CSCD 434-040 Network Security

Lab 7, Examine Quantum Insertion Logs - Due, February 28, 2024

February 22, 2024

Overview

Today you'll examine, in depth, quantum insertion! By examining logs and knowing what quantum insertion is, you should be able to identify exactly what packets belong to the "shooter" and possibly rebuild any discarded payloads.

Finding shooters

Examine the two `pcap` files and tell me where in the connection the shooters are inserting data (the exact packet numbers should be in your write up).

You should be able to:

1. Find the inserted packet(s).
2. Find the real packet(s).
3. Retrieve the original requested page/payload.
    - Additionally, you need to decode the payload section and include it in your tarball.

Make sure to state for each `pcap` file, which site the user was originally trying to access as well as what exactly was inserted.

Automatic identification

Evaluate the `pcap` files and try to discover residual evidence in the packet headers.[1] Write a program to detect the packets and report them to the user. You may write to the terminal or designate a log file as the output. Include in your write up your reasoning for identifying a packet as inserted.

Turn in

Turn in your code, requested payload, as well as a README and PDF write up. Answer all questions in the sections above and include any code requested. Turn in a tarball (`yourname.tar.gz`) of your assignment.

[1] You may be able to use fields similar to those in the previous labs. Write a script to identify suspicious packets.