- Filename: eccouncil-ceh31250-v11-8-2-1-dhcp-sniffing-attacks.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Sniffing
- Episode Name: DHCP Sniffing Attacks
  ==

DHCP Sniffing Attacks

Objectives:

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

- How does DHCP work?
    - DORA
        - Discover
        - Offer
        - Request
        - Acknowledgment
            - Demo: `dhclient` and Wireshark
- Common attacks?
    - Rogue DHCP
        - Connects targets to rogue network (maybe, gotta win the race or trick user)
            - DHCP sets...
                - IP addresses
                - DNS info
                - Gateway info
        - Results in...
            - DoS attack
                - Users that connect to rogue DHCP have no actual network access
            - Set's attacker as default gateway
                - Gateway bound traffic is intercepted by attacker
                    - MitM can occur (forward traffic to real gateway)
            - Set's attacker as DNS
                - Attacker can serve fake websites
                    - Credential Harvesting
                    - Sensitive info stealing