- Filename: eccouncil-ceh31250-v10-10-1-1-denial_of_service.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Denial of Service
- 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 begin by looking at explaining the types of DoS/DDoS attacks and the difference between the two. They also explain the concepts behind amplification and reflective DoS attacks.

==========

Denial of Service

- **Could you start us off by defining Denial of Service?**
    - A partial or total interruption of access to a network service
        - Usually caused by malicious intent
        - Achieved through
            - Bandwidth consumption (volumetric)
                - *Bits-per-Second*
            - Protocol Attacks
                - Local resource consumption (CPU/RAM/DISK)
                - Intermediate communication equipment resources
                    - Firewall
                    - Load Balancer
                    - *Packets-per-second*
            - Application Layer Attacks
                - Specifically targets the functions and resources of a particular app
                    - Can disable just that particular service
                        - Other services not affected
                    - Can disable specific functions of a specific service
                - *Requests-per-second*
- **Could you clear up the difference between Denial of Service and Distributed Denial of Service?**
    - DIAGRAM
    - DoS
        - Single point of attack
    - DDoS
        - Multiple attack points
            - Coordinated attack
                - Anonymous attack on Church of Scientology
            - Unintentional
                - Michael Jackson's death takes down google/twitter
                - Ellen crashes twitter
                - "Reddit hug of death" or "Slashdotting"
                    - Large popular site links to smaller site
            - Botnets

        - Large number of zombie IoT devices
        - Then rented out for DDoS
            - DDoSaaS
                - Zombies/Bots
                - C&C/C2
                - Scanning methods
                    - DIAGRAM
- Amplification attacks
    - Make a request using spoofed source address
        - Reply is exponentially larger than request
            - Do this a bunch of times :)
    - Examples
        - Smurf, Fraggle, DNS amplification
- Reflected DoS attacks
    - Make a request using a spoofed source address
        - Replies are returned to target IP instead of attacker
            - This can be a distributed attack
                - Increases the effectiveness