1. What is Service Attack?

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

1. Dos Attack?

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash

1. Type of Dos Attack?

* Application-layer Flood. In this attack type, an attacker simply floods the service with requests from a spoofed IP address in an attempt to slow or crash the service, illustrated in. This could take the form of millions of requests per second or a few thousand requests to a particularly resource-intensive service that eat up resources until the service is unable to continue processing the requests.
* Distributed Denial of Service Attacks (DDoS).
* Unintended Denial of Service Attacks.

1. Distributed Dos Attack?

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

1. Type of Distributed Dos Attack?

* ICMP (Ping) Flood.
* SYN Flood.
* Ping of Death.
* Slowlories.
* NTP Application.
* HTTP Flood.
* Zero-day DDoS Attacks.
* Volume Based Attacks. Imperva counters these attacks by absorbing them with a global network of scrubbing centers that scale, on demand, to counter multi-gigabyte DDoS Attacks.