Chapter 02 The Need for Security

TRUEFALSE

1. Information security's primary mission is to ensure that systems and their contents retain their confidentiality at any cost.

(A) True

(B) False

Answer : (B)

2. The information security function in an organization safeguards its technology assets.

(A) True

(B) False

Answer : (A)

3. As an organization grows, it must often use more robust technology to replace the security technologies it may have outgrown.

(A) True

(B) False

Answer : (A)

4. Suppose an act of theft performed by a hacker was accompanied by defacement actions to delay discovery. The first act is obviously in the category of "theft" but the second act is another category-in this case it is a "force of nature."

(A) True

(B) False

Answer : (B)

5. Two watchdog organizations that investigate allegations of software abuse are the Software & Information Industry Association (SIIA) and National Security Agency (NSA).

(A) True

(B) False

Answer : (B)

6. A number of technical mechanisms-digital watermarks and embedded code, copyright codes, and even the intentional placement of bad sectors on software media-have been used to deter or prevent the theft of software intellectual property.

(A) True

(B) False

Answer : (A)

7. Expert hackers are extremely talented individuals who usually devote lots of time and energy to attempting to break into other people's information systems.

(A) True

(B) False

Answer : (A)

8. Attacks conducted by scripts are usually unpredictable.

(A) True

(B) False

Answer : (B)

9. With the removal of copyright protection mechanisms, software can be easily distributed and installed.

(A) True

(B) False

Answer : (A)

10. Organizations can use dictionaries to regulate password selection during the reset process and thus guard against easy-to-guess passwords.

(A) True

(B) False

Answer : (A)

11. Forces of nature, sometimes called acts of God, can present some of the most dangerous threats because they usually occur with very little warning and are beyond the control of people.

(A) True

(B) False

Answer : (A)

12. Much human error or failure can be prevented with effective training and ongoing awareness activities.

(A) True

(B) False

Answer : (A)

13. An advance-fee fraud attack involves the interception of cryptographic elements to determine keys and encryption algorithms.

(A) True

(B) False

Answer : (B)

14. Compared to Web site defacement, vandalism within a network is less malicious in intent and more public.

(A) True

(B) False

Answer : (B)

15. A worm may be able to deposit copies of itself onto all Web servers that the infected system can reach, so that users who subsequently visit those sites become infected.

(A) True

(B) False

Answer : (A)

16. A worm requires that another program is running before it can begin functioning.

(A) True

(B) False

Answer : (B)

17. DoS attacks cannot be launched against routers.

(A) True

(B) False

Answer : (B)

18. A mail bomb is a form of DoS attack.

(A) True

(B) False

Answer : (A)

19. A sniffer program can reveal data transmitted on a network segment, including passwords, the embedded and attached files-such as word-processing documents-and sensitive data transmitted to or from applications.

(A) True

(B) False

Answer : (A)

20. When electronic information is stolen, the crime is readily apparent.

(A) True

(B) False

Answer : (B)

21. Media are items of fact collected by an organization and include raw numbers, facts, and words.

(A) True

(B) False

Answer : (B)

22. Media as a subset of information assets are the systems and networks that store, process, and transmit information.

(A) True

(B) False

Answer : (A)

23. Intellectual property is defined as "the creation, ownership, and control of ideas as well as the representation of those ideas." ________________________

(A) True

(B) False

Answer : (A)

24. Hackers are "persons who access systems and information without authorization and often illegally." ________________________

(A) True

(B) False

Answer : (A)

25. When voltage levels lag (experience a momentary increase), the extra voltage can severely damage or destroy equipment. ________________________

(A) True

(B) False

Answer : (B)

26. "Shoulder spying" is used in public or semi-public settings when individuals gather information they are not authorized to have by looking over another individual's shoulder or viewing the information from a distance. ________________________

(A) True

(B) False

Answer : (B)

27. Packet munchkins use automated exploits to engage in distributed denial-of-service attacks.

____

(A) True

(B) False

Answer : (B)

28. The term phreaker is now commonly associated with an individual who cracks or removes software protection that is designed to prevent unauthorized duplication. ________________________

(A) True

(B) False

Answer : (B)

29. The application of computing and network resources to try every possible combination of options of a password is called a dictionary attack. ________________________

(A) True

(B) False

Answer : (B)

30. Cyberterrorists hack systems to conduct terrorist activities via network or Internet pathways. ________________________

(A) True

(B) False

Answer : (A)

31. Software code known as a(n) cookie can allow an attacker to track a victim's activity on Web sites. ________________________

(A) True

(B) False

Answer : (A)

32. A(n) polymorphic threat is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures. ________________________

(A) True

(B) False

Answer : (A)

33. The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. ________________________

(A) True

(B) False

Answer : (A)

34. The macro virus infects the key operating system files located in a computer's start-up sector. ________________________

(A) True

(B) False

Answer : (B)

35. Once a(n) back door has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system. ________________________

(A) True

(B) False

Answer : (B)

36. One form of e-mail attack that is also a DoS attack is called a mail spoof, in which an attacker overwhelms the receiver with excessive quantities of e-mail. ________________________

(A) True

(B) False

Answer : (B)

37. A device (or a software program on a computer) that can monitor data traveling on a network is known as a socket sniffer. ________________________

(A) True

(B) False

Answer : (B)

38. Computer assets are the focus of information security and are the information that has value to theorganization, as well as the systems that store, process, and transmit the information.

____

(A) True

(B) False

Answer : (B)

MULTICHOICE

39. Which of the following functions does information security perform for an organization?

(A) Protecting the organization's ability to function.

(B) Enabling the safe operation of applications implemented on the organization's IT systems.

(C) Protecting the data the organization collects and uses.

(D) All of the above.

Answer : (D)

40. Web hosting services are usually arranged with an agreement defining minimum service levels known as a(n) ____.

(A) SSL

(B) SLA

(C) MSL

(D) MIN

Answer : (B)

41. A short-term interruption in electrical power availability is known as a ____.

(A) fault

(B) brownout

(C) blackout

(D) lag

Answer : (A)

42. Hackers can be generalized into two skill groups: expert and ____________________.

(A) novice

(B) journeyman

(C) packet monkey

(D) professional

Answer : (A)

43. Acts of ____________________ can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

(A) bypass

(B) theft

(C) trespass

(D) security

Answer : (C)

44. The ____________________ data file contains the hashed representation of the user's password.

(A) SLA

(B) SNMP

(C) FBI

(D) SAM

Answer : (D)

45. Human error or failure often can be prevented with training, ongoing awareness activities, and ____________________.

(A) threats

(B) education

(C) hugs

(D) paperwork

Answer : (B)

46. "4-1-9" fraud is an example of a ____________________ attack.

(A) social engineering

(B) virus

(C) worm

(D) spam

Answer : (A)

47. One form of online vandalism is ____________________ operations, which interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.

(A) hacktivist

(B) phreak

(C) hackcyber

(D) cyberhack

Answer : (A)

48. ____________________ is the premeditated, politically motivated attacks against information, computer systems, computer programs, and data that result in violence against noncombatant targets by subnational groups or clandestine agents.

(A) infoterrorism

(B) cyberterrorism

(C) hacking

(D) cracking

Answer : (B)

49. ____ is any technology that aids in gathering information about a person or organization without their knowledge.

(A) A bot

(B) Spyware

(C) A Trojan

(D) A worm

Answer : (B)

50. ____________________ are malware programs that hide their true nature and reveal their designed behavior only when activated.

(A) Viruses

(B) Worms

(C) Spam

(D) Trojan horses

Answer : (D)

51. Which of the following is an example of a Trojan horse program?

(A) Netsky

(B) MyDoom

(C) Klez

(D) Happy99.exe

Answer : (D)

52. As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus ___________________.

(A) false alarms

(B) polymorphisms

(C) hoaxes

(D) urban legends

Answer : (C)

53. In a ___________________ attack, the attacker sends a large number of connection or information requests to disrupt a target from a small number of sources.

(A) denial-of-service

(B) distributed denial-of-service

(C) virus

(D) spam

Answer : (A)

54. A ___________________ is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

(A) denial-of-service

(B) distributed denial-of-service

(C) virus

(D) spam

Answer : (B)

55. ____________________ are compromised systems that are directed remotely (usually by a transmitted command) by the attacker to participate in an attack.

(A) Drones

(B) Helpers

(C) Zombies

(D) Servants

Answer : (C)

56. In the ____________________ attack, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network.

(A) zombie-in-the-middle

(B) sniff-in-the-middle

(C) server-in-the-middle

(D) man-in-the-middle

Answer : (D)

57. The ____________________ hijacking attack uses IP spoofing to enable an attacker to impersonate another entity on the network.

(A) WWW

(B) TCP

(C) FTP

(D) HTTP

Answer : (B)

58. Microsoft acknowledged that if you type a res:// URL (a Microsoft-devised type of URL) longer than ____________________ characters in Internet Explorer 4.0, the browser will crash.

(A) 64

(B) 128

(C) 256

(D) 512

Answer : (C)

59. When information gatherers employ techniques that cross a legal or ethical threshold, they are conducting __________.

(A) industrial espionage

(B) competitive intelligence

(C) opposition research

(D) hostile investigation

Answer : (A)

60. The process of maintaining the confidentiality, integrity, and availability of data managed by a DBMS is known as __________ security.

(A) database

(B) data

(C) information

(D) residual

Answer : (A)

61. A long-term interruption (outage) in electrical power availability is known as a(n) ___________.

(A) blackout

(B) sag

(C) brownout

(D) fault

Answer : (A)

62. A short-term decrease in electrical power availability is known as a(n) ___________.

(A) blackout

(B) sag

(C) brownout

(D) fault

Answer : (C)

63. A table of hash values and their corresponding plaintext values that can be used to look up password values if an attacker is able to steal a system's encrypted password file is known as a(n) _________.

(A) rainbow table

(B) dictionary

(C) crib

(D) crack file

Answer : (A)

64. The redirection of legitimate user Web traffic to illegitimate Web sites with the intent to collect personal information is known as _________.

(A) pharming

(B) phishing

(C) sniffing

(D) pharming

Answer : (A)

65. The average amount of time between hardware failures, calculated as the total amount of operation time for a specified number of units divided by the total number of failures, is known as _________.

(A) mean time between failure (MTBF)

(B) mean time to diagnose (MTTD)

(C) mean time to failure (MTTF)

(D) mean time to repair (MTTR)

Answer : (A)

66. The average amount of time until the next hardware failure is known as _________.

(A) mean time between failure (MTBF)

(B) mean time to diagnose (MTTD)

(C) mean time to failure (MTTF)

(D) mean time to repair (MTTR)

Answer : (C)

SHORTANSWER

67. A(n) ___________________ is a potential risk to an information asset.**Answer :** threat

68. A(n) ___________________ is a potential weakness in an asset or its defensive control(s).**Answer :** vulnerability

69. A(n) ___________________ is an act against an asset that could result in a loss.**Answer :** attack

70. Duplication of software-based intellectual property is more commonly known as software ___________________.**Answer :** piracy

71. A momentary low voltage is called a(n) ___________________.**Answer :** fault

72. Some information gathering techniques are quite legal-for example, using a Web browser to perform market research. These legal techniques are called, collectively, competitive ___________________.**Answer :** intelligence

73. When information gatherers employ techniques in a commercial setting that cross the threshold of what is legal or ethical, they are conducting industrial ___________________.**Answer :** espionage

74. The expert hacker sometimes is called a(n) ___________________ hacker.**Answer :** elite

75. Script ___________________ are hackers of limited skill who use expertly written software to attack a system.**Answer :** kiddies

76. A(n) ___________________ hacks the public telephone network to make free calls or disrupt services.**Answer :** phreaker

77. Attempting to reverse-calculate a password is called ___________________.**Answer :** cracking

78. ESD is the acronym for ___________________ discharge.**Answer :** electrostatic

79. In the context of information security, ___________________ is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.**Answer :** social engineering

80. The ___________________ fraud is a social engineering attack that involves convincing the victim to participate in a seeming money-making venture while getting the victim to pay fees or bribes or to refund uncleared international payments.**Answer :** advance-fee
Answer : advance fee

81. A computer virus consists of segments of code that perform ___________________ actions.**Answer**

: malicious

82. A(n) ____________________ is a malicious program that replicates itself constantly without requiring another program environment.**Answer :** worm

83. A virus or worm can have a payload that installs a(n) ____________________ door or trap door component in a system, which allows the attacker to access the system at will with special privileges.**Answer :** back

84. ____________________ is unsolicited commercial e-mail.**Answer :** Spam

85. ____________________ is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host.**Answer :** Spoofing

86. A(n) ____________________ is an application error that occurs when more data is sent to a program than it is designed to handle.**Answer :** buffer overrun
Answer : buffer overflow

87. _________ is the percentage of time a particular service is available.**Answer :** uptime
Answer : up-time
Answer : up time

88. __________ occurs when an application running on a Web server inserts commands into a user's browser session and causes information to be sent to a hostile server.**Answer :** cross-site scripting (XSS)
Answer : cross-site scripting
Answer : XSS
Answer : cross site scripting (XSS)
Answer : cross site scripting

ESSAY

89. There are 12 general categories of threat to an organization's people, information, and systems. List at least six of the general categories of threat and identify at least one example of those listed.

Graders Info :

Compromises to intellectual propertySoftware attacks
Deviations in quality of service
Espionage or trespass
Forces of nature
Human error or failure
Information extortion
Sabotage or vandalism
Theft
Technical hardware failures or errors
Technical software failures or errors

Technological obsolescence

90. Describe viruses and worms.

Graders Info :

A computer virus consists of segments of code that perform malicious actions. This code behaves very much like a virus pathogen attacking animals and plants, using the cell's own replication machinery to propagate and attack. The code attaches itself to the existing program and takes control of that program's access to the targeted computer. The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems.
A worm is a malicious program that replicates itself constantly without requiring another program to provide a safe environment for replication. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.

91. Describe the capabilities of a sniffer.

Graders Info :

A sniffer is a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. Sniffers often work on TCP/IP networks, where they're sometimes called packet sniffers. Sniffers add risk to the network because many systems and users send information on local networks in clear text. A sniffer program shows all the data going by, including passwords, the data inside files, and screens full of sensitive data from applications.