Lab 4 - WireShark (Network Sniffing)

In this lab, we explore how network sniffing works.

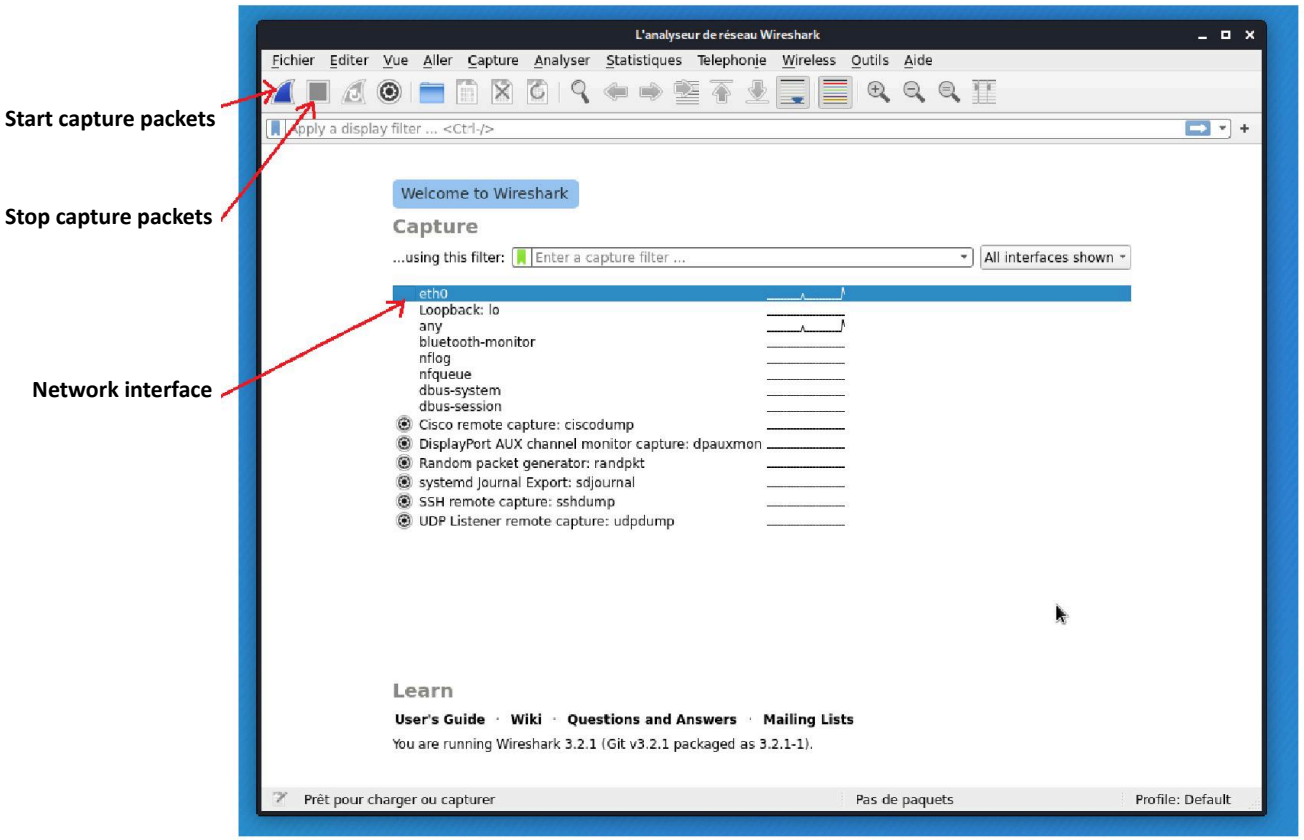
- Network sniffing involves observing the various packets, frames, or segments that travel between machines connected to a network.

- Network sniffing is independent of the communication medium used to transfer data. That is, we can sniff data transmitted over a wired cable or wirelessly. Wireless medium is advantageous for an attacker because radio waves propagate everywhere, so other machines can also listen to the traffic.

- There are several tools available for network sniffing, such as **Airodump** and **Wireshark**. In this lab, we use Wireshark; the world's leading network protocol analyzer.

Capturing and Analyzing Network Traffic

Launch the Wireshark application on your Kali machine and choose the eth0 interface. Then start the capture by clicking **Start capture packets**.



1. Start your **Metasploitable** VM and from it **ping** your **Kali** machine.

   Stop the capture and answer the following questions:
   - What is the source and destination IP address of this ping?
   - Which transport-layer protocol is used?
   - Which network-layer protocol is used?
   - Which ICMP message types are exchanged between source and destination and in which directions?

2. This step requires an Internet connection on your Kali machine. Start a new capture, open Firefox and go to `www.google.com`.

   Stop the capture, select the first TCP request, right-click it, choose **Conversation Filter → TCP**.

   Answer the following questions:
   - Which IP address initiated the three-way handshake?
   - What message did the machine receiving the first packet of the three-way handshake use to respond?

   Click on each of the three lines corresponding to the TCP three-way handshake. Then, in the analysis section, click on **Transmission Control Protocol** to retrieve each time:
   - The sequence number
   - The acknowledgment number

3. Start a new capture, and from your Windows machine, run the command `tracert <metasploitable IP>` toward the Metasploitable machine.

   Stop the capture and answer the following question:
   - What network layer protocol is used by `tracert`?

4. Start a new capture, and from your Kali machine, run the command `traceroute <Windows IP>` toward the Windows machine.

   Stop the capture and answer the following questions:
   - What is the transport layer protocol used by `traceroute`?

5. Start a new capture, then run the command `telnet <Metasploitable IP>`.
   - What information could you recover from the capture in Wireshark?
   - What alternative could you use to counter this problem?