崑山科技大學資工系IPAS證照輔導班 練習

名稱: *CompTIA SecurityPLUS\_Ch3\_Threats, Attacks, andVulnerabilities*

|  |  |  |
| --- | --- | --- |
| 答案 | 編號 | 題目 |
|  | 1. | Caroline has been asked to find a standard to guide her company’s choices in implementing information security management systems. She is looking for a standard that is international. Which of the following would be the best choice for her?  **A.** ISO 27002 **B.** ISO 27017 **C.** NIST 800-12 **D.** NIST 800-14 |
|  | 2. | You are responsible for network security at an e-commerce company. You want to ensure that you are using best practices for the e-commerce website your company hosts. What standard would be the best for you to review?  **A.** OWASP **B.** NERC **C.** NIST **D.** ISA/IEC |
|  | 3. | Cheryl is responsible for cybersecurity at a mid-sized insurance company. She has decided to utilize a different vendor for network antimalware than she uses for host antimalware. Is this a recommended action, and why or why not?  **A.** This is not recommended; you should use a single vendor for a particular security control.  **B.** This is recommended; this is described as vendor diversity.  **C.** This is not recommended; this is described as vendor forking.  **D.** It is neutral. This does not improve or detract from security |
|  | 4. | Maria is a security administrator for a large bank. She is concerned about malware, particularly spyware that could compromise customer dat**A.** Which of the following would be the best approach for her to mitigate the threat of spyware?  **A.** Computer usage policies, network antimalware, and host antimalware  **B.** Host antimalware and network antimalware  **C.** Host and network antimalware, computer usage policies, and website whitelisting  **D.** Host and network antimalware, computer usage policies, and employee training |
|  | 5. | Gabriel is setting up a new e-commerce server. He is concerned about security issues. Which of the following would be the best location to place an e-commerce server?  **A.** DMZ **B.** Intranet **C.** Guest network **D.** Extranet |
|  | 6. | . Enrique is concerned about backup data being infected by malware. The company backs up key servers to digital storage on a backup server. Which of the following would be most effective in preventing the backup data being infected by malware?  **A.** Place the backup server on a separate VLAN.  **B.** Air-gap the backup server.  **C.** Place the backup server on a different network segment.  **D.** Use a honeynet. |
|  | 7. | . Janelle is the security administrator for a small company. She is trying to improve security throughout the network. Which of the following steps should she take first?  **A.** Implement antimalware on all computers.  **B.** Implement acceptable use policies.  **C.** Turn off unneeded services on all computers.  **D.** Turn on host-based firewalls on all computers. |
|  | 8. | Mary is the CISO for a mid-sized company. She is attempting to mitigate the danger of computer viruses. Which administrative control can she implement to help achieve this goal?  **A.** Implement host-based antimalware.  **B.** Implement policies regarding email attachments and file downloads.  **C.** Implement network-based antimalware.  **D.** Block portable storage devices from being connected to computers. |
|  | 9. | You are the network administrator for a large company. Your company frequently has nonemployees in the company such as clients and vendors. You have been directed to provide these nonemployees with access to the Internet. Which of the following is the best way to implement this?  **A.** Establish a guest network.  **B.** Allow nonemployees to connect only to the DMZ.  **C.** Allow nonemployees to connect only to the intranet.  **D.** Establish limited accounts on your network for nonemployees to use. |
|  | 10. | Juan is a network administrator for an insurance company. His company has a number of traveling salespeople. He is concerned about confidential data on their laptops. What is the best way for him to address this?  **A.** FDE **B.** TPM **C.** SDN **D.** DMZ |
|  | 11. | Terrance is responsible for secure communications on his company’s network. The company has a number of traveling salespeople who need to connect to network resources. What technology would be most helpful in addressing this need?  **A.** VPN concentrator **B.** SSL accelerator **C.** DMZ **D.** Guest network |
|  | 12. | Mohaned is concerned about malware infecting machines on his network. One of his concerns is that malware would be able to access sensitive system functionality that requires administrative access. What technique would best address this issue?  **A.** Implementing host-based antimalware  **B.** Using a nonadministrative account for normal activities  **C.** Implementing FDE  **D.** Making certain the operating systems are patched |
|  | 13. | John works for an insurance company. His company uses a number of operating systems, including Windows and Linux. In this mixed environment, what determines the network operating system?  **A.** The OS of the DNS server  **B.** The OS of the domain controller  **C.** The OS of the majority of servers  **D.** The OS of the majority of client comput |
|  | 14. | Juanita is implementing virtualized systems in her network. She is using Type I hypervisors. What operating system should be on the machines for her to install the hypervisor?  **A.** None **B.** Windows  **C.** Any operating system **D.** Windows or Linux |
|  | 15. | You are responsible for security at your company. You want to improve cloud security by following the guidelines of an established international standar**D.** What standard would be most helpful?  **A.** NIST 800-14 **B.** NIST 800-53 **C.** ISO 27017 **D.** ISO 27002 |
|  | 16. | You are responsible for setting up a kiosk computer that will be in your company’s lobby. It will be accessible for visitors to locate employee offices, obtain the guest WiFi password, and retrieve general public company information. What is the most important thing to consider when configuring this system?  **A.** Using a strong administrator password  **B.** Limiting functionality to only what is needed  **C.** Using good antivirus protection  **D.** Implementing a host-based firewall |
|  | 17. | You are concerned about peripheral devices being exploited by an attacker. Which of the following is the first step you should take to mitigate this threat? **A.** Disable WiFi for any peripheral that does not absolutely need it.  **B.** Enable BIOS protection for peripheral devices.  **C.** Use strong encryption on all peripheral devices.  **D.** Configure antivirus on all peripherals. |
|  | 18. | Which design concept limits access to systems from outside users while protecting users and systems inside the LAN?  **A.** DMZ **B.** VLAN **C.** Router **D.** Guest network |
|  | 19. | Which of the following is the equivalent of a VLAN from a physical security perspective?  **A.** Perimeter security **B.** Partitioning **C.** Security zones **D.** Firewal |
|  | 20. | In an attempt to observe hacker techniques, a security administrator configures a nonproduction network to be used as a target so that he can covertly monitor network attacks. What is this type of network called?  **A.** Active detection **B.** False subnet **C.** IDS **D.** Honeynet |
|  | 21. | You have instructed all administrators to disable all nonessential ports on servers at their sites. Why are nonessential protocols a security issue that you should be concerned about?  **A.** Nonessential ports provide additional areas of attack.  **B.** Nonessential ports can’t be secure**D.**  **C.** Nonessential ports are less secure.  **D.** Nonessential ports require more administrative effort to secure. |
|  | 22. | Which type of firewall examines the content and context of each packet it encounters?  **A.** Packet filtering firewall **B.** Stateful packet filtering firewall  **C.** Application layer firewall **D.** Gateway firewall |
|  | 23. | Which of the following would prevent a user from installing a program on a companyowned mobile device?  **A.** Whitelisting **B.** Blacklisting **C.** ACL **D.** HIDS |
|  | 24. | You’re designing a new network infrastructure so that your company can allow unauthenticated users connecting from the Internet to access certain areas. Your goal is to protect the internal network while providing access to those areas. You decide to put the web server on a separate subnet open to public contact. What is this subnet called?  **A.** Guest network **B.** DMZ **C.** Intranet **D.** VLAN |
|  | 25. | Upper management has decreed that a firewall must be put in place immediately, before your site suffers an attack similar to one that struck a sister company. Responding to this order, your boss instructs you to implement a packet filter by the end of the week. A packet filter performs which function?  **A.** Prevents unauthorized packets from entering the network  **B.** Allows all packets to leave the network  **C.** Allows all packets to enter the network  **D.** Eliminates collisions in the network |
|  | 26. | . You’re outlining your plans for implementing a wireless network to upper management. Which protocol was designed to provide security for a wireless network and is considered equivalent to the security of a wired network?  **A.** WAP **B.** WPA **C.** WPA2 **D.** WEP |
|  | 27. | An IV attack is usually associated with which of the following wireless protocols? **A.** WEP **B.** WAP **C.** WPA **D.** WPA2 |
|  | 28. | Suzan is responsible for application development in her company. She wants to have all web applications tested prior to being deployed live. She wants to use a test system that is identical to the live server. What is this called?  **A.** Production server **B.** Development server  **C.** Test server **D.** Predeployment server |
|  | 29. | John is responsible for security in his company. He is implementing a kernel integrity subsystem for key servers. What is the primary benefit of this action?  **A.** To detect malware  **B.** To detect whether files have been altered  **C.** To detect rogue programs being installed  **D.** To detect changes to user accounts |
|  | 30. | You are responsible for BIOS security in your company. Which of the following is the most fundamental BIOS integrity technique?  **A.** Verifying the BIOS version **B.** Using a TPM  **C.** Managing BIOS passwords **D.** Backing up the BIOS |
|  | 31. | You have been asked to implement security for SCADA systems in your company. Which of the following standards will be most helpful to you?  **A.** NIST 800-82 **B.** PCI-DSS **C.** NIST 800-30 **D.** ISO 27002 |
|  | 32. | Joanne works for a large insurance company. Some employees have wearable technology, such as smart watches. What is the most significant security concern from such devices?  **A.** These devices can distract employees.  **B.** These devices can be used to carry data in and out of the company.  **C.** These devices may not have encrypted drives.  **D.** These devices may not have strong passwords. |
|  | 33. | John is installing an HVAC system in his datacenter. What will this HVAC have the most impact on?  **A.** Confidentiality **B.** Availability  **C.** Fire suppression **D.** Monitoring access to the datacenter |
|  | 34. | Maria is a security engineer with a manufacturing company. During a recent investigation, she discovered that an engineer’s compromised workstation was being used to connect to SCADA systems while the engineer was not logged in. The engineer is responsible for administering the SCADA systems and cannot be blocked from connecting to them. What should Maria do to mitigate this threat?  **A.** Install host-based antivirus software on the engineer’s system.  **B.** Implement account usage auditing on the SCADA system.  **C.** Implement an NIPS on the SCADA system.  **D.** Use FDE on the engineer’s system. |
|  | 35. | Lucy works as a network administrator for a large company. She needs to administer several servers. Her objective is to make it easy to administer and secure these servers, as well as making the installation of new servers more streamline**D.** Which of the following best addresses these issues?  **A.** Setting up a cluster **B.** Virtualizing the servers  **C.** Putting the servers on a VLAN **D.** Putting the servers on a separate subnet |
|  | 36. | Gerard is responsible for secure communications with his company’s e-commerce server. All communications with the server use TLS. What is the most secure option for Gerard to store the private key on the e-commerce server? **A.** HSM **B.** FDE **C.** SED **D.** SDN |
|  | 37. | You are the security officer for a large company. You have discovered malware on one of the workstations. You are concerned that the malware might have multiple functions and might have caused more security issues with the computer than you can currently detect. What is the best way to test this malware?  **A.** Leave the malware on that workstation until it is teste**D.**  **B.** Place the malware in a sandbox environment for testing.  **C.** It is not important to test it; just remove it from the machine.  **D.** Place the malware on a honeypot for testing. |
|  | 38. | Web developers in your company currently have direct access to the production server and can deploy code directly to it. This can lead to unsecure code, or simply code flaws being deployed to the live system. What would be the best change you could make to mitigate this risk?  **A.** Implement sandboxing. **B.** Implement virtualized servers.  **C.** Implement a staging server. **D.** Implement deployment policies. |
|  | 39. | Denish is concerned about the security of embedded devices in his company. He is most concerned about the operating system security for such devices. Which of the following would be the best option for mitigating this threat?  **A.** RTOS **B.** SCADA **C.** FDE **D.** TPM |
|  | 40. | Which of the following 802.11 standards is supported in WPA2, but not in WEP or WPA? **A.** 802.11a **B.** 802.11b **C.** 802.11i **D.** 802.11n |
|  | 41. | Teresa is responsible for WiFi security in her company. Which wireless security protocol uses TKIP? **A.** WPA **B.** CCMP **C.** WEP **D.** WPA2 |
|  | 42. | Juan is responsible for wireless security in his company. He has decided to disable the SSID broadcast on the single AP the company uses. What will the effect be on client machines?  **A.** They will no longer be able to use wireless networking.  **B.** They will no longer see the SSID as a preferred network when they are connecte**D.**  **C.** They will no longer see the SSID as an available network.  **D.** They will be required to make the SSID part of their HomeGroup. |
|  | 43. | Which cloud service model provides the consumer with the infrastructure to create applications and host them? **A.** SaaS **B.** PaaS **C.** IaaS **D.** CaaS |
|  | 44. | Which cloud service model gives the consumer the ability to use applications provided by the cloud provider over the Internet?  **A.** SaaS **B.** PaaS **C.** IaaS **D.** Caa |
|  | 45. | Which feature of cloud computing involves dynamically provisioning (or deprovisioning) resources as needed?  **A.** Multitenancy **B.** Elasticity **C.** CMDB **D.** Sandboxing |
|  | 46. | Which type of hypervisor implementation is known as “bare metal”?  **A.** Type I **B.** Type II **C.** Type III **D.** Type IV |
|  | 47. | Mohaned is a security analyst and has just removed malware from a virtual server. What feature of virtualization would he use to return the virtual server to a last known good state?  **A.** Sandboxing **B.** Hypervisor **C.** Snapshot **D.** Elasticity |
|  | 48. | Lisa is concerned about fault tolerance for her database server. She wants to ensure that if any single drive fails, it can be recovere**D.** What RAID level would support this goal while using distributed parity bits?  **A.** RAID 0 **B.** RAID 1 **C.** RAID 3 **D.** RAID 5 |
|  | 49. | Jarod is concerned about EMI affecting a key escrow server. Which method would be most effective in mitigating this risk?  **A.** VLAN **B.** SDN **C.** Trusted platform module **D.** Faraday cag |
|  | 50. | John is responsible for physical security at his company. He is particularly concerned about an attacker driving a vehicle into the building. Which of the following would provide the best protection against this threat?  **A.** A gate **B.** Bollards **C.** A security guard on duty **D.** Security cameras |
|  | 51. | Mark is responsible for cybersecurity at a small college. There are many computer labs that are open for students to use. These labs are monitored only by a student worker, who may or may not be very attentive. Mark is concerned about the theft of computers. Which of the following would be the best way for him to mitigate this threat?  **A.** Cable locks **B.** FDE on the lab computers  **C.** Strong passwords on the lab computers **D.** Having a lab sign-in sheet |
|  | 52. | Joanne is responsible for security at a power plant. The facility is very sensitive and security is extremely important. She wants to incorporate two-factor authentication with physical security. What would be the best way to accomplish this?  **A.** Smart cards  **B.** A mantrap with a smart card at one door and a pin keypad at the other door  **C.** A mantrap with video surveillance  **D.** A fence with a smart card gate access |
|  | 53. | Which of the following terms refers to the process of establishing a standard for security?  **A.** Baselining **B.** Security evaluation **C.** Hardening **D.** Normalization |
|  | 54. | You are trying to increase security at your company. You’re currently creating an outline of all the aspects of security that will need to be examined and acted on. Which of the following terms describes the process of improving security in a trusted OS?  **A.** FDE **B.** Hardening **C.** SED **D.** Baselining |
|  | 55. | Which level of RAID is a “stripe of mirrors”?  **A.** RAID 1+0 **B.** RAID 6 **C.** RAID 0 **D.** RAID 1 |
|  | 56. | Isabella is responsible for database management and security. She is attempting to remove redundancy in the database. What is this process called?  **A.** Integrity checking **B.** Deprovisioning **C.** Baselining **D.** Normalization |
|  | 57. | A list of applications approved for use on your network would be known as which of the following?  **A.** Blacklist **B.** Red list **C.** Whitelist **D.** Orange list |
|  | 58. | Hans is a security administrator for a large company. Users on his network visit a wide range of websites. He is concerned they might get malware from one of these many websites. Which of the following would be his best approach to mitigate this threat?  **A.** Implement host-based antivirus.  **B.** Blacklist known infected sites.  **C.** Set browsers to allow only signed components.  **D.** Set browsers to block all active content (ActiveX, JavaScript, et**C.**). |
|  | 59. | Elizabeth has implemented agile development for her company. What is the primary difference between agile development and the waterfall method?  **A.** Agile has fewer phases. **B.** Waterfall has fewer phases.  **C.** Agile is more secure. **D.** Agile repeats phases. |
|  | 60. | John is using the waterfall method for application development. At which phase should he implement security measures?  **A.** Requirements **B.** Design **C.** Implementation **D.** All |
|  | 61. | You are responsible for database security at your company. You are concerned that programmers might pass badly written SQL commands to the database, or that an attacker might exploit badly written SQL in applications. What is the best way to mitigate this threat?  **A.** Programmer training **B.** Programming policies  **C.** Agile programming **D.** Stored procedures |
|  | 62. | Mary is concerned about application security for her company’s application development. Which of the following is the most important step for addressing application security?  **A.** Proper error handling **B.** Regular data backups  **C.** Encrypted data transmission **D.** Strong authentication |
|  | 63. | Farès is responsible for managing the many virtual machines on his company’s networks. Over the past two years, the company has increased the number of virtual machines significantly. Farès is no longer able to effectively manage the large number of machines. What is the term for this situation?  **A.** VM overload **B.** VM sprawl **C.** VM spread **D.** VM zombies |
|  | 64. | Mary is responsible for virtualization management in her company. She is concerned about VM escape. Which of the following methods would be the most effective in mitigating this risk?  **A.** Only share resources between the VM and host if absolutely necessary.  **B.** Keep the VM patche**D.**  **C.** Use a firewall on the VM. **D.** Use host-based antimalware on the VM. |
|  | 65. | You work at a large company. You are concerned about ensuring that all workstations have a common configuration, no rogue software is installed, and all patches are kept up to date. Which of the following would be the most effective for accomplishing this?  **A.** Use VDE. **B.** Implement strong policies.  **C.** Use an image for all workstations.  **D.** Implement strong patch management. |
|  | 66. | Juan is responsible for the physical security of the company server room. He has been asked to recommend a type of fire suppression system for the server room. Which of the following would be the best choice?  **A.** Wet pipe **B.** Deluge **C.** Pre-action **D.** Halon |
|  | 67. | You are responsible for server room security for your company. You are concerned about physical theft of the computers. Which of the following would be best able to detect theft or attempted theft?  **A.** Motion sensor–activated cameras  **B.** Smart card access to the server rooms  **C.** Strong deadbolt locks for the server rooms  **D.** Logging everyone who enters the server room |
|  | 68. | Teresa has deployed session tokens on her network. These would be most effective against which of the following attacks?  **A.** DDoS **B.** Replay **C.** SYN flood **D.** Malware |
|  | 69. | . Hector is using infrared cameras to verify that servers in his datacenter are being properly racke**D.** Which of the following datacenter elements is he concerned about?  **A.** EMI blocking **B.** Humidity control **C.** Hot and cold aisles **D.** HVAC |
|  | 70. | Gerald is concerned about unauthorized people entering the company’s building. Which of the following would be most effective in preventing this? **A.** Alarm systems **B.** Fencing **C.** Cameras **D.** Security guards |
|  | 71. | Which of the following is the most important benefit from implementing SDN?  **A.** It will stop malware. **B.** It provides scalability.  **C.** It will detect intrusions. **D.** It will prevent session hijacking. |
|  | 72. | Mark is an administrator for a health care company. He has to support an older, legacy application. He is concerned that this legacy application might have vulnerabilities that would affect the rest of the network. What is the most efficient way to mitigate this?  **A.** Use an application container. **B.** Implement SDN.  **C.** Run the application on a separate VLAN.  **D.** Insist on an updated version of the application. |
|  | 73. | Lars is auditing the physical security of a company. The company uses chain-link fences on its perimeter. The fence is over pavement, not soft groun**D.** How close to the ground should the bottom of the fence be?  **A.** Touching the ground **B.** Within 4 inches  **C.** There is no standard for this. **D.** Within 2 inches |
|  | 74. | Mia has to deploy and support a legacy application. The configuration for this application and the OS it runs on are very specific and cannot be change**D.** What is the best approach for her to deploy this?  **A.** Use an immutable server. **B.** Use a VM.  **C.** Set permissions on the application so it cannot be change**D.**  **D.** Place the application on a separate VLAN. |
|  | 75. | To mitigate the impact of a software vendor going out of business, a company that uses vendor software should require which one of the following?  **A.** A detailed credit investigation prior to acquisition  **B.** A third-party source-code escrow  **C.** Substantial penalties for breach of contract  **D.** Standby contracts with other vendors |
|  | 76. | Abigail is responsible for datacenters in a large, multinational company. She has to support multiple datacenters in diverse geographic regions. What would be the most effective way for her to manage these centers consistently across the enterprise?  **A.** Hire datacenter managers for each center.  **B.** Implement enterprise-wide SDN.  **C.** Implement Infrastructure as Code (IaC).  **D.** Automate provisioning and deprovisioning. |
|  | 77. | Olivia is responsible for web application security for her company’s e-commerce server. She is particularly concerned about XSS and SQL injection. Which technique would be most effective in mitigating these attacks?  **A.** Proper error handling **B.** The use of stored procedures  **C.** Proper input validation **D.** Code signing |
|  | 78. | Sophia wants to test her company’s web application to see if it is handling input validation and data validation properly. Which testing method would be most effective for this?  **A.** Static code analysis **B.** Fuzzing **C.** Baselining **D.** Version control |
|  | 79. | Omar is using the waterfall method for software development in his company. Which of the following is the proper sequence for the waterfall method?  **A.** Requirements, design, implementation, testing, deployment, maintenance **B.** Planning, designing, coding, testing, deployment  **C.** Requirements, planning, designing, coding, testing, deployment  **D.** Design, coding, testing, deployment, maintenance |
|  | 80. | Lilly is responsible for security on web applications for her company. She is checking to see that all applications have robust input validation. What is the best way to implement validation?  **A.** Server-side validation **B.** Client-side validation  **C.** Validate in transit **D.** Client-side and server-side validation |
|  | 81. | Edward is responsible for web application security at a large insurance company. One of the applications that he is particularly concerned about is used by insurance adjusters in the fiel**D.** He wants to have strong authentication methods to mitigate misuse of the application. What would be his best choice?  **A.** Authenticate the client with a digital certificate.  **B.** Implement a very strong password policy.  **C.** Secure application communication with TLS.  **D.** Implement a web application firewall (WAF). |
|  | 82. | . Sarah is the CIO for a small company. The company uses several custom applications that have complicated interactions with the host operating system. She is concerned about ensuring that systems on her network are all properly patche**D.** What is the best approach in her environment?  **A.** Implement automatic patching.  **B.** Implement a policy that has individual users patch their systems.  **C.** Delegate patch management to managers of departments so they can find the best patch management for their departments.  **D.** Immediately deploy patches to a test environment, then as soon as testing is complete have a staged rollout to the network. |
|  | 83. | John is examining the logs for his company’s web applications. He discovers what he believes is a breach. After further investigation, it appears as if the attacker executed code from one of the libraries the application uses, code that is no longer even used by the application. What best describes this attack?  **A.** Buffer overflow **B.** Code reuse attack  **C.** DoS attack **D.** Session hijacking |
|  | 84. | Emiliano is a network administrator and is concerned about the security of peripheral devices. Which of the following would be a basic step he could take to improve security for those devices?  **A.** Implement FDE.  **B.** Turn off remote access (SSH, telnet, et**C.**) if not neede**D.**  **C.** Utilize fuzzy testing for all peripherals.  **D.** Implement digital certificates for all peripherals. |
|  | 85. | Ixxia is a software development team manager. She is concerned about memory leaks in code. What type of testing is most likely to find memory leaks?  **A.** Fuzzing **B.** Stress testing **C.** Static code analysis **D.** Normalization |
|  | 86. | Victor is a network administrator for a medium-sized company. He wants to be able to access servers remotely so that he can perform small administrative tasks from remote locations. Which of the following would be the best protocol for him to use?  **A.** SSH **B.** Telnet **C.** RSH **D.** SNMP |
|  | 87. | . Mark is responsible for a server that runs sensitive software for a major research facility. He is very concerned that only authorized software execute on this server. He is also concerned about malware masquerading as legitimate, authorized software. What technique would best address this concern?  **A.** Secure boot **B.** Software attestation **C.** Sandboxing **D.** TPM |
|  | 88. | Hannah is a programmer with a large software company. She is interested in ensuring that the module she just created will work well with a module created by another program. What type of testing is this?  **A.** Unit testing **B.** Regression testing  **C.** Stress testing **D.** Integration testing |
|  | 89. | Erik is responsible for the security of a SCADA system. Availability is a critical issue. Which of the following is most important to implement?  **A.** SIEM **B.** IPS **C.** Automated patch control **D.** Honeypot |
|  | 90. | You are concerned about the security of new devices your company has implemente**D.** Some of these devices use SoC technology. What would be the best security measure you could take for these?  **A.** Using a TPM **B.** Ensuring each has its own cryptographic key  **C.** Using SED **D.** Using BIOS protection |
|  | 91. | Vincent works for a company that manufactures portable medical devices, such as insulin pumps. He is concerned about ensuring these devices are secure. Which of the following is the most important step for him to take?  **A.** Ensure all communications with the device are encrypte**D.**  **B.** Ensure the devices have FDE.  **C.** Ensure the devices have individual antimalware.  **D.** Ensure the devices have been fuzz teste**D.** |
|  | 92. | Emile is concerned about securing the computer systems in vehicles. Which of the following vehicle types has significant cybersecurity vulnerabilities?  **A.** UAV **B.** Automobiles **C.** Airplanes **D.** All of the above |
|  | 93. | Ariel is responsible for software development in her company. She is concerned that the software development team integrate well with the network system. She wants to ensure that software development processes are aligned with the security needs of the entire network. Which of the following would be most important for her to implement?  **A.** Integration testing **B.** Secure DevOps  **C.** Clear policies **D.** Employee training |
|  | 94. | Greg is a programmer with a small company. He is responsible for the web application. He has become aware that one of the modules his web application uses may have a security flaw allowing an attacker to circumvent authentication. There is an update available for this module that fixes the flaw. What is the best approach for him to take to mitigate this threat?  **A.** Submit an RF**C.** **B.** Immediately apply the update.  **C.** Place the update on a test server, then if it works apply it to the production server.  **D.** Document the issue. |
|  | 95. | You are using a sophisticated system that models various attacks on your networks. You intend for this system to help your team realize weak areas and improve response to incidents. What is the most important step to take before relying on data from this system?  **A.** Get approval from a CA**B.**  **B.** Thoroughly review the systems documentation.  **C.** Verify the models being use**D.**  **D.** Perform integration testing on the system. |
|  | 96. | Your company has an accounting application that was developed in-house. It has been in place for 36 months, and functioning very well, with very few issues. You have just made a minor change to the tax calculation based on a change in tax law. What should be your next step?  **A.** Deploy the change. **B.** Get CAB approval for the change.  **C.** Perform stress testing. **D.** Perform regression testing. |
|  | 97. | Tom works as a software development manager for a large company. He is trying to explain to management the difference between compiled code and runtime code. What is the biggest advantage of compiled code?  **A.** Better performance **B.** Platform independence  **C.** More secure **D.** Faster development time |
|  | 98. | Your company is interested in keeping data in the clou**D.** Management feels that public clouds are not secure but is concerned about the cost of a private clou**D.** What is the solution you would recommend?  **A.** Tell them there are no risks with public clouds.  **B.** Tell them they will have to find a way to budget for a private clou**D.**  **C.** Suggest that they consider a community clou**D.**  **D.** Recommend against a cloud solution at this time. |
|  | 99. | Your development team primarily uses Windows, but they need to develop a specific solution that will run on Linux. What is the best solution to getting your programmers access to Linux systems for development and testing?  **A.** Set their machines to dual-boot Windows and Linux. **B.** PaaS  **C.** Set up a few Linux machines for them to work with as neede**D.** **D.** IaaS |
|  | 100. | Daniel works for a mid-sized financial institution. The company has recently moved some of its data to a cloud solution. Daniel is concerned that the cloud provider may not support the same security policies as the company’s internal network. What is the best way to mitigate this concern?  **A.** Implement a cloud access security broker. **B.** Perform integration testing.  **C.** Establish cloud security policies. **D.** Implement Security as a Service. |
|  | 101. | Hanz is responsible for the e-commerce servers at his company. He is concerned about how they will respond to a DoS attack. Which software testing methodology would be most helpful in determining this?  **A.** Regression testing **B.** Stress testing  **C.** Integration testing **D.** Fuzz testing |
|  | 102. | You are the CIO for a small company. The company wants to use cloud storage for some of its data, but cost is a major concern. Which of the following cloud deployment models would be best?  **A.** Community cloud **B.** Private cloud **C.** Public cloud **D.** Hybrid cloud |
|  | 103. | Alisha is monitoring security for a mid-sized financial institution. Under her predecessor there were multiple high-profile breaches. Management is very concerned about detecting any security issues or breach of policy as soon as possible. Which of the following would be the best solution for this?  **A.** Monthly audits **B.** NIPS **C.** NIDS **D.** Continuous monitoring |
|  | 104. | Helga works for a bank and is responsible for secure communications with the online banking application. The application uses TLS to secure all customer communications. She has noticed that since migrating to larger encryption keys, the server’s performance has decline**D.** What would be the best way to address this issue?  **A.** Implement a VPN concentrator. **B.** Implement an SSL accelerator.  **C.** Return to smaller encryption keys. **D.** Upgrade all servers. |
|  | 105. | What is the primary advantage of allowing only signed code to be installed on computers?  **A.** It guarantees that malware will not be installe**D.**  **B.** It improves patch management.  **C.** It verifies who created the software.  **D.** It executes faster on computers with a TPM. |
|  | 106. | Which of the following is the best description for VM sprawl?  **A.** When VMs on your network outnumber physical machines  **B.** When there are more VMs than IT can effectively manage  **C.** When a VM on a computer begins to consume too many resources  **D.** When VMs are spread across a wide area network |
|  | 107. | Which of the following is the best description of a stored procedure?  **A.** Code that is in a DLL, rather than the executable  **B.** Server-side code that is called from a client  **C.** SQL statements compiled on the database server as a single procedure that can be called  **D.** Procedures that are kept on a separate server from the calling application, such as in middleware |
|  | 108. | Farès is responsible for security at his company. He has had bollards installed around the front of the building. What is Farès trying to accomplish?  **A.** Gated access for people entering the building  **B.** Video monitoring around the building  **C.** Protecting against EMI  **D.** Preventing a vehicle from being driven into the building |
|  | 109. | Jane is concerned about servers in her datacenter. She is particularly worried about EMI. What damage might EMI most likely cause to servers?  **A.** Damage to chips (CPU or RAM) **B.** Temperature control issues  **C.** Malware infections **D.** The staff could be locked out of the servers. |
|  | 110. | You are concerned about VM escape attacks. Which of the following would provide the most protection against this?  **A.** Completely isolate the VM from the host.  **B.** Install a host-based antivirus on both the VM and the host.  **C.** Implement FDE on both the VM and the host.  **D.** Use a TPM on the host. |
|  | 111. | Teresa is the network administrator for a small company. The company is interested in a robust and modern network defense strategy but lacks the staff to support it. What would be the best solution for Teresa to use?  **A.** Implement SDN. **B.** Use automated security.  **C.** Use Security as a Service.  **D.** Implement only as much security controls as they can support. |
|  | 112. | Dennis is trying to set up a system to analyze the integrity of applications on his network. He wants to make sure that the applications have not been tampered with or Trojane**D.** What would be most useful in accomplishing this goal?  **A.** Implement NIPS. **B.** Use cryptographic hashes.  **C.** Sandbox the applications in question. **D.** Implement NIDS. |
|  | 113. | George is a network administrator at a power plant. He notices that several turbines had unusual ramp-ups in cycles last week. After investigating, he finds that an executable was uploaded to the system control console and caused this. Which of the following would be most effective in preventing this from affecting the SCADA system in the future?  **A.** Implement SDN. **B.** Improve patch management.  **C.** Place the SCADA system on a separate VLAN.  **D.** Implement encrypted data transmissions. |
|  | 114. | Tom is responsible for VPN connections in his company. His company uses IPSec for VPNs. What is the primary purpose of AH in IPSec?  **A.** Encrypt the entire packet. **B.** Encrypt just the header.  **C.** Authenticate the entire packet. **D.** Authenticate just the header. |
|  | 115. | Mia is a network administrator for a bank. She is responsible for secure communications with her company’s customer website. Which of the following would be the best for her to implement?  **A.** SSL **B.** PPTP **C.** IPSec **D.** TLS |
|  | 116. | Abigail is responsible for setting up an NIPS on her network. The NIPS is located in one particular network segment. She is looking for a passive method to get a copy of all traffic to the NIPS network segment so that it can analyze the traffi**C.** Which of the following would be her best choice?  **A.** Using a network tap **B.** Using port mirroring  **C.** Setting the NIPS on a VLAN that is connected to all other segments  **D.** Setting up an NIPS on each segment |
|  | 117. | Janice is explaining how IPSec works to a new network administrator. She is trying to explain the role of IKE. Which of the following most closely matches the role of IKE in IPSec?  **A.** It encrypts the packet. **B.** It establishes the SAs.  **C.** It authenticates the packet. **D.** It establishes the tunnel. |
|  | 118. | . Jeff is the security administrator for an e-commerce site. He is concerned about DoS attacks. Which of the following would be the most effective in addressing this?  **A.** DDoS mitigator **B.** WAF with SPI  **C.** NIPS **D.** Increased available bandwidth |
|  | 119. | Doug is a network administrator for a small company. The company has recently implemented an e-commerce server. This has placed a strain on network bandwidth. What would be the most cost-effective means for him to address this issue?  **A.** Isolate the new server on a separate network segment.  **B.** Upgrade the network to CAT 7.  **C.** Move to fiber opti**C.** **D.** Implement aggregation switches. |
|  | 120. | Liam is responsible for monitoring security events in his company. He wants to see how diverse events may connect. He is interested in identifying different indicators of compromise that may point to the same breach. Which of the following would be most helpful for him to implement?  **A.** NIDS **B.** SIEM **C.** Correlation engine **D.** Aggregation switch |
|  | 121. | Emily manages the IDS/IPS for her network. She has an NIPS installed and properly configure**D.** It is not detecting obvious attacks on one specific network segment. She has verified that the NIPS is properly configured and working properly. What would be the most efficient way for her to address this?  **A.** Implement port mirroring for that segment.  **B.** Install an NIPS on that segment.  **C.** Upgrade to a more effective NIPS.  **D.** Isolate that segment on its own VLAN. |
|  | 122. | You have been instructed to find a VPN solution for your company. Your company uses TACACS+ for remote access. Which of the following would be the best VPN solution for your company?  **A.** PPTP **B.** RADIUS **C.** L2TP **D.** CHAP |
|  | 123. | Jacob is the CIO for a mid-sized company. His company has very good security policies and procedures. The company has outsourced its web application development to a wellknown web programming company. Which of the following should be the most important security issue for Jacob to address? **A.** The web application vendor’s hiring practices  **B.** The financial stability of the web application vendor  **C.** Security practices of the web application vendor  **D.** Having an escrow for the source code |
|  | 124. | Gerard is responsible for physical security at his company. He is considering using cameras that would detect a burglar entering the building at night. Which of the following would be most useful in accomplishing this goal?  **A.** Motion-sensing camera **B.** Infrared-sensing camera  **C.** Sound-activated camera **D.** HD camera |
|  | 125. | Tim is implementing a Faraday cage around his server room. What is the primary purpose of a Faraday cage?  **A.** Regulate temperature **B.** Regulate current  **C.** Block intrusions **D.** Block EMI |
|  | 126. | You are working for a large company. You are trying to find a solution that will provide controlled physical access to the building and record every employee who enters the building. Which of the following would be the best for you to implement?  **A.** A security guard with a sign-in sheet **B.** Smart card access  **C.** A camera by the entrance **D.** A sign-in sheet by the front door |
|  | 127. | David is responsible for cryptographic keys in his company. What is the best way to deauthorize a public key?  **A.** Send out a network alert. **B.** Delete the digital certificate.  **C.** Publish that certificate in the CRL. **D.** Notify the R**A.** |
|  | 128. | Thomas is trying to select the right fire extinguisher for his company’s server room. Which of the following would be his best choice?  **A.** Type A **B.** Type B **C.** Type C **D.** Type D |
|  | 129. | Carole is concerned about security for her server room. She wants the most secure lock she can find for the server room door. Which of the following would be the best choice for her?  **A.** Combination lock **B.** Key-in-knob **C.** Deadbolt **D.** Padlock |
|  | 130. | What is the ideal humidity range for a server room?  **A.** 70% to 80% **B.** 40% to 60% **C.** Below 30% **D.** Above 70% |
|  | 131. | Molly is implementing biometrics in her company. Which of the following should be her biggest concern? **A.** FAR **B.** FRR **C.** CER **D.** EER |
|  | 132. | Daniel is responsible for physical security in his company. All external doors have electronic smart card access. In an emergency such as a power failure, how should the doors fail?  **A.** Fail secure **B.** Fail closed **C.** Fail open **D.** Fail locked |
|  | 133. | Donald is responsible for networking for a defense contractor. He is concerned that emanations from UTP cable could reveal classified information. Which of the following would be his most effective way to address this?  **A.** Migrate to CAT 7 cable. **B.** Implement protected cabling.  **C.** Place all cable in a Faraday cage.  **D.** Don’t send any classified information over the cable. |
|  | 134. | Fred is responsible for physical security in his company. He wants to find a good way to protect the USB thumb drives that have BitLocker keys stored on them. Which of the following would be the best solution for this situation?  **A.** Store the drives in a secure cabinet. **B.** Encrypt the thumb drives.  **C.** Don’t store BitLocker keys on these drives.  **D.** Lock the thumb drives in desk drawers. |
|  | 135. | Juanita is responsible for servers in her company. She is looking for a fault-tolerant solution that can handle two drives failing. Which of the following should she select? **A.** RAID 1+0 **B.** RAID 3 **C.** RAID 5 **D.** RAID 6 |
|  | 136. | You are a network administrator for a mid-sized company. You need all workstations to have the same configuration. What would be the best way for you to accomplish this?  **A.** Push out a configuration file.  **B.** Implement a policy requiring all workstations to be configured the same way.  **C.** Ensure all computers have the same version of the operating system and the same applications installe**D.**  **D.** Use a master image that is properly configured and image all workstations from that. |
|  | 137. | Mike is a network administrator for an e-commerce company. There have been several updates to the operating system, the web server software, and the web application, all within the last 24 hours. It appears that one of these updates has caused a significant security problem. What would be the best approach for Mike to take to correct this problem?  **A.** Remove the updates one at a time to see which corrects the problem.  **B.** Roll the server back to the last known good state.  **C.** Investigate and find out which update caused the problem, and remove only that update.  **D.** Investigate and find out which update caused the problem, and find a patch for that issue. |
|  | 138. | Which device would most likely process the following rules?  PERMIT IP ANY EQ 443 DENY IP ANY ANY  **A.** NIPS **B.** HIPS **C.** Content filter **D.** Firewall |
|  | 139. | Ixxia is responsible for security at a mid-sized company. She wants to prevent users on her network from visiting job-hunting sites while at work. Which of the following would be the best device to accomplish this goal?  **A.** Proxy server **B.** NAT **C.** Firewall **D.** NIPS |
|  | 140. | You are responsible for an e-commerce site. The site is hosted in a cluster. Which of the following techniques would be best in assuring availability?  **A.** A VPN concentrator **B.** Aggregate switching  **C.** An SSL accelerator **D.** Load balancing |
|  | 141. | When you are concerned about application security, what is the most important issue in memory management?  **A.** Never allocate a variable any larger than is neede**D.**  **B.** Always check bounds on arrays.  **C.** Always declare a variable where you need it (i.e., at function or file level if possible).  **D.** Make sure you release any memory you allocate. |
|  | 142. | Darrel is looking for a cloud solution for his company. One of the requirements is that the IT staff can make the transition with as little change to the existing infrastructure as possible. Which of the following would be his best choice?  **A.** Off-premises cloud **B.** On-premises cloud  **C.** Hybrid solution **D.** Use only a community cloud |
|  | 143. | Ryan is concerned about the security of his company’s web application. Since the application processes confidential data, he is most concerned about data exposure. Which of the following would be the most important for him to implement? **A.** WAF **B.** TLS **C.** NIPS **D.** NIDS |
|  | 144. | Arjun has just taken over web application security for a small company. He notices that some values are temporarily stored in hidden fields on one of the web pages. What is this called and how would it be best characterized?  **A.** This is obfuscation, a weak security measure.  **B.** This is data hiding, a weak security measure.  **C.** This is obfuscation, a possible security flaw.  **D.** This is data hiding, a possible security flaw. |
|  | 145. | What is the primary reason a company would consider implementing Agile programming?  **A.** To speed up development time  **B.** To improve development documentation  **C.** To focus more on design **D.** To focus more on testing |
|  | 146. | When you’re implementing security cameras in your company, which of the following is the most important concern?  **A.** High-definition video **B.** Large storage capacity  **C.** How large an area the camera can cover  **D.** Security of the camera and video storage |
|  | 147. | What is the primary security issue presented by monitors?  **A.** Unauthorized users may see confidential dat**A.**  **B.** Data can be detected from electromagnetic emanations.  **C.** Poor authentication **D.** Screen burn |
|  | 148. | Clark is responsible for mobile device security in his company. Which of the following is the most important security measure for him to implement?  **A.** Encrypted drives **B.** Patch management  **C.** Remote wiping **D.** Geotagging |
|  | 149. | Which of the following security measures is most effective against phishing attacks? **A.** User training **B.** NIPS **C.** Spam filters **D.** Content filter |
|  | 150 | You are the CISO for a mid-sized health care company. Which of the following is the most important for you to implement?  **A.** Industry best practices **B.** Contractual requirements  **C.** Strong security policies **D.** Regulatory requirements |