|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. An automated patch update service is used to manage patches within the enterprise instead of relying on the vendor's online updates.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. The BIOS was software that was integrated into the computer's motherboard.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. Tightening security during the design and coding of an OS is called "locking."   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. An access log is a record or list of individuals who have permission to enter a secure area, along with the time they entered and the time they left the area.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. When securing a laptop, it can be placed in an office or a desk drawer.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. In the production stage the application is released to be used in its actual setting.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. The testing stage is a "quality assurance" test to verify that the code functions as intended.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. One tool for change management is version control software that allows changes to be automatically recorded and if necessary "rolled back" to a previous version of the software.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. A compiled code test is used to ensure that the projected application meets all specifications at that point   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. Static program analyzers are tools that examine the software without actually executing the program; instead, the source code is reviewed and analyzed.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. What security standard was introduced in conjunction with UEFI?   |  |  |  | | --- | --- | --- | |  | a. | Unified Boot | |  | b. | BIOS | |  | c. | Secure Boot | |  | d. | Firmware Interface |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. What U.S. government classified standard is intended to prevent attackers from picking up electromagnetic fields from government buildings?   |  |  |  | | --- | --- | --- | |  | a. | RAIN | |  | b. | EMIF | |  | c. | TEMPEST | |  | d. | MaSec |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What type of OS manages hardware and software on a client computer?   |  |  |  | | --- | --- | --- | |  | a. | network OS | |  | b. | client OS | |  | c. | workstation OS | |  | d. | appliance OS |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. What type of OS in firmware is designed to manage a specific device like a video game console?   |  |  |  | | --- | --- | --- | |  | a. | network OS | |  | b. | client OS | |  | c. | workstation OS | |  | d. | appliance OS |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. Which of the following are considered to be part of a typical OS security configuration? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | Disabling unnecessary ports and services | |  | b. | Employing least functionality | |  | c. | Password auditing | |  | d. | Disabling default accounts/passwords |  |  |  | | --- | --- | | *ANSWER:* | a, b, c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. What security concept states a user should only be given the minimum set of permissions required to perform necessary tasks?   |  |  |  | | --- | --- | --- | |  | a. | least functionality | |  | b. | whitelisting | |  | c. | blacklisting | |  | d. | function limiting |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. In Microsoft Windows, what type of templates are a collection of security configuration settings?   |  |  |  | | --- | --- | --- | |  | a. | security | |  | b. | user | |  | c. | system | |  | d. | administrator |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. What type of filtering software divides email messages that have been received into two piles, spam and non-spam and then analyzes every word in each email and determines how frequently a word occurs in the spam pile compared to the not-spam pile?   |  |  |  | | --- | --- | --- | |  | a. | Blacklist filtering | |  | b. | Whitelist filtering | |  | c. | Bayesian filtering | |  | d. | Extension filtering |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. Anti-virus products typically utilize what type of virus scanning analysis?   |  |  |  | | --- | --- | --- | |  | a. | Static analysis | |  | b. | Wildcard scanning analysis | |  | c. | Heuristic detection analysis | |  | d. | String scanning analysis |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. What is the name for a cumulative package of all patches and hot-fixes as well as additional features up to a given point?   |  |  |  | | --- | --- | --- | |  | a. | feature pack | |  | b. | roll-up | |  | c. | service pack | |  | d. | patch |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. Which AV approach uses a variety of techniques to spot the characteristics of a virus instead of attempting to make matches?   |  |  |  | | --- | --- | --- | |  | a. | heuristic monitoring | |  | b. | pattern detection | |  | c. | hybrid monitoring | |  | d. | combination detection |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What publicly released software security update is intended to repair a vulnerability?   |  |  |  | | --- | --- | --- | |  | a. | update | |  | b. | service pack | |  | c. | patch | |  | d. | renewal |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. What type of update does not allow a user to refuse or delay security updates?   |  |  |  | | --- | --- | --- | |  | a. | preventative | |  | b. | forced | |  | c. | mandatory | |  | d. | security |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. What specific software can examine a computer for any infections as well as monitor computer activity and scan new documents that might contain a virus?   |  |  |  | | --- | --- | --- | |  | a. | anti-malware | |  | b. | antivirus | |  | c. | security applications | |  | d. | firewall |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. Which of the following is an AV heuristic monitoring technique?   |  |  |  | | --- | --- | --- | |  | a. | code emulation | |  | b. | environment scanning | |  | c. | code monitoring | |  | d. | OS simulation |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. What monitors emails for spam and other unwanted content to prevent these messages from being delivered?   |  |  |  | | --- | --- | --- | |  | a. | mail gateway | |  | b. | firewall | |  | c. | router gateway | |  | d. | code emulation |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. Which OS hardening technique removes all unnecessary features that may compromise an operating system?   |  |  |  | | --- | --- | --- | |  | a. | least privilege | |  | b. | OS priority | |  | c. | kernel pruning | |  | d. | reduce capabilities |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. What type of storage is used on mobile devices?   |  |  |  | | --- | --- | --- | |  | a. | volatile memory | |  | b. | ROM | |  | c. | RAM | |  | d. | flash memory |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. Which of the following is a popular type of removable data storage used on mobile devices?   |  |  |  | | --- | --- | --- | |  | a. | SSD | |  | b. | SD | |  | c. | HDD | |  | d. | USB |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What type of tools are involved in effective patch management? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | patch verification | |  | b. | patch distribution | |  | c. | patch monitoring | |  | d. | patch reception |  |  |  | | --- | --- | | *ANSWER:* | b, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. An independently rotating large cup affixed to the top of a fence prevents the hands of intruders from gripping the top of a fence to climb over it. What is the name for this technology?   |  |  |  | | --- | --- | --- | |  | a. | bollard | |  | b. | fence | |  | c. | roller barrier | |  | d. | top hat |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. Most portable devices, and some computer monitors have a special steel bracket security slot built into the case, which can be used in conjunction with a:   |  |  |  | | --- | --- | --- | |  | a. | U-lock | |  | b. | safe lock | |  | c. | shield lock | |  | d. | cable lock |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What type of video surveillance is typically used by banks, casinos, airports, and military installations, and commonly employs guards who actively monitor the surveillance?   |  |  |  | | --- | --- | --- | |  | a. | CCTV | |  | b. | ICTV | |  | c. | IPTV | |  | d. | ITV |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. A spiked collar that extends horizontally for up to 3 feet from the pole is an example of what kind of technology?   |  |  |  | | --- | --- | --- | |  | a. | Anti-climb | |  | b. | Spiked barrier | |  | c. | Roller barrier | |  | d. | Rotating spikes |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. How can an area be made secure from a non-secured area via two interlocking doors to a small room?   |  |  |  | | --- | --- | --- | |  | a. | Using a lockout | |  | b. | Using a mantrap | |  | c. | Using a closet | |  | d. | Using a pit |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. A Wi-Fi enabled microSD card is an example of what type of device?   |  |  |  | | --- | --- | --- | |  | a. | PCIe | |  | b. | mobile card | |  | c. | SDIO | |  | d. | Secure Digital |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. Which of the following are application development stages? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | analysis | |  | b. | proofing | |  | c. | testing | |  | d. | staging |  |  |  | | --- | --- | | *ANSWER:* | c, d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which application development life-cycle model uses a sequential design process?   |  |  |  | | --- | --- | --- | |  | a. | agile | |  | b. | linear | |  | c. | waterfall | |  | d. | serial |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. What software methodology includes security automation?   |  |  |  | | --- | --- | --- | |  | a. | DevOps | |  | b. | Secure DevOps | |  | c. | Agile | |  | d. | Secure Agile |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. What specific process in application development removes a resource that is no longer needed?   |  |  |  | | --- | --- | --- | |  | a. | deprovisioning | |  | b. | version control | |  | c. | change management | |  | d. | baselining |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |
| --- | --- | --- |
| 41. Describe a mantrap.   |  |  | | --- | --- | | *ANSWER:* | A mantrap is designed to separate a nonsecured area from a secured area. A mantrap device monitors and controls two interlocking doors to a small room (a vestibule). When in operation, only one door is able to be open at any time. Mantraps are used at high-security areas where only authorized persons are allowed to enter, such as sensitive data-processing rooms, cash-handling areas, and research laboratories. | |

|  |  |  |
| --- | --- | --- |
| 42. How can cable conduits that run between two secure areas be protected?   |  |  | | --- | --- | | *ANSWER:* | A protected distribution system (PDS) can be used to protect conduit cables between two locations. This can consist of a hardened carrier PDS, in which the conduit is constructed of special electrical metallic tubing or similar material, or an alarmed carrier PDS, which uses optical fibers and acoustic sensors that can detect vibrations from a potential intruder. | |

|  |  |  |
| --- | --- | --- |
| 43. How is the UEFI Secure Boot security standard designed to combat BIOS attacks?   |  |  | | --- | --- | | *ANSWER:* | Secure Boot is designed to ensure that a computer boots using only software that is trusted by the computer manufacturer. When using UEFI and Secure Boot, as computer boots it checks the digital signature of each piece of boot software, including firmware drivers and the operating system. If the signatures are deemed valid the computer boots; otherwise, the computer does not boot. | |

|  |  |  |
| --- | --- | --- |
| 44. What is a supply chain and why is it critical to understand that it needs to be secured?   |  |  | | --- | --- | | *ANSWER:* | A supply chain is a network that moves a product from the supplier to the customer. It is made up of vendors that supply raw material, manufacturers who convert the material into products, warehouses that store products, distribution centers that deliver them to the retailers, and retailers who bring the product to the consumer. Supply chain infections are considered especially dangerous. First, if the malware is planted in the ROM firmware of the device, it can be difficult or sometimes impossible to clean an infected device. | |

|  |  |  |
| --- | --- | --- |
| 45. What are some of the advantages to an automated patch update service?   |  |  | | --- | --- | | *ANSWER:* | Downloading patches from a local server instead of using the vendor's online update service can save bandwidth and time because each computer does not have to connect to an external server. Administrators can approve or decline updates for client systems, force updates to install by a specific date, and obtain reports on what updates each computer needs. Administrators can approve updates for "detection" only; this allows them to see which computers require the update without installing it. | |

|  |  |  |
| --- | --- | --- |
| 46. What type of package helps prevent computers from becoming infected by different types of spyware?   |  |  | | --- | --- | | *ANSWER:* | A package known as antispyware helps prevent computers from becoming infected by different types of spyware. | |

|  |  |  |
| --- | --- | --- |
| 47. What is a multi-functional device (MFD)?   |  |  | | --- | --- | | *ANSWER:* | A multi-functional device (MFD) combines the functions of a printer, copier, scanner, and fax machine. | |

|  |  |  |
| --- | --- | --- |
| 48. What is a bollard?   |  |  | | --- | --- | | *ANSWER:* | A bollard is a short but sturdy vertical post that is used to as a vehicular traffic barricade to prevent a car from "ramming" into a secured area. | |

|  |  |  |
| --- | --- | --- |
| 49. What is provisioning?   |  |  | | --- | --- | | *ANSWER:* | Provisioning is the enterprise-wide configuration, deployment, and management of multiple types of IT system resources, of which the new application would be viewed as a new resource. | |

|  |  |  |
| --- | --- | --- |
| 50. Explain the security advantages of "code signing" and "stored procedure"?   |  |  | | --- | --- | | *ANSWER:* | Code signing Confirms the software author and guarantees the code has not been altered or corrupted. Stored procedure eliminates the need to write a subroutine that could have vulnerabilities. | |