SDN Firewall with POX

Wireshark/Tshark Tutorial Video

OMSCS/OMSCY CS 6250 Computer Networks

What is Wireshark/Tshark?

Wireshark (and it’s text-based counterpart tshark) is a multi-faceted network analyzer toolkit. Primarily this involves capturing all of the network traffic crossing through an interface or tap. For this project, we will be capturing simple network traffic that will pass through the local ethernet port on one of the virtual machines (using tshark) and then analyzing this data using the GUI version (Wireshark).

However, Wireshark has many other features that make it an important tool in a network engineer or security analyst toolkit – the ability to decrypt traffic, find exploited vulnerabilities and many other possibilities.

Wireshark in OMSCS/OMSCY

You will use Wireshark for a portion of the SDN Firewall project in this course. If you take the Introduction to Cyber-Physical Security course, you will use Wireshark to find devices on an industrial network bus. Other classes in the Cyber Security program will also use Wireshark for its many capabilities.

Wireshark/Tshark Resources?

The Wireshark Project - https://www.wireshark.org/
Wireshark Documentation - https://www.wireshark.org/docs/

Tshark (Command-Line Wireshark) - https://www.wireshark.org/docs/man-pages/tshark.html

Alternatives to Wireshark/Tshark?
TCPDUMP/LibPCAP - https://www.tcpdump.org/
In Windows, netsh can capture packets.

Demo Time

We will be demonstrating a brief packet capture and a simple evaluation of a set of network packets to demonstrate the different attributes in the Frame, IP, and Application headers that you will need to use to build your firewall.

This demo follows Part 4a of your Project Instructions with commentary by a TA.

Next Steps

Using what you have learned going through this tutorial, you will be creating a new packet capture file using different hosts and connection requirements as detailed in Part 4b of the Project Documentation. The process is the same as previously demonstrated.

You will include the packet capture file with your submittal. Please examine your file in Wireshark to make sure that you have captured the appropriate traffic.

If you have questions, please post in EdStem.