

Learning Wireshark with Me - Blee

Welcome to the Wireshark Learning Guide! This document will help you get started with Wireshark, a powerful tool for network protocol analysis.


Introduction

Wireshark is an open-source packet analyzer used for network troubleshooting, analysis, and communications protocol development. It allows you to capture and interactively browse the traffic running on a computer network.

Installation

1. Download Wireshark:

- Visit the [Wireshark website](https://www.wireshark.org/download.html) to download the latest version of Wireshark for your operating system.

Here's a Youtube video for guide:  [How to download and install Wireshark on Windows](#)

2. Install Wireshark:

- Follow the installation instructions specific to your operating system.

I personally used the wireshark in my Kali Linux

Setting Up Wireshark

1. Edit Preferences:

- Go to `Edit > Preferences` and choose the layout you prefer (Frame Layout).

2. Adjust Delta Time:

- If needed, change the delta time settings to UTC.

3. Customise Colour Rules:

- Set up colouring rules to highlight specific protocols or types of traffic. Navigate to `View > Colouring Rules` and adjust as necessary.

4. Set Display Filters:

- Learn to use display filters to focus on specific types of packets. This is essential for efficient analysis.

Capturing Network Traffic

1. Check Interfaces:

- Determine which interface Wireshark will use to capture packets.
- Use the command: `help -> About Wireshark -> OK`

2. Capture Options:

- Go to `Capture > Options` to manage interfaces and settings.
- Adjust capture options such as `Manage Interfaces`, buffer sizes, and output locations.

3. Start Capturing:

- Select the appropriate interface and click the `Start` button to begin capturing traffic.

Using Dumpcap for Command-Line Capture

1. List Available Interfaces:

- Use the command: `dumpcap -D` to list all interfaces.

2. Capture Packets:

- Choose an interface and start capturing with: ``dumpcap -i 1`` (replace ``1`` with the desired interface number).

- Store the captured data: ``dumpcap -i 1 -w /path/to/store/file.pcapng``

3. **Advanced Capture Options:**

- Split files if needed: ``dumpcap -i 1 -W /path/to/store/file.pcapng -b filesize:1000 -b files:10``

Filtering Traffic

1. **Capture Filters:**

- Define how data is brought into the network card. Set capture filters before starting the capture.

2. **Display Filters:**

- Apply display filters to focus on specific packets of interest after the capture.

Resources

Chris Greer:  Wireshark Tutorial for BEGINNERS // Where to start with Wireshark

Lisa Bock: <https://lnkd.in/dzHGnrJQ>

There is also more platform on which you can learn Wireshark, I will highly recommend TryHackMe cause of the labs