408217 Information Security Sem 1 2015

LAB ASSIGNMENT – Firewalls . Use Wireshark if available for packet tracing.

Attempt all questions – search including on-line for answers but limit for own answer to the space provided in the box

1. Why does your computer send so many packets? Why not send just one big packet?

2. What do SYN, ACK, FIN, GET mean?

3. Why do some packets have TCP sequence numbers?

Based on **“CORPORATE COMPUTER SECURITY”, by Boyle and Panko, 2014, CHAPTER 6: FIREWALLS**

4. During a session between your computer and a webserver many packets will be exchanged, of all the three types listed : ACK, SYN,FIN. Which ones will be the nost numerous? Why?

5. Will your computer get packets that are addressed to another computer? Why?

6. How many packets does your computer send/ receive in a single mouse click when you visit a website?

7. How could blocking all ICMP traffic protect you?

Based on **"CORPORATE COMPUTER SECURITY", by Boyle and Panko, 2014, CHAPTER 6: FIREWALLS**

8. Could you still access some websites with your Port 80 rule enabled? Why?

9. Why would you want to allow incoming (not outgoing) Port 443, but block incoming Port 80?

10. Could malware rename itself in order to get through a firewall?

Based on **"CORPORATE COMPUTER SECURITY", by Boyle and Panko, 2014, CHAPTER 6: FIREWALLS**