

6.B. Perform the DDoS Attack using the following tools

◆ (i) HOIC (High Orbit Ion Cannon)

Aim

To simulate a Distributed Denial-of-Service (DDoS) attack using HOIC.

Tools Used

- HOIC Tool
 - Windows Operating System
-

Theory

HOIC is a network stress-testing tool used to send a large number of HTTP requests to a target server, making it unavailable to legitimate users.

Steps / Procedure

1. Open **HOIC** tool.
 2. Enter the **target website URL**.
 3. Select attack method.
 4. Set number of threads.
 5. Click on **Fire** to start the attack.
 6. Monitor traffic sent to the target.
-

Result

DDoS traffic was generated using HOIC.

◆ (ii) LOIC (Low Orbit Ion Cannon)

Aim

To perform a simulated DDoS attack using LOIC.

Tools Used

- LOIC Tool
-

Steps / Procedure

1. Open **LOIC**.
 2. Enter target IP address or URL.
 3. Select protocol (TCP/UDP/HTTP).
 4. Set attack speed.
 5. Click **IMMA CHARGIN MAH LAZER**.
 6. Observe outgoing traffic.
-

Result

LOIC successfully generated high traffic towards the target.

◆ (iii) HULK (HTTP Unbearable Load King)

Aim

To perform HTTP flood attack using HULK.

Tools Used

- Kali Linux
- HULK Script

Steps / Procedure

1. Open **Kali Linux Terminal**.
2. Navigate to HULK directory.
3. Run HULK script.
4. Enter target URL.
5. Observe multiple HTTP requests sent to server.

Result

HTTP flood attack was simulated using HULK.

⚠ Note (Important for Examiner)

DDoS attacks are demonstrated **only for academic and testing purposes** in a controlled environment.