- Filename: eccouncil-ceh31250-v10-8-1-2-network_sniffing_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Network Sniffing Pt.2
- Description: In this episode, Daniel and Zach take the time to dive into the merits and practice of sniffing networks. Here they look at methods for packet sniffing on a switched network through MAC flooding, port stealing, and ARP poisoning. Finally, they discuss sniffing detection methods.

==

Network Sniffing Pt.2

- MAC Flooding
  - Fill the CAM table with fake entries
  - Switch then acts like a hub
    - Forwards all packets out all ports
- Port Stealing
  - MAC Spoofing/Duplicating
    - Windows
      - NIC properties > Advanced > Network Address > Value
    - Linux
      - `macchanger -m 11:aa:33:bb:55:ff`
  - DIAGRAM
- DHCP Starvation
  - Request IPs until scope is exhausted
  - A DoS type of attack
- Rogue DHCP
  - Competes for DHCP requests
  - Another DoS
- ARP Spoofing/Poisoning
  - Creates entries in victim's ARP Cache
  - Defend using
    - DHCP Snooping
    - ARP Spoof Detection Tools
- DNS Spoofing/Poisoning
  - Intercepts the DNS requests and returns malicious info
  - Changes DNS info
    - DNS Server IP to malicious DNS IP
    - DNS Resolver Cache poisoning
- **Is there any way to defend against these kinds of attacks?**
- Sniffing detection methods
  - Check for reverse DNS lookup traffic
    - Likely to be a sniffer
  - Ping suspected client with wrong MAC
    - Good clients reject
    - Sniffers accept and respond

- Nmap
    - `nmap --script=sniffer-detect 10.0.0.165`
        - DON'T FORGET TO ENABLE TCPDUMP!!!