- Filename: eccouncil-ceh31250-v10-10-1-3-denial_of_service_pt3.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Denial of Service Pt.3
- 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 explore protocol type attacks, specifically demonstrating a SYN flood attack. Finally they get into application layer attacks like HTTP GET/POST attacks and Slowloris using Metasploit. They also look at other DoS tools like the High and Low Orbit Ion Canons.

==

Denial of Service Pt.3

- **What about protocol attacks?**
- Protocol attacks
    - SYN Flood
        - Abuses the way the TCP 3-way handshake works
            - Ignores the SYN-ACK response of the target server
                - Target server will wait some time before closing the connection
                    - We exhaust the available TCP concurrent connections
        - `hping3 -c 10000000 -d 120 -S -w 64 -p 80 --flood --rand-source 10.0.0.165`
            - -d = data size
            - -w = window size
            - -S = SYN flag set
    - Fragmentation Attack
- **I guess all that's left is Application Layer attacks?**
- Application Layer attacks
    - HTTP GET/POST attacks
        - GET
            - Requests a connection using GET
                - Header has a time/wait feature
                    - Used to hold the connection
                        - Do this until connections are exhausted
        - POST
            - Body of message is incomplete
                - Forces server to wait for the rest of the body
    - Slowloris
        - Opens multiple connections
            - Send partial HTTP requests
                - Never intends to complete them
                    - Keeps them open as long as possible
        - When enough connections are open...
            - Server cannot service legitimate requests
        - Use Metasploit

      - `search slowloris`
      - `use auxiliary/dos/http/slowloris`
      - `set rhost TARGET_IP`
      - `exploit`
      - Attempt to browse target website :)

- **Any other attacks that we should be aware of?**
- Other attacks
  - Multi-vector
    - Simultaneous or sequential attacks via each attack category
  - Permanent DoS
    - Bricking device(s)
    - Phlashing
      - Upload damaging firmware
        - Infiltrate update repository
- **We've seen a lot of tools so far. Are there any others that we should know about for the CEH exam?**
- Tools
  - LOIC
    - TCP and UDP flooding
      - Mobile version exists
  - HOIC
    - Same as LOIC
    - Adds HTTP flooding capabilities
- **What are some ways that we can protect agains DoS?**
  - Traffic analysis and filtering
  - Rate limiting
  - Deflect to honeypots
  - Load balancing
  - DoS Prevention software/hardware