|  |  |  |
| --- | --- | --- |
| 第一章 | | |
| 答案 | 編號 | 題目 |
| A | 1 | You are using encryption technology in an attempt to protect a file containing customer credit card numbers from unauthorized access.  What information security goal are you pursuing?  A. Confidentiality  B. Integrity  C. Disclosure  D. Availability |
| D | 2 | You are performing a risk assessment of an organization and decide that the likelihood of a particular risk materializing is “low.”  What type of risk assessment are you performing?  A. Operational  B. Quantitative  C. Technical  D. Qualitative |
| A | 3 | You are conducting a quantitative risk assessment for an organization to identify the risk of a fire in a data center. The data center is valued at $10 million and you expect a fire to occur once every 50 years that will damage three-quarters of the data center (including equipment).  What is your exposure factor?  A. 75 percent  B. 10 percent  C. 50 percent  D. 25 percent |
| D | 4 | You are conducting a quantitative risk assessment for an organization to identify the risk of a fire in a data center. The data center is valued at $10 million and you expect a fire to occur once every 50 years that will damage three-quarters of the data center (including equipment).  What is your annualized loss expectancy?  A. 75 percent  B. $7.5 million  C. 0.02  D. $150,000 |
| C | 5 | You are evaluating methods to manage the risk posed to your organization by hackers and decide that you will pursue a strategy of aggressively prosecuting anyone who attempts to break into your systems.  What risk management strategy are you implementing?  A. Risk mitigation  B. Risk transference  C. Risk deterrence  D. Risk acceptance |
| D | 6 | You are conducting a lessons-learned session to identify gaps in your response to an information security incident. What phase in the incident response life cycle are you participating in?  A. Preparation  B. Detection and analysis  C. Containment, eradication, and recovery  D. Post-incident activity |
| 第二章 | | |
| 答案 | 編號 | 題目 |
| C | 1 | If your organization wants to monitor for attacks but is worried about possible outages if your network traffic is accidentally blocked,  what technology should you deploy?  A. A sniffer  B. An IPS  C. An IDS  D. A firewall |
| D | 2 | A firewall that can block traffic based only on the IP address, protocol, or port that traffic is sent to is what type of firewall?  A. A stateful firewall  B. A host firewall  C. A network firewall  D. A packet filter |
| D | 3 | Which of the following network devices connects two networks and sends traffic to the appropriate network based on its destination?  A. A switch  B. A firewall  C. An IPS D.  A router |
| A | 4 | If you wanted to use a proxy to send traffic directly in an unmodified form to its destination, what type of proxy would you use?  A. A gateway  B. A reverse tunneling proxy  C. A reverse proxy  D. A side-to-side proxy |
| D | 5 | An attack on a device that fills the device’s CAM table, making it send traffic to every port, is an attack against what type of device?  A. A firewall  B. A router  C. A packet filter  D. A switch |
| C | 6 | What type of network security tool would you use to manually inspect traffic?  A. An IDS  B. An IPS  C. A sniffer  D. A firewall |
| 第三章 | | |
| 答案 | 編號 | 題目 |
| B | 1 | What major issue led to the creation of IPv6?  A. IPv4 was vulnerable to attacks.  B. IPv4 address space was limited to 4.3 billion addresses.  C. IPv5 was updated.  D. Major vendors released the new version to add additional networking features. |
| C | 2 | Which protocol uses a three-way handshake to establish sessions?  A. ICMP  B. IPsec  C. TCP  D. UDP |
| D | 3 | What advantage does an IPsec VPN have over an SSL or TLS VPN?  A. IPsec VPNs work with IPv6.  B. IPsec VPN devices are less expensive.  C. An IPsec VPN can be established by using a web browser.  D. IPsec VPNs can tunnel all traffic from a system. |
| A | 4 | What ports do SSH, HTTP, and NetBIOS use?  A. 22, 80, 137–139, and 445  B. 21, 88, and 443  C. 22, 8080, 123, and 443  D. 1024, 4000, and 8888 |
| A | 5 | What technology is frequently used for secure remote access to networks?  A. VPN  B. Routers  C. 802.1x  D. IPv6 |
| C | 6 | . If you want to outsource an entire Linux server without having to install the operating system itself to the cloud, what type of cloud service would you look for?  A. IaaS  B. SaaS  C. PaaS  D. BaaS |
| D | 7 | What are the rules routers use to restrict the flow of traffic through them?  A. Port security  B. VLANs  C. PEAP  D. ACLs |
| B | 8 | What switch security tool can help you limit the systems that can connect to a specified port based on the hardware MAC address of the system?  A. VLANs  B. Port security  C. Flood guards  D. 802.1x |
| 第四章 | | |
| 答案 | 編號 | 題目 |
| A | 1 | Richard is the director of information security for A.  Datum Corporation. He is developing a set of documents that will guide the organization’s information security efforts and is working on language that will require the use of appropriate network security controls. He wants to describe the specific models of firewall that are authorized for use within the organization. He expects to add and remove models from this list every few months and needs to create a document that is mandatory but can be easily changed. What type of document would be best suited for Richard’s needs?  A. Standard  B. Policy  C. Guideline  D. Procedure |
| B | 2 | Renee is an information security professional for a retail business that accepts credit cards at several locations around the country. She is concerned about the compliance obligations that her firm might have when handling payment card transactions. What regulation governs the storage, processing, and transmission of credit card information?  A. COPPA  B. PCI DSS  C. SOX  D. HIPAA |
| D | 3 | Matthew is designing a password security poster as part of his company’s information security awareness program. Which one of the following is NOT a password best practice that he might include on his poster?  A. Use different passwords for each website you visit.  B. Use long, complex passwords.  C. Change passwords regularly.  D. Store shared passwords in a secure location |
| C | 4 | Christopher is verifying that the temperature in his data center is within the standard acceptable range, as recommended by ASHRAE. Which one of the following temperatures is within ASHRAE’s extended environmental envelope?  A. 52 degrees Fahrenheit  B. 62 degrees Fahrenheit  C. 72 degrees Fahrenheit  D. 82 degrees Fahrenheit |
| D | 5 | Darcy is reviewing the disaster recovery plan for an organization and would like to know the amount of time that the organization believes it will take to restore a critical technology function.  What metric should Darcy review?  A. MTO  B. RPO  C. MTBF  D. RTO |
| C | 6 | Samantha would like to configure RAID 5, disk striping with distributed parity, to preserve information in the event of a disk failure. What is the minimum number of disks that she must use to implement RAID 5?  A. One  B. Two  C. Three  D. Five |
| 第五章 | | |
| 答案 | 編號 | 題目 |
| A | 1 | Which type of malware spreads itself through a network by exploiting services and systems?  A. Worms  B. Adware  C. Trojans  D. Viruses |
| C | 2 | What type of injection attack often uses logic to attack databases?  A. Command injection  B. Header injection  C. SQL injection  D. LDAP injection |
| D | 3 | Attacks that occur before the vulnerability they exploit is announced are known as what type of attack?  A. Unpatched attacks  B. Zombie attacks  C. Injection attacks  D. Zero-day attacks |
| D | 4 | Which attack is most likely after an attacker has captured authentication session information crossing your network?  A. Spoofing  B. A smurf attack  C. ARP poisoning  D. A replay attack |
| C | 5 | What is a fake wireless network access point that appears to be legitimate called?  A. A rogue access point  B. A man-in-the-middle  C. An evil twin  D. A strange attractor |
| C | 6 | Targeted phishing attacks against specific organizations are known as what type of phishing?  A. Vishing  B. Whaling  C. Spear phishing  D. Pharming |
| 第六章 | | |
| 答案 | 編號 | 題目 |
| C | 1 | What is the difference between fail open and fail safe?  A. Fail open fails to a secure mode.  B. Fail safe is always the proper failure mode.  C. Fail safe fails to a secure mode.  D. Fail open is always the proper failure mode. |
| C | 2 | Which of the following techniques is not part of a typical hardening process?  A. Disabling unnecessary services and accounts  B. Protecting management interfaces  C. Upgrading the operating system  D. Changing default passwords |
| A | 3 | What security techniques can be used to prevent access to network ports by attackers?  A. MAC limiting, 802.1x, and disabling unused ports  B. BIOS passwords  C. Using a hardening standard and patching  D. ACLs and a SIEM |
| D | 4 | Which Windows log contains logon information?  A. The application log  B. The setup log  C. The system log  D. The security log |
| A | 5 | What type of physical access control system is designed to prevent attackers from following legitimate staff through to access a secure area?  A. A mantrap  B. Gates  C. Locks  D. Fences |
| B | 6 | What type of hardware lock uses codes to allow access and can be reprogrammed?  A. Preset  B. Cipher  C. Biometric  D. Multifactor |
| 第七章 | | |
| 答案 | 編號 | 題目 |
| D | 1 | A security tool that is designed to allow attackers to attack a simulated system and thatgathers information about the attackers’ tools and techniques is known as what?  A. A vulnerability detection system  B. A port scanner  C. A darknet  D. A honeypot |
| C | 2 | What type of vulnerability review focuses on how systems are put together?  A. A penetration test  B. A vulnerability scan  C. A design or architecture review  D. A code review |
| A | 3 | The potential that a threat will exploit vulnerabilities is known as what? A. A risk  B. A vulnerability  C. A threat  D. An exploit |
| D | 4 | The equation to calculate risk is:  A. Risk = Likelihood × Vulnerability  B. Risk = Impact × Vulnerability  C. Risk = Vulnerabilities × Threats  D. Risk = Likelihood × Impact |
| C | 5 | What type of penetration test provides partial visibility into the details of the environment to the testers?  A. Red box  B. White box  C. Gray box  D. Black box |
| A | 6 | What type of testing would you perform to identify services and accessible ports via a network?  A. A port scan  B. A penetration test  C. A vulnerability scan  D. A ping sweep |
| 第八章 | | |
| 答案 | 編號 | 題目 |
| B | 1 | Fuzz testing is used to send \_\_\_\_\_\_\_\_\_\_\_ input to a target in order to detect programming flaws.  A. Standard  B. Abnormal  C. Bounded  D. Predictable |
| C | 2 | Which of the following is not a typical element of SDLC with respect to secure coding concepts?  A. Design from a standpoint of implicit denial and the principle of least privilege.  B. Perform code reviews throughout the programming process.  C. Focus on completing the code on deadline in order to be first to market.  D. Sanitize output to minimize data loss or disclosure to unauthorized users |
| A | 3 | Which of the following is not considered a secure event in relation to error and exception handling?  A. Providing users with complete details of faults and errors as they are encountered  B. Controlling error messages to prevent fault disclosure to users  C. Creating a default fault-handling mechanism or response for the application to use rather than relying on the host operating system to handle failures  D. Recording error details into a log file for administrative use |
| C | 4 | Which of the following is not an example of input validation?  A. Escaping metacharacters  B. Performing input limit checks  C. Accepting arbitrary responses  D. Setting boundary and domain restrictions |
| D | 5 | Which of the following statements is true with respect to XSS?  A. An exceedingly large amount of data is sent to a vulnerable web server.  B. A client is tricked into clicking on a hyperlink, which takes the user to a spoofed version of a website. 312 CHAPTER 8 The importance of application security  C. Sessions encrypted with SSL/TLS (Secure Sockets Layer / Transport Layer Security) can be used to reduce the risk of XSS.  D. Attack code is sent to a vulnerable web server in order to plant altered content. This altered content is then sent to subsequent visitors, on whose systems the client-side execution of the injected malicious code takes effect. |
| B | 6 | An XSRF attack is able to bypass what common security mechanism by infiltrating the client before attacking a targeted server?  A. Input sanitization  B. TLS sessions  C. Hashed passwords  D. Auditing |
| A and D | 7 | Which of the following are potential solutions to eliminate or reduce XSRF vulnerabilities? [Select all that apply]  A. Use a challenge-response dialog.  B. Limit the length of input.  C. Set a time out on sessions.  D. Require a re-authentication process |
| C | 8 | Which of the following is not an element of application configuration baseline security management?  A. Crafting a written document  B. Making a digital image of a pilot system  C. Configuring access to external public wireless networks  D. Reviewing production systems for compliance |
| A | 9 | Which of the following is more likely to be an early step in the process of application hardening?  A. Installing updates and patches  B. Training users  C. Reviewing audit logs  D. Performing compliance testing |
| D | 10 | Which of the following is a part of application patch management?  A. Filtering abnormal input  B. Re-authenticating users  C. Ensuring a rollback path  D. Setting ingress filter rules |
| 第九章 | | |
| 答案 | 編號 | 題目 |
| D | 1 | Which operating system is inherently more secure than the others?  A. Windows  B. Linux  C. Macintosh  D. None |
| B | 2 | Which of the following is false?  A. All configuration settings should be customized for a specific environment.  B. The default settings of an operating system are often preferred.  C. Default settings are often designed with ease of use in mind.  D. Default settings are often insecure. |
| C | 3 | A typical malware scanner is unable to detect and prevent what type of unwanted activity?  A. Installation of spyware  B. Infection with a rootkit  C. An unauthorized user attempting to guess an account password  D. Compromise by a trojan |
| D | 4 | What platforms need anti-virus products?  A. Servers  B. Linux  C. Database hosts  D. All of the above |
| B | 5 | The biggest reason why is it unsafe to attempt to close a pop-up by using on-screen visible controls is what?  A. Social engineering  B. Malware infection  C. False advertising  D. Better deals on sales are available elsewhere |
| B | 6 | Which of the following is not a primary benefit or purpose of using patch management?  A. Minimizing the risk of downtime  B. Reducing administration responsibilities  C. Diminishing the threat of compromise  D. Reducing productivity loss due to bad or interfering code |
| D | 7 | What should not be kept in a locking cabinet?  A. Blank media  B. Replacement parts  C. Operating system and application installation disks  D. Private data of customers |
| A | 8 | What is an important goal of host software baselining?  A. Keeping systems in compliance with stated security policies  B. Reducing hardware failures  C. Training users  D. Implementing open-source software |
| C | 9 | Which of the following statements is false?  A. Mobile devices are more susceptible to loss or theft than traditional desktop or notebook computers.  B. The increasing BYOD (bring your own device) policies or freedoms offered by companies is a much bigger concern than most realize.  C. A screen lock is sufficient security against data loss in the event of a device theft.  D. Many tablets and audio players with Wi-Fi connectivity can run apps that enable voice and video call capabilities. |
| A | 10 | According to CompTIA, which type of mobile device security is the least likely to be on a mobile device?  A. Storage encryption  B. Remote wipe  C. GPS tracking  D. A screen lock |
| 第十章 | | |
| 答案 | 編號 | 題目 |
| C | 1 | Which of the following is the most common means of data loss or data leakage for organizations?  A. Sending out digitally signed email messages  B. Using social networks  C. Misplacing a USB drive  D. Working with open source software |
| B | 2 | What is the primary tool used to provide confidentiality protection for data on a storage device?  A. Multifactor authentication  B. Symmetric encryption  C. Detailed logging  D. Firewalls |
| D | 3 | What type of attack is designed to steal the master encryption key used by full-disk encryption directly from memory?  A. Birthday attack  B. Buffer overflow attack  C. XSRF attack  D. Cold boot attack |
| C | 4 | Which of the following is a true statement?  A. Full-disk encryption requires a TPM be present on the system’s motherboard.  B. Only file encryption is transparent to the end user.  C. Encryption is not a substitute for a backup.  D. Disk encryption provides protection against all forms of data leakage attacks. |
| A | 5 | What is the purpose of implementing an HSM in support of database encryption?  A. Performing centralized key management  B. Managing time-stamp expiration  C. Tracking user privileges and permissions  D. Securing data destruction |
| C | 6 | Where or how are encryption keys stored or managed for individual file encryption?  A. On a master per-user key ring  B. In a hashing table  C. By using a digital envelope on the encrypted file  D. In a local database |
| D | 7 | Which of the following is not a valid means by which to have encrypted data stored on USB devices?  A. Software-controlled file encryption  B. Full-disk encryption  C. Hardware-provided on-device encryption  D. Session encryption |
| C | 8 | Which of the following statements is false?  A. BYOD still requires organizations to establish mobile device security and use policies.  B. A mobile device connected to a computer often can be used as an external or portable storage device.  C. An organizational ban on mobile devices removes all threats and risks associated with those devices.  D. A mobile phone can provide an unfiltered Internet link for company computers |
| B | 9 | Which of the following is not a typical function of a TPM?  A. Encryption key storage  B. Revocation service  C. Random number generation  D. Crafting of a non-forgeable identity reference of hardware |
| D | 10 | Which of the following is not true in regard to an HSM?  A. Some HSMs have PCI interfaces.  B. HSMs provide for accelerated encryption computation.  C. Proprietary forms of HSM are used in specialty situations, such as ATMs, point-ofsale devices (credit card terminals), and smart card readers.  D. HSMs are commonly found as components on most off-the-shelf motherboards. |
| 第十一章 | | |
| 答案 | 編號 | 題目 |
| D | 1 | A token is what type of authenticator?  A. Something you are  B. Something you know  C. Biometric D  . Something you have |
| B | 2 | An access control system that relies on users to set rights uses what model?  A. MAC  B. DAC  C. RBAC  D. ABAC |
| D | 3 | Mandatory vacations help detect what?  A. Least privilege  B. Mandatory access control  C. Inappropriate privileges  D. Fraud |
| C | 4 | . Privilege management that provides privileges based on a person’s job role and responsibilities in the organization is known as what?  A. User-based privilege management  B. Group-based privilege management  C. Role-based privilege management  D. Mandatory privilege management |
| B | 5 | Which authentication protocol uses the concept of a ticket that is issued to a user’s workstation?  A. Active Directory Domain Services  B. The Kerberos protocol  C. TACACS+  D. LDAP |
| C | 6 | The US government uses what type of token to identify its employees? A. A biometric token  B. A CAC  C. A PIV card  D. A USB token |
| 第十二章 | | |
| 答案 | 編號 | 題目 |
| A | 1 | Matthew is preparing a purchase order system for his company and wants to use cryptographic technology that would allow the company to prove in court that the originator of a purchase order actually created the order and that it was not forged.  What goal of cryptography is Matthew trying to achieve?  A. Nonrepudiation  B. Confidentiality  C. Authentication  D. Integrity |
| B | 2 | Alice would like to send a message to Bob by using asymmetric cryptography. She wants to ensure that only Bob is able to decrypt the message.  What key should she use for the encryption?  A. Alice’s public key  B. Bob’s public key  C. Alice’s private key  D. Bob’s private key |
| D | 3 | Jim is planning an encryption system to protect sensitive data in his organization. He would like to use the Advanced Encryption Standard (AES) and is considering the best key length to use.  Which one of the following is not an acceptable key length supported by AES?  A. 128 bits  B. 192 bits  C. 256 bits  D. 512 bits |
| C | 4 | Christopher received a message from Richard that contains a digital signature. When Christopher wants to verify the digital signature, what key should he use to decrypt it?  A. Christopher’s public key  B. Christopher’s private key  C. Richard’s public key  D. Richard’s private key |
| D | 5 | Darcy would like to create a digital certificate to enable TLS encryption on her website. What type of organization must she contact to obtain a valid digital certificate that will be automatically accepted by the web browsers of her users?  A. SSH  B. ESP  C. CRL  D. CA |
| C | 6 | Ryan is selecting an authentication protocol to secure client/server communications on his network. Which one of the following protocols is best suited to provide this security?  A. MS-CHAP  B. PAP  C. CHAP  D. NTLMv1 |