- Filename: eccouncil-ceh31250-v11-8-3-1-arp-poisoning.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Sniffing
- Episode Name: ARP Poisoning
  ==

ARP Poisoning

Objectives:

- Describe how ARP works
- List and describe common vulnerabilities and attacks against ARP

- How does ARP work?
  - Resolves IP to MAC
  - Helps hosts find other hosts
    - ARP Broadcasts
      - Wireshark demo (Who has this IP? Tell this device)
    - ARP Table
      - Dynamic ARP
      - `arp -a`
- Attacking ARP
  - ARP Cache Poisoning or ARP Spoofing Attack
    - Attacker can go after the switch
    - Attacker can go after the host
      - Threats
        - Sniffing
        - MitM
        - Session Hijacking
        - DoS
- ARP Poisoning Tools
  - BetterCAP
  - Ettercap - DEMO
  - dsniff
  - arpspoof
- Defenses?
  - DHCP Snooping and Dynamic ARP Inspection
    - Distrusts ARP packets until DHCP Snooping has verified it
  - Use STATIC ARP
  - ARP Attack detection tools
    - XARP
    - ARP AntiSpoofer