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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. The Security Administrator reports directly to the CIO.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2. The CompTIA Security+ certification is a vendor-neutral credential.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3. Successful attacks are usually not from software that is poorly designed and has architecture/design weaknesses.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4. Smart phones give the owner of the device the ability to download security updates.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 5. As security is increased, convenience is often increased.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 6. A vulnerability is a flaw or weakness that allows a threat to bypass security.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 7. To mitigate risk is the attempt to address risk by making the risk less serious.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 8. The Sarbanes-Oxley Act restricts electronic and paper data containing personally identifiable financial information.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 9. One of the challenges in combating cyberterrorism is that many of the prime targets are not owned and managed by the federal government.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 10. Brokers steal new product research or a list of current customers to gain a competitive advantage.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False | |

|  |
| --- |
| **Multiple Choice** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. What information security position reports to the CISO and supervises technicians, administrators, and security staff?   |  |  |  | | --- | --- | --- | |  | a. | security manager | |  | b. | security engineer | |  | c. | security auditor | |  | d. | security administrator | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. According to the U.S. Bureau of Labor Statistics, what percentage of growth for information security analysts is the available job outlook supposed to reach through 2024?   |  |  |  | | --- | --- | --- | |  | a. | 10 | |  | b. | 15 | |  | c. | 18 | |  | d. | 27 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. Which position below is considered an entry-level position for a person who has the necessary technical skills?   |  |  |  | | --- | --- | --- | |  | a. | security technician | |  | b. | security administrator | |  | c. | CISO | |  | d. | security manager | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. What term refers to an action that provides an immediate solution to a problem by cutting through the complexity that surrounds it?   |  |  |  | | --- | --- | --- | |  | a. | unicorn | |  | b. | approved action | |  | c. | secure solution | |  | d. | silver bullet | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. In what kind of attack can attackers make use of millions of computers under their control in an attack against a single server or network?   |  |  |  | | --- | --- | --- | |  | a. | centered | |  | b. | local | |  | c. | remote | |  | d. | distributed | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. Which term below is frequently used to describe the tasks of securing information that is in a digital format?   |  |  |  | | --- | --- | --- | |  | a. | network security | |  | b. | information security | |  | c. | physical security | |  | d. | logical security | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. Which of the three protections ensures that only authorized parties can view information?   |  |  |  | | --- | --- | --- | |  | a. | security | |  | b. | availability | |  | c. | integrity | |  | d. | confidentiality | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. Select the information protection item that ensures that information is correct and that no unauthorized person or malicious software has altered that data.   |  |  |  | | --- | --- | --- | |  | a. | availability | |  | b. | confidentiality | |  | c. | integrity | |  | d. | identity | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. Which of the following ensures that data is accessible to authorized users?   |  |  |  | | --- | --- | --- | |  | a. | availability | |  | b. | confidentiality | |  | c. | integrity | |  | d. | identity | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. In information security, what can constitute a loss?   |  |  |  | | --- | --- | --- | |  | a. | theft of information | |  | b. | a delay in transmitting information that results in a financial penalty | |  | c. | the loss of good will or a reputation | |  | d. | all of the above | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. In information security, which of the following is an example of a threat actor?   |  |  |  | | --- | --- | --- | |  | a. | a force of nature such as a tornado that could destroy computer equipment | |  | b. | a virus that attacks a computer network | |  | c. | a person attempting to break into a secure computer network | |  | d. | all of the above | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What type of theft involves stealing another person's personal information, such as a Social Security number, and then using the information to impersonate the victim, generally for financial gain?   |  |  |  | | --- | --- | --- | |  | a. | cyberterrorism | |  | b. | identity theft | |  | c. | phishing | |  | d. | social scam | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. Under which laws are health care enterprises required to guard protected health information and implement policies and procedures whether it be in paper or electronic format?   |  |  |  | | --- | --- | --- | |  | a. | HIPAA | |  | b. | HLPDA | |  | c. | HCPA | |  | d. | USHIPA | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. Those who wrongfully disclose individually identifiable health information can be fined up to what amount per calendar year?   |  |  |  | | --- | --- | --- | |  | a. | $50,000 | |  | b. | $250,000 | |  | c. | $500,000 | |  | d. | $1,500,000 | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. Which law requires banks and financial institutions to alert customers of their policies and practices in disclosing customer information?   |  |  |  | | --- | --- | --- | |  | a. | Gramm-Leach-Bliley | |  | b. | Sarbanes-Oxley | |  | c. | California Database Security Breach | |  | d. | USA Patriot | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. To date, the single most expensive malicious attack occurred in 2000, which cost an estimated $8.7 billion. What was the name of this attack?   |  |  |  | | --- | --- | --- | |  | a. | Nimda | |  | b. | Slammer | |  | c. | Love Bug | |  | d. | Code Red | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. What term is used to describe a group that is strongly motivated by ideology, but is usually not considered to be well-defined and well-organized?   |  |  |  | | --- | --- | --- | |  | a. | hactivists | |  | b. | hacker | |  | c. | script kiddies | |  | d. | cyberterrorist | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. Which term is used to describe individuals who want to attack computers yet lack the knowledge of computers and networks needed to do so?   |  |  |  | | --- | --- | --- | |  | a. | cybercriminal | |  | b. | hacker | |  | c. | script kiddies | |  | d. | cyberterrorist | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. Select the term that best describes automated attack software?   |  |  |  | | --- | --- | --- | |  | a. | open-source utility | |  | b. | insider software | |  | c. | open-source intelligence | |  | d. | intrusion application | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What class of attacks use innovative attack tools and once a system is infected it silently extracts data over an extended period?   |  |  |  | | --- | --- | --- | |  | a. | Inside Attacks | |  | b. | Advanced Persistent Threat | |  | c. | Embedded Attacks | |  | d. | Modified Threat | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. What term is used to describe state-sponsored attackers that are used for launching computer attacks against their foes?   |  |  |  | | --- | --- | --- | |  | a. | nation state threats | |  | b. | cyber military | |  | c. | nation state actors | |  | d. | state hackers | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. What term describes a layered security approach that provides the comprehensive protection?   |  |  |  | | --- | --- | --- | |  | a. | comprehensive-security | |  | b. | diverse-defense | |  | c. | limiting-defense | |  | d. | defense-in-depth | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What process describes using technology as a basis for controlling the access and usage of sensitive data?   |  |  |  | | --- | --- | --- | |  | a. | technical controls | |  | b. | administrative controls | |  | c. | control diversity | |  | d. | vendor diversity | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. What type of diversity is being implemented if a company is using multiple security products from different manufacturers?   |  |  |  | | --- | --- | --- | |  | a. | multiple-product security | |  | b. | manufacturer diversity | |  | c. | vendor diversity | |  | d. | vendor-control security | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What level of security access should a computer user have to do their job?   |  |  |  | | --- | --- | --- | |  | a. | password protected | |  | b. | least amount | |  | c. | limiting amount | |  | d. | authorized access | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. What term best describes any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against noncombatant targets by subnational groups or clandestine agents?   |  |  |  | | --- | --- | --- | |  | a. | cybercriminal | |  | b. | cracking | |  | c. | cyberterrorism | |  | d. | hacking | |

|  |
| --- |
| **Multiple Response** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. Which of the following is a valid fundamental security principle? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | signature | |  | b. | diversity | |  | c. | simplicity | |  | d. | layering | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which of the following describes various supporting structures for implementing security that provides a resource of how to create a secure IT environment? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | regulatory frameworks | |  | b. | reference architectures | |  | c. | industry-standard frameworks | |  | d. | reference frameworks | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following is a common security framework? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | ISO | |  | b. | COBIT | |  | c. | RFC | |  | d. | ASA | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. Which of the following are considered threat actors? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | brokers | |  | b. | competitors | |  | c. | administrators | |  | d. | individuals | |

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

|  |
| --- |
| 41. Why is the speed of malicious attacks making the challenge of keeping computers secure more difficult? |

|  |
| --- |
| 42. Why are there delays in updating products such as anti-virus software to resist attacks? |

|  |
| --- |
| 43. List and describe three of the characteristics of information that must be protected by information security? |

|  |
| --- |
| 44. Information security is achieved through a combination of what three entities? Provide at least one example of each entity. |

|  |
| --- |
| 45. What are script kiddies? |

|  |
| --- |
| 46. What threat actors are generally believed to be the most dangerous threat actors? Explain your answer. |

|  |
| --- |
| 47. What is the Payment Card Industry Data Security Standard (PCI DSS)? |

|  |
| --- |
| 48. What are the four different risk response techniques? |

|  |
| --- |
| 49. What is occurring when an attacker manipulates commonplace actions that are routinely performed in a business? |

|  |
| --- |
| 50. Describe the security principle of simplicity. |