# **Chapter 02 The Need for Security**

# TRUEFALSE

**Answer:** (B)

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)
<b>3.</b> 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)
<b>4.</b> 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)
<b>5.</b> 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

<b>6.</b> 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)
<b>9.</b> 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)
<b>16.</b> 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)
<b>18.</b> A mail bomb is a form of DoS attack.
(A) True
(B) False
Answer: (A)
<b>19.</b> 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)
<b>22.</b> Media as a subset of information assets are the systems and networks that store, process, and transmit information.
(A) True
(B) False

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)
<b>24.</b> <u>Hackers</u> are "persons who access systems and information without authorization and often illegally."
(A) True
(B) False
Answer: (A)
<b>25.</b> When voltage levels <u>lag</u> (experience a momentary increase), the extra voltage can severely damage or destroy equipment
(A) True
(B) False
Answer: (B)
<b>26.</b> "Shoulder <u>spying</u> " 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 <u>munchkins</u> use automated exploits to engage in distributed denial-of-service attacks.
(A) True
(B) False
(D) I CLOC

**Answer**: (A)

**Answer**: (B)

<b>28.</b> 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.
(A) True
(B) False
Answer: (B)
<b>29.</b> The application of computing and network resources to try every possible combination of options of a password is called a <u>dictionary</u> attack.
(A) True
(B) False
Answer: (B)
<b>30.</b> Cyberterrorists hack systems to conduct terrorist activities via network or Internet pathways.
(A) True
(B) False
Answer: (A)
<b>31.</b> Software code known as a(n) <u>cookie</u> can allow an attacker to track a victim's activity on Web sites
(A) True
(B) False
Answer: (A)
<b>32.</b> 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.
(A) True
(B) False
Answer: (A)
<b>33.</b> 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.

(A) True
(B) False
Answer: (A)
<b>34.</b> The <u>macro</u> virus infects the key operating system files located in a computer's start-up sector.
(A) True
(B) False
Answer: (B)
<b>35.</b> 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.
(A) True
(B) False
Answer: (B)
<b>36.</b> One form of e-mail attack that is also a DoS attack is called a mail <u>spoof</u> , in which an attacker overwhelms the receiver with excessive quantities of e-mail.
(A) True
(B) False
Answer: (B)
<b>37.</b> A device (or a software program on a computer) that can monitor data traveling on a network is known as a <u>socket</u> sniffer
(A) True
(B) False
Answer: (B)
<b>38.</b> 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)
<b>40.</b> 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)
<b>41.</b> 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)
<b>43.</b> 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)
<b>44.</b> The data file contains the hashed representation of the user's password.
(A) SLA
(B) SNMP
(C) FBI
(D) SAM
Answer: (D)
<b>45.</b> Human error or failure often can be prevented with training, ongoing awareness activities, and
(A) threats
(B) education
(C) hugs
(D) paperwork
Answer: (B)
<b>46.</b> "4-1-9" fraud is an example of a attack.
(A) social engineering
(B) virus
(C) worm
(D) spam

Answer: (A)
<b>47.</b> 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)
<b>48.</b> 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)
$oldsymbol{49.}$ 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)
<b>50.</b> 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)
<b>52.</b> 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)
<b>53.</b> 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)
<b>54.</b> 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

O) spam	
nswer: (B)	
are compromised systems that are directed remotely (usually by a ransmitted command) by the attacker to participate in an attack.	
A) Drones	
B) Helpers	
C) Zombies	
O) Servants	
nswer: (C)	
6. In the attack, an attacker monitors (or sniffs) packets from the network, and inserts them back into the network.	
A) zombie-in-the-middle	
3) sniff-in-the-middle	
C) server-in-the-middle	
O) man-in-the-middle	
nswer: (D)	
7. The hijacking attack uses IP spoofing to enable an attacker to imperson nother entity on the network.	ate
A) WWW	
B) TCP	
C) FTP	
D) HTTP	
nswer: (B)	
8. Microsoft acknowledged that if you type a res:// URL (a Microsoft-devised type of URL) long nan characters in Internet Explorer 4.0, the browser will crash.	er
A) 64	
3) 128	

(C) 256
(D) 512
Answer: (C)
<b>59.</b> 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)
<b>60.</b> 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 intermention (outego) in electrical newer availability is known as a(n)
<b>61.</b> A long-term interruption (outage) in electrical power availability is known as a(n)
(A) blackout
(B) sag
(C) brownout
(D) fault
Answer: (A)
<b>62.</b> A short-term decrease in electrical power availability is known as a(n)
(A) blackout
(B) sag
(C) brownout

(D) fault
Answer: (C)
<b>63.</b> 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)
<b>64.</b> 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)
<b>65.</b> 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)
<b>66.</b> 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**

<b>67.</b> A(n)	is a potential ris	k to an information asset.A	Answer: threat
<b>68.</b> A(n)vulnerability	is a potential we	akness in an asset or its d	efensive control(s). <b>Answer:</b>
<b>69.</b> A(n)	is an act against	an asset that could result	in a loss. <b>Answer:</b> attack
-	ware-based intellectual	l property is more common	ıly known as software
71. A momentary low	voltage is called a(n) _	.Answei	: fault
	rch. These legal technic	re quite legal-for example ques are called, collectivel	•
	2 2	_	tting that cross the thresholdAnswer: espionage
74. The expert hacker	sometimes is called a(	n) hac	ker. <b>Answer</b> : elite
<b>75.</b> Scriptattack a system. <b>Answ</b>		limited skill who use expe	rtly written software to
<b>76.</b> A(n) services. <b>Answer</b> : phr		telephone network to ma	ke free calls or disrupt
77. Attempting to rev	erse-calculate a passwo	rd is called	Answer: cracking
<b>78.</b> ESD is the acrony	m for	discharge. <b>Answer :</b> ele	ctrostatic
			ocess of using social skills to ion to the attacker. <b>Answer</b> :
		nture while getting the vic	volves convincing the victim tim to pay fees or bribes or to
81. A computer virus	consists of segments of	code that perform	actions. <b>Answer</b>

: malicious	
	is a malicious program that replicates itself constantly without ner program environment. <b>Answer:</b> worm
<b>83.</b> A virus or v component in a privileges. <b>Ansv</b>	worm can have a payload that installs a(n) door or trap door a system, which allows the attacker to access the system at will with special wer: back
84	is unsolicited commercial e-mail. Answer: Spam
intruder sends	is a technique used to gain unauthorized access to computers, wherein the messages with a source IP address that has been forged to indicate that the oming from a trusted host. Answer: Spoofing
<b>86.</b> A(n) than it is design <b>Answer</b> : buffe	is an application error that occurs when more data is sent to a programmed to handle. Answer: buffer overrun r overflow
87 is Answer : up-tin Answer : up tin	
browser session (XSS)	occurs when an application running on a Web server inserts commands into a user's and causes information to be sent to a hostile server. <b>Answer:</b> cross-site scripting
Answer: cross	-site scripting
Answer: XSS	
	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.