of firewalls, intrusion prevention systems (IPS), and web application firewalls (WAF) to filter out malicious traffic.
- **Rate Limiting**: Limiting the rate of incoming requests to ensure that the server isn't overwhelmed.
- **Content Delivery Networks (CDNs)**: Distributing traffic across multiple servers to reduce the impact of DDoS attacks.

- **DDoS Mitigation Services**: Specialized services that detect and mitigate DDoS attacks in real time, often by absorbing and filtering traffic before it reaches the target.