- Filename: eccouncil-ceh31250-v11-8-4-1-dns-poisoning.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Sniffing
- Episode Name: DNS Poisoning
  ==========

DNS Poisoning

Objectives:

- List and describe common DNS poisoning attack techniques and tools

---

- DNS basics
  - Resolve domains to IP
    - Windows DNS Lookup order
      - Checks self (am I the device I'm looking for?)
      - Checks DNS Resolver Cache
      - Checks the Hosts file (do I already know where this is?)
      - Checks with DNS Servers
- DNS Attacks
  - Modifying hosts DNS info
  - Tricks hosts to query malicious DNS
    - Host file entries
    - Malicious proxy
- DNS cache poisoning
  - Tricking clients into thinking that attacker is legit DNS
    - Redirect targets to malicious sites
  - **DEMO: Ettercap for DNS poisoning**
    1. Modify `etter.dns` file to have fake A records
       - Copy from Kali `/Tools/fakeArec.txt`
       - Change IP to match IP of bWAPP
    2. `ettercap -T -q -i eth0 -P dns_spoof -M arp /10.0.0.225//`
       - `-T` = Text Only
       - `-q` = Quiet. Do not display packet contents
       - `-i` = Set interface
       - `-P` = Choose plugin to use
       - `-M` = Perform MITM
       - /192.168.241.130//
         - /IPv4/IPv6/Port
    3. Browse to facebook from target
    4. Login to facebook/bWAPP and see user/pass info in Kali
- DNS Poisoning and Spoofing Tools
  - Ettercap
  - DNS Spoof
  - DerpNSpoof