Wireshark Analysis

14th June 2018

IT Center,
University of
Peradeniya

Dilum Samarasinhe
(LEARN)

Overview

- Why do we need packet capturing
- Packet capturing tools
- What is wireshark
- About wireshark
- Why wireshark
- Features

Why do we need packet capturing?

- Security
- Identification of Data Leakage
- Troubleshooting
- Identifying Data/Packet Loss
- Forensics

Packet Capturing Tools

- Tcpdump
- Wireshark

tcpdump Definition

tcpdump is a utility used to capture and analyze packets on network interfaces. Details about these packets can either be displayed to the screen or they can be saved to a file for later analysis. tcpdump utilizes the libpcap library for packet capturing.

What is Wireshark?

- Wireshark is a network packet/protocol analyzer.
  - A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.
- Wireshark is perhaps one of the best open source packet analyzers available today for UNIX and Windows.

About Wireshark

- Formerly known as “Ethereal” – Author, Gerald Combs quit Network Integration Services – Free
- Requirement – Need to install winpcap – Latest wireshark installer contains winpcap, don’t worry – (On Windows Vista) Need Administrator Privilege to capture
- GUI – Dramatically improved

Why Wireshark?

- network administrators use it to troubleshoot network problems
- network security engineers use it to examine security problems
- developers use it to debug protocol implementations
- people use it to learn network protocol internals
- Wireshark isn't an intrusion detection system
- Wireshark will not manipulate things on the network, it will only "measure" things from it

Features

- Filters
  - Capture filter
  - Display filter
  - Tweak appearance
- Follow TCP Stream
- Use Statistics

Thank You

Dilum Samarasinghe/LEARN

Email: dilum@learn.ac.lk