Lecture 12: Application and Operations Security

QUESTION 1

a. What are typical phases of operation of a virus or worm?
b. How does behavior-blocking software work?
c. In general terms, how does a worm propagate?

QUESTION 2

a. What is a botnet?
b. What is a DDoS, and how can a botnet be used to mount a DDoS attack?
c. Describer two other attacks that can be executed with botnet.

QUESTION 3

a. What is a buffer overflow attack, and how can it be prevented?
b. What is an SQL injection attack and how can it be prevented?
c. What is a Cross-Site Scripting attack, and how can it be prevented?

QUESTION 4

Assume that Company A and Company B of similar size become victims of cyber attacks, and that as a result both companies suffer heavy damages that negatively affect customers and shareholders. When investigating the events it was found that Company A had practiced due dilligence and due care, whereas Company B had not. Assuming that the damages to both companies were equal, explain the possible differences, if any, in consequences and sanctions against management of the companies.

QUESTION 5

Many things can go wrong when deploying new patches to systems.
a. List possible options for obtaining assurance that the patch comes from the correct source in the first place.
b. When a new patch is deployed to multiple systems, it is wise to update the systems in a sequence, not all at the same time. Explain why this is so.