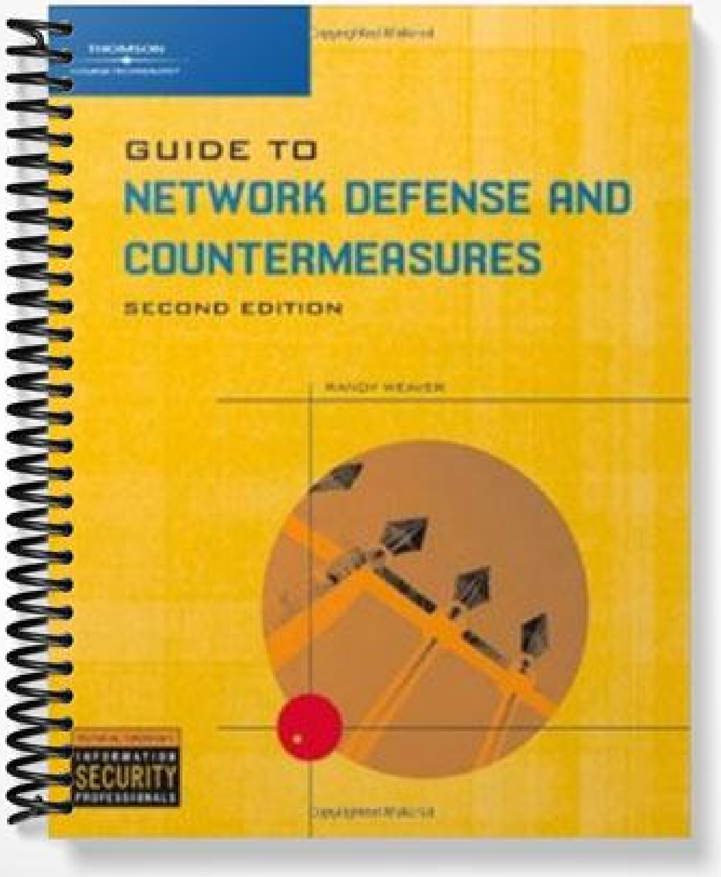
TEST BANK


THOMSON
COURSE TECHNOLOGY
Copyrighted Material
GUIDE TO
NETWORK DEFENSE AND
COUNTERMEASURES
SECOND EDITION
RANDY WEAVER
INFORMATION
SECURITY
PROFESSIONALS
Copyrighted Material

ch02

True/False

Indicate whether the statement is true or false.

____ 1. There is no situation in which security is perfect.

____ 2. All assets are tangible objects that you can actually touch or work with, such as computers.

____ 3. The seriousness of a threat depends on the probability that it will occur.

____ 4. Freeware Web servers do not suffer from software flaws.

____ 5. Substantial consequences can result from a virus that forces you to take your Web site offline for a week.

Multiple Choice

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

____ 6. ____ determines the threats that face the organization, precisely what resources are at risk, and what priority should be given each asset.

a. Security policy
b. Risk analysis
c. Implementation
d. Enforcement and monitoring

____ 7. ____ is a statement that spells out exactly what defenses should be configured to block unauthorized access, how the organization will respond to attacks, and how employees should safely handle the organization’s resources to discourage loss of data or damage to files.

a. A security policy
b. Risk management
c. Risk assessment
d. An implementation

____ 8. ____ is the study of the likelihood of damage or loss in a particular situation or environment.

a. Risk assessment
b. Risk mitigation
c. Risk management
d. Risk analysis

____ 9. ____ are the hardware, software, and informational resources you need to protect by developing and implementing a comprehensive security policy.

a. Risk
b. Vulnerabilities
c. Assets
d. Consequences

____ 10. ____, even though it is not something you can touch, might be the most important asset to continuing business operations.

a. Data
b. A computer
c. A password
d. A power supply

____ 11. Geographic or physical location, habitual, and other factors affect the ____ that a threat will actually occur.

a. risk
b. consequence
c. probability
d. vulnerability

____ 12. ____ are what’s left over after countermeasures and defenses are implemented.

a. Vulnerabilities
b. Residual risks
c. Probabilities
d. Consequences

____ 13. ____ means the capability of a system to repel attacks.

a. Adaptation and evolution
b. Recovery
c. Recognition
d. Resistance

____ 14. ____ means the capability to detect attacks when they occur and to evaluate the extent of damage and compromise.

a. Adaptation and evolution
b. Recovery
c. Recognition
d. Resistance

____ 15. ____ means the capability to maintain essential services during an attack and to restore all services following an attack.

a. Adaptation and evolution
b. Recovery
c. Recognition
d. Resistance

____ 16. ____ means the capability to improve system survivability based on knowledge gained from attacks.

a. Adaptation and evolution
b. Recovery
c. Recognition
d. Resistance

____ 17. ____ approaches risk analysis from the standpoint of threats and risks to an organization's assets and the consequences of those threats and risks if they occur.

a. Survivable Network Analysis (SNA)
b. Threat and Risk Assessment (TRA)
c. Security Incident Response Team (SIRT)
d. Electronic Security Instruction (ESI)

____ 18. When estimating cost, the ____ represents the most realistic estimate of the money you'll have to spend to replace the item.

a. high cost
b. medium cost
c. likely cost
d. low cost

____ 19. Your company's ____ assets—the actual hardware devices that keep data flowing throughout the network—are the most obvious objects that need to be identified.

a. logical
b. electronic
c. data
d. physical computing

____ 20. A company's ____ assets are the routers, cables, servers, and firewall hardware and software that enable employees to communicate with one another and other computers on the Internet.

a. network
b. electronic
c. logical
d. data

____ 21. ____ assets include e-mail messages, any records of instant messaging conversations, and the log files compiled by firewalls and IDSs.

a. Physical
b. Network
c. Data
d. Logical

____ 22. ____ assets include personnel, customer, and financial information that your company needs to protect.

a. Physical
b. Network
c. Data
d. Logical

____ 23. The ____ section of a security policy describes in detail who will respond to security incidents, what needs to be done, and why these procedures need to happen.

a. incident analysis
b. incident response
c. risk assessment
d. return on investment

____ 24. The ____ is a group of staff people designated to take countermeasures when an incident is reported.

a. security incident response team (SIRT)
b. survivable network team (SVT)
c. threat and risk team (TRT)
d. network emergency team (NET)

____ 25. You might see a SIRT referred to as a ____, which can respond to any type of system failure, not just a security-related intrusion.
a. survivable network team (SNT)
b. threat and risk team (TRT)
c. computer emergency response team (CERT)
d. network emergency team (NET)

____ 26. A(n) ____ is a set of roles, responsibilities, and measures taken in response to a security incident.
a. role-and-responsibility procedure
b. incident response procedure
c. worst-case scenario
d. escalation procedure

Completion

Complete each statement.

27. ____________________ are measures you can take to reduce threats, such as installing firewalls and IDSs, locking doors, and using passwords and encryption.

28. ____________________ means the capability to continue functioning during attacks, system faults, accidents, or disasters.

29. ____________________ is the capability of an object or a system to continue operations despite a failure, such as a system shutdown.

30. ____________________ simulation is an analytical method meant to simulate a real-life system by randomly generating values for variables.

31. ____________________ is the term that describes the process of identifying, choosing, and setting up countermeasures justified by the risks you identify.

Matching

Match each term with the correct statement below.
a. Risk
b. Threats
c. Exposure
d. Vulnerabilities
e. Lion
f. ROI
g. Survivable Network Analysis (SNA)
h. Project Risk Analysis
i. Electronic assets

____ 32. is software developed by Katmar Software that helps you estimate the financial impact of losses.

____ 33. are the word processing, spreadsheet, Web page, and other documents on your network computers.

____ 34. are events and conditions that haven’t occurred but could potentially occur, and their presence increases risk.

____ 35. are situations or conditions that increase the probability of a threat, which in turn increases risk.

____ 36. is a worm that affects Linux systems.

____ 37. is the possibility of damage or loss.

____ 38. is increased if you have one or more factors that increase threat probabilities.

____ 39. stands for return on investment

____ 40. is a security process developed by the CERT Coordination Center security group.

Short Answer

41. What are the four types of assets you are likely to encounter in an organization?

42. Give some examples of circumstance-specific threats.

43. What is the Common Vulnerabilities and Exploits (CVE) list?

44. Explain various consequences of threats that you should consider when conducting a risk analysis.

45. What is a cost-benefit analysis?

46. Describe the four steps in Survivable Network Analysis.

47. Describe the four steps in Threat and Risk Assessment (TRA).

48. Explain why risk analysis is an ongoing process.

49. What measures can you use to protect sensitive information?

50. What measures can you use to minimize the risk of security problems with corporate information?

ch02
Answer Section

TRUE/FALSE

1.	ANS:	T	PTS:	1	REF:	48
2.	ANS:	F	PTS:	1	REF:	50
3.	ANS:	T	PTS:	1	REF:	50
4.	ANS:	F	PTS:	1	REF:	52
5.	ANS:	T	PTS:	1	REF:	52

MULTIPLE CHOICE

6.	ANS:	B	PTS:	1	REF:	48
7.	ANS:	A	PTS:	1	REF:	48
8.	ANS:	D	PTS:	1	REF:	49
9.	ANS:	C	PTS:	1	REF:	49
10.	ANS:	A	PTS:	1	REF:	50
11.	ANS:	C	PTS:	1	REF:	50
12.	ANS:	B	PTS:	1	REF:	55
13.	ANS:	D	PTS:	1	REF:	57
14.	ANS:	C	PTS:	1	REF:	57
15.	ANS:	B	PTS:	1	REF:	57
16.	ANS:	A	PTS:	1	REF:	57
17.	ANS:	B	PTS:	1	REF:	58
18.	ANS:	C	PTS:	1	REF:	61
19.	ANS:	D	PTS:	1	REF:	64
20.	ANS:	A	PTS:	1	REF:	65
21.	ANS:	D	PTS:	1	REF:	66
22.	ANS:	C	PTS:	1	REF:	66
23.	ANS:	B	PTS:	1	REF:	69
24.	ANS:	A	PTS:	1	REF:	70
25.	ANS:	C	PTS:	1	REF:	70
26.	ANS:	D	PTS:	1	REF:	71

COMPLETION

27. ANS: Safeguards

PTS: 1 REF: 54

28. ANS: Survivability

PTS: 1 REF: 56

29. ANS: Fault tolerance

PTS: 1 REF: 57

30. ANS: Monte Carlo

PTS: 1 REF: 61

31. ANS: Risk management

PTS: 1 REF: 64

MATCHING

32.	ANS:	H	PTS:	1	REF:	61
33.	ANS:	I	PTS:	1	REF:	66
34.	ANS:	B	PTS:	1	REF:	50
35.	ANS:	D	PTS:	1	REF:	52
36.	ANS:	E	PTS:	1	REF:	52
37.	ANS:	A	PTS:	1	REF:	49
38.	ANS:	C	PTS:	1	REF:	51
39.	ANS:	F	PTS:	1	REF:	53
40.	ANS:	G	PTS:	1	REF:	56

SHORT ANSWER

41. ANS:

You're likely to encounter four different types of assets:
* *Physical assets*—Equipment and buildings in the organization
* *Data assets*—Databases, personnel records, customer or client information, and other data the organization stores
* *Application software assets*—Server programs, security programs, and other applications used on a day-to-day basis to communicate and carry out the organization's typical activities
* *Personnel assets*—People who work in the organization as well as customers, business partners, contractors, and freelance employees who contribute to the organization

PTS: 1 REF: 49-50

42. ANS:

Examples of circumstance-specific threats include the following:
* *Power supply*—The power supply in your area might be unreliable, making your company subject to brownouts, blackouts, and sudden surges called voltage spikes.
* *Crime rate*—If you work in a high-crime area, or if other offices in your area have been broken into, your risk is increased.
* *Facility-related*—If your building has old wiring prone to fluctuations or has insufficient fire suppression, the risk of water or fire damage increases.
* *Industry*—Your organization operates in a highly competitive industry or in one that requires high security. A security breach could result in litigation or major loss of revenue or even closure of the business.

PTS: 1 REF: 50

43. ANS:

By identifying any vulnerability associated with a client's network,you can determine which type of attack the network is susceptible to. Security professionals have many resources for finding information on current vulnerabilities or possible network attacks. One site that should be bookmarked in any security professional's Web browser is the Common Vulnerabilities and Exploits (CVE) list (*www.cve.mitre.org*) sponsored by US-CERT (*www.us-cert.gov*). The primary mission of the CVE is to standardize naming of vulnerabilities and exploits, but its database is essentially a dictionary of security threats. The list is free to download and can be searched easily. As of this writing, the CVE contained 10,423 entries.

PTS: 1 REF: 52

44. ANS:
Besides the consequences of getting a system back online after an attack, there's a cost impact as well as other effects that can be more difficult to anticipate. They include insurance claims, police reports, shipping or delivery charges, and the time and effort to obtain and reinstall software or hardware. A return on investment (ROI) calculator, such as the one offered by Cisco Systems Cisco Security Agent, can help you calculate these losses, which can amount to far more than the actual price of hardware.

PTS: 1 REF: 53

45. ANS:
The actual cost of an incident is usually much higher than the cost of replacing equipment and restoring data (if it can be restored). When you go to management to justify investing in security, estimating the cost of the investment and benefit to the company (commonly called a cost-benefit analysis) is vital. The most critical numbers you want management to understand are the ones for the actual cost per year the company is paying because of security incidents. The benefit is the amount per year saved by preventing incidents.

PTS: 1 REF: 54

46. ANS:
The steps in SNA are as follows:
* *System definition*—First, you create an overview of the system's organizational requirements. You analyze system architecture while taking into account its hardware components, software installations, databases, servers, and other computers that store your information.
* *Essential capability definition*—You identify a system's essential services and assets that are critical to fulfilling your organization's missions and goals.
* *Compromisable capability definition*—You design scenarios in which intrusions to the system occur, and then trace the intrusion through your system architecture to identify what can be accessed and what sorts of damage can occur.
* *Survivability analysis*—You identify potential points of fault in the system—integral components that can be compromised. You then make recommendations for correcting the points of fault and suggest specific ways to improve the system's resistance to intrusions and its capability to recover from attacks, accidents, and other disasters.

PTS: 1 REF: 57

47. ANS:
TRA has four steps:
* *Asset definition*—You identify software, hardware, and information you need to defend.
* *Threat assessment*—You identify the kinds of threats that place the asset at risk. These threats include vandalism, fire, natural disasters such as floods, and attacks from the Internet. Threat assessment also includes an evaluation of the probability and consequences of each threat.

* *Risk assessment*—You evaluate each asset for any existing safeguards, the severity of threats and risks to assets, and the consequences of the threat or risk actually taking place. The combination of these factors creates an assessment of the actual risk to each asset.
* *Recommendations*—Based on the risks and current safeguards, you make recommendations to reduce the risk. These recommendations should then be made part of a security policy.

PTS: 1 REF: 58

48. ANS:

Risk analysis is not a one-time activity used solely to create a security policy. Rather, risk analysis evolves to take into account an organization's changing size and activities, the progression to larger and more complex computer systems,and new threats from both inside and outside the corporate network.

The initial risk analysis is used to formulate a security policy; the security policy is then enforced and security is monitored. New threats and intrusion attempts create the need for a reassessment of the risk the organization faces.

PTS: 1 REF: 59

49. ANS:

You can use the following measures to protect information:
* *Encryption*—By encrypting data, you can protect it as it passes from one network to another so that it can't be read if it's intercepted or captured.
* *Message filtering*—This measure keeps potentially harmful messages from entering the network from the outside.
* *Data encapsulation*—The data in packets can be encrypted in such a way that the packets are encapsulated (or "wrapped") for extra protection.
* *Redundancy*—By providing redundancy through backup systems, you ensure that databases and other stores of information remain accessible if primary systems go offline.
* *Backups*—Systematic and periodic backups of information on the network are one of the most basic and important ways to protect that information.

PTS: 1 REF: 67

50. ANS:

You might decide to minimize risks by specifying the following measures in a security policy:
* Never leave company-owned laptops or handheld devices unattended.
* Always password-protect information on corporate devices.
* Encrypt any financial information.
* Password-protect all job records and customer information.
* Restrict all personnel information to human resources staff and/or upper management.

PTS: 1 REF: 67