Chapter_02_The_Need_for_Security

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

   ○ True
   ● False

2. ■ ■ Information security safeguards the technology assets in use at the organization.

   ● True
   ○ False

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

   ● True
   ○ False

4. ■ ■ An act of theft performed by a hacker falls into the category of "theft," but is also often accompanied by defacement actions to delay discovery and thus may also be placed within the category of "forces of nature."

   ○ True
   ● False

5. ■ ■ Two watchdog organizations that investigate allegations of software abuse are SIIA and NSA.

   ○ True
   ● False

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.

   ● True
   ○ False

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.

○ True
○ False

8 ■ ■ Attacks conducted by scripts are usually unpredictable.

○ True
● False

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

● True
○ False

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

● True
○ False

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

● True
○ False

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

● True
○ False

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

○ True
● False

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

○ True
● False

---

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

● True
○ False

---

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

○ True
● False

---

17 ▪ ▪ DoS attacks cannot be launched against routers.

○ True
● False

---

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

● True
○ False

---

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.

● True
○ False

---

20 ▪ ▪ With electronic information is stolen, the crime is readily apparent.

○ True
● False

---

21 ▪ ▪ Intellectual property is defined as "the creation, ownership, and control of

ideas as well as the representation of those ideas."

_____

- ⦿ True
- ○ False

---

22 ■ ■ <u>Hackers</u> are "persons who access systems and information without authorization and often illegally." _____

- ⦿ True
- ○ False

---

23 ■ ■ When voltage levels <u>lag</u> (experience a momentary increase), the extra voltage can severely damage or destroy equipment.

_____

- ○ True
- ⦿ False

---

24 ■ ■ "Shoulder <u>spying</u>" is used in public or semipublic 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.

_____

- ○ True
- ⦿ False

---

25 ■ ■ Packet <u>munchkins</u> use automated exploits to engage in distributed denial-of-service attacks. _____

- ○ True
- ⦿ False

---

26 ■ ■ The term <u>phreaker</u> is now commonly associated with an individual who cracks or removes software protection that is designed to prevent unauthorized duplication. _____

- ○ True
- ⦿ False

---

27 ■ ■ The application of computing and network resources to try every possible combination of options of a password is called a <u>dictionary</u> attack.

_____

- ○ True
- ⦿ False

---

28 <u>Cyberterrorists</u> hack systems to conduct terrorist activities via network or

Internet pathways. _____

○ True
○ False

---

29 ▪ ▪ Software code known as a(n) <u>cookie</u> can allow an attacker to track a victim's activity on Web sites. _____

● True
○ False

---

30 ▪ ▪ A(n) <u>polymorphic</u> 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. _____

● True
○ False

---

31 ▪ ▪ The <u>malicious</u> code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. _____

● True
○ False

---

32 ▪ ▪ The <u>macro</u> virus infects the key operating system files located in a computer's boot sector. _____

○ True
● False

---

33 ▪ ▪ Once a(n) <u>back door</u> has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system.

_____

○ True
● False

---

34 ▪ ▪ One form of e-mail attack that is also a DoS is called a mail <u>spoof</u>, in which an attacker overwhelms the receiver with excessive quantities of e-mail. _____

○ True
● False

35 A device (or a software program on a computer) that can monitor data traveling on a network is known as a <u>socket</u> sniffers.

_____

○ True
◉ False

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

○ Protecting the organization's ability to function.
○ Enabling the safe operation of applications implemented on the organization's IT systems.
○ Protecting the data the organization collects and uses.
◉ All of the above.

37 A(n) _____ is an a potential risk to an information asset.

Answer:
threat

38 A(n) _____ is a potential weakness in an asset or its defensive control(s).

Answer:
vulnerability

39 A(n) _____ is an act against an asset that could result in a loss.

Answer:
attack

40 Duplication of software-based intellectual property is more commonly known as software _____ .

Answer:
piracy

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

○ SSL
◉ SLA

○ MSL
○ MIN

42 Complete loss of power for a moment is known as a ____.

- ◉ fault
- ○ brownout
- ○ blackout
- ○ lag

43 A momentary low voltage is called a(n) _____.

Answer:
sag

44 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

45 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

46 The expert hacker sometimes is called a(n) _____ hacker.

Answer:
elite

47 Hackers can be generalized into two skill groups: expert and

_____.

- ◉ novice
- ○ journeyman
- ○ packet monkey
- ○ professional

48 Script _____ are hackers of limited skill who use expertly written software to attack a system.

Answer:
kiddies

---

49. 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.
   - ○ bypass
   - ○ theft
   - ◉ trespass
   - ○ security

---

50. A(n) _____ hacks the public telephone network to make free calls or disrupt services.

   Answer:
   phreaker

---

51. Attempting to reverse-calculate a password is called _____.

   Answer:
   cracking

---

52. The _____ data file contains the hashed representation of the user's password.
   - ○ SLA
   - ○ SNMP
   - ○ FBI
   - ◉ SAM

---

53. ESD is the acronym for electrostatic _____.

   Answer:
   discharge

---

54. Human error or failure often can be prevented with training, ongoing awareness activities, and _____.
   - ○ threats
   - ◉ controls
   - ○ hugs
   - ○ paperwork

55. 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

---

56 "4-1-9" fraud is an example of a _____ attack.

- ⦿ social engineering
- ○ virus
- ○ worm
- ○ spam

---

57 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, bribes or refund uncleared international payments.

Answer:
advance-fee
Answer:
advance fee

---

58 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.

- ⦿ hacktivist
- ○ phreak
- ○ hackcyber
- ○ cyberhack

---

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

- ○ infoterrorism
- ⦿ cyberterrorism
- ○ hacking
- ○ cracking

---

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

- ○ A bot
- ⦿ Spyware
- ○ Trojan
- ○ Worm

---

61 _____ are malware programs that hide their true nature, and reveal their designed behavior only when activated.

- ○ Viruses

- ○ Worms
- ○ Spam
- ⦿ Trojan horses

---

62 ▭ A computer virus consists of segments of code that perform _____ actions.

Answer:
malicious

---

63 ▭ A(n) _____ is a malicious program that replicates itself constantly, without requiring another program environment.

Answer:
worm

---

64 ▤ Which of the following is an example of a Trojan horse program?

- ○ Netsky
- ○ MyDoom
- ○ Klez
- ⦿ Happy99.exe

---

65 ▤ As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus _____.

- ○ false alarms
- ○ polymorphisms
- ⦿ hoaxes
- ○ urban legends

---

66 ▭ 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

---

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

- ⦿ denial-of-service
- ○ distributed denial-of-service
- ○ virus
- ○ spam

---

68   A _____ is an attack in which a coordinated stream of

requests is launched against a target from many locations at the same time.

- ○ denial-of-service
- ● distributed denial-of-service
- ○ virus
- ○ spam

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

- ○ Drones
- ○ Helpers
- ● Zombies
- ○ Servants

70 _____ is unsolicited commercial e-mail.

Answer:
Spam

71 _____ 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

72 In the well-known _____ attack, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network.

- ○ zombie-in-the-middle
- ○ sniff-in-the-middle
- ○ server-in-the-middle
- ● man-in-the-middle

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

- ○ WWW
- ● TCP
- ○ FTP
- ○ HTTP

74 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

---

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

- ○ 64
- ○ 128
- ◉ 256
- ○ 512

---

76 List at least six general categories of threat.

Answer:

Compromises to intellectual property
Software attacks
Deviations in quality of service
Espionage or trespass
Forces of nature
Human error or failure
Information extortion
Missing, inadequate, or incomplete
Missing, inadequate, or incomplete controls
Sabotage or vandalism
Theft
Technical hardware failures or errors
Technical software failures or errors
Technological obsolescence

---

77 Describe viruses and worms.

Answer:

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.

---

78 Describe the capabilities of a sniffer.

Answer:

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.