Security Awareness 6th edition Ciampa Test Bank

SKU: 9780357883761-TEST-BANK

Name:_____ Class:_____ Date:_____

Module 01: Introduction to Cybersecurity

1. There is a straightforward and easy solution to securing computers.
   a. True
   b. False

ANSWER: False

2. Attack tools can initiate new attacks without any human participation, thus increasing the speed at which systems are attacked.
   a. True
   b. False

ANSWER: True

3. Today, many attack tools are freely available and do not require any technical knowledge to use.
   a. True
   b. False

ANSWER: True

4. Script kiddies typically have advanced knowledge of computers and networks.
   a. True
   b. False

ANSWER: False

5. In a well-run information security program, attacks will never get through security perimeters and local defenses.
   a. True
   b. False

ANSWER: False

6. Browsers such as Chrome, Safari, and Firefox are the most popular attack vectors, that is, they are the favored way to deliver malware.
   a. True
   b. False

ANSWER: False

7. A doorbell camera is an example of a universally connected device and can be hacked.
   a. True
   b. False

ANSWER: True

8. Automated attack software downloaded from websites is primarily used by script kiddies.
   a. True
   b. False

ANSWER: True

9. Spying on computer input over an extended period of time is usually accomplished by the work of state actors.
   a. True
   b. False

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank

Module 01: Introduction to Cybersecurity

ANSWER: True

10. Which of the following is NOT a factor that contributes to difficulties faced in defending against attacks?
    a. universally connected devices
    b. greater sophistication of attacks
    c. enhanced encryption algorithms
    d. faster detection of vulnerabilities

ANSWER: c

11. Which phrase best describes security?
    a. the procedures used to protect data
    b. the goal to be free from danger as well as the process that achieves that freedom
    c. the protection of data from harm
    d. the process of hiding sensitive data with the goal of maintaining privacy

ANSWER: b

12. Which of the following is the term for a hacker who probes a system for weaknesses and provides that information back to the organization?
    a. gray hat hacker
    b. white hat hacker
    c. black hat hacker
    d. red hat hacker

ANSWER: b

13. The AV-TEST Institute states that it expects the total number of malware attacks for this year to exceed:
    a. 450,000.
    b. 250,000.
    c. 1.2 million.
    d. 1.34 billion.

ANSWER: d

14. How do attackers today make it difficult to distinguish an attack from legitimate traffic?
    a. by using a common language
    b. by using diverse interfaces
    c. by using universally connected devices
    d. by using simple scripting

ANSWER: c

15. Security is _____ convenience.
    a. more important than
    b. inversely proportional to
    c. proportional to
    d. less important than

ANSWER: b

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank

Module 01: Introduction to Cybersecurity

16. What term is frequently used to describe the tasks of securing technology?
    a. network security
    b. information assurance
    c. cybersecurity
    d. information warfare

ANSWER: c

17. Which of the following ensures that information is correct and no unauthorized person or malicious software has altered it?
    a. protection
    b. availability
    c. confidentiality
    d. integrity

ANSWER: d

18. Which of the following ensures that data is accessible when needed to authorized users?
    a. confidentiality
    b. non-repudiation
    c. integrity
    d. availability

ANSWER: d

19. Information contained on devices is protected by three layers: Two of the layers are products and policies and procedures. What is the third layer?
    a. people
    b. systems
    c. applications
    d. tools

ANSWER: a

20. Which of the following is a type of action that has the potential to cause harm?
    a. asset
    b. vulnerability
    c. threat
    d. threat agent

ANSWER: c

21. Which term is best described as a person or element that has the power to carry out a threat?
    a. threat agent
    b. vulnerability
    c. risk
    d. attack agent

ANSWER: a

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank

Module 01: Introduction to Cybersecurity

22. What do you call a flaw or weakness in a computer system that allows access by threat actors?
    a. risk
    b. vulnerability
    c. asset
    d. threat

ANSWER: b

23. Which of the following involves stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain?
    a. white hat hacking
    b. identity theft
    c. cyberterrorism
    d. Digital fraud

ANSWER: b

24. Under which law must healthcare enterprises guard protected health information and implement policies and procedures to safeguard it, whether it be in paper or electronic format?
    a. Sarbox
    b. COPPA
    c. GLBA
    d. HIPAA

ANSWER: d

25. Which law requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information?
    a. Sarbox
    b. COPPA
    c. GLBA
    d. HIPAA

ANSWER: c

26. What does the FBI define as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents?"
    a. information warfare
    b. cyberware
    c. cyberterrorism
    d. eTerrorism

ANSWER: c

27. In the past, which term was commonly used to refer to a person who uses advanced computer skills to attack computers?
    a. slacker
    b. hacker
    c. white-hat

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank

d. black-hat

ANSWER: b

28. Which term is best described as individuals who want to attack computers yet who lack the knowledge of computers and networks needed to do so?

a. hackers
b. elites
c. crackers
d. script kiddies

ANSWER: d

29. Which attacker category might have the objective of retaliation against an employer?

a. cybercriminal
b. insider
c. hactivist
d. state-sponsored attacker

ANSWER: b

30. Terrorists who turn their attacks to the network and computer infrastructure to cause panic among citizens are known as which of the following?

a. cyberterrorists
b. spies
c. hackers
d. hactivists

ANSWER: a

31. Which of the following is NOT a protection that must be extended over information?

a. policies and procedures
b. integrity
c. availability
d. confidentiality

ANSWER: a

32. Which of the following threat actors would be responsible for making a political statement or a retaliatory attack?

a. cyberterrorist
b. hactivist
c. broker
d. script kiddie

ANSWER: b

33. Which of the following is NOT a term associated with cybersecurity?

a. risk
b. information assurance
c. malware

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank

d. goal

ANSWER: d

34. In a general sense, _____ can be defined as the necessary steps to protect a person or property from harm.
ANSWER: security

35. A(n) _____ is defined as something that has a value.
ANSWER: asset

36. Targeted attacks against individual users, enterprises, and governments with the focus of financial gain are known as _____.
ANSWER: cybercrime

37. It is vital to have _____ security on all personal computers to defend against any attack that breaches the perimeter.
ANSWER: local

38. It is important that action be taken in advance in order to _____. This may involve keeping backup copies of important data stored in a safe place.
ANSWER: minimize losses

Matching

Match each item with a statement below.
a. authentication
b. authorization
c. confidentiality
d. cybercrime
e. cyberterrorism
f. identity theft
g. insiders
h. integrity
i. attack vector

39. Steps that ensure that the individual is who they claim to be
ANSWER: a

40. The process of providing proof of genuineness
ANSWER: a

41. The act of providing permission or approval to technology resources
ANSWER: b

42. Targeted attacks against financial networks, unauthorized access to information, and the theft of personal information
ANSWER: d

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank

Module 01: Introduction to Cybersecurity

43. Permission to access an accounting database once a user is verified to log into the system
ANSWER: b

44. Stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain
ANSWER: f

45. Employees, contractors, and business partners who can be responsible for an attack
ANSWER: g

46. Security actions that ensure that the information is correct and no unauthorized person or malicious software has altered the data
ANSWER: h

47. Means by which an attack could occur
ANSWER: i

48. What are state actors and who employs them?
ANSWER: State actors are cyber attackers that are under the direction of a government or nation to launch cyberattacks against other governments. These attacks can be against financial institutions, government entities, utilities, or other areas with the purpose of creating cyberterrorism.

49. Discuss the difficulties in defending against the speed of attacks.
ANSWER: With modern technology, attackers can quickly scan millions of devices to find weaknesses and launch attacks with unprecedented speed. Today's attack tools initiate new attacks without any human participation, thus increasing the speed at which systems are attacked.

50. Discuss the difficulties in defending against the greater sophistication of attacks.
ANSWER: Attacks are becoming more complex, making it more difficult to detect and defend against them. Attackers today use common Internet tools and protocols to send malicious data or commands to attack computers, making it difficult to distinguish an attack from legitimate traffic. Other attack tools vary their behavior, so the same attack appears differently each time, further complicating detection.

51. Discuss the difficulties in defending against the availability and simplicity of attack tools.
ANSWER: Whereas in the past an attacker needed to have an extensive technical knowledge of networks and computers, as well as the ability to write a program to generate the attack, that is no longer the case. Today's attack tools do not require any sophisticated knowledge. In fact, many of the tools have a graphical user interface (GUI) that allows the user to easily select options from a menu. These tools are freely available or can be purchased from other attackers at a low cost.

52. Discuss the difficulties in defending systems when there are delays in security updating products.
ANSWER: Hardware and software vendors are overwhelmed trying to keep pace with updating their products against attacks. One antivirus software security institute receives more than 450,000 submissions of potential malware each day. At this rate, the antivirus vendors would have to create and distribute updates every few seconds to keep users fully protected. This delay in distributing security updates adds to the difficulties in defending against attacks.

53. Discuss the difficulties in defending against distributed attacks.
ANSWER: Attackers can use hundreds of thousands of computers under their control in an attack against a single server

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank

or network. This "many against one" approach makes it virtually impossible to stop an attack by identifying and blocking a single source.

54. Discuss the difficulties in defending systems when dealing with user confusion.

ANSWER: Increasingly, users are called upon to make difficult security decisions regarding their computer systems, sometimes with little or no information to direct them. It is not uncommon for a user to be asked security questions such as Do you want to view only the content that was delivered securely? Or is it safe to quarantine this attachment? Or do you want to install this extension? With little or no direction, users are inclined to provide answers to questions without understanding the security risks. In addition, popular information that is circulated about security through consumer news outlets or websites is often inaccurate or misleading, resulting in even more user confusion.

55. Briefly describe state notification and security laws.

ANSWER: These laws typically require businesses to inform residents within a specific period of time (typically 48 hours) if a breach of personal information has or is believed to have occurred. The penalties for violating these laws can be sizeable. Businesses must make every effort to keep electronic data secure from hostile outside forces to ensure compliance with these laws and avoid serious legal consequences.

56. What are cybercriminals?

ANSWER: The generic term cybercriminals is often used to describe individuals who launch attacks against other users and their computers (another generic word is simply attackers) usually for financial gain. However, strictly speaking, cybercriminals are a loose network of attackers, identity thieves, and financial fraudsters who are highly motivated, less risk averse, well-funded, and tenacious.

57. Briefly describe hactivists from an information security point of view.

ANSWER: Hactivists are motivated by ideology. Unlike cyberterrorists, who launch attacks against nations, hactivists (a combination of the words hack and activism) direct their attacks at specific websites. Generally, these attacks are intended to promote a political agenda and are in retaliation for a prior event. For example, hactivists might attempt to disable a bank's website because that bank stopped accepting online payments that were deposited into accounts belonging to the hactivists.

58. Explain the concept of layering as it relates to protection against cybercrime.

ANSWER: Layering is the concept of establishing multiple defenses against attacks, making it much more difficult to reach the goal. For example, using a firewall, malware scanner, email scanner, and authorization tables presents a multiple approach to defense.

59. Explain the difference between risk acceptance and risk mitigation as it pertains to cybercrime.

ANSWER: Risk acceptance is the chance that an attack will happen and understanding how that will affect the business or situation. Risk mitigation is making the risk less serious by taking action. The level of mitigation will determine how much acceptance the company will take.

60. Explain the difference between a computer threat agent and a thief.

ANSWER: A threat agent has the power to carry out a threat by using the tools they have at hand. The threat agent may or may not steal something but may cause harm, destruction, or terror due to their actions. The thief is a person who has a distinct goal of taking something. A threat agent may or may not be a thief.

61. Give three reasons why cybersecurity is important.

ANSWER: Cybersecurity is important to foil cyberterrorism and prevent panic. It is also important to prevent data theft and to ensure data integrity. A third reason is to ensure that identity theft does not occur.

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank

Module 01: Introduction to Cybersecurity

62. Some attacks likely will get through security perimeters and local defenses. Explain how an enterprise can minimize its losses to cyber attacks.

ANSWER: Enterprises can minimize losses by keeping backup copies of important data stored in a safe place and having an entire business recovery policy in place that details what to do in the event of a successful attack.

63. Explain why cybersecurity can be defined as an art.

ANSWER: Cybersecurity can be defined as an art because security must be applied to meet the specific needs of the data and systems and each security level is designed as part of a total security package.

64. Explain the relationship between threat likelihood and risk.

ANSWER: The threat likelihood is a probability number, such as 30 percent that an attack will succeed. A risk is the exposure of something valuable, such as data, passwords, etc.

65. Explain the concept of a distributed attack.

ANSWER: A distributed attack that uses multiple, even millions of computers to direct a remote attack against a single device. An attack of such magnitude from so many sources makes it impossible to block the attacking computer and stop the attack.

Copyright Cengage Learning. Powered by Cognero.

Security Awareness 6th edition Ciampa Test Bank