COMP4337/9337 Securing Fixed and Wireless Network
Lab 4: Security Analysis Using TShark

Due: Friday, 18.03.2021 23:59h

Objectives

This lab is designed to help the students to:

- get familiar with TShark which is the command line version of Wireshark, a network analyser tool, and
- show how TShark can be utilised to analyse security risks to your network.

Lab Overview

A network analyser tool, such as TShark and Wireshark, is used for network troubleshooting, analysis, software and communications protocol development, and education. TShark is very similar to tcpdump, another tool for network analysis, while Wireshark has a graphical user interface, plus some integrated sorting and filtering options.

TShark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic that is not sent to the network interface controller's MAC address. TShark can also read previously captured network packets to perform network analysis.

In this lab, you will be running TShark on the Raspberry Pi remotely via an SSH connection. Specifically, lab 4 consists of two parts:

- Part A: We will use TShark to analyse some previously captured normal/anomalous traffic. The traffic is generated by a machine that had been infected by a well-known piece of Malware, which is distributed by email.
- Part B: Here, we will investigate the Secure Sockets Layer (SSL) protocol, focusing on the SSL records sent over a TCP connection. We will do so by analysing a trace of the SSL records sent between a host and an e-commerce server.

Assessment and Marking

Students are required to modify this document by answering questions, which are part of this document and submit the modified document to Moodle. Only one submission from a group. Please also include your name and zID. The details of the marks are as follows:

- Total mark for Lab 4 is 100 and the weight is 0.15/1.
- **25 marks** are awarded for **Part A**, while **75 marks** are awarded for **Part B**.
- You should attempt Part A during the lab hours and show your work to the tutor. You are free to start working before the lab session. A penalty will be applied for students who do not show up for the lab.

Submission deadline is **Friday 18th March 2022, 23:59h**. The marks will be made available on Moodle within 2 weeks of the submission date.

- The standard late penalty introduced under UNSW new assessment implementation procedure will be applied for this course.
    - 5% per day,
    - for all assessments where a penalty applies,
    - capped at five days (120 hours) from the assessment deadline, after which a student cannot submit an assessment, and
    - no permitted variation.

Starting the Lab

To begin the lab, open your preferred SSH client, either in Terminal for Linux/Mac systems or PuTTY for Windows systems. Connect to your Raspberry Pi using steps described in Prep 2 docs. After successfully logging in, run TShark from the command line. We have provided two pre-captured pcap files located in `~/sfwn/` directory of your Raspberry Pi.

To open `part-A-trace.pcap` file type this command in the terminal:

```
$ tshark -r ~/sfwn/part-A-trace.pcap
```

The command will print all pre-captured network packets as a text with similar format on Wireshark. Take a look at the following example of packet 1 and 3:

```
1   0.000000  192.168.1.1 → 192.168.1.254 DNS 87 Standard query 0x297e A
windowsupdate.microsoft.com

3   0.773068  192.168.1.1 → 207.46.18.94 TCP 62 1099 → 80 [SYN] Seq=0
Win=65535 Len=0 MSS=1460 SACK_PERM=1
```

The column description is as follows:

Column/Displayed Text	**Description**
`1` `3`	Packet number
`0.000000` `0.773068`	Time since beginning of capture (seconds)
`192.168.1.1 → 192.168.1.254` `192.168.1.1 → 207.46.18.94`	Source and destination IP address
`DNS` `TCP`	Protocol
`87` `62`	Packet length (bytes)
`Standard query 0x297e A windowsupdate.microsoft.com` `1099 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1`	Packet information, depending on the protocol used. For TCP, it also shows the source and destination port number.

Part A: Analysing Network Traffic from an Infected System

In Part A, you need to open `part-A-trace.pcap` file that was created by a piece of malware on an infected system. Try to determine from the packet analysis and internet search tools what is the source and operation of that malware.

Now log-in to Moodle and attempt Lab 4 Assessment A.

Part B: Analysing Secure Sockets Layer Protocol

In Part B, open `part-B-trace.pcap` file. We will investigate various SSL record types as well as the fields in the SSL messages from the file packet trace.

It is important to keep in mind that an Ethernet frame may contain one or more SSL records. This is very different from HTTP, for which each frame contains either one complete HTTP message or a portion of a HTTP message. Also, an SSL record may not completely fit into an Ethernet frame, in which case, multiple frames will be needed to carry the record.

You should use a display filter to show SSL records only by typing the following command:

```
$ tshark -r ~/sfwn/part-B-trace.pcap -Y "ssl"
```

You may also want to display the details of a packet to inspect what information contained in a packet to answer the questions. You can write this command:

```
$ tshark -r ~/sfwn/part-B-trace.pcap -Y "frame.number==106" -V
```

The above command will print the information packet 106, using `-Y` flag to filter the frame number and using `-V` flag to display the packet details. You may change the packet number accordingly. Note that packets in Layer 2 are referred to as frames.

Now log-in to Moodle and attempt Lab 4 Assessment B.

If you want to use more complex options, consult TShark documentation, which contains full descriptions and examples for each of TShark options. The TShark documentation is available at https://www.wireshark.org/docs/man-pages/tshark.html.