# Module 10: Denial-of-Service - Practical Guide

This guide details the technical tools and hands-on laboratory procedures for testing and defending against Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks.

## 1. Comprehensive **DoS**/DDoS Toolset

### Volumetric Attack Tools (Bandwidth Exhaustion)

* **LOIC (Low Orbit Ion Cannon):** A user-friendly, GUI-based tool that performs TCP, UDP, and HTTP floods. It is "noisy" because it does not mask the attacker's IP.
* **HOIC (High Orbit Ion Cannon):** An evolution of LOIC that uses "Boost" scripts to randomize headers and bypass simple firewalls.
* **XOIC:** Another easy-to-use GUI flood tool with three modes: test, small-scale, and professional.

### Protocol Attack Tools (TCP/IP Stack Exhaustion)

* **Hping3:** The most versatile command-line tool. It allows for manual packet crafting to perform SYN floods, ICMP floods, and UDP floods with IP spoofing capabilities.
* **Metasploit Auxiliary Modules:** Contains specific modules like auxiliary/dos/tcp/synflood to automate the process within the MSF console.

### Application Layer Attack Tools (Resource Exhaustion)

* **Slowloris:** A specialized tool that keeps many HTTP connections open by sending partial headers and never finishing the request. Highly effective against Apache servers.
* **R.U.D.Y. (R U Dead Yet?):** Performs a "Low and Slow" attack by submitting long form-field data one byte at a time to exhaust web server threads.
* **Mantis:** A high-power modern botnet tool used specifically for targeting Cloud and HTTP/2 infrastructure with high-intensity request floods.

## 2. Hands-On Lab Sessions

### Lab 1: Performing a SYN Flood Attack (Hping3)

**Goal:** Exhaust the connection table of a target system to prevent new legitimate connections.

1. **Preparation:** Identify the target IP address in your lab environment.
2. **Execution:** Run the following command in the Parrot OS terminal:  
   sudo hping3 -S [Target\_IP] -p 80 --flood --rand-source
3. **Command Breakdown:**
   * -S: Sets the SYN flag.
   * -p 80: Targets the HTTP port.
   * --flood: Sends packets as fast as possible without waiting for responses.
   * --rand-source: Spoofs random source IP addresses to bypass simple IP-based blocking.
4. **Verification:** On the target machine, run netstat -an | grep SYN\_RECV. You should see a massive list of connections "stuck" in the half-open state.

### Lab 2: Application Layer "Low and Slow" Attack (Slowloris)

**Goal:** Crash a web server using minimal bandwidth by exhausting its available worker threads.

1. **Preparation:** Ensure the target web server (e.g., Apache) is running.
2. **Execution:** Use the slowloris tool (often available as a Python script or apt package):  
   slowloris [Target\_URL\_or\_IP]
3. **Analysis:** Observe that the tool does not send large amounts of data. Instead, it maintains hundreds of connections simultaneously.
4. **Verification:** Try to load the target website in a browser. It will likely hang indefinitely or return a "Connection Timed Out" error.

### Lab 3: Generating Volumetric Traffic (LOIC)

**Goal:** Simulate a basic volumetric flood.

1. **Launch:** Open LOIC (on Windows or via Wine in Parrot).
2. **Targeting:** Enter the IP or URL in the "Selected Target" box and click **Lock On**.
3. **Configuration:**
   * Set the **Method** to UDP or TCP.
   * Increase the **Threads** (e.g., 50-100).
   * Ensure the **Speed** slider is set to the maximum.
4. **Attack:** Click the large button labeled **"IMMA CHARGIN MAH LAZER"**.
5. **Note:** LOIC is primarily used to demonstrate how bandwidth can be consumed; it provides no anonymity for the attacker.

### Lab 4: Capturing and Analyzing DoS Traffic (Wireshark)

**Goal:** Identify the signature of a DoS attack in progress.

1. **Start Capture:** Launch Wireshark on the target or a gateway and monitor the active interface.
2. **Launch Attack:** Start the SYN flood from Lab 1.
3. **Analysis:** \* Look for a sudden spike in the **IO Graph**.
   * Identify the high frequency of packets with only the **SYN** flag set.
   * Notice the lack of **ACK** packets returning from the scanner's IP (or spoofed IPs).

## 3. CEH Practical Tips for Module 10

* **Metric Distinction:** Remember that **Volumetric** attacks are measured in **bps** (bits per second), while **Protocol** attacks are measured in **pps** (packets per second).
* **The "Half-Open" State:** Any question regarding a SYN flood is referring to a "Half-Open" connection where the final ACK of the 3-way handshake is never sent.
* **Amplification Logic:** In amplification attacks (DNS/NTP), the attacker spoofs the **Victim's IP** as the source, sending small requests to third-party servers to trigger huge responses directed at the victim.