Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 2

Aim : The MGTech assurance Pvt. Ltd. company has appointed you as server administrator. Your task is to ensure the server is always available to process the client request. Also identify the threats to availability of server. Prepare a detailed document for the said task with below topic detailed study.

1) Types of DOS

1. What is DOS (Denial Of Service) Attack?

- A Denial of Service (DOS) attack is a malicious attempt to disrupt the normal operation of a computer system, network, or service by overwhelming it with a flood of illegitimate requests, rendering it inaccessible to legitimate users.

- It generally happens in context of a server responding to the online requests.

2. Types of DOS attacks :

a) **Volume-Based Attacks** : They aim to overwhelm the target's bandwidth or network resources by flooding it with a massive volume of traffic. This type of attack doesn't necessarily target vulnerabilities in the application or infrastructure but seeks to exhaust available resources.

Examples :

- Ping Flood : Overloads the target with a massive number of ICMP Echo Request (ping) packets. Impact : Exhausts network bandwidth and overwhelms the target's resources.
- UDP Flood : Floods the target with User Datagram Protocol (UDP) packets. Impact : Consumes network resources, leading to service unavailability.

b) **Protocol-Based Attacks :** Protocol attacks exploit weaknesses in the communication protocols used in networking. These attacks consume server resources by exploiting the way protocols are designed to handle communication.

Examples :

- SYN/ACK Flood : A protocol-based DoS attack exploiting the TCP three-way handshake. The attacker sends a massive number of SYN (synchronization) requests to the target, but does not complete the handshake, leading to resource exhaustion on the target system.
- HTTP/S Flood : A protocol-based DoS attack where the attacker floods a web server with an excessive number of HTTP or HTTPS requests. The goal is to overwhelm the server's processing capacity, causing it to slow down or become unresponsive.

c) **Application-Layer Attacks :** Application-layer attacks target vulnerabilities in specific applications or services, aiming to exhaust resources at the application level. These attacks often require less bandwidth compared to volumetric attacks but can be highly effective in disrupting services.

Examples :

- HTTP/S Request Flood : An application layer DoS attack that involves overwhelming a web application with an exceptionally high volume of HTTP or HTTPS requests. This flood of requests is designed to exhaust the application's resources, making it unresponsive to legitimate users.
- Slowloris : An application layer DoS attack where the attacker deliberately delays sending parts of an HTTP request to a web server. By keeping multiple connections open with partial requests, the attacker exhausts the server's connection-handling capacity, leading to a denial of service.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 2

2) One Case Study - How it happened? When it happened? What is impact or damage caused? What Precautions they took for Prevention? How did they overcome this situation?

In May 2023, Samsung disclosed that hackers exploited a vulnerability in a third-party business application to access the contact information of some U.K. customers who made purchases at Samsung's online store between July 2019 and June 2020.

The issue, tracked as CVE-2023-21492 (CVSS score: 4.4), impacts select Samsung devices running Android versions 11, 12, and 13.

A tracking spreadsheet maintained by Google Project Zero documenting known cases of detected zero-day exploits shows that the Samsung security vulnerability was discovered by Clement Lecigne of the Google Threat Analysis Group (TAG), indicating likely abuse in connection with a spyware campaign.

Samsung said it reported the issue to the authorities and fixed the flaw, but did not reveal how many customers were affected or how the hackers carried out the attack.