- Filename: eccouncil-ceh31250-v12-10-3-1-protocol-attacks.md
- Show Name: CEHv12 (312-50)
- Topic Name: Network and Perimeter Hacking: Denial of Service
- Episode Name: Protocol Attacks
  ==

Protocol Attacks

Objectives:

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

---

- Give us some info about common Protocol-based DoS/DDoS attacks.

    - SYN Flood

        - Remember TCP 3-way handshake

            - What does the SYN packet do? (starts to establish a connection)

                - The target must track partially open connections (**listen queue**)

                    - Listen Queue tracks for at least 75 seconds

        - Attacker sends multiple SYN request

            - Never responds to the SYN/ACK (SYN/ACK flood is similar to this attack)

                - `sudo hping3 --syn --flood -p RPORT RHOST`
                - Target's listen queue is overwhelmed

                    - Target can no longer service connection requests

    - ACK / PSH-ACK Flood

        - Send a bunch of ACK or PSH-ACK packets to target

            - LOIC DEMO (tcp attack is a PSH-ACK attack)

    - Fragmentation

        - Attacker sends large number of fragmented packets

            - Target's resources are consumed as it is overwhelmed trying to reassemble fragmented packets

                - Attack is more effective if fragments are randomized

        - Can bypass firewalls/IDS/IPS solutions