

Security in Organizations (I00153)

Monday January 16 2006, 10.30 – 12.30, E0003

This is a “closed book” exam and consists of three (3) problems. In the border next to each problem is indicated the maximum number of credits you earn by solving the problem. The total number of credits is 100. You have already earned your first 10 credits if you succeed in correctly writing your name and student number on every sheet of paper that you hand in. Good luck!

Exercise 1

30

Answer the following multiple-choice questions by indicating *a*, *b*, *c*, or *d*.

1. Your company has just opened a call center in India and you have been asked to review the site’s security controls. Specifically, you have been asked which of the following is the strongest form of authentication. What will your answer be?
 - (a) Something you know
 - (b) Something you are
 - (c) Passwords
 - (d) Tokens
2. Which of the following is the easiest and most common form of password attack used to pick off insecure passwords?
 - (a) Hybrid
 - (b) Dictionary
 - (c) Brute force
 - (d) Man-in-the-middle
3. Administrative controls form an important part of security, and although most of us don’t like paperwork, that is a large part of this security control. Which of the following describes a high-level document that states a management plan for how security should be practiced throughout the organization?
 - (a) Guidelines
 - (b) Policies
 - (c) Procedures
 - (d) Standards

4. One of your co-workers has joined a study group and is discussing today's list of topics. One of the topics is this: What is an example of a passive attack?
 - (a) Dumpster diving
 - (b) Sniffing
 - (c) Installing SubSeven
 - (d) Social engineering
5. What term is used to describe that "a user cannot deny a specific action because there is positive proof they performed it."
 - (a) Accountability
 - (b) Audit
 - (c) Non-repudiation
 - (d) Validation
6. The absolute first requirement of computer security is which of the following?
 - (a) Password policy
 - (b) Application security
 - (c) Logical security
 - (d) Physical security
7. What is one of the largest drawbacks in using a *dog* as a physical security control?
 - (a) Cost
 - (b) Liability
 - (c) Investment
 - (d) Training
8. Which type of attack relies on the trusting nature of employees and the art of deception?
 - (a) Hijacking
 - (b) Social engineering
 - (c) Spoofing
 - (d) Deception
9. Which of the following would you define as neutral organizations that offer notarization for digital certificates?
 - (a) Certificate authorities
 - (b) Public key authorities
 - (c) Public key infrastructures
 - (d) Authorization zones

10. Which method of encryption was rumored to have been used by Al-Qaeda before 9-11 and functions by hiding information inside of a bitmap?
 - (a) Port redirection
 - (b) Stealthography
 - (c) Steganography
 - (d) Tunneling
11. Which of the following is *not* contained in a digital certificate?
 - (a) Serial number
 - (b) Subject's name
 - (c) Subject's private key
 - (d) X.509 version
12. Bob and Alice want to use *symmetric* encryption to exchange information. How many keys are required?
 - (a) 1
 - (b) 2
 - (c) 3
 - (d) 4
13. You have just won a contract for a small software development firm, which has asked you to perform a risk analysis. The firm's president believes that risk is something that can be eliminated. As a Security in Organizations graduate, how should you respond to this statement?
 - (a) Although it can be prohibitively expensive, risk can be eliminated.
 - (b) Risk can be reduced but cannot be totally eliminated.
 - (c) A qualitative risk analysis can eliminate risk.
 - (d) A quantitative risk analysis can eliminate risk.
14. Proper security management dictates separation of duties for all the following reasons except which one?
 - (a) Reduces the possibility of fraud
 - (b) Reduces dependency on individual workers
 - (c) Reduces the need for personnel
 - (d) Provides integrity
15. Which of the following is used to verify a user's identity?
 - (a) Authorization
 - (b) Identification
 - (c) Authentication
 - (d) Accountability

16. Your consulting firm has won a contract for a small, yet growing, technology firm. The CEO has wisely decided that the firm's proprietary technology is worth protecting. Which of the following is *not* a reason why this organization should develop information classifications?
- (a) Information classification should be implemented to demonstrate the organization's commitment to good security practices.
 - (b) Information classification should be implemented to ensure successful prosecution of intellectual property violators located in third-world countries.
 - (c) Information classification identifies which level of protection should be applied to the organization's data.
 - (d) Information classification should be implemented to meet regulatory and industry standards.
17. Which of the following do *not* require prior employee notification?
- (a) Monitoring of emails
 - (b) Monitoring of unsuccessful login attempts
 - (c) Monitoring of voice communications
 - (d) Monitoring of web traffic
18. Which of the following should be performed in conjunction with a termination?
- (a) Exit interview
 - (b) Limitation of computer access
 - (c) Prior notice of termination
 - (d) Adequate private time to say good-bye to friends and co-workers
19. Your manager has become concerned over a new piece of software being developed by a contractor. Your manager wants you to verify that no means of unauthenticated access is being left in the finished product. What is another name for a method of unauthenticated access into a program?
- (a) Covert wrapper
 - (b) Slip
 - (c) Wrapper
 - (d) Backdoor
20. Which of the following is *not* an acceptable response to risk?
- (a) Acceptance
 - (b) Displacement
 - (c) Reduction
 - (d) Transference
21. Your director has asked you to implement a security awareness program. Which of the following will a security awareness program *not* provide?

- (a) A security awareness program improves awareness of security policies and procedures.
 - (b) A security awareness program should run continuously and visibly reprimand those who are in noncompliance.
 - (c) A security awareness program helps employees understand the need to protect company assets.
 - (d) A security awareness program teaches employees how to perform their jobs more securely.
22. When a team is investigating a possible network intrusion, which of the following would be the best way for team members to communicate?
- (a) Email
 - (b) The organization's wireless network
 - (c) Instant Messenger
 - (d) Cell phone
23. Mike has recently discovered that the material he had written for a new book is being used by a competitor as a course manual. What laws has the competitor potentially broken?
- (a) Trademark
 - (b) Copyright
 - (c) Trade secret
 - (d) Patent
24. Because of your recent good work in building the incident response team, you have been asked to work with the newly created mobile sales force. Your success in this venture will certainly move you up the corporate ladder. You have been asked to propose the best way to secure the data on the laptops that each salesperson will carry. Which of the following will you recommend?
- (a) Issue each salesperson a laptop locking cable
 - (b) Use file encryption on the hard drives
 - (c) Require each salesperson to VPN into the network remotely
 - (d) Enforce the use of WEP for all wireless communication
25. Which type of protection control is used to discourage violations?
- (a) Security
 - (b) Recovery
 - (c) Response
 - (d) Deterrent
26. Potential employees should *not* have which of the following performed?
- (a) Background checks

- (b) Reference checks
 - (c) Credit status checks
 - (d) Education claim checks
27. Jim has been asked to assist with a security evaluation. He has heard other members of the teams speak of TCB. What does TCB stand for?
- (a) Taking care of business
 - (b) Total computer base
 - (c) Trusted computer base
 - (d) Total communication bandwidth
28. Which of the following assurance standards was developed through collaboration with the U.S., UK, France, Germany and others to align existing standards and provide for a globally accepted standard?
- (a) CTCPEC
 - (b) Common Criteria
 - (c) TCSEC
 - (d) ITSEC
29. Which of the following is an example of risk transference?
- (a) Spare equipment
 - (b) Insurance
 - (c) Offsite storage
 - (d) Fire suppression
30. Which of the following is *not* an example of penetration testing?
- (a) Dumpster diving
 - (b) War driving
 - (c) Port scanning
 - (d) War diving

Exercise 2

30

Answer the following questions in a short way (one or two sentences per question).

1. Consider a normal, modern, private car. Name three safety controls present in or on the vehicle. For each of these indicate whether they are deterrent, preventative, corrective, or detective controls.
2. If you are required to use several passwords at a time, you may consider keeping them in a *password book*. A password book is a protected file containing your passwords. Access to the password book can again be controlled through a *master* password. Does such a scheme offer any real advantages (over using the master password many times)?

3. A common criteria certification can only be conducted by specific organizations (e.g. TNO-ITSEF). Many such organizations exist distributed over different countries. Describe how these organizations can maintain the same level of certification.
4. Risk analysis can be done either qualitatively or quantitatively. Name one advantage for each method.
5. Is a social engineering attack more likely to succeed in person, over the telephone, or through email? Justify your answer.
6. Firewalls are targets for penetrators. Why are there few compromises of firewalls?

Exercise 3

30

Answer the following questions in 200 words or less.

1. The *defense-in-depth* security principle states that assets should be protected by multiple layers of controls. The *keep-it-simple* security principle states that systems of controls should be kept simple, since complex systems usually contain many vulnerabilities. Explain how the two principles can both apply, even though they seem to contradict each other.
2. Job rotation refers to the practice of moving people from job function to job function, with or without notice. Does job rotation increase or decrease the level of security within the organization. Justify your answer.