TRUE/FALSE

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

   ANS: F PTS: 1 REF: 41

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

   ANS: T PTS: 1 REF: 41

3. A firewall is a mechanism that keeps certain kinds of network traffic out of a private network.

   ANS: T PTS: 1 REF: 42

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."

   ANS: F PTS: 1 REF: 44

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

   ANS: F PTS: 1 REF: 46

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 enforce copyright laws.

   ANS: T PTS: 1 REF: 46

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

   ANS: F PTS: 1 REF: 48

8. 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.

   ANS: T PTS: 1 REF: 48

9. Attacks conducted by scripts are usually unpredictable.

   ANS: F PTS: 1 REF: 53

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

    ANS: T PTS: 1 REF: 53

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

ANS: T PTS: 1 REF: 56

12. 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.

ANS: T PTS: 1 REF: 56

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

ANS: T PTS: 1 REF: 59

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

ANS: F PTS: 1 REF: 61

15. With electronic information is stolen, the crime is readily apparent.

ANS: F PTS: 1 REF: 63

16. Organizations can use dictionaries to disallow passwords during the reset process and thus guard against easy-to-guess passwords.

ANS: T PTS: 1 REF: 67

17. DoS attacks cannot be launched against routers.

ANS: F PTS: 1 REF: 68

18. A mail bomb is a form of DoS.

ANS: T PTS: 1 REF: 70

19. A sniffer program shows all the data going by on a network segment including passwords, the data inside files—such as word-processing documents—and screens full of sensitive data from applications.

ANS: T PTS: 1 REF: 70

20. A timing attack involves the interception of cryptographic elements to determine keys and encryption algorithms.

ANS: T PTS: 1 REF: 74

MODIFIED TRUE/FALSE

1. Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas.” _____

ANS: T PTS: 1 REF: 44

---

2. The macro virus infects the key operating system files located in a computer's boot sector. _____

   ANS: F, boot

   PTS: 1 REF: 47

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

   ANS: F
   virus
   worm

   PTS: 1 REF: 48

4. 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. _____

   ANS: T PTS: 1 REF: 49-50

5. When voltage levels surge (experience a momentary increase), the extra voltage can severely damage or destroy equipment. _____

   ANS: F, spike

   PTS: 1 REF: 51

6. The shoulder looking technique 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. _____

   ANS: F, surfing

   PTS: 1 REF: 52

7. Hackers are "people who use and create computer software to gain access to information illegally." _____

   ANS: T PTS: 1 REF: 52

8. Packet kiddies use automated exploits to engage in distributed denial-of-service attacks. _____

   ANS: F, monkeys

   PTS: 1 REF: 53

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

   ANS: F, cracker

PTS: 1 REF: 56

10. Cyberterrorists hack systems to conduct terrorist activities via network or Internet pathways. _____

ANS: T PTS: 1 REF: 62

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

ANS: T PTS: 1 REF: 65

12. The application of computing and network resources to try every possible combination of options of a password is called a brute crack attack. _____

ANS: F, force

PTS: 1 REF: 67

13. One form of e-mail attack that is also a DoS is called a mail spoof, in which an attacker routes large quantities of e-mail to the target. _____

ANS: F, bomb

PTS: 1 REF: 70

14. Sniffers often work on TCP/IP networks, where they're sometimes called packet sniffers. _____

ANS: T PTS: 1 REF: 70

15. A(n) cookie can allow an attacker to collect information on how to access password-protected sites. _____

ANS: T PTS: 1 REF: 74

MULTIPLE CHOICE

1. 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.

   ANS: D PTS: 1 REF: 41

2. ____ is an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure of an organization.
   a. SSL
   b. PKI
   c. PKC
   d. SIS

   ANS: B PTS: 1 REF: 42

3. ____ are software programs that hide their true nature, and reveal their designed behavior only when activated.
   a. Viruses
   b. Worms
   c. Spam
   d. Trojan horses

   ANS: D PTS: 1 REF: 48

4. Which of the following is an example of a Trojan horse program?
   a. Netsky
   b. MyDoom
   c. Klez
   d. Happy99.exe

   ANS: D PTS: 1 REF: 48

5. As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus ____.
   a. false alarms
   b. power faults
   c. hoaxes
   d. urban legends

   ANS: C PTS: 1 REF: 50

6. Web hosting services are usually arranged with an agreement providing minimum service levels known as a(n) ____.
   a. SSL
   b. SLA
   c. MSL
   d. MIN

   ANS: B PTS: 1 REF: 51

7. Complete loss of power for a moment is known as a ____.
   a. sag
   b. fault
   c. brownout
   d. blackout

   ANS: B PTS: 1 REF: 51

8. 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. nature
   c. trespass
   d. security

   ANS: C PTS: 1 REF: 52

9. There are generally two skill levels among hackers: expert and ____.
   a. novice
   b. journeyman
   c. packet monkey
   d. professional

   ANS: A PTS: 1 REF: 53

10. 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. phvist
    c. hackcyber
    d. cyberhack

    ANS: A PTS: 1 REF: 61

11. According to Mark Pollitt, ____ 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.

a. infoterrorism
b. cyberterrorism
c. hacking
d. cracking

ANS: B PTS: 1 REF: 62

12. ____ is any technology that aids in gathering information about a person or organization without their knowledge.
a. A bot
b. Spyware
c. Trojan
d. Worm

ANS: B PTS: 1 REF: 65

13. The ____ data file contains the hashed representation of the user's password.
a. SLA
b. SNMP
c. FBI
d. SAM

ANS: D PTS: 1 REF: 67

14. In a ____ attack, the attacker sends a large number of connection or information requests to a target.
a. denial-of-service
b. distributed denial-of-service
c. virus
d. spam

ANS: A PTS: 1 REF: 67

15. 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

ANS: B PTS: 1 REF: 67

16. ____ are machines 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

ANS: C PTS: 1 REF: 67

17. In the well-known ____ 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

ANS: D PTS: 1 REF: 68

18. 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

ANS: B PTS: 1 REF: 68

19. "4-1-9" fraud is an example of a ____ attack.
a. social engineering
b. virus
c. worm
d. spam

ANS: A PTS: 1 REF: 70

20. 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.
    a. 64
    b. 128
    c. 256
    d. 512

    ANS: C PTS: 1 REF: 76

COMPLETION

1. A(n) _____ is an object, person, or other entity that represents an ongoing danger to an asset.

   ANS: threat

   PTS: 1 REF: 43

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

   ANS: piracy

   PTS: 1 REF: 45

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

   ANS: malicious

   PTS: 1 REF: 46

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

   ANS: worm

   PTS: 1 REF: 47

5. 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.

   ANS: back

   PTS: 1 REF: 50

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

   ANS: sag

   PTS: 1 REF: 51

7. Some information gathering techniques are quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, competitive _____.

ANS: intelligence

PTS: 1 REF: 52

8. When information gatherers employ techniques that cross the threshold of what is legal or ethical, they are conducting industrial _____.

ANS: espionage

PTS: 1 REF: 51

9. The expert hacker sometimes is called _____ hacker.

ANS: elite

PTS: 1 REF: 53

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

ANS: kiddies

PTS: 1 REF: 53

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

ANS: phreaker

PTS: 1 REF: 56

12. ESD means electrostatic _____.

ANS: discharge

PTS: 1 REF: 58

13. A(n) _____ is an act that takes advantage of a vulnerability to compromise a controlled system.

ANS: attack

PTS: 1 REF: 65

14. A(n) _____ is an identified weakness in a controlled system, where controls are not present or are no longer effective.

ANS: vulnerability

PTS: 1 REF: 65

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

ANS: cracking

PTS: 1 REF: 67

16. _____ 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.

    ANS: Spoofing

    PTS: 1 REF: 68

17. _____ is unsolicited commercial e-mail.

    ANS: Spam

    PTS: 1 REF: 69

18. 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.

    ANS: social engineering

    PTS: 1 REF: 70

19. The timing attack explores the contents of a Web browser's _____.

    ANS: cache

    PTS: 1 REF: 74

20. A(n) _____ is an application error that occurs when more data is sent to a program buffer than it is designed to handle.

    ANS:
    buffer overrun
    buffer overflow

    PTS: 1 REF: 76

ESSAY

1. List at least six general categories of threat.

   ANS:
   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

PTS: 1 REF: 44

2. Describe viruses and worms.

ANS:
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.

PTS: 1 REF: 46 - 47

3. Describe the capabilities of a sniffer.

ANS:
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.

PTS: 1 REF: 70