Try Hack Me - Wireshark 101

↳ Wireshark, a tool used for creating and analyzing PCAPs, is used as a package analysis tools.

↳ Wireshark give us information like:

- ↳ Packet Number
- ↳ Time
- ↳ Source
- ↳ Destination
- ↳ Protocol
- ↳ Length
- ↳ Packet info

↳ PCAP collection methods:

- ↳ Begin by starting with a simple capture to ensure that everything is set up and you are successfully capturing traffic.
- ↳ Ensure that you have enough computer power to handle the number of packets.
- ↳ Ensure enough disk space to ensure all of the packet captures.
- ↳ Network Taps: physical implants in which you physically tap between a cable
  - ① ↳ use hardware to ~~intercept~~ intercept traffic as it come across.
  - ② ↳ plant hardware between 2 network devices, the tap will replicate packets as they pass the tap.

↳ MAC Flood: it is intended to stress the switch and fill the CAM table. Once the CAM table is filled the switch will no longer accept new MAC addresses and so in order to keep network alive, the switch will send packets to all ports of the switch.

↳ ARP Poisoning: You can redirect traffic from host to the machine you are monitoring from.

↳ Filtering Operators

- ↳ and operator: and / &&
- ↳ or operator: or / ||
- ↳ equal operator: eq / ==
- ↳ not equal operator: ne / !=
- ↳ greater than operator: gt / >
- ↳ less than operator: lt / <

↳ Basic Filtering

- ↳ ip.addr == <IP Address>
- ↳ ip.src == <SRC IP Address> and ip.dst == <DST IP Address>
- ↳ tcp.port eq <port #> or <Protocol Name>
- ↳ udp.port eq <port #> or <Protocol Name>

- Packet Dissection
  - Layers: (OSI Model)
    - Application: End user layer
      HTTP, FTP, IRC, SSH, DNS
    - Presentation: Syntax layer
      SSL, SSH, IMAP, FTP, MPEG, JPEG
    - Session: Sync & Send to port
      API's, Sockets, WinSock
    - Transport: End to End Connections
      TCP, UDP
    - Network: Packets
      IP, ICMP, IPSec, IGMP
    - Data link: Frames
      Ethernet, PPP, Switch, Bridge
    - Physical: Physical Structure
      Coax, Fiber, Wireless, Hubs, Repeaters
- Packet details
  - Frame (layer 1): This will show you what packet you are looking at as well as details specific to the physical layer of the OSI model.

↳ Source [MAC] (Layer 2): This shows you the source, destination MAC addresses ; from data link layer of the OSI Model.

↳ Source [IP] (Layer 3): This will show source and destination IP addresses ; from the network layer of OSI Model.

↳ Protocol (Layer 4): This will show you details of the protocol used (UDP/TCP) along with source and destination ports ; from the transport layer of OSI Model.

↳ Protocol Errors: This is a continuation of the 4th layer showing specific segments from TCP that needed to be reassembled.

↳ Application protocol (Layer 5): This shows details specific to protocol being used (HTTP, FTP, SMB, etc.). From application layer of OSI Model.

↳ Application Data : This is an extension of layer 5 that can show the application specific data.