**CTF Challenge: Denial-of-Service**

**What is Denial-of-Service?**

****

"Denial-of-service" (DoS) attacks are malicious attempts to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic. Here are some key points about denial-of-service:

### **Types of DoS Attacks**



1. **Volumetric Attacks**: Consume the bandwidth of the target or between the target and the rest of the internet. Examples include UDP floods and ICMP floods.
2. **Protocol Attacks**: Exploit weaknesses in network protocols. Examples include SYN floods and Ping of Death.
3. **Application Layer Attacks**: Target specific applications or services, exhausting their resources. Examples include HTTP floods and Slowloris.

### **Distributed Denial-of-Service (DDoS)**

* **DDoS Attacks**: Similar to DoS but involve multiple compromised systems (often part of a botnet) attacking a single target, making it harder to mitigate.

### **Tools for DoS Attacks**

* **LOIC (Low Orbit Ion Cannon)**: An open-source network stress testing and DoS attack tool.
* **HOIC (High Orbit Ion Cannon)**: A more powerful version of LOIC with improved features.
* **hping**: A command-line tool used to generate custom TCP/IP packets for testing network security.

### 

# **Capture the Flag (CTF) Challenges**

**Flag 1. Which type of DoS attack consumes the bandwidth of the target?**

Answer: **Volumetric**

**Flag 2. What is the more powerful version of LOIC called?**

Answer: **HOIC**

**Flag 3. Which protocol attack involves exploiting weaknesses in network protocols?**

Answer: **SYN Flood**

**Flag 4. What tool is used to generate custom TCP/IP packets for network security testing?**

Answer: **hping**

**Flag 5. What term describes using multiple compromised systems to attack a single target?**

Answer: **DDoS**