- Filename: eccouncil-ceh31250-v11-10-2-1-volumetric-attacks.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Denial of Service
- Episode Name: Volumetric Attacks
  ==========

Volumetric Attacks

Objectives:

- List and describe common types of Volumetric DoS/DDoS attacks

---

- Volumetric Attacks
  - Amplification attacks
    - UDP Flood
      - Attacker floods target with UDP packets from spoofed IP
      - Target checks for UDP service
      - Target responds with 'Destination Unreachable' error
      - Legit traffic can't access server
        - `hping3 --flood --spoof 192.168.241.133 --udp -p 53 192.168.241.130`
    - ICMP Flood
      - Reflection networks are useful here
      - Requests and Replies saturates the network
        - `hping3 --flood --spoof 192.168.241.133 --icmp -p 53 192.168.241.130`
    - Ping of Death
      - Oversized packet
        - Size greater than 65535 bytes
          - System crashes
    - Smurf & Fraggle
      - DDoS target with ICMP echo replies
        - Send ICMP echo request to network broadcast address with spoofed source IP of target
        - If network allows directed broadcast requests, all hosts on network will respond to target with ICMP echo replies
          - `hping3 --flood --spoof --icmp 192.168.241.130 192.168.241.255`
      - Fraggle
        - Similar to Smurf
          - UDP instead of ICMP
          - Targets ports 7(Echo) and 19(CHARGEN)
    - Pulse Wave
      - Attacker sends data to target for every 10 minutes
      - Attack pulses(attack session) can last for hours or days
      - Pulses are 300Gbps