

Why security is needed

[Engineering](#), [Computer Security](#)



True/ False

1. Information security's primary mission is to ensure that systems and their contents retain their confidentiality at all costs. ANS: FPTS: 1
2. Information security safeguards the technology assets in use at the organization. ANS: TPTS: 1
3. A firewall is a mechanism that keeps certain kinds of network traffic out of a private network. ANS: TPTS: 1
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: FPTS: 1
5. Two watchdog organizations that investigate allegations of software abuse: SIIA and NSA. ANS: FPTS: 1
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: TPTS: 1
7. A worm requires that another program is running before it can begin functioning. ANS: FPTS: 1
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: TPTS: 1
9. Attacks conducted by scripts are usually unpredictable. ANS: FPTS: 1

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: TPTS: 1
11. With the removal of copyright protection, software can be easily distributed and installed. ANS: TPTS: 1
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: TPTS: 1
13. Much human error or failure can be prevented with training and ongoing awareness activities. ANS: TPTS: 1
14. Compared to Web site defacement, vandalism within a network is less malicious in intent and more public. ANS: FPTS: 1
15. With electronic information is stolen, the crime is readily apparent. ANS: FPTS: 1
16. Organizations can use dictionaries to disallow passwords during the reset process and thus guard against easy-to-guess passwords. ANS: TPTS: 1
17. DoS attacks cannot be launched against routers. ANS: FPTS: 1
17. A mail bomb is a form of DoS. ANS: TPTS: 1
18. 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: TPTS: 1.
19. A timing attack involves the interception of cryptographic elements to determine keys and encryption algorithms. ANS: TPTS: 1

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: TPTS: 1
2. The macro virus infects the key operating system files located in a computer’s boot sector. ANS: F, boot PTS: 1
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
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: TPTS: 1
5. When voltage levels surge (experience a momentary increase), the extra voltage can severely damage or destroy equipment. ANS: F, spike PTS: 1
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
7. Hackers are “ people who use and create computer software to gain access to information illegally. ” ANS: TPTS: 1
8. Packet kiddies use automated exploits to engage in distributed denial-of-service attacks. ANS: F, monkeys PTS: 1

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
10. Cyberterrorists hack systems to conduct terrorist activities via network or Internet pathways. ANS: TPTS: 1
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: TPTS: 1
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
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
14. Sniffers often work on TCP/IP networks, where they're sometimes called packet sniffers. ANS: TPTS: 1
15. A(n) cookie can allow an attacker to collect information on how to access password-protected sites. ANS: TPTS: 1

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: DPTS: 1

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: BPTS: 1

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: DPTS: 1

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

- a. Netsky
- b. MyDoom
- c. Klez

- d. Happy99. exe

ANS: DPTS: 1

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: CPTS: 1

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: BPTS: 1

7. Complete loss of power for a moment is known as a _.

- a. sag
- b. fault
- c. brownout
- d. blackout

ANS: BPTS: 1

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: CPTS: 1

9. There are generally two skill levels among hackers: expert and _.

- a. novice
- b. journeyman
- c. packet monkey
- d. professional

ANS: APTS: 1

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: APTS: 1

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. info terrorism
- b. cyberterrorism
- c. hacking
- d. cracking

ANS: BPTS: 1

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: BPTS: 1

13. The _data file contains the hashed representation of the user's password.

- a. SLA
- b. SNMP
- c. FBI
- d. SAM

ANS: DPTS: 1

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: APTS: 1

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: BPTS: 1

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: CPTS: 1

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: DPTS: 1

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: BPTS: 1

19. “ 4-1-9” fraud is an example of a _ attack.

- a. social engineering
- b. virus
- c. worm
- d. spam

ANS: APTS: 1

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: CPTS: 1

Completion

1. A(n) _ is an object, person, or other entity that represents an ongoing danger to an asset. ANS: threat PTS: 1
2. Duplication of software-based intellectual property is more commonly known as software _. ANS: piracy PTS: 1
3. A computer virus consists of segments of code that perform _ actions. ANS: malicious PTS: 1
4. A(n) _ is a malicious program that replicates itself constantly, without requiring another program environment. ANS: worm PTS: 1
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
6. A momentary low voltage is called a(n) _. ANS: sag PTS: 1
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
8. When information gatherers employ techniques that cross the threshold of what is legal or ethical, they are conducting industrial __. ANS: espionage PTS: 1
9. The expert hacker sometimes is called __ hacker. ANS: elite PTS: 1
10. Script __ are hackers of limited skill who use expertly written software to attack a system. ANS: kiddies PTS: 1
11. A(n) __ hacks the public telephone network to make free calls or disrupt services. ANS: phreaker PTS: 1
12. ESD means electrostatic __. ANS: discharge PTS: 1
13. A(n) __ is an act that takes advantage of a vulnerability to compromise a controlled system. ANS: attack PTS: 1
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
15. Attempting to reverse-calculate a password is called __. ANS: cracking PTS: 1
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
17. __ is unsolicited commercial e-mail. ANS: Spam PTS: 1
18. 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

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

ANS: cache PTS: 1

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

Essay

- List at least six general categories of threat.

ANS: Compromises to intellectual property : piracy, copyright infringement

Software attacks : viruses, worms macros, denial of service

Deviations in quality of service : ISP, power, or wan service issues from service providers Espionage or trespass : unauthorized access and /or data collection

Sabotage or vandalism : destruction of system or information Forces of nature Human error or failure Information extortion Missing, inadequate, or incomplete Missing, inadequate, or incomplete controls Theft Technical hardware failures or errors Technical software failures or errors

Technological obsolescence PTS: 1

- Describe viruses and worms.

ANS: A computer virus consists of segments of code that perform malicious actions.

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

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