Securing Fixed and Wireless Networks

COMP4337/COMP9337

Lab #4

Security Analysis using Wireshark

Use eng.cse.COMP4337@unsw.edu.au and WebCMS3 forum for all lab related communications

---

Overview

Learning Objective: The purpose of this lab is to get you familiar with Wireshark and to show you how it can be utilized to analyze security risks to your network.

This lab has two parts:

- **Part A:** We will use Wireshark (a widely known packet capturing tool) to analyze some previously captured normal/abnormal traffic. The traffic is generated by a machine that had been infected by a well-known piece of Malware, distributed by email. (Total marks: 25)
- **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 analyzing a trace of the SSL records sent between a host and an e-commerce server. (Total marks: 75)

During the lab:

1) We will be using "Wireshark" network packet analyzer in this lab. It can be downloaded from here: https://www.wireshark.org/download.html
2) Download "part-A-trace.pcap" and "part-B-trace.pcap".
3) We strongly recommend social distancing and use collaboration tools. However, we also recognise that lab groups may not be unable to submit a joint report. We will do arrangement for marking of individual submissions in such cases. However, there is no change in marking criteria in terms of individual or joint submission.

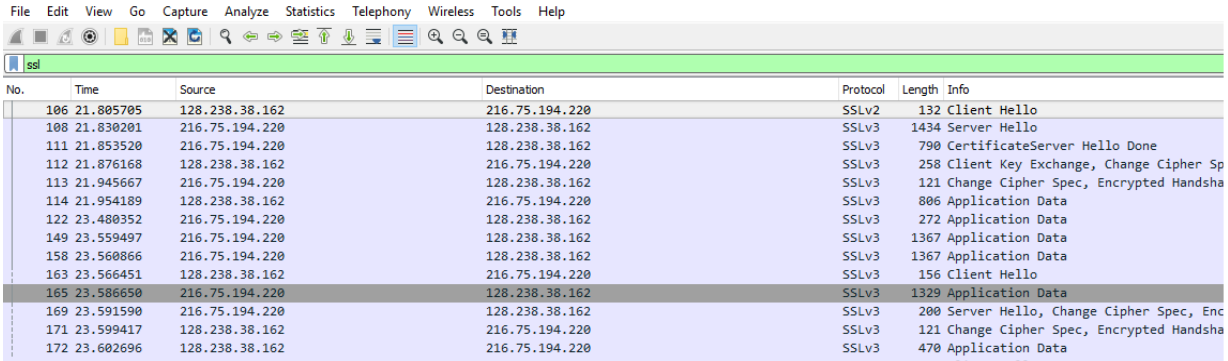
Part A

In this exercise, you will open the file part-A-trace.pcap 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 1. You have 48-hours to complete this assessment.

Part B

For this exercise open the file part-B-trace. We'll investigate the various SSL record types as well as the fields in the SSL messages from the file packet trace.

Your Wireshark GUI should be displaying **only the Ethernet frames that have SSL records**. You should obtain something like screenshot as below. 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.



No.	Time	Source	Destination	Protocol	Length	Info
106	21.805705	128.238.38.162	216.75.194.220	SSLv2	132	Client Hello
108	21.830201	216.75.194.220	128.238.38.162	SSLv3	1434	Server Hello
111	21.853520	216.75.194.220	128.238.38.162	SSLv3	790	CertificateServer Hello Done
112	21.876168	128.238.38.162	216.75.194.220	SSLv3	258	Client Key Exchange, Change Cipher Sp
113	21.945667	216.75.194.220	128.238.38.162	SSLv3	121	Change Cipher Spec, Encrypted Handsha
114	21.954189	128.238.38.162	216.75.194.220	SSLv3	806	Application Data
122	23.480352	216.75.194.220	128.238.38.162	SSLv3	272	Application Data
149	23.559497	216.75.194.220	128.238.38.162	SSLv3	1367	Application Data
158	23.560866	216.75.194.220	128.238.38.162	SSLv3	1367	Application Data
163	23.566451	128.238.38.162	216.75.194.220	SSLv3	156	Client Hello
165	23.586650	216.75.194.220	128.238.38.162	SSLv3	1329	Application Data
169	23.591590	216.75.194.220	128.238.38.162	SSLv3	200	Server Hello, Change Cipher Spec, Enc
171	23.599417	128.238.38.162	216.75.194.220	SSLv3	121	Change Cipher Spec, Encrypted Handsha
172	23.602696	128.238.38.162	216.75.194.220	SSLv3	470	Application Data

Now log-in to Moodle and attempt Lab 4 Assessment 2. You have 48-hours to complete this assessment.