



Lecture 10: 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 gateway;
 - an application gateway.
- b. Briefly discuss the strengths and weaknesses of deploying:
 - a packet filter;
 - application gateway.

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 detect suspicious events.

- a. An IDS can be either host-based or network-based. Briefly describe the operation of a host-based IDS and a network-based IDS.
- b. Detection methods used by IDS are normally considered to be either misuse or anomaly-based. Briefly describe each of these detection methods.
- c. Briefly discuss the strengths and weaknesses of misuse 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 is the base-rate fallacy a common problem?
- 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.