- Filename: eccouncil-ceh31250-v11-8-1-1-network-sniffing-basics.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Sniffing
- Episode Name: Network Sniffing Basics
  ==========

Network Sniffing Basics

Objectives:

- Define network sniffing
- Explain the process of network sniffing
- Explain the usefulness of network sniffing to an attacker
- Describe how an attacker can sniff a switched network
- List and describe common sniffing attacks against network switches

---

- Sniffing Concepts and Tools
    - Capturing network traffic and inspecting its contents
        - Promiscuous Mode
            - Wireshark
            - TCP-Dump
            - Mobile apps
        - SPAN port aka "Port Mirroring"
        - Hardware Sniffers
            - https://www.gigamon.com/products/access-traffic/network-taps.html
- Sniffing Types
    - Passive
        - No activity to solicit or generate further network traffic
    - Active
        - Activity which generates more network traffic
            - Spoofing
            - Poisoning
            - Host Compromise
                - Compromised host used as internal sniffer
            - Malware
- Sniffing Switched Networks
    - Hubs vs. Switches
    - Switching
        - Switch Ports
        - Content Addressable Memory (CAM) Table
            - VLAN ID
            - MAC Address
            - Port ID
            - Learning Mode
                - Broadcasts out all ports

- CAM Attack
    - Flooding the switch with fake MACs will fill up the CAM
        - Learning Mode becomes the default mode
            - Switch fails open to Learning Mode
        - **macof** CAM flooding tool
            - Look at `macof` man page
- Switch Port Stealing
    - Is a 'MAC spoofing', 'Flooding' and 'Poisoning' attack against switch
        - Flood switch with spoofed MAC via ARP
            - MAC Spoofing Tools
                - `macchanger`
                - Advanced Properties of Network Interface in Windows
                    - Labled 'Network Address'
                - Windows Registry entry
                - Technitium MAC Address Changer
                    - https://technitium.com/tmac/
        - Race real host for control over switch "truth"
        - Switch is fooled or 'Poisoned', data is sent to attacker

◦ Other Switch-based attacks

- VLAN Hopping
    - Allows you to access to other VLANs
        - Attacker can now sniff that traffic
    - Accomplished through...
        - Switch Spoofing
            - Attacker-controlled switch
                - Connects to target network
                    - Forces trunk link to attacker switch
        - or Double-Tagging
            - Attacker creates Ethernet Frames with 2 802.1Q tags
                - Inner tag
                - Outer tag
            - Target switches receive malicious Frame
                - Strips off outer tag
                    - Forwards Frame using Inner tag through all trunk interfaces
- STP Attack
    - Attack switch is set to gain Root-Bridge status
        - All traffic now flows through Root-Bridge and can be sniffed