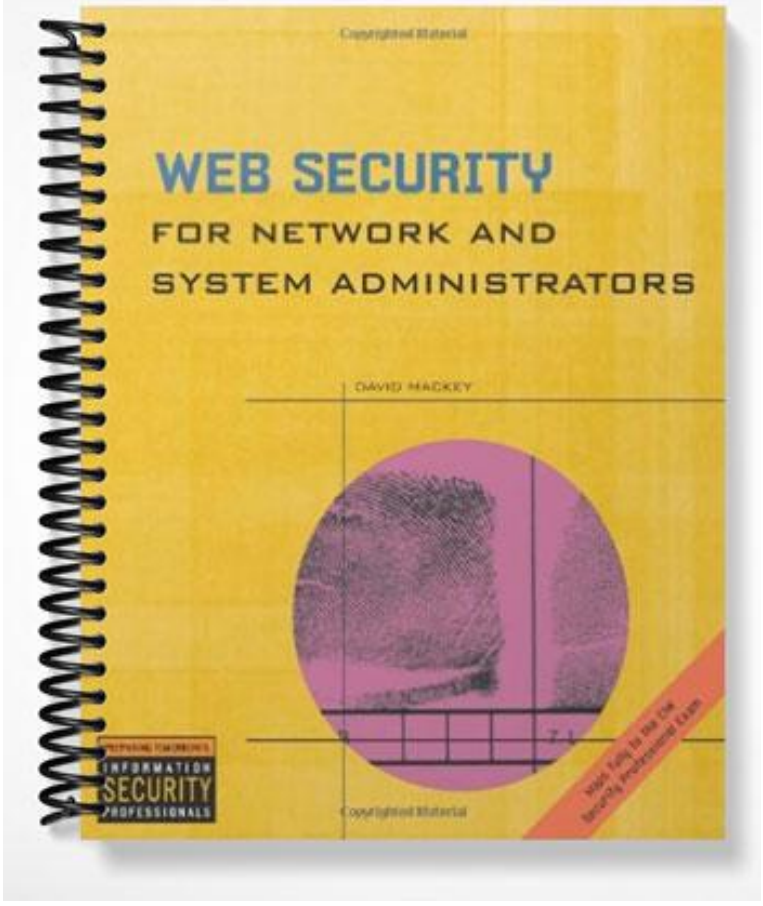
TEST BANK


Copyrighted Material
WEB SECURITY
FOR NETWORK AND
SYSTEM ADMINISTRATORS
DAVID MACKEY
INFORMATION
SECURITY
PROFESSIONALS
Copyrighted Material

ch02

True/False
Indicate whether the statement is true or false.

____ 1. Not all users need to be educated on protecting their workstations and sensitive information, for it is the role of the IT department to secure the company.

____ 2. According to the textbook, it can be argued that software development is 40% typing skills, 40% creativity, and 20% code compiler.

____ 3. Because some bugs do not yet have a solution provided by the manufacturer, an attack exploiting a zero day vulnerability can be devastating.

____ 4. In many cases when an exploit is discovered, it is still possible that many companies remain unaware of the vulnerability.

____ 5. No one organization can stay abreast of all the software bugs for all software packages.

____ 6. In choosing an advisory service, first select a trusted source, for example, a newsgroup.

____ 7. When dealing with risk, accepting the risk and deciding not to address the security problem is never an option for any organization with a good security policy.

____ 8. The ALE evaluation process occurs only in the initial security assessment of an environment.

____ 9. As a general rule, managers and executives are not concerned about the security measures deployed throughout the environment; their concern is profit.

____ 10. In most environments, the official risk assessment process combines both quantitative and qualitative approaches.

____ 11. Many companies have no intention of prosecuting security incidents and are concerned instead with removing the threat and returning to normal business operations.

____ 12. Perhaps the most important response to suspicious activity in the environment is to restore business operations.

____ 13. Although most companies recognize the need for a response plan to handle robbery and vandalism, most have no idea how to react to the similar occurrences of robbery or vandalism of the company's computer systems.

____ 14. Prosecution of intruders is one of the five pillars of a sound security infrastructure.

____ 15. Users' workstations and test servers fall into the category of medium security level.

Modified True/False
Indicate whether the statement is true or false. If false, change the identified word or phrase to make the statement true.

____ 16. When weighing security risks against security costs, <u>management</u> support is necessary.
_____

____ 17. A CIRT includes two major roles: <u>communication</u> and control (CnC) and forensic analysis.
_____

____ 18. Among the categories of security controls, education is listed under the heading of a(n) <u>detective</u> control.
_____

____ 19. A(n) education plan allows an organization to mobilize all employees in the fight against abusers, and informs them on where to find the corporate security policies. _____

____ 20. For an education plan to be effective, there must be management-supported penalties and rewards attached to its accountability. _____

____ 21. To combat the imperfections in software, it is important that every software consumer have a process in place to receive security options and apply the necessary patches quickly. _____

____ 22. Ideally, the security advisory and the fix are released in the classification stage in the vulnerability life cycle. _____

____ 23. The process of establishing formal guidelines to determine the severity of the exposures to the environment caused by software bugs, the time line to apply fixes, and the group responsible for applying the fixes is referred to as the risk management process. _____

____ 24. Among the categories of security controls, risk management is listed under the heading of a(n) detective control. _____

____ 25. Security incident management consists of three overarching concepts: endlessly prepare, effectively react, thoroughly prosecute. _____

____ 26. Accountability can be achieved by requiring employees to sign a contract, certify acceptance over the Web, or send a(n) e-mail confirming review and acceptance of security policies. _____

____ 27. An organization's security advisory management process is a preventive and corrective measure that identifies and fixes exposures before the bad guys can take advantage of them. _____

____ 28. Internet-connected and business-critical servers most likely fall into the category of medium security. _____

Multiple Choice
Identify the choice that best completes the statement or answers the question.

____ 29. In this chapter, the five major security processes are explained in terms of ____ categories of security controls.
a. two
b. three
c. four
d. five

____ 30. An effective security education plan is a(n) ____ control.
a. detective
b. preventive
c. corrective
d. assistive

____ 31. The first item you tackle when developing an education plan is to determine ____.
a. how frequently security education is presented to the organization
b. the cost of establishing an education plan
c. the interest of employees
d. the duration of the education plan

____ 32. A good guideline to follow when determining how frequently security education is presented to the organization is to educate ____.
a. every time before extending an offer to a perspective candidate
b. at the brink of the start of a new project
c. at least once a quarter
d. at least as frequently as security policies are modified

____ 33. Arrange the following steps to implement security education in their correct order, from the first to the last: delivery, frequency, accountability, and audience.
a. frequency, delivery, audience, accountability
b. accountability, audience, delivery, frequency
c. accountability, delivery, audience, frequency
d. frequency, audience, delivery, accountability

____ 34. Which of the following steps is the most flexible and customizable of all the aspects of security education?
a. frequency
b. audience
c. delivery
d. accountability

____ 35. Which of the following steps is the last and most crucial component of the education plan?
a. frequency
b. audience
c. delivery
d. accountability

____ 36. To combat error in coding or logic, most manufacturers release additional software code called ____ and notify the IT community of software problems.
a. spices
b. bits
c. patches
d. badges

____ 37. Every software vulnerability follows a cycle consisting of ____ major stages.
a. three
b. four
c. five
d. six

____ 38. All of the following are major stages in a software vulnerability cycle except _____.
a. Discovery
b. Repair
c. Analysis
d. Notification

____ 39. The optimal action for someone who discovers a software problem is to ____.
a. stop using the product right away and sue for compensation
b. continue using the product as a patch issued by the manufacturer is most likely in development
c. consult with the company's software development group to attempt to have the problem fixed
d. notify the manufacturer of the problem, so the manufacturer, in turn, can fix it

____ 40. When a problem cannot be fixed using software, the manufacturer may recommend configuration changes within the software that may fix the problem. This type of solution is usually labeled a ____.
a. reconciliation
b. workaround
c. compromise
d. settlement

____ 41. In a software vulnerability cycle, what happens after the patch or workaround has been developed?
a. The manufacturer offers a formal apology to the public.
b. The manufacturer notifies the public about the problem and releases a fix.
c. The manufacturer offers monetary compensation to the victim.
d. The IT community may be left unprotected, as attackers begin to exploit the vulnerability.

____ 42. Which of the following pairs of stages of software vulnerability cycle pose the greatest threats to all IT environments?
a. discovery and repair
b. repair and notification
c. notification and deployment
d. discovery and deployment

____ 43. Systems or architectures that are financially insignificant to the company and that pose the least risk of being compromised are categorized as ____ in terms of the severity of the issue and the required deadlines for addressing problems.
a. low
b. null
c. short
d. soft

____ 44. File and print servers, internal application servers, and some workstations may fall into the ____ category in terms of the severity of the issue and the required deadlines for addressing problems.

a. low
b. medium
c. high
d. top

____ 45. Systems categorized as requiring medium security should have all the controls used for systems categorized as ____, with additional protections.
a. low
b. medium
c. high
d. top

____ 46. What is the goal of security risk management?
a. To provide an estimate on the risk of certain types of threats
b. To provide a guideline on what type of security personnel should be hired and when
c. To provide a preventive security control that compares the financial costs of implementing security measures with the possible cost of a security breach
d. To provide thorough explanation on the types of threats that the company faces and to ensure that there is no misunderstanding between the management and the security personnel regarding the scope of the threats

____ 47. In simple terms, the risk management process is an extension of the ____ management process.
a. policy
b. personnel
c. threat
d. issue

____ 48. Normally, the ____ follows the security issue management process and ensures that patches are installed.
a. system administrator
b. network technician
c. CTO
d. designated software developer

____ 49. Risk ____ is the first step in the risk management process.
a. penetration
b. assessment
c. control
d. prevention

____ 50. Whenever a security issue clashes with a business concern, ____ assessment must be performed.
a. profit
b. organization
c. loss
d. risk

____ 51. Many companies recognize the need for a response plan to handle robbery and vandalism. The ____ incident management process is the equivalent response plan for IT systems.
a. security
b. risk
c. loss
d. expected

____ 52. All of the following are overarching concepts of the security incident management process as stated in the book except for _____.
a. timely responses
b. endlessly prepare
c. effectively react
d. thoroughly assess

____ 53. Like other legal warnings, a ____ provides a necessary first cautionary statement that trespassers are NOT authorized and identifies the server as off-limits.
a. banner
b. marker
c. door
d. tag

____ 54. A(n) ____ should be started immediately after enacting the response plan.
a. log
b. alarm
c. meeting
d. transition

Completion
Complete each statement.

55. In addition to the imperfections that affect the usability and stability of the software product, errors in coding or logic, called _____, introduced during development can produce security exposure.

56. In the software vulnerability cycle, the _____ stage begins when someone encounters a software vulnerability.

57. A newly discovered vulnerability--otherwise known as _____ day vulnerability--can be exploited by an abuser. Since the bug does not yet have a solution provided by the manufacturer, an attack exploiting this type of vulnerability can be devastating.

58. When the manufacturer finally discovers the software problem, the _____ stage begins.

59. An organization's security _____ management process is a preventive and corrective measure that identifies and fixes exposures before the bad guys can take advantage of them.

60. The annualized _____ expectancy (ALE) equation is a valuable tool in determining how much the business is willing to spend on a security countermeasure versus the projected financial protection the countermeasure provides.

61. _____ risk assessment methods provide actual financial figures to allow an objective comparison of control costs versus threat costs.

62. _____ risk assessment approaches consist of subjective components, such as the professional experience, education, judgment, and intuition, that are applied to analyze the risk.

63. In CIRT, the _____ analysis group is made up of the technical people that have both system and security expertise. Using the automated tools and manual inspection, this team is responsible for collecting and analyzing evidence, containing and preventing further intrusions, and developing a recovery plan.

64. Systems or architectures of moderate financial value to the company and that pose moderate risk of being compromised fall into the category of _____ level security.

65. The security incident management process is a(n) _____ and corrective security control.

66. The hallmark of any successful security service or program is _____.

67. A(n) _____ should be started immediately after enacting the response plan.

Essay

68. What kind of goals does an education plan fulfill?

69. Give a brief explanation of the security advisory process.

70. What is a security issue? Name some of the items that may be included.

71. As part of creating the security incident management process, a number of tasks lay the groundwork for an effective incident response. What are they? Give a brief description of each.

72. What is a CIRT?

73. List some of the steps the FA group should initiate in response to suspicious activity in the environment.

ch02
Answer Section

TRUE/FALSE

1. ANS: F PTS: 1 REF: 32
2. ANS: T PTS: 1 REF: 34
3. ANS: T PTS: 1 REF: 35
4. ANS: T PTS: 1 REF: 36
5. ANS: T PTS: 1 REF: 36
6. ANS: F PTS: 1 REF: 36
7. ANS: F PTS: 1 REF: 41
8. ANS: F PTS: 1 REF: 42
9. ANS: T PTS: 1 REF: 42
10. ANS: T PTS: 1 REF: 43
11. ANS: T PTS: 1 REF: 49
12. ANS: F PTS: 1 REF: 48
13. ANS: T PTS: 1 REF: 44
14. ANS: F PTS: 1 REF: 30
15. ANS: F PTS: 1 REF: 39

MODIFIED TRUE/FALSE

16. ANS: T PTS: 1 REF: 42
17. ANS: F, command

    PTS: 1 REF: 45
18. ANS: F, preventive

    PTS: 1 REF: 30
19. ANS: T PTS: 1 REF: 31
20. ANS: T PTS: 1 REF: 33
21. ANS: F, advisories

    PTS: 1 REF: 34
22. ANS: F, notification

    PTS: 1 REF: 35
23. ANS: F, vulnerability

    PTS: 1 REF: 36
24. ANS: F, corrective

    PTS: 1 REF: 31
25. ANS: F, assess

PTS: 1 REF: 45

26. ANS: T PTS: 1 REF: 33

27. ANS: F, issue

PTS: 1 REF: 38

28. ANS: F, high

PTS: 1 REF: 40

MULTIPLE CHOICE

29. ANS: B PTS: 1 REF: 30
30. ANS: B PTS: 1 REF: 31
31. ANS: A PTS: 1 REF: 31
32. ANS: D PTS: 1 REF: 31
33. ANS: D PTS: 1 REF: 31
34. ANS: C PTS: 1 REF: 32
35. ANS: D PTS: 1 REF: 33
36. ANS: C PTS: 1 REF: 34
37. ANS: B PTS: 1 REF: 34
38. ANS: C PTS: 1 REF: 34
39. ANS: D PTS: 1 REF: 35
40. ANS: B PTS: 1 REF: 35
41. ANS: B PTS: 1 REF: 35
42. ANS: C PTS: 1 REF: 35
43. ANS: A PTS: 1 REF: 39
44. ANS: B PTS: 1 REF: 40
45. ANS: A PTS: 1 REF: 40
46. ANS: C PTS: 1 REF: 42
47. ANS: D PTS: 1 REF: 42
48. ANS: A PTS: 1 REF: 42
49. ANS: B PTS: 1 REF: 43
50. ANS: D PTS: 1 REF: 43
51. ANS: A PTS: 1 REF: 45
52. ANS: A PTS: 1 REF: 45
53. ANS: A PTS: 1 REF: 47
54. ANS: A PTS: 1 REF: 49

COMPLETION

55. ANS: bugs

PTS: 1 REF: 34

56. ANS: discovery

PTS: 1 REF: 35

57. ANS:

zero
0

PTS: 1 REF: 35

58. ANS: repair

PTS: 1 REF: 35

59. ANS: issue

PTS: 1 REF: 38

60. ANS: loss

PTS: 1 REF: 42

61. ANS: Quantitative

PTS: 1 REF: 43

62. ANS: Qualitative

PTS: 1 REF: 43

63. ANS: forensic

PTS: 1 REF: 46

64. ANS: medium

PTS: 1 REF: 40

65. ANS: detective

PTS: 1 REF: 45

66. ANS: education

PTS: 1 REF: 47

67. ANS: log

PTS: 1 REF: 49

ESSAY

68. ANS:
An effective security education plan is a preventive control. Generally speaking, security education gives users the knowledge to help prevent potential security breaches by abusers. The education can provide security knowledge that is shared among the employees. The education is then applied to the computer environment, where it can save the organization money.

An education plan also fulfills several major goals. First, it allows an organization to mobilize all employees in the fight against abusers. Second, effective education informs employees on where to find the corporate security policies. Third, education clearly defines employees' responsibilities in adhering to security guidelines. And finally, and most importantly, an effective education plan outlines the security guidelines that relate to an employee's job.

PTS: 1 REF: 31

69. ANS:
1. Receive the necessary advisories in a timely manner. Once a software problem is announced to the general public, it is only a matter of time before attackers start building automated tools to exploit the bug.
2. Assess the advisory and determine whether the publicized problem poses a threat to the organization. If the organization does not use the software or does not have the particular versions installed, disregard and archive the advisory for future reference.
3. Using predefined criteria documented within the security policy, assess how quickly the patch(es) must be installed on affected systems. For example, systems connected to the Internet should be addressed much more quickly than those on an Intranet, and business-critical systems should be fixed sooner than non-critical systems.These deadlines should be documented and applied consistently throughout the environment. In basic terms, the greater the threat or possible loss from the exploit, the quicker fixes should be implemented.
4. Once the impact and timelines have been assessed, assign the work and track progress. This type of tracking should only cease once all affected systems are addressed.
5. Once the exposure has been closed with the appropriate patch from the manufacturer, periodically check systems to ensure the process is followed and the latest patches are installed on systems.

PTS: 1 REF: 37

70. ANS:
The following list of security issues and their treatment cover some of the items that may be included:
1. Vulnerabilities uncovered by the security advisory process: The software vulnerabilities on all affected systems must be fixed, addressed within a specified amount of time, and may require management to intercede to force the installation of patches.
2. Deviations from security policy: During the course of day-to-day operations and during security reviews or audits, deviations to security policies may be uncovered.These items should be tracked and addressed.
3. Vulnerabilities uncovered during security testing: Although the numbers reported by some security tools may seem daunting, each system and vulnerability should be tracked by the security issue management process.
4. Security incidents: Incidents tend to be handled more delicately than other security information; however, tracking incidents within the security issue management process for future trending and analysis is valuable.

PTS: 1 REF: 38

71. ANS:
1. Learn applicable laws-This knowledge applies in prosecuting computer crimes, handling evidence, and a variety of other aspects of the incident management plan
2. Build a computer incidence response team (CIRT)- A CIRT comprises the resources necessary to respond effectively to a security incident
3. Develop a communication plan-A communication path must be designed to report suspicious activity
4. Develop a response plan- The communication plan organizes communication paths for notifying agencies of suspicious computer activity, and in contrast, the response plan defines how CIRT and other organizations respond to the security incident
5. Conduct training-The hallmark of any successful security service or program is education
6. Post no trespassing signs- As a preventive measure, it is important to warn all visitors that unauthorized access to systems is not permitted
7. Detect malicious activity- To those familiar with information security measures, the term detective measures immediately brings to mind automated tools installed within the IT environment to detect malicious network or system activity. Because these measures are the alarm systems for computer system trespassing, it is crucial that they be installed and monitored on a regular basis

PTS: 1 REF: 45

72. ANS:
A computer incident response team (CIRT) comprises the resources necessary to respond effectively to a security incident.The team includes two major roles: command and control (CnC) and forensic analysis (FA).The CnC function can be one person or a group of people dedicated to the following:
1) Deciding when an incident response plan should be followed
2) Coordinating activities among the FA group and other organizations
3) Deciding on responses that may impact business operations
4) Briefing managers and executives
5) Interfacing with the public relations office
6) Communicating with the Internet and telecommunications service provider
7) Escalating issues to the Legal Department and law enforcement

PTS: 1 REF: 46

73. ANS:
The steps that are outlined within the response plan differ with every organization; however, the following 11 actions establish a solid foundation for a measured response:
Stay calm
Start a detailed log
Conduct thorough interviews
Coordinate communications
Determine the extent of the intrusion
Protect evidence
Contain the problem
Determine the root of the problem
Restore business operations

PTS: 1 REF: 48