CSS 322 – QUIZ 7 ANSWERS

First name: _____ Last name: _____

ID: _____ Total Marks: _____

out of 10

Question 1 [4 marks]

Multiple choice. Select the most accurate answer. Choose only one. You receive 1 mark for a correct answer. You lose 0.5 marks for an incorrect answer. 0 marks for an unanswered question.

a) The preferred (most secure) method to authenticate users on the Web is using:

   a. HTTP Digest Authentication
   b. HTTP Basic Authentication, combined with cookies
   c. HTTP over TLS
   d. HTTP with session identifiers included in the URL

b) A logic bomb is best described as:

   a. Program modification that allows unauthorized access to functionality
   b. Program that propagates copies of itself to other computers
   c. Code embedded in a program that executes when certain conditions are met
   d. Code specific to a single vulnerability (bug) or set of vulnerabilities (bugs)

c) Web cookies were designed to:

   a. Prevent web sites from impersonating (pretending to be) other web sites
   b. Provide state information for web transactions
   c. Provide simple method for submitting username/password
   d. Prevent tracking of users' web browsing habits

d) The "I Love You" worm used the following method for propagation:

   a. Exploiting bugs/limitations of remote login commands, like rsh and rexec
   b. Sending HTTP GET Requests to web servers with bugs
   c. Emailing files to other people
   d. Forcing your web browser to download a malicious program from a web site

Question 2 [1.5 mark]

Explain one major difference between a virus and a worm.

Answer:

A virus attaches itself to another program, whereas a worm is an independent program.

Question 3 [2 marks]

The original Code Red worm did not modify files on a web server, whereas Code Red II did allow modification and deletion of web server files. Then describe two malicious activities that the original Code Red performed (that is, how did it cause damage?).

Answer:

Denial of service attack (on Whitehouse.gov)

Use up resources (memory/CPU) of servers under attack

Increased traffic due to sending of worm

Question 4 [2.5 marks]

a) Explain the difference between a metamorphic virus and a polymorphic virus.

Answer:

Polymorphic virus will change the code so it looks different (change its appearance), although operates the same as all other copies. Metamorphic virus will change the code and its behaviour.

b) Which one (polymorphic or metamorphic) is harder to detect?

Answer:

Metamorphic, since detection mechanisms (anti-virus) usually rely on detecting a pattern of code. By changing the code (appearance and behaviour) there are less patterns to detect.