**崑山科技大學資工系IPAS證照輔導班 練習**

**名稱:** *Practice Test*

|  |  |  |
| --- | --- | --- |
|  | | |
| 答案 | 編號 | 題目 |
|  | 1. | You are asked to separate the Sales and Marketing department’s network traffic on a layer 2 device within a LAN. This will reduce broadcast traffic and prevent the departments from seeing each other’s resources. Which of the following types of network design would be the best choice?  A. MAC　 　B. NAT 　　C. VLAN 　　D. DMZ |
|  | 2. | You are a network administrator and your company has asked you to perform a survey of the campus for open Wi-Fi access points. You walk around with your smartphone looking for unsecured access points that you can connect to without a password. What type of penetration testing concept is this called?  A. Escalation of privilege 　　　B. Active reconnaissance  C. Passive reconnaissance 　　 D. Black-box |
|  | 3. | Which of the following is a certificate-based authentication that allows individuals access to U.S. federal resources and facilities?  A. Proximity card B. TOTP C. PIV card D. HOTP |
|  | 4. | You attempt to log into your company’s network with a laptop. The laptop is quarantined to a restricted VLAN until the laptop’s virus definitions are updated. Which of the following best describes this network component?  A. NAT 　　B. HIPS 　　C. DMZ 　　D. NAC |
|  | 5. | You have been asked to implement a security control that will limit tailgating in highsecured areas. Which of the following security control would you choose?  A. Mantrap　　 B. Faraday cage 　　C. Airgap 　　D. Cable locks |
|  | 6. | Your company’s network administrator is placing an Internet web server in an isolated area of the company’s network for security purposes. Which of the following architecture concepts is the network administrator implementing?  A. Honeynet 　　B. DMZ　　C. Proxy 　　D. Intranet |
|  | 7. | Your company is offering a new product on its website. You are asked to ensure availability of the web server when it receives a large number of requests. Which of the following would be the best option to fulfill this request?  A. VPN concentrator　　 B. NIPS 　　C. SIEM 　　D. Load balancer |
|  | 8. | You are a security administrator for a manufacturing company that produces compounded medications. To ensure individuals are not accessing sensitive areas where the medications are created, you want to implement a physical security control. Which of the following would be the best option?  A. Security guard　　 B. Signs 　　C. Faraday cage　　 D. Cameras |
|  | 9. | An attacker exploited a bug, unknown to the developer, to gain access to a database server. Which of the following best describes this type of attack?  A. Zero-day 　　　　　 　 B. Cross-site scripting  C. ARP poisoning 　　　 　D. Domain hijacking |
|  | 10. | A new employee added network drops to a new section of the company’s building. The cables were placed across several fluorescent lights. When users attempted to connect to the data center on the network, they experienced intermittent connectivity. Which of the following environmental controls was the most likely cause of this issue?  A. DMZ 　B. EMI 　　C. BIOS 　　D. TPM |
|  | 11. | What method should you choose to authenticate a remote workstation before it gains access to a local LAN?  A. Router 　　B. Proxy server 　C. VPN concentrator 　D. Firewall |
|  | 12. | Which of the following allows a company to store a cryptographic key with a trusted third party and release it only to the sender or receiver with proper authorization?  A. CRL 　　B. Key escrow 　　C. Trust model 　D. Intermediate CA |
|  | 13. | Your company recently upgraded the HVAC system for its server room. Which of the following security implications would the company be most concerned about?  A. Confidentiality 　B. Availability 　C. Integrity 　　D. Airgap |
|  | 14. | Your company provides secure wireless Internet access to visitors and vendors working onsite. Some of the vendors are reporting they are unable to view the wireless network. Which of the following best describes the issue?  A. MAC filtering is enabled on the WAP.  B. The SSID broadcast is disabled.  C. The wrong antenna type is being used.  D. The wrong band selection is being used. |
|  | 15. | Your company’s sales team is working late at the end of the month to ensure all sales are reported for the month. The sales members notice they cannot save or print reports after regular hours. Which of the following general concepts is preventing the sales members from performing their job?  A. Job rotation 　　　　　B. Time-of-day restrictions  C. Least privilege 　　　　D. Location-based policy |
|  | 16. | Which of the following symmetric algorithms are block ciphers? (Choose three.)  A. 3DES 　B. ECDHE 　C. RSA 　D. RC4 　E. SHA 　F. Twofish |
|  | 17. | A security officer has asked you to use a password cracking tool on the company’s computers. Which of the following best describes what the security officer is trying to accomplish?  A. Looking for strong passwords  B. Enforcing a minimum password length policy  C. Enforcing a password complexity policy  D. Looking for weak passwords |
|  | 18. | . Which of the following test gives testers comprehensive network design information?  A. White box 　　B. Black box 　　C. Gray box 　　D. Purple box |
|  | 19. | You are the network administrator for your company and want to implement a wireless network and prevent unauthorized access. Which of the following would be the best option?  A. RADIUS 　　B. TACACS+ 　　C. Kerberos 　　D. OAUTH |
|  | 20. | Why is input validation important to secure coding techniques? (Choose two.)  A. It mitigates shoulder surfing. B. It mitigates buffer overflow attacks. C. It mitigates ARP poisoning. D. It mitigates XSS vulnerabilities. |
|  | 21. | To authenticate, a Windows 10 user draws a circle around a picture of a dog’s nose and then touches each ear starting with the right ear. Which of the following concepts is this describing?  A. Something you do 　　　B. Something you know  C. Something you have 　　　 D. Somewhere you are |
|  | 22. | Which of the following countermeasures is designed to best protect against a brute-force password attack?  A. Password complexity 　　B. Account disablement  C. Password length 　　　D. Account lockout |
|  | 23. | You are a security administrator reviewing the results from a network security audit. You are reviewing options to implement a solution to address the potential poisoning of name resolution server records. Which of the following would be the best choice?  A. SSL 　　B. SSH 　　C. DNSSEC 　　D. TLS |
|  | 24. | Your manager has implemented a new policy that requires employees to shred all sensitive documents. Which of the following attacks is your manager attempting to prevent?  A. Tailgating 　　　　　　　B. Dumpster diving  C. Shoulder surfing 　　　　D. Man-in-the-middle |
|  | 25. | Which of the following cryptography algorithms support multiple bit strengths?  A. DES 　　B. HMAC 　　C. MD5 　　D. AES |
|  | 26. | A network security auditor will perform various simulated network attacks against your company’s network. Which should the security auditor acquire first?  A. Vulnerability testing authorization 　　B. Transfer risk response  C. Penetration testing authorization 　　 D. Change management |
|  | 27. | A system administrator is told an application is not able to handle the large amount of traffic the server is receiving on a daily basis. The attack takes the server offline and causes it to drop packets occasionally. The system administrator needs to find another solution while keeping the application secure and available. Which of the following would be the best solution?  A. Sandboxing B. DMZ C. Cloud computing D. DLP |
|  | 28. | You are a security administrator and are observing unusual behavior in your network from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. You have updated the antivirus definition files and performed a full antivirus scan. The scan doesn’t show any clues of infection. Which of the following best describes what has happened on the workstation?  A. Buffer overflow B. Session hijacking C. Zero-day attack D. DDoS |
|  | 29. | You are the security engineer and have discovered that communication within your company’s encrypted wireless network is being captured with a sniffing program. The data being captured is then being decrypted to obtain the employee’s credentials to be used at a later time. Which of the following protocols is most likely being used on the wireless access point? (Choose two.)  A. WPA2 Personal B. WPA2 Enterprise C. WPA D. WEP |
|  | 30. | A network manager has implemented a strategy so that all workstations on the network will receive required security updates regularly. Which of the following best describes what the network manager implemented?  A. Sandboxing B. Ad hoc C. Virtualization D. Patch management |
|  | 31. | Your manager wants to secure the FTP server by using SSL. Which of the following should you configure?  A. FTPS B. SFTP C. SSH D. LDAPS |
|  | 32. | You are an IT security officer and you want to classify and assess privacy risks throughout the development life cycle of a program or system. Which of the following tools would be best to use for this purpose?  A. BIA 　　　 B. PIA 　　 C. RTO 　 D. MTBF |
|  | 33. | Which of the following types of risk analysis makes use of ALE?  A. Qualitative 　　B. ROI 　　C. SLE 　　D. Quantitative |
|  | 34. | Which of the following statements best describes mandatory vacations?  A. Companies ensure their employees can take time off to conduct activities together.  B. Companies use them as a tool to ensure employees are taking the correct amount of days off.  C. Companies ensure their employees are properly recharged to perform their duties.  D. Companies use them as a tool for security protection to detect fraud. |
|  | 35. | Users of your company have been visiting the website www.abccompany.com and a recent increase in virus detection has been noted. Your company has developed a relationship with another company using the web address www.abccompany.com, but not with the site that has been causing the increase of viruses. Which of the following would best describe this attack?  A. Session hijacking 　　　 B. Cross-site scripting  C. Replay attack 　　　　　D. Typo squatting |
|  | 36. | Which of the following would you enable in a laptop’s BIOS to provide full disk encryption?  A. RAID 　　 B. USB 　　 　 C. HSM 　　 　 D. TPM |
|  | 37. | Your company has hired a third-party auditing firm to conduct a penetration test against your network. The firm wasn’t given any information related to the company’s network. What type of test is the company performing?  A. White box 　　B. Red box　　 C. Black box 　　D. Gray box |
|  | 38. | Server room access is controlled with proximity cards and records all entries and exits. These records are referred to if missing equipment is discovered, so employees can be identified. Which of the following must be prevented for this policy to become effective?  A. Shoulder surfing 　B. Tailgating 　C. Vishing 　D. Dumpster diving |
|  | 39. | Company users are stating they are unable to access the network file server. A company security administrator checks the router ACL and knows users can access the web server, email server, and printing services. Which of the following is preventing access to the network file server?  A. Implicit deny B. Port security 　C. Flood guard D. Signal strength |
|  | 40. | An employee informs you that the Internet connection is slow and they are having difficulty accessing websites to perform their job. You analyze their computer and discover the MAC address of the default gateway in the ARP cache is not correct. What type of attack have you discovered?  A. DNS poisoning B. Injection C. Impersonation D. ARP poisoning |
|  | 41. | Tony, a college student, downloaded a free word editor program to complete his essay. After downloading and installing the software, Tony noticed his computer was running slow and he was receiving notifications from his antivirus program. Which of the following best describes the malware that he installed?  A. Keylogger B. Worm C. Ransomware D. Trojan |
|  | 42. | Which of the following measures the amount of time required to return a failed device, component, or network to normal functionality? A. RTO B. MTTR C. MTBF D. RPO |
|  | 43. | Natural disasters and intentional man-made attacks can cause the death of employees and customers. What type of impact is this?  A. Safety B. Life C. Finance D. Reputation |
|  | 44. | . A user finds and downloads an exploit that will take advantage of website vulnerabilities. The user isn’t knowledgeable about the exploit and runs the exploit against multiple websites to gain access. Which of the following best describes this user?  A. Man-in-the-middle B. Script kiddie C. White hat D. Hacktivist |
|  | 45. | You are the IT security officer and you plan to develop a general cybersecurity awareness training program for the employees. Which of the following best describes these employees?  A. Data owners B. Users  C. System administrators D. System owners |
|  | 46. | The system administrator needs to secure the company’s data-at-rest. Which of the following would provide the strongest protection?  A. Implement biometrics controls on each workstation.  B. Implement full-disk encryption.  C. Implement a host intrusion prevention system.  D. Implement a host intrusion detection system. |
|  | 47. | Which of the following is a true statement about qualitative risk analysis?  A. It uses numeric values to measure the impact of risk.  B. It uses descriptions and words to measure the impact of risk.  C. It uses industry best practices and records.  D. It uses statistical theories, testing, and experiments. |
|  | 48. | Which of the following firewalls tracks the operating state and characteristics of network connections traversing it?  A. Stateful firewall B. Stateless firewall  C. Application firewall D. Packet filter firewall |
|  | 49. | Which of the following are examples of PII? (Choose two.)  A. Fingerprint B. MAC address C. Home address D. Gender |
|  | 50. | An employee informs you they have lost a corporate mobile device. What is the first action you perform?  A. Enable push notification services.  B. Remotely wipe the mobile device.  C. Enable screen lock.  D. Enable geofencing. |
|  | 51. | You have created a backup routine that includes a full backup each Sunday night and a backup each night of all data that has changed since Sunday’s backup. Which of the following best describes this backup schedule?  A. Full and incremental B. Full and differential C. Snapshots D. Full |
|  | 52. | One of your colleagues attempted to ping a computer name and received the response of fe80::3281:80ea:b72b:0b55. What type of address did the colleague view?  A. IPv6 B. IPv4 C. MAC address D. APIPA |
|  | 53. | Which of the following defines the act of sending unsolicited messages to nearby Bluetooth devices?  A. Jamming B. Bluesnarfing C. Brute force D. Bluejacking |
|  | 54. | You are a system administrator and you are creating a public and private key pair. You have to specify the key strength. Which of the following would be your best choice?  A. RSA B. DES C. MD5 D. SHA |
|  | 55. | . You are the security administrator for the sales department and the department needs to email high volumes of sensitive information to clients to help close sales. All emails go through a DLP scanner. Which of the following is the best solution to help the department protect the sensitive information?  A. Automatically encrypt outgoing emails.  B. Monitor all outgoing emails.  C. Automatically encrypt incoming emails.  D. Monitor all incoming emails. |
|  | 56. | You are the IT security officer of your company and have established a security policy that requires users to protect all sensitive documents to avoid their being stolen. What policy have you implemented?  A. Separation of duties B. Clean desk C. Job rotation D. Privacy |
|  | 57. | Which of the following options can a security administrator deploy on a mobile device that will deter undesirable people from seeing the data on the device if it is left unattended?  A. Screen lock B. Push notification services  C. Remote wipe D. Full device encryption |
|  | 58. | You are a system administrator and are asked to prevent staff members from using each other’s credentials to access secured areas of the building. Which of the following will best address this request?  A. Install a biometric reader at the entrance of the secure area.  B. Install a proximity card reader at the entrance of the secure area.  C. Implement least privilege.  D. Implement group policy enforcement. |
|  | 59. | A sales manager has asked for an option for sales reps who travel to have secure remote access to your company’s database server. Which of the following should you configure for the sales reps?  A. VPN B. WLAN C. NAT D. Ad hoc |
|  | 60. | An attacker tricks one of your employees into clicking on a malicious link that causes an unwanted action on the website the employee is currently authenticated to. What type of attack is this?  A. Replay B. Cross-site request forgery  C. Cross-site scripting D. Buffer overflow |
|  | 61. | Which of the following is considered the strongest access control?  A. RBAC B. DAC C. MAC D. ABAC |
|  | 62. | Your company wants to expand its data center, but has limited space to store additional hardware. The IT staff needs to continue their operations while expansion is underway. Which of the following would best accomplish this expansion idea?  A. IaaS B. Virtualization C. SaaS D. Public cloud |
|  | 63. | Which of the following algorithms have known collisions? (Choose two.)  A. MD5 B. AES C. SHA D. SHA-256 E. RSA |
|  | 64. | Which of the following must a security administrator implement to allow customers, vendors, suppliers, and other businesses to obtain information while preventing access to the company’s entire network? A. Intranet B. Internet C. Extranet D. Honeynet |
|  | 65. | The head of HR is conducting an exit interview with an IT network administrator named Matt. The interview questions include Matt’s view of his manager, why he is leaving his current position, and what he liked most about his job. Which of the following should also be addressed in this exit interview?  A. Job rotation B. NDA  C. Background checks D. Property return form |
|  | 66. | Which of the following is considered the least secure authentication method?  A. TACACS+ B. CHAP C. NTLM D. PAP |
|  | 67. | You are a security administrator for your company and have been asked to recommend a secure method for storing passwords due to recent brute-force attempts. Which of the following will provide the best protection? (Choose two.)  A. ROT13 B. BCRYPT C. RIPEMD D. PBKDF2 |
|  | 68. | You installed a WAP for a local coffee shop and have discovered the signal is extending into the parking lot. Which of the following configurations will best correct this issue?  A. Change the antenna type.  B. Disable the SSID broadcast.  C. Reduce the signal strength for indoor coverage only.  D. Enable MAC filtering to prevent devices from accessing the wireless network. |
|  | 69. | You are a network administrator for a bank. A branch manager discovers that the deskside employees have the ability to delete lending policies found in a folder within the file server. You review the permissions and notice the deskside employees have “modify” permissions to the folder. The employees should have read permissions only. Which of the following security principles has been violated?  A. Job rotation B. Time-of-day restrictions  C. Separation of duties D. Least privilege |
|  | 70. | Which of the following concepts of cryptography ensures integrity of data by the use of digital signatures?  A. Key stretching B. Steganography C. Key exchange D. Hashing |
|  | 71. | Your manager has asked you to recommend a public key infrastructure component to store certificates that are no longer valid. Which of the following is the best choice?  A. Intermediate CA B. CSR C. CRL D. Key escrow |
|  | 72. | You are a backup operator and receive a call from a user asking you to send sensitive documents immediately because their manager is going to a meeting with the company’s executives. The user states the manager’s files are corrupted and he is attending the meeting in the next 5 minutes. Which of the following forms of social engineering best describes this situation?  A. Scarcity B. Consensus C. Intimidation D. Authority |
|  | 73. | Which of the following controls can you implement together to prevent data loss if a mobile device is lost or stolen? (Choose two.)  A. Geofencing B. Full-device encryption  C. Screen locks D. Push notification services |
|  | 74. | You are asked to find the MAC address on a Linux machine. Which of the following commands can you use to discover it?  A. ipconfig 　　B. ifconfig 　　C. tracert　　 D. ping |
|  | 75. | A chief security officer (CSO) notices that a large number of contractors work for the company. When a contractor leaves the company, the provisioning team is not notified. The CSO wants to ensure the contractors cannot access the network when they leave. Which of the following polices best supports the CSO’s plan?  A. Account disablement 　　　B. Account lockout policy  C. Enforce password history 　　D. Account expiration policy |
|  | 76. | The CISO wants to strengthen the password policy by adding special characters to users’ passwords. Which of the following control best achieves this goal?  A. Password complexity 　　　B. Password length  C. Password history 　　　　　D. Group policy |
|  | 77. | Which of the following deployment models allows a business to have more control of the devices given to employees that handle company information?  A. DLP 　　　B. COPE 　　　C. BYOD 　　　　D. CYOD |
|  | 78. | A network administrator uses their fingerprint and enters a PIN to log onto a server. Which of the following best describes this example?  A. Identification 　　　　　　B. Single authentication  C. Multifactor authentication 　D. Transitive trust |
|  | 79. | Your company wants to perform a privacy threshold assessment (PTA) to identify all PII residing in its systems before retiring hardware. Which of the following would be examples of PII? (Choose two.)  A. Date of birth 　　B. Email address 　　C. Race 　D. Fingerprint |
|  | 80. | Your HIPS is incorrectly reporting legitimate network traffic as suspicious activity. What is this best known as?  A. False positive 　　　　B. False negative  C. Credentialed 　　　　D. Noncredentialed |
|  | 81. | Matt, a network administrator, is asking how to configure the switches and routers to securely monitor their status. Which of the following protocols would he need to implement on the devices?  A. SSH 　　B. SNMP 　　C. SMTP 　　D. SNMPv3 |
|  | 82. | Your company has issued a hardware token-based authentication to administrators to reduce the risk of password compromise. The tokens display a code that automatically changes every 30 seconds. Which of the following best describes this authentication mechanism?  A. TOTP 　　B. HOTP 　　C. Smartcard　　 D. Proximity card |
|  | 83. | You are the network administrator for your company’s Microsoft network. Your CISO is planning the network security and wants a secure protocol that will authenticate all users logging into the network. Which of the following authentication protocols would be the best choice?  A. RADIUS 　　B. TACACS+　　 C. Kerberos 　　D. SAML |
|  | 84. | Which of the following is not a vulnerability of end-of-life systems?  A. When systems can’t be updated, firewalls and antiviruses are not sufficient protection.  B. Out-of-date systems can result in fines in regulated industries.  C. When an out-of-date system reaches the end-of-life, it will automatically shut down.  D. Operating out-of-date systems can result in poor performance and reliability and can lead to denial of services. |
|  | 85. | Which of the following statements are true regarding viruses and worms? (Choose two.)  A. A virus is a malware that self-replicates over the network.  B. A worm is a malware that self-replicates over the network.  C. A virus is a malware that replicates by attaching itself to a file.  D. A worm is a malware that replicates by attaching itself to a file. |
|  | 86. | Which of the following wireless attacks would be used to impersonate another WAP to obtain unauthorized information from nearby mobile users?  A. Rogue access point　B. Evil twin 　C. Bluejacking D. Bluesnarfing |
|  | 87. | Tony, a security administrator, discovered through an audit that all the company’s access points are currently configured to use WPA with TKIP for encryption. Tony needs to improve the encryption on the access points. Which of the following would be the best option for Tony?  A. WPA2 with CCMP B. WEP C. WPA with CCMP D. WPS |
|  | 88. | Your department manager assigns Tony, a network administrator, the job of expressing the business and financial effects that a failed SQL server would cause if it was down for 4 hours. What type of analysis must Tony perform?  A. Security audit B. Asset identification  C. Business impact analysis D. Disaster recovery plan |
|  | 89. | You are the security administrator for a local hospital. The doctors want to prevent the data from being altered while working on their mobile devices. Which of the following would most likely accomplish the request?  A. Cloud storage B. Wiping C. SIEM D. SCADA |
|  | 90. | You are a Unix engineer, and on October 29 you discovered that a former employee had planted malicious code that would destroy 4,000 servers at your company. This malicious code would have caused millions of dollars worth of damage and shut down your company for at least a week. The malware was set to detonate at 9:00 a.m. on January 31. What type of malware did you discover?  A. Logic bomb B. RAT C. Spyware D. Ransomware |
|  | 91 | Which of the following is defined as hacking into a computer system for a politically or socially motivated purpose?  A. Hacktivist B. Insider C. Script kiddie D. Evil twin |
|  | 92 | A network administrator with your company has received phone calls from an individual who is requesting information about their personal finances. Which of the following type of attack is occurring?  A. Whaling B. Phishing C. Vishing D. Spear phishing |
|  | 93 | Which of the following can be restricted on a mobile device to prevent security violations? (Choose three.)  A. Third-party app stores B. Biometrics C. Content management D. Rooting E. Sideloading |
|  | 94 | Which of the following does a remote access VPN usually rely on? (Choose two.) A. IPSec B. DES C. SSL D. SFTP |
|  | 95 | Matt, a security administrator, wants to use a two-way trust model for the owner of a certificate and the entity relying on the certificate. Which of the following is the best option to use?  A. WPA B. Object identifiers C. PFX D. PKI |
|  | 96 | If domain A trusts domain B, and domain B trusts domain C, then domain A trusts domain C. Which concept does this describe?  A. Multifactor authentication B. Federation  C. Single sign-on D. Transitive trust |
|  | 97 | A user entered a username and password to log into the company’s network. Which of the following best describes the username?  A. Authorization B. Authentication C. Identification D. Accounting |
|  | 98 | Which of the following tools can be used to hide messages within a file?  A. Data sanitization B. Steganography  C. Tracert D. Network mapping |
|  | 99 | Which of the following is best used to prevent ARP poisoning on a local network? (Choose two.)  A. Antivirus B. Static ARP entries  C. Patching management D. Port security |
|  | 100 | Which of the following is the best practice to place at the end of an ACL?  A. USB blocking B. Time synchronization  C. MAC filtering D. Implicit deny |