Lab 02- Working with Wireshark

Sherif Saad

June 4, 2021

Purpose

This lab aims to introduce the students perform basic network analysis and inspection with Wireshark. To complete this lab make sure to download the archive files (.zip) from this https://tinyurl.com/yrvzdbdz directly to your course VM

1 Introduction to Wireshark

What is Wireshark?

- Wireshark is an open source tool for analyzing network traffic.
- Wireshark enables network traffic profiling and inspection.
- Wireshark is also a network traffic sniffer that can capture and record network packets over wired or wireless networks.
- The best known packet analyzer and network sniffer that is commonly used by government agencies, enterprises, educational institutions.
- Started by Gerald Combs in 1998.
- Wireshark runs on almost all popular platforms. It runs on Windows, Linux, and macOS.

Why using Wireshark?

- Provide network traffic insights by enabling data in motion recording and monitoring.
- Gather and report network statistics about network usage.
- Debug and troubleshooting network problems and protocol implementation and configuration issue.
- Detect network intrusion and misuse by internal and external users
- Help in web filters, spam filters, and provide information to understand and inspect network intrusion and other malicious network activities.

2 Using Wireshark

In this lab, we will go over the basic usages and functions of Wireshark, in particular, we will go over the following activities:

- Live Packet Capturing with Wireshark
- Exploring PCAP file or Traffic with Wireshark and Filters
- View/Reconstruct TCP Stream
- Extract Payload from Network Traffic

Important Notes

Note: Installing wireshark on your machine at work could be a violation to your company or organization policies.

Note: Make sure to only complete this lab and download the pcap files on your VM only