COMP6445

Week 6/7 activity – quiz answer sheet

Quiz Questions and your Answers

Name:
Student Number:

Q1. Wireshark is a software tool that is built-in for all Linux distributions. Yes/No and support with short answer.

A1.

Q2. How is Wireshark licensed? Support your answer by providing the first two lines of the Wireshark licence (i.e. title and date) and the last sentence of the licence file for the version you are using for your laboratory.

A2.

Q3. Wireshark provides a large number of sample files for reference and testing. Where can the files be accessed? Provide the URL and give the name of one of the virus/malware sample files.

A3.

Q4. You are provided with a PCAP file that is said to come from a Windows 10 laptop and the accompanying report says that WinPcap was used to create the PCAP file. Is this report correct? Provide the reason(s) for your answer.

A4.

Q5. One of the infected computers is 90.237.150.132. To which company is the IP registered? Why is your answer reliable (hint: refer to the ICANN appointed authoritative regional registry and why you picked that region)?

A5.

Q6. Which components cause Netflow to regard TCP traffic to be in the same flow?

A - IP address
B - Interface name
C - Port numbers
D – Layer 3 protocol type
E - MAC address

A6.

Q7. Explain the difference between a PCAP and a netflow. Short answer.

A7.

Q8. As part of the mini-lab, you converted a PCAP to a netflow. How do you convert a netflow to PCAP? Provide the reason(s) for your answer.

A8.

Q9. Scenario 2 is usually conducted as part of an incident detection and rapid response activity. When conducting it as a post-incident forensic activity, what extra steps would you take (hint: the key difference is demonstrating the sufficiency and reliability of your examinations)

A9.

Q10. List two alternate software that you could use to perform netflow analysis in a similar fashion to Scenario 2 i.e. use to check reliability of your examination. Support each choice with a short reason.

A10.