University of Oslo
INF3510 Information Security
Spring 2018
Workshop Questions

Lecture 11: Network Perimeter Security

Question 1

A firewall is a component or set of components that restricts access between a protected network and other sets of networks and are often used to protect an organisation's networks from the Internet.

a. Briefly describe the operational characteristics of:
   - a simple packet filter;
   - a stateful packet filter;
   - a circuit level proxy;
   - an application layer proxy.
b. Briefly discuss the strengths and weaknesses of deploying:
   - a packet filter;
   - application layer proxy.

Question 2

a. How can a firewall inspect TLS traffic?
b. How can a user know whether TLS traffic is being inspected?

Question 3

Intrusion detection systems (IDS) are automated systems (programs) that can detect suspicious activity.

a. An IDS can be either host-based or network-based. Briefly describe the operation of a host-based IDS, and of a network-based IDS.
b. Detection methods used by IDS are normally considered to be either misuse-based or anomaly-based. Briefly describe each of these detection methods.
c. Briefly discuss the strengths and weaknesses of misuse-based and anomaly-based IDS.
d. Briefly discuss the major operational issue associated with the deployment of an IDS.
e. Give typical reasons why many alarms can be ignored.

Question 4

The so-called base-rate fallacy is a common reason for false alarms in IDS.

a. What is meant by the base-rate fallacy?
b. In which other disciplines (other than information security) is the base-rate fallacy common?
c. What can be done to avoid the base-rate fallacy?

Question 5

a. What do the abbreviations BSS, ESS and DS mean in relation to IEEE 802.11 WLAN? Briefly describe each concept and how they are related.
b. List and briefly describe the 5 IEEE 802.11i phases of operation.