- Filename: eccouncil-ceh31250-v10-10-1-2-denial_of_service_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Denial of Service Pt.2
- Description: In this episode, Daniel and Zach discuss the concepts and techniques for performing Denial of Service and Distributed Denial of Service attacks. Here they pick up by looking at Volumetric attacks like the Ping-of-Death, Smurf, Fraggle, UDP flood, and ICMP flood attacks.

==========

Denial of Service Pt.2

- **With that said, can you give us some examples of a volumetric DoS attack?**
- Volumetric attacks
    - Ping of Death
        - Been patched for years
        - Send an oversized packet using ping
            - RFC 791 IP only allows for packets no greater than 65535 bytes in size
            - `ping -c 10000000 -s 65555 -w 0.000001 10.0.0.200`
    - Smurf
        - DDoS target with ICMP echo replies
            1. Send ICMP echo request to network broadcast address with spoofed source IP of target
            2. If network allows directed broadcast requests, all hosts on network will respond to target with ICMP echo replies
        - `hping3 -1 -c 10000000 10.0.0.255 --fast -a 10.0.0.165`
        - Demo **smurfy.sh**
    - Fraggle
        - Smurf with UDP
    - UDP Flood attack
        - Hammer the target with UDP requests
            - `hping3 --flood --rand-source --udp -p 53 10.0.0.165`
                - Watch ping response times in another terminal
                    - Response time will continue to drop as new instances of hping3 are instantiated
                        - Eventually target will respond with errors
    - ICMP Flood
        - `hping3 -1 --flood --rand-source 10.0.0.165`