|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. The first step in solving problems is to gather facts and make assumptions.

|  |  |  |
| --- | --- | --- |
|   | a.  | True |
|   | b.  | False |

|  |  |
| --- | --- |
| *ANSWER:* | False |
| *POINTS:* | 1 |
| *REFERENCES:* | Solving Problems |
| *QUESTION TYPE:* | True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 9:59 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. Corruption of information can occur only while information is being stored.

|  |  |  |
| --- | --- | --- |
|   | a.  | True |
|   | b.  | False |

|  |  |
| --- | --- |
| *ANSWER:* | False |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 9:54 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. The authorization process takes place before the authentication process.

|  |  |  |
| --- | --- | --- |
|   | a.  | True |
|   | b.  | False |

|  |  |
| --- | --- |
| *ANSWER:* | False |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 3:52 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 3/20/2016 10:20 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. DoS attacks cannot be launched against routers.

|  |  |  |
| --- | --- | --- |
|   | a.  | True |
|   | b.  | False |

|  |  |
| --- | --- |
| *ANSWER:* | False |
| *POINTS:* | 1 |
| *REFERENCES:* | Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks |
| *QUESTION TYPE:* | True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:24 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. "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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Espionage or Trespass |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/24/2016 5:47 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. When voltage levels lag (experience a momentary increase), the extra voltage can severely damage or destroy equipment. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| *ANSWER:* | False - spike |
| *POINTS:* | 1 |
| *REFERENCES:* | Deviations in Quality of Service |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:27 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. The macro virus infects the key operating system files located in a computer’s start up sector. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| *ANSWER:* | False - boot |
| *POINTS:* | 1 |
| *REFERENCES:* | Software Attacks |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 3/20/2016 10:21 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Password Attacks |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:29 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Hackers |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:30 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Malware |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:31 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Software Attacks |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:32 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 3/20/2016 10:22 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | Modified True / False |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 3/20/2016 10:22 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Introduction to Security |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 3:53 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. According to the C.I.A. triad, which of the following is a desirable characteristic for computer security?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   | a.  | accountability | b.  | availability |
|   | c.  | authorization | d.  | authentication |

|  |  |
| --- | --- |
| *ANSWER:* | b |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 10:36 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. Which of the following is a C.I.A. characteristic that ensures that only those with sufficient privileges and a demonstrated need may access certain information?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   | a.  | Integrity | b.  | Availability |
|   | c.  | Authentication | d.  | Confidentiality |

|  |  |
| --- | --- |
| *ANSWER:* | d |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 10:41 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 3:54 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. What do audit logs that track user activity on an information system provide?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   | a.  | identification | b.  | authorization |
|   | c.  | accountability | d.  | authentication |

|  |  |
| --- | --- |
| *ANSWER:* | c |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 3:55 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Management Characteristics |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 3/20/2016 10:23 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Management Characteristics |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 3:59 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Communications Interception Attacks |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 3/20/2016 10:24 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Solving Problems |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:02 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Solving Problems |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:04 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. Which of the following is NOT a primary function of Information Security Management?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   | a.  | planning | b.  | protection |
|   | c.  | projects | d.  | performance |

|  |  |
| --- | --- |
| *ANSWER:* | d |
| *POINTS:* | 1 |
| *REFERENCES:* | Principles of Information Security Management |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 3/20/2016 10:24 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Principles of Information Security Management |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:08 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Principles of Information Security Management |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:09 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Espionage or Trespass |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:46 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Malware |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:37 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Malware |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:48 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. Human error or failure often can be prevented with training, ongoing awareness activities, and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   | a.  | threats | b.  | education |
|   | c.  | hugs | d.  | paperwork |

|  |  |
| --- | --- |
| *ANSWER:* | b |
| *POINTS:* | 1 |
| *REFERENCES:* | Human Error or Failure |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 3/20/2016 10:25 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. “4-1-9” fraud is an example of a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attack.

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

|  |  |
| --- | --- |
| *ANSWER:* | a |
| *POINTS:* | 1 |
| *REFERENCES:* | Human Error or Failure |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:36 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | E-mail Attacks |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/27/2016 10:17 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. ​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 |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/23/2016 5:07 PM |
| *DATE MODIFIED:* | 3/20/2016 10:27 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:13 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Information Extortion |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/25/2016 5:37 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:19 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:19 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Software Attacks |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/27/2016 10:19 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. A short-term interruption in electrical power availability is known as a \_\_\_\_.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   | a.  | ​fault | b.  | ​brownout |
|   | c.  | ​blackout | d.  | ​lag |

|  |  |
| --- | --- |
| *ANSWER:* | a |
| *POINTS:* | 1 |
| *REFERENCES:* | Deviations in Quality of Service |
| *QUESTION TYPE:* | Multiple Choice |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:44 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 41. The three levels of planning are strategic planning, tactical planning, and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ planning.

|  |  |
| --- | --- |
| *ANSWER:* | operational |
| *POINTS:* | 1 |
| *REFERENCES:* | Management Characteristics |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:11 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 42. The set of organizational guidelines that dictates certain behavior within the organization is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| *ANSWER:* | policy |
| *POINTS:* | 1 |
| *REFERENCES:* | Policy |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:16 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 43. Attempting to reverse-calculate a password is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| *ANSWER:* | cracking |
| *POINTS:* | 1 |
| *REFERENCES:* | Password Attacks |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:34 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 44. ESD is the acronym for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ discharge.

|  |  |
| --- | --- |
| *ANSWER:* | electrostatic |
| *POINTS:* | 1 |
| *REFERENCES:* | Forces of Nature |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 3/20/2016 10:28 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 45. Duplication of software-based intellectual property is more commonly known as software \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| *ANSWER:* | piracy |
| *POINTS:* | 1 |
| *REFERENCES:* | Compromises to Intellectual Property |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:42 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 46. A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ hacks the public telephone network to make free calls or disrupt services.

|  |  |
| --- | --- |
| *ANSWER:* | phreaker |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:14 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 47. A momentary low voltage is called a(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| *ANSWER:* | sag |
| *POINTS:* | 1 |
| *REFERENCES:* | Deviations in Quality of Service |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:45 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 48. Some information gathering techniques are quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, competitive \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| *ANSWER:* | intelligence |
| *POINTS:* | 1 |
| *REFERENCES:* | Espionage or Trespass |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:45 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 49. A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a potential weakness in an asset or its defensive control(s).

|  |  |
| --- | --- |
| *ANSWER:* | vulnerability |
| *POINTS:* | 1 |
| *REFERENCES:* | Key Concepts of Information Security: Threats and Attacks |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:41 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 50. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is unsolicited commercial e-mail.

|  |  |
| --- | --- |
| *ANSWER:* | Spam |
| *POINTS:* | 1 |
| *REFERENCES:* | E-mail Attacks |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:38 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 51. 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 |
| *POINTS:* | 1 |
| *REFERENCES:* | Back Doors |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:39 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 52. A(n) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is an act against an asset that could result in a loss.

|  |  |
| --- | --- |
| *ANSWER:* | attack |
| *POINTS:* | 1 |
| *REFERENCES:* | Key Concepts of Information Security: Threats and Attacks |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/23/2016 5:42 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 53. A \_\_\_\_\_\_\_\_\_\_\_\_ overflow is an application error that occurs when the system can’t handle the amount of data that is sent.

|  |  |
| --- | --- |
| *ANSWER:* | buffer |
| *POINTS:* | 1 |
| *REFERENCES:* | Technical Software Failures or Errors |
| *QUESTION TYPE:* | Completion |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/27/2016 10:16 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 54. 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. |
| *POINTS:* | 1 |
| *REFERENCES:* | Management Characteristics |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 5:50 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 55. 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 useable format. |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 3/20/2016 10:29 AM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 56. List and explain the four principles of management under the contemporary or popular management theory. Briefly define each.

|  |  |
| --- | --- |
| *ANSWER:* | Popular management theory, which 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. |
| *POINTS:* | 1 |
| *REFERENCES:* | Management Characteristics |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:19 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 57. List the steps that can be used as a basic blueprint for solving organizational problems.

|  |  |
| --- | --- |
| *ANSWER:* | 1. Recognize and Define the Problem2. Gather Facts and Make Assumptions3. Develop Possible Solutions4. Analyze and Compare Possible Solutions.5. Select, Implement and Evaluate a Solution. |
| *POINTS:* | 1 |
| *REFERENCES:* | Solving Problems |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:20 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 58. 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 securityManagers and professionals in the field of ITManagers and professionals from the rest of the organization |
| *POINTS:* | 1 |
| *REFERENCES:* | Introduction to Security |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:22 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 59. List the specialized areas of security.

|  |  |
| --- | --- |
| *ANSWER:* | Physical securityOperations securityCommunications securityNetwork security |
| *POINTS:* | 1 |
| *REFERENCES:* | Introduction to Security |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 5:26 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 60. List the measures that are commonly used to protect the confidentiality of information.

|  |  |
| --- | --- |
| *ANSWER:* | Information classificationSecure document (and data) storageApplication of general security policiesEducation of information custodians and end usersCryptography (encryption) |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:24 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 61. 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. |
| *POINTS:* | 1 |
| *REFERENCES:* | The Value of Information and the C.I.A. Triad |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:26 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 62. 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. |
| *POINTS:* | 1 |
| *REFERENCES:* | Planning |
| *QUESTION TYPE:* | Subjective Short Answer |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 2/22/2016 4:24 PM |
| *DATE MODIFIED:* | 2/23/2016 4:26 PM |

 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 63. 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 propertySoftware attacksDeviations in quality of serviceEspionage or trespassForces of natureHuman error or failureInformation extortionMissing, inadequate, or incompleteMissing, inadequate, or incomplete controlsSabotage or vandalismTheftTechnical hardware failures or errorsTechnical software failures or errorsTechnological obsolescence |
| *POINTS:* | 1 |
| *REFERENCES:* | The 12 Categories of Threats |
| *QUESTION TYPE:* | Essay |
| *HAS VARIABLES:* | False |
| *DATE CREATED:* | 9/9/2014 1:38 PM |
| *DATE MODIFIED:* | 2/27/2016 10:12 AM |

 |