**Module 8 Denial of Service**

**8.0 Denial of Service**

**DoS (Denial of Service) /DDoS (Distributed DoS)**

1. Prevent legit users from accessing resource
2. C.I.A. Triad
3. Types of attacks
   1. UDP Flood
      1. Large number of UDP packets to random ports
      2. Target replies with ICMP Destination Unreachable
      3. Tools – LOIC, UDP Unicorn
   2. ICMP Flood
      1. Ping (echo request) packets
      2. More successful if attacker has bandwidth advantage
   3. Ping of Death & Smurf
      1. Ping of death – send malformed ping packet with goal of causing buffer overflow
      2. Smurf attack – spoofs victim IP & sends large amount of ICMP packets
   4. SYN Flood – attacker sends SYN packets
   5. Slowloris
      1. Opens connections on target
      2. Never completes the request
      3. Goal is to have server block other connections
      4. Mitigation – limit number of connections for single IP address
   6. Distributed Reflection Denial-of-Service (DRDoS)
      1. Use UDP packets
      2. Availability

**Botnets**

1. “Zombie” computers or devices controlled remotely

**DDoS & botnet Countermeasures**

1. Recognise early signs
2. Contact ISP
3. Incident response plan
4. Load balancer
5. Anti-DDoS Solution (Cloud)