- Filename: eccouncil-ceh31250-v10-8-1-1-network_sniffing.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Network Sniffing
- Description: In this episode, Daniel and Zach take the time to dive into the merits and practice of sniffing networks. Here they explain why you would want to sniff network traffic and how that is accomplished. Then they show you how to capture packets and sift through that data using Wireshark.

==========

Network Sniffing

- **What is the purpose of sniffing a network?**
    - Look at network data
    - Could contain sensitive information
        - CC Numbers
        - PII
        - Usernames:Passwords
- **How is this accomplished?**
    - BASICALLY
    - Promiscuous mode
    - Passive sniffing
        - Simply "listens" to network traffic
            - Usually on hub network
    - Active sniffing
        - Switched networks
            - Performs attack to force switch into sending all data out all ports
                - MAC Flooding
                - Spoofing
                - DNS|ARP Poisoning
        - Port Mirroring
            - SPAN Port (Switched Port Analyzer)
                - Send copy of all packets to SPAN
            - TAP (Test Access Point)
                - Hardware device
                - Creates separate channels
- **How can the attacker read the information? Don't we use encryption?**
    - Not everything uses encryption
        - Telnet
        - FTP
        - HTTP
        - POP/IMAP/SMTP
- **Can we go into more detail about those sniffing methods?**
    - Wireshark
        - Sniff Telnet username/password
        - Filters
            - Filter by protocol

    - ARP, TELNET, FTP, HTTP, IP, DNS, etc
- By port
    - `tcp.port == 21`
- By IP
    - `ip.addr == 10.0.0.212`
    - `ip.addr == 10.0.0.212 or ip.addr == 10.0.0.165`
- By source and/or destination IP
    - `ip.src == 10.0.0.212`
    - `ip.dst == 10.0.0.165`
- By HTTP GET request
    - `http.request`
- By negation
    - Blacklisting
    - `!(arp or telnet or ftp)`
    - `ip.src != 10.0.0.1 && ip.dst != 10.0.0.1`