## Lab 8b

## Examining Network Traffic

**Introduction**

This week, we will be looking in depth at packet capture files, and the indicators of abnormal traffic. For this lab, we will be using Wireshark for network analysis.

## **Learning Outcomes**

After this session you should be able to:

1. Continue to develop skillset with Wireshark
2. Be able to use Wireshark filters efficiently
3. Be able to pinpoint causes or actions based on network traffic
4. Develop knowledge of how to spot abnormal traffic

**Task 1 – Analysing network traffic**

First you will need to download the file Lab\_8.pcap from Moodle. Once you download and load the file on Wireshark, you will have to change the way timestamps are displayed. In its native form, the display consists of the date (in days since 1/1/1970, and the time of day (in nanoseconds from midnight). Wireshark gets its timestamps from libpcap (Linux) or WinPCap (Windows) library, which in turn gets them from the OS kernel. Go to “**View >> Time Display Format >> Date and Time…**”. This evidence file will be all you need in order to answer or perform the rest of this lab.

1. What is the first thing that happened and which destination address did it involve? (Hint: Look at the first captured packets)

**TCP 3 way handshake, destination address 192.168.76.141**

1. What packet identifier(s) tell you this and why?

**1-3 – packets were sent with TCP flags for SYN, SYN ACK and then ACK in that order**

1. What was the purpose of the DNS request in packet 9?

**Reverse DNS Lookup**

1. What was the IP address that has been used for the above lookup?

**192.168.76.2**

1. Look at packets 46, 47, 48. What has happened here?

**TCP 3 way handshake**

1. What is the purpose of the above packet exchange?

**Communication Establishment**

1. What is the MAC address for 192.168.76.141?

**00:0c:29:8d:11:39**

1. What is the IP address for 00:50:56:f8:dd:22?

**192.168.76.2**

1. What was the second thing that happened (Hint: Look at packets 4-9523)?

**TCP SYN scan (lots of packets send with SYN flag set to different ports)**

1. How long did this activity run for?

**About 2 minutes and 10 seconds**

1. What might be the purpose or aim of doing this?
2. What was the third thing that happened (Look at packet 9524-11533)? How can you tell?
3. Look at packet 9580: based on the query response was the port open or closed? How can you tell?
4. What was the port number and what service is attached to this port?
5. Now look at packet 9582: Was this port open or closed? How can you tell?
6. How long did this third activity run for?
7. What was the next thing to happen (after packet 11533)?
8. Look at packet 13815 – what do the [FIN,PSH,URG] flags indicate?
9. Was the SSH port open on 192.168.76.141? How can you tell?

**Task 2 – Analysing network traffic**

After gathering all the information you need, you are ready to build a recreation of events and a timeline including:

1. Source and destination addresses and source/destination ports
2. What the user was using to perform any/all activities, and what protocols and layers that might be in use during these activities
3. All the actual activities themselves, and the results of user activity
4. Timestamp everything
5. A list of laws relevant along with a brief explanation as to why it might be relevant