# DDoS Offensive & Defensive Tools Cheat Sheet

## Offensive DDoS Tools (For Educational & Testing Purposes Only)

### LOIC (Low Orbit Ion Cannon)

Description: Open-source stress testing tool that sends massive amounts of TCP/UDP/HTTP requests.

Usage: loic.exe or java -jar LOIC.jar, select target IP/URL, choose method, set thread count, and fire.

### HOIC (High Orbit Ion Cannon)

Description: Advanced LOIC variant supporting booster scripts for stronger attacks.

Usage: Run HOIC.exe, load target list, set booster scripts, adjust threads, and start attack.

### UDP Flood (Hping3)

Description: Floods target with UDP packets to consume bandwidth.

Usage: hping3 --udp -p 80 -i u100 <target-ip>

### ICMP Flood (Ping)

Description: Sends continuous ICMP echo requests to exhaust network capacity.

Usage: ping <target-ip> -t -l 65000 (Windows) | ping -s 65500 <target-ip> (Linux)

### PBotnet

Description: Python-based botnet framework for simulated DDoS testing.

Usage: python pbotnet.py --attack <target-ip> --method udp --time 60

## Defensive DDoS Tools

### Anti-DDoS Guardian

Description: Filters suspicious traffic, limits connections, prevents UDP/TCP floods.

Usage: Install → Configure connection limit rules → Set packet filter policies.

### DDoS-Guard

Description: Cloud-based DDoS protection that blocks malicious requests before they reach the server.

Usage: Sign up → Point DNS to DDoS-Guard → Configure filtering rules.

### Radware DefensePro

Description: Real-time attack mitigation using behavioral analysis.

Usage: Deploy appliance → Set attack thresholds → Monitor real-time dashboard.

### Cloudflare

Description: Reverse proxy filtering malicious traffic before reaching your site.

Usage: Sign up → Change DNS to Cloudflare → Enable DDoS protection in dashboard.

### Akamai Kona Site Defender

Description: Cloud WAF + DDoS protection with traffic scrubbing.

Usage: Integrate with DNS/CDN → Enable site defender profile → Configure security rules.