|  |
| --- |
| True / False |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Corruption of information can occur only while information is being stored.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. The authorization process takes place before the authentication process.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. 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:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. DoS attacks cannot be launched against routers.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. The first step in solving problems is to gather facts and make assumptions.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |
| --- |
| Modified True / False |

|  |  |  |
| --- | --- | --- |
| 6. A device (or a software program on a computer) that can monitor data traveling on a network is known as a socket sniffer. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | False - packet | |

|  |  |  |
| --- | --- | --- |
| 7. 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. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | False - bomb | |

|  |  |  |
| --- | --- | --- |
| 8. When voltage levels lag (experience a momentary increase), the extra voltage can severely damage or destroy equipment. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | False - spike | |

|  |  |  |
| --- | --- | --- |
| 9. "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. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | False - surfing | |

|  |  |  |
| --- | --- | --- |
| 10. The term phreaker is now commonly associated with an individual who cracks or removes software protection that is designed to prevent unauthorized duplication. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | False - cracker | |

|  |  |  |
| --- | --- | --- |
| 11. The application of computing and network resources to try every possible combination of options of a password is called a dictionary attack. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | False - brute force | |

|  |  |  |
| --- | --- | --- |
| 12. The macro virus infects the key operating system files located in a computer’s start-up sector. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | False - boot | |

|  |  |  |
| --- | --- | --- |
| 13. The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |
| --- | --- | --- |
| 14. 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 pre-configured signatures. \_\_\_\_\_\_\_\_\_\_   |  |  | | --- | --- | | *ANSWER:* | True | |

|  |
| --- |
| Multiple Choice |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. Communications security involves the protection of which of the following?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | radio handsets | b. | people, physical assets | |  | c. | the IT department | d. | media, technology, and content |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. The protection of voice and data components, connections, and content is known as \_\_\_\_\_\_\_\_\_\_ security.   |  |  |  | | --- | --- | --- | |  | a. | network | |  | b. | national | |  | c. | cyber | |  | d. | operational |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. The protection of confidentiality, integrity, and availability of data regardless of its location is known as \_\_\_\_\_\_\_\_\_\_ security.   |  |  |  | | --- | --- | --- | |  | a. | information | |  | b. | network | |  | c. | cyber | |  | d. | operational |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. A model of InfoSec that offers a comprehensive view of security for data while being stored, processed, or transmitted is the \_\_\_\_\_\_\_\_\_\_ security model.   |  |  |  | | --- | --- | --- | |  | a. | CNSS | |  | b. | USMC | |  | c. | USNA | |  | d. | NPC |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. Which of the following is a C.I.A. triad characteristic that addresses the threat from corruption, damage, destruction, or other disruption of its authentic state?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | integrity | b. | availability | |  | c. | authentication | d. | accountability |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. According to the C.I.A. triad, which of the following is the most desirable characteristic for privacy?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | confidentiality | b. | availability | |  | c. | integrity | d. | accountability |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. Which of the following is recognition that data used by an organization should only be used for the purposes stated by the information owner at the time it was collected?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | accountability | b. | availability | |  | c. | privacy | d. | confidentiality |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. Which of the following is a C.I.A. triad characteristic that ensures only those with sufficient privileges and a demonstrated need may access certain information?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | integrity | b. | availability | |  | c. | authentication | d. | confidentiality |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. The use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections is an example of which process?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | accountability | b. | authorization | |  | c. | identification | d. | authentication |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. A process that defines what the user is permitted to do is known as \_\_\_\_\_\_\_\_\_\_.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | identification | b. | authorization | |  | c. | accountability | d. | authentication |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. What do audit logs that track user activity on an information system provide?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | identification | b. | authorization | |  | c. | accountability | d. | authentication |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. Any event or circumstance that has the potential to adversely affect operations and assets is known as a(n) \_\_\_\_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | threat | |  | b. | attack | |  | c. | exploit | |  | d. | vulnerability |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it is known as a(n) \_\_\_\_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | threat | |  | b. | attack | |  | c. | exploit | |  | d. | vulnerability |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. A technique used to compromise a system is known as a(n) \_\_\_\_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | threat | |  | b. | attack | |  | c. | exploit | |  | d. | vulnerability |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. A potential weakness in an asset or its defensive control system(s) is known as a(n) \_\_\_\_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | threat | |  | b. | attack | |  | c. | exploit | |  | d. | vulnerability |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. The unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property, is called \_\_\_\_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | software piracy | |  | b. | copyright infringement | |  | c. | trademark violation | |  | d. | data hijacking |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. Technology 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. A short-term interruption in electrical power availability is known as a \_\_\_\_\_\_\_\_\_\_.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | fault | b. | brownout | |  | c. | blackout | d. | lag |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. 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 access.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | bypass | b. | theft | |  | c. | trespass | d. | security |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. An information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems is known as a(n) \_\_\_\_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | penetration tester | |  | b. | expert hacker | |  | c. | phreaker | |  | d. | cracker |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. A hacker who intentionally removes or bypasses software copyright protection designed to prevent unauthorized duplication or use is known as a(n) \_\_\_\_\_\_\_\_\_\_.   |  |  |  | | --- | --- | --- | |  | a. | penetration tester | |  | b. | expert hacker | |  | c. | phreaker | |  | d. | cracker |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. \_\_\_\_\_\_\_\_\_\_ is the collection and analysis of information about an organization’s business competitors, often through illegal or unethical means, to gain an unfair edge over them.   |  |  |  | | --- | --- | --- | |  | a. | Dumpster diving | |  | b. | Packet sniffing | |  | c. | Competitive advantage | |  | d. | Industrial espionage |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. The hash values for a wide variety of passwords can be stored in a database known as a(n) \_\_\_\_\_\_\_\_\_\_, which can be indexed and quickly searched using the hash value, allowing the corresponding plaintext password to be determined.   |  |  |  | | --- | --- | --- | |  | a. | rainbow table | |  | b. | unicorn table | |  | c. | rainbow matrix | |  | d. | poison box |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which of the following is NOT an approach to password cracking?   |  |  |  | | --- | --- | --- | |  | a. | ransomware | |  | b. | brute force | |  | c. | dictionary attacks | |  | d. | social engineering attacks |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Force majeure includes all of the following EXCEPT:   |  |  |  | | --- | --- | --- | |  | a. | armed robbery | |  | b. | acts of war | |  | c. | civil disorder | |  | d. | forces of nature |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. Human error or failure often can be prevented with training and awareness programs, policy, and \_\_\_\_\_\_\_\_\_\_.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | outsourcing | b. | technical controls | |  | c. | hugs | d. | ISO 27000 |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 41. “4-1-9” fraud is an example of a \_\_\_\_\_\_\_\_\_\_ attack.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | social engineering | b. | virus | |  | c. | worm | d. | spam |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 42. “4-1-9” is one form of a(n)  \_\_\_\_\_\_\_\_\_\_ fraud.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | advance fee | b. | privilege escalation | |  | c. | check kiting | d. | "Spanish Prisoner" |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 43. Blackmail threat of informational disclosure is an example of which threat category?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | espionage or trespass | b. | information extortion | |  | c. | sabotage or vandalism | d. | compromises of intellectual property |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 44. An attack that uses phishing techniques along with specialized forms of malware to encrypt the victim's data files is known as \_\_\_\_\_\_\_\_\_\_.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | crypto locking | b. | ransomware | |  | c. | jailbreaking | d. | spam |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 45. One form of online vandalism is \_\_\_\_\_\_\_\_\_\_, in which individuals interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | hacktivism | b. | phreaking | |  | c. | red teaming | d. | cyberhacking |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 46. \_\_\_\_\_\_\_\_\_\_ 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 47. 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 48. Which of the following is a feature left behind by system designers or maintenance staff that allows quick access to a system at a later time by bypassing access controls?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | brute force | b. | DoS | |  | c. | back door | d. | hoax |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 49. 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 50. Which type of attack involves sending a large number of connection or information requests to a target?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | malicious code | b. | denial of service (DoS) | |  | c. | brute force | d. | spear fishing |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 51. 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 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 52. Which statement defines the differences between a computer virus and a computer worm?   |  |  |  | | --- | --- | --- | |  | a. | Worms and viruses are the same. | |  | b. | Worms can make copies all by themselves on one kind of computer but viruses can make copies all by themselves on any kind of computer. | |  | c. | Worms can copy themselves to computers and viruses can copy themselves to smartphones. | |  | d. | Worms can make copies all by themselves but viruses need to attach to an existing program on the host computer to replicate. |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 53. Which of the following is not among the "deadly sins of software security"?   |  |  |  | | --- | --- | --- | |  | a. | extortion sins | |  | b. | implementation sins | |  | c. | Web application sins | |  | d. | networking sins |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 54. Which of the 12 categories of threats best describes a situation where the adversary removes data from a victim's computer?   |  |  |  | | --- | --- | --- | |  | a. | theft | |  | b. | espionage or trespass | |  | c. | sabotage or vandalism | |  | d. | information extortion |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 55. Which of the following is the principle of management that develops, creates, and implements strategies for the accomplishment of objectives?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | leading | b. | controlling | |  | c. | organizing | d. | planning |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 56. Which of the following is the principle of management dedicated to the structuring of resources to support the accomplishment of objectives?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | organization | b. | planning | |  | c. | controlling | d. | leading |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 57. \_\_\_\_\_\_\_\_\_\_ is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise’s resources are used responsibly.   |  |  |  | | --- | --- | --- | |  | a. | Governance | |  | b. | Controlling | |  | c. | Leading | |  | d. | Strategy |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 58. Which of the following is the first step in the problem-solving process?   |  |  |  | | --- | --- | --- | |  | a. | Analyze and compare the possible solutions. | |  | b. | Develop possible solutions. | |  | c. | Recognize and define the problem. | |  | d. | Select, implement, and evaluate a solution. |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 59. Which of the following is NOT a step in the problem-solving process?   |  |  |  | | --- | --- | --- | |  | a. | Select, implement, and evaluate a solution. | |  | b. | Analyze and compare possible solutions. | |  | c. | Build support among management for the candidate solution. | |  | d. | Gather facts and make assumptions. |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 60. Which of the following is NOT a primary function of information security management?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | planning | b. | protection | |  | c. | projects | d. | performance |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 61. Which of the following functions of information security management seeks to dictate certain behavior within the organization through a set of organizational guidelines?   |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | a. | planning | b. | policy | |  | c. | programs | d. | people |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 62. Which function of InfoSec management encompasses security personnel as well as aspects of the SETA program?   |  |  |  | | --- | --- | --- | |  | a. | protection | |  | b. | people | |  | c. | projects | |  | d. | policy |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |
| --- |
| Completion |

|  |  |  |
| --- | --- | --- |
| 63. A(n) \_\_\_\_\_\_\_\_\_\_ is a potential weakness in an asset or its defensive control(s).   |  |  | | --- | --- | | *ANSWER:* | vulnerability | |

|  |  |  |
| --- | --- | --- |
| 64. A(n) \_\_\_\_\_\_\_\_\_\_ is an act against an asset that could result in a loss.   |  |  | | --- | --- | | *ANSWER:* | attack | |

|  |  |  |
| --- | --- | --- |
| 65. Duplication of software-based intellectual property is more commonly known as software \_\_\_\_\_\_\_\_\_\_.   |  |  | | --- | --- | | *ANSWER:* | piracy | |

|  |  |  |
| --- | --- | --- |
| 66. A(n) \_\_\_\_\_\_\_\_\_\_ hacks the public telephone network to make free calls or disrupt services.   |  |  | | --- | --- | | *ANSWER:* | phreaker | |

|  |  |  |
| --- | --- | --- |
| 67. A momentary low voltage is called a(n) \_\_\_\_\_\_\_\_\_\_.   |  |  | | --- | --- | | *ANSWER:* | sag | |

|  |  |  |
| --- | --- | --- |
| 68. Some information gathering techniques are quite legal—for example, using a Web browser to perform market research. These legal techniques are called, collectively, \_\_\_\_\_\_\_\_\_\_.   |  |  | | --- | --- | | *ANSWER:* | competitive intelligence | |

|  |  |  |
| --- | --- | --- |
| 69. Attempting to reverse-calculate a password or bypass encryption is called \_\_\_\_\_\_\_\_\_\_.   |  |  | | --- | --- | | *ANSWER:* | cracking | |

|  |  |  |
| --- | --- | --- |
| 70. ESD is the acronym for \_\_\_\_\_\_\_\_\_\_.   |  |  | | --- | --- | | *ANSWER:* | electrostatic discharge | |

|  |  |  |
| --- | --- | --- |
| 71. 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 | |

|  |  |  |
| --- | --- | --- |
| 72. \_\_\_\_\_\_\_\_\_\_ is unsolicited commercial e-mail.   |  |  | | --- | --- | | *ANSWER:* | Spam | |

|  |  |  |
| --- | --- | --- |
| 73. A \_\_\_\_\_\_\_\_\_\_\_ overflow is an application error that occurs when the system can’t handle the amount of data that is sent.   |  |  | | --- | --- | | *ANSWER:* | buffer | |

|  |  |  |
| --- | --- | --- |
| 74. The three levels of planning are strategic planning, tactical planning, and \_\_\_\_\_\_\_\_\_\_ planning.   |  |  | | --- | --- | | *ANSWER:* | operational | |

|  |  |  |
| --- | --- | --- |
| 75. The set of organizational guidelines that dictates certain behavior within the organization is called \_\_\_\_\_\_\_\_\_\_.   |  |  | | --- | --- | | *ANSWER:* | policy | |

|  |
| --- |
| Subjective Short Answer |

|  |  |  |
| --- | --- | --- |
| 76. Explain the differences between a leader and a manager.   |  |  | | --- | --- | | *ANSWER:* | The distinctions between a leader and a manager arise in the execution of organizational tasks. A leader provides purpose, direction, and motivation to those that follow. By comparison, a manager administers the resources of the organization. He or she creates budgets, authorizes expenditures, and hires employees. | |

|  |  |  |
| --- | --- | --- |
| 77. List and explain the critical characteristics of information as defined by the C.I.A. triad.   |  |  | | --- | --- | | *ANSWER:* | ​  Confidentiality of information ensures that only those with sufficient privileges and a demonstrated need may access certain information. When unauthorized individuals or systems can view information, confidentiality is breached.  ​  Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state.  ​  Availability is the characteristic of information that enables user access to information without interference or obstruction and in a usable format. | |

|  |  |  |
| --- | --- | --- |
| 78. List and explain the four principles of management under the contemporary or popular management theory. Briefly define each.   |  |  | | --- | --- | | *ANSWER:* | Popular management theory categorizes the principles of management into planning, organizing, leading, and controlling (POLC).  ​  The process that develops, creates, and implements strategies for the accomplishment of objectives is called planning.  ​  The management function dedicated to the structuring of resources to support the accomplishment of objectives is called organization.  ​  Leadership includes supervising employee behavior, performance, attendance, and attitude. Leadership generally addresses the direction and motivation of the human resource.  ​  Monitoring progress toward completion, and making necessary adjustments to achieve desired objectives, requires the exercise of control. | |

|  |  |  |
| --- | --- | --- |
| 79. List the steps that can be used as a basic blueprint for solving organizational problems.   |  |  | | --- | --- | | *ANSWER:* | 1. Recognize and define the problem.  2. Gather facts and make assumptions.  3. Develop possible solutions.  4. Analyze and compare possible solutions.  5. Select, implement, and evaluate a solution. | |

|  |  |  |
| --- | --- | --- |
| 80. What are the three distinct groups of decision makers or communities of interest on an information security team?   |  |  | | --- | --- | | *ANSWER:* | Managers and professionals in the field of information security  Managers and professionals in the field of IT  Managers and professionals from the rest of the organization | |

|  |  |  |
| --- | --- | --- |
| 81. List the specialized areas of security.   |  |  | | --- | --- | | *ANSWER:* | Physical security  Operations security  Communications security  Network security | |

|  |  |  |
| --- | --- | --- |
| 82. List the measures that are commonly used to protect the confidentiality of information.   |  |  | | --- | --- | | *ANSWER:* | Information classification  Secure document (and data) storage  Application of general security policies  Education of information custodians and end users  Cryptography (encryption) | |

|  |  |  |
| --- | --- | --- |
| 83. What is authentication?  Provide some examples.   |  |  | | --- | --- | | *ANSWER:* | Authentication is the process by which a control establishes whether a user (or system) has the identity it claims to have. Examples include the use of cryptographic certificates to establish Secure Sockets Layer (SSL) connections as well as the use of cryptographic hardware devices—for example, hardware tokens such as RSA’s SecurID. Individual users may disclose a personal identification number (PIN) or a password to authenticate their identities to a computer system. | |

|  |  |  |
| --- | --- | --- |
| 84. Discuss the planning element of information security.   |  |  | | --- | --- | | *ANSWER:* | Planning in InfoSec management is an extension of the basic planning model. Included in the InfoSec planning model are activities necessary to support the design, creation, and implementation of InfoSec strategies within the IT planning environment. The business strategy is translated into the IT strategy. Both the business strategy and the IT strategy are then used to develop the InfoSec strategy. For example, the CIO uses the IT objectives gleaned from the business unit plans to create the organization’s IT strategy. | |

|  |
| --- |
| Essay |

|  |  |  |
| --- | --- | --- |
| 85. 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.   |  |  | | --- | --- | | *ANSWER:* | Compromises to intellectual property  Software 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 | |