CS-480I/585I Information Security:

Questions Based on Student Reviews of Published Papers

1. Which of the following was a part of the Morris Worm?
   (a) the main program
   (b) the sub program
   (c) the vector program
   (d) the hash program
   (e) all of the above
   (f) more than one, but not all, of the above.

   Answer: f

2. Which of the following actions could be taken to protect a system from the Morris Worm?
   (a) Use shadowed password files.
   (b) Use kerberos to authenticate trusted systems.
   (c) Perform bounds checking on buffers.
   (d) Use a method of creating strong passwords.
   (e) all of the above
   (f) more than one, but not all, of the above

   Answer: e

3. The paper, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988" about the ***mal-ware*** incident of November 1988 came from:
   (a) Harvard
   (b) Berkeley
   (c) MIT
   (d) none of the above

   Answer: C

4. What types of computers were affected by the ***mal-ware*** incident of 1988?
   (a) Suns
   (b) Vaxes
   (c) HPs
   (d) all of the above
   (e) more than one, but not all, of the above

   Answer: D

5. The accountability category of the TCSEC criteria supports which of the following policy(s):
   (a) Mandatory Access Control
   (b) System Integrity
   (c) Discretionary Access Control
   (d) Test Documentation
   (e) more than one, but not all, of the above
   (f) none of the above

   Answer: e

6. What is the purpose of the TCSEC criteria?
   (a) to give government complete control over security software development.
   (b) to facilitate consistency among security products.
   (c) to create a joint venture between industry and government.
   (d) to ensure that all software products are secure.
   (e) more than one, but not all, of the above
   (f) none of the above

   Answer: e

7. In general, corporations implement privacy policies regarding the appropriate use of personal information because of:
   (a) negative media attention
   (b) ethical concerns
   (c) legislative scrutiny
   (d) market competition
   (e) all of the above
   (f) more than one, but not all, of the above

   Answer: F

8. Corporations should have a privacy policy in place to address:
   (a) appropriate collection of personal information
   (b) uses of personal information for purposes other than for which it is originally collected
   (c) sharing of personal information with other entities
   (d) all of the above
   (e) more than one, but not all, of the above
   (f) none of the above

   Answer: D

9. The **fscanf** and **gets** functions, as used in many UNIX utilities, compromise the security of a computer because:

(a) they take in unbounded strings.
(b) they were written in the Ada programming language.
(c) they open holes for potential worm attacks.
(d) all of the above
(e) more than one, but not all of the above
(f) none of the above

Answer: e

10. Many UNIX utilities are vulnerable to crashes and to being used by hackers to bypass system security because:
(a) users failed to report bugs when they found them.
(b) programmers failed to provide adequate bounds and error condition checking.
(c) it was often easier to work around a crash than to fix the bug that caused it.
(d) all of the above
(e) more than one, but not all of the above
(f) none of the above

Answer: d

11. What is/are the main area(s) of concern in UNIX security?
(a) password Security
(b) network security
(c) file system security
(d) physical security
(e) password security
(f) account security
(g) items (a), (d), and (e) above
(h) items (b), (c), and (f) above
(i) items (b), (d), and (e) above

Answer: h

12. What is the purpose of the UNIX /etc/exports file?
(a) It lists the hosts that can access your network file system.
(b) It lists the system devices that can be accessed remotely.
(c) It indicates which files are available to other systems for mounting.
(d) all of the above
(e) none of the above

Answer: c

13. What was done in Word 7 to thwart macro viruses?

(a) Virus protection was implemented in the software.
(b) Macro viruses were disabled by default.
(c) Macro source viewing was enabled.
(d) The macro feature was deleted altogether.
(e) none of the above

Answer: b

14. Macro virus mutators are likely to cause more damage than MS-DOS based virus mutators because:
(a) macro viruses are "more powerful" than MS-DOS viruses.
(b) MS-DOS viruses are no longer a problem and can be ignored.
(c) DOS is not in use anymore.
(d) macro virus source code is always available.
(e) macro virus mutators are more readily available than their MS-DOS counterparts.

Answer: d

15. Which of the following was **not** one of the improvements on the authors' approach to password security?
(a) Slower encryption
(b) Less predictable passwords
(c) Random generated passwords
(d) Salted passwords
(e) none of the Above

Answer: C.

16. How is the password stored on a ***UNIIX/Linux*** system?
(a) encrypted
(b) in a Hidden file
(c) Password is used as an encryption key for a standard ciphertext.
(d) all of the above
(e) none of the above

Answer: C.

17. In a mail system, when using conventional encryption algorithms, a message:
    (a) is self-authenticating.
    (b) contains a timestamp.
    (c) is delivered by some intermediate transport mechanism.
    (d) utilizes public keys.
    (e) all of the above
    (f) more than one, but not all, of the above
    (g) none of the above

    Answer: f

18. With public key algorithms, doubly encrypting plain-text with the sender's private key and then with the recipient's public key provides:
    (a) confidentiality.
    (b) accountability.
    (c) integrity.
    (d) all of the above.
    (e) more than one, but not all, of the above.
    (f) none of the above.

    Answer: d