- Filename: eccouncil-ceh31250-v12-12-3-1-honeypots.md
- Show Name: CEHv12 (312-50)
- Topic Name: Network and Perimeter Hacking: Evading Firewalls, IDS, and Honeypots
- Episode Name: Honeypots
  ==

Honeypots

Objectives:

- What is a Honeypot?
    - IT'S A TRAP!!!
- Types of Honeypots
    - Low-Interaction
        - Narrow set of available services/apps
    - Medium-Interaction
        - Mimics a 'realistic' host
            - OS
            - Apps
            - Services
    - High-Interaction
        - Deploys ALL production services
    - Pure
        - Mimics real production host/network
- Honeypot Varieties
    - Client Honeypot
        - Puposefully gets pwned so the admins can see how the attacker utilizes it and any modifications that get made to it
    - Database Honeypot
        - Helps with gaining insights to DB-specific attacks
            - SQLi
    - Spam Honeypot
    - Malware Honeypot
        - Meant to capture malware samples
            - Handy for discovering new malware
    - HoneyNets
        - A mixed bag of Honeypots
            - Allows researchers to study multiple types of threats simultaneously
- Honeypot solutions
    - https://www.honeynetproject.com/honeypots.html
    - https://sourceforge.net/projects/honeydrive/