|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. A digital certificate is a technology used to associate a user's identity to a private key.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2. A certificate repository (CR) is a publicly accessible centralized directory of digital certificates.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3. Digital certificates should last forever.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4. Stream ciphers work on multiple characters at a time.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5. Some cryptographic algorithms require that in addition to a key another value can or must be input.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6. A user electronically signs a Certificate Signing Request (CSR) by affixing their public key and then sending it to an intermediate certificate authority.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7. Root digital certificates are should never be self-signed.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | False | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Some CAs issue only entry-level certificates that provide domain-only validation.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9. A Subject Alternative Name (SAN) digital certificate, is also known as a Unified Communications Certificate (UCC).   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10. SSL v3.0 served as the basis for TLS v1.0.   |  |  |  | | --- | --- | --- | |  | a. | True | |  | b. | False |  |  |  | | --- | --- | | *ANSWER:* | True | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. What term best represents the resiliency of a cryptographic key to attacks?   |  |  |  | | --- | --- | --- | |  | a. | key bits | |  | b. | key resiliency | |  | c. | key strength | |  | d. | key space |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 12. Select the term that is used to describe a trusted third-party agency that is responsible for issuing digital certificates:   |  |  |  | | --- | --- | --- | |  | a. | Registration Authority | |  | b. | Delegation Authority | |  | c. | Certification Authority | |  | d. | Participation Authority |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 13. What kind of digital certificate is typically used to ensure the authenticity of a web server to a client?   |  |  |  | | --- | --- | --- | |  | a. | private | |  | b. | web server | |  | c. | public web | |  | d. | web client |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14. A framework for all of the entities involved in digital certificates for digital certificate management is known as:   |  |  |  | | --- | --- | --- | |  | a. | public key infrastructure | |  | b. | network key infrastructure | |  | c. | private key infrastructure | |  | d. | shared key infrastructure |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 15. When two individuals trust each other because of the trust that exists between the individuals and a separate entity, what type of trust has been established?   |  |  |  | | --- | --- | --- | |  | a. | web of | |  | b. | mutual | |  | c. | third-party | |  | d. | distributed |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16. What type of trust model is used as the basis for most digital certificates used on the Internet?   |  |  |  | | --- | --- | --- | |  | a. | third-party trust | |  | b. | related trust | |  | c. | managed trust | |  | d. | distributed trust |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17. What type of trust model has a single CA that acts as a facilitator to interconnect all other CAs?   |  |  |  | | --- | --- | --- | |  | a. | bridge trust | |  | b. | distributed trust | |  | c. | third-party trust | |  | d. | transitive trust |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 18. A document that describes in detail how a CA uses and manages certificates, as well as how end users register for a digital certificate, is known as?   |  |  |  | | --- | --- | --- | |  | a. | Certificate practice statement (CPS) | |  | b. | Certificate policy (CP) | |  | c. | Lifecycle policy (LP) | |  | d. | Access policy (AP) |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 19. At what stage can a certificate no longer be used for any type of authentication?   |  |  |  | | --- | --- | --- | |  | a. | creation | |  | b. | suspension | |  | c. | revocation | |  | d. | expiration |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 20. The process by which keys are managed by a third party, such as a trusted CA, is known as?   |  |  |  | | --- | --- | --- | |  | a. | key escrow | |  | b. | key destruction | |  | c. | key renewal | |  | d. | key management |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 21. What protocol, developed by Netscape in 1994, is designed to create an encrypted data path between a client and server that could be used on any platform or operating system?   |  |  |  | | --- | --- | --- | |  | a. | SSL | |  | b. | TLS | |  | c. | PEAP | |  | d. | EAP |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 22. What cryptographic transport algorithm is considered to be significantly more secure than SSL?   |  |  |  | | --- | --- | --- | |  | a. | AES | |  | b. | HTTPS | |  | c. | ESSL | |  | d. | TLS |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 23. What protocol below supports two encryption modes: transport and tunnel?   |  |  |  | | --- | --- | --- | |  | a. | HTTPS | |  | b. | IPSec | |  | c. | SSL | |  | d. | TLS |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24. The Authentication Header (AH) protocol is a part of what encryption protocol suite below?   |  |  |  | | --- | --- | --- | |  | a. | TLS 3.0 | |  | b. | IPSec | |  | c. | GPG | |  | d. | SSL |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 25. Why is IPsec considered to be a transparent security protocol?   |  |  |  | | --- | --- | --- | |  | a. | IPsec packets can be viewed by anyone. | |  | b. | IPsec is designed to not require modifications of programs, or additional training, or additional client setup. | |  | c. | IPsec's design and packet header contents are open sourced technologies. | |  | d. | IPsec uses the Transparent Encryption (TE) algorithm. |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 26. Select the secure alternative to the telnet protocol:   |  |  |  | | --- | --- | --- | |  | a. | HTTPS | |  | b. | TLS | |  | c. | IPsec | |  | d. | SSH |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 27. What length SSL and TLS keys are generally considered to be strong?   |  |  |  | | --- | --- | --- | |  | a. | 128 | |  | b. | 1024 | |  | c. | 2048 | |  | d. | 4096 |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 28. What block cipher mode of operation uses the most basic approach where the plaintext is divided into blocks, and each block is then encrypted separately?   |  |  |  | | --- | --- | --- | |  | a. | Electronic Code Book | |  | b. | Galois/Counter | |  | c. | Cipher Block Chaining | |  | d. | Counter |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 29. What block cipher mode of operation encrypts plaintext and computes a message authentication code to ensure that the message was created by the sender and that it was not tampered with during transmission?   |  |  |  | | --- | --- | --- | |  | a. | Electronic Code Book | |  | b. | Galois/Counter | |  | c. | Cipher Block Chaining | |  | d. | Counter |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30. What allows an application to implement an encryption algorithm for execution?   |  |  |  | | --- | --- | --- | |  | a. | counters | |  | b. | crypto service providers | |  | c. | initialization vectors | |  | d. | crypto modules |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 31. What is a value that can be used to ensure that plaintext, when hashed, will not consistently result in the same digest?   |  |  |  | | --- | --- | --- | |  | a. | salt | |  | b. | initialization vector | |  | c. | counter | |  | d. | nonce |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 32. Which of the following is an input value that must be unique within some specified scope, such as for a given period or an entire session?   |  |  |  | | --- | --- | --- | |  | a. | salt | |  | b. | initialization vector | |  | c. | counter | |  | d. | nonce |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33. What common method is used to ensure the security and integrity of a root CA?   |  |  |  | | --- | --- | --- | |  | a. | Keep it in an offline state from the network. | |  | b. | Only use the root CA infrequently. | |  | c. | Password protect the root CA | |  | d. | Keep it in an online state and encrypt it. |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 34. Which of the following is a valid way to check the status of a certificate? (Choose all that apply.)   |  |  |  | | --- | --- | --- | |  | a. | Online Certificate Status Protocol | |  | b. | Certificate Revocation Authority | |  | c. | Certificate Revocation List | |  | d. | Revocation List Protocol |  |  |  | | --- | --- | | *ANSWER:* | a, c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 35. What process links several certificates together to establish trust between all the certificates involved?   |  |  |  | | --- | --- | --- | |  | a. | certificate pairing | |  | b. | certificate linking | |  | c. | certificate joining | |  | d. | certificate chaining |  |  |  | | --- | --- | | *ANSWER:* | d | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 36. Which of the following certificates are self-signed?   |  |  |  | | --- | --- | --- | |  | a. | trusted digital certificates | |  | b. | root digital certificates | |  | c. | web digital certificates | |  | d. | user digital certificate |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 37. What is used to create session keys?   |  |  |  | | --- | --- | --- | |  | a. | master secret | |  | b. | crypto modules | |  | c. | validation | |  | d. | domain validation |  |  |  | | --- | --- | | *ANSWER:* | a | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 38. Which of the following certificates verifies the identity of the entity that has control over the domain name?   |  |  |  | | --- | --- | --- | |  | a. | validation digital certificate | |  | b. | root digital certificates | |  | c. | domain validation digital certificate | |  | d. | web digital certificates |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 39. Which of the following is an enhanced type of domain digital certificate?   |  |  |  | | --- | --- | --- | |  | a. | Primary Validation | |  | b. | Extended Validation | |  | c. | Authorized Validation | |  | d. | Trusted Validation |  |  |  | | --- | --- | | *ANSWER:* | b | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 40. What process will remove all private and public keys along with the user's identification information in the CA?   |  |  |  | | --- | --- | --- | |  | a. | suspension | |  | b. | deletion | |  | c. | destruction | |  | d. | revocation |  |  |  | | --- | --- | | *ANSWER:* | c | |

|  |  |  |
| --- | --- | --- |
| 41. Explain how digital certificates are managed.   |  |  | | --- | --- | | *ANSWER:* | Several entities and technologies are used for the management of digital certificates, such as applying, registering, and revoking. These include the Certificate Authority (CA), along with a Certificate Revocation List (CRL) and a Certificate Repository (CR). In addition, digital certificates can be managed through a Web browser. | |

|  |  |  |
| --- | --- | --- |
| 42. What is the S/MIME protocol used for?   |  |  | | --- | --- | | *ANSWER:* | The Secure/Multipurpose Internet Mail Extensions protocol is for securing email messages. It allows users to send encrypted messages that are also digitally signed. | |

|  |  |  |
| --- | --- | --- |
| 43. What are the three areas of protection provided by IPSEC?   |  |  | | --- | --- | | *ANSWER:* | Authentication, confidentiality, and key management. | |

|  |  |  |
| --- | --- | --- |
| 44. What protocol uses SSL or TLS to secure communications between a browser and a web server?   |  |  | | --- | --- | | *ANSWER:* | The Hypertext Transport Protocol Secure (HTTPS) | |

|  |  |  |
| --- | --- | --- |
| 45. What role does a key recovery agent fulfill in an enterprise environment?   |  |  | | --- | --- | | *ANSWER:* | The KRA is a highly trusted person responsible for recovering lost or damaged digital certificates. Digital certificates can then be archived along with the user's private key. If the user is unavailable or if the certificate is lost, the certificate with the private key can be recovered. | |

|  |  |  |
| --- | --- | --- |
| 46. What is a cipher suite?   |  |  | | --- | --- | | *ANSWER:* | A cipher suite is a named combination of the encryption, authentication, and message authentication code (MAC) algorithms that are used with SSL and TLS. | |

|  |  |  |
| --- | --- | --- |
| 47. List the four stages of a certificate life cycle.   |  |  | | --- | --- | | *ANSWER:* | Creation, suspension, revocation, and expiration. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 48. List the three PKI trust models that use a CA.   |  |  | | --- | --- | | *ANSWER:* | The models are the hierarchical trust model, the distributed trust model, and the bridge trust model. | | *POINTS:* | 1 | |

|  |  |  |
| --- | --- | --- |
| 49. Explain how Cipher Block Chaining (CBC) operates.   |  |  | | --- | --- | | *ANSWER:* | After being encrypted, each ciphertext block gets "fed back" into the encryption process to encrypt the next plaintext block. Using CBC, each block of plaintext is XORed with the previous block of ciphertext before being encrypted. CBC is also dependent on the previous ciphertext block, making it much more difficult to break. | |

|  |  |  |
| --- | --- | --- |
| 50. What is a cryptographic key?   |  |  | | --- | --- | | *ANSWER:* | cryptographic key is a value that serves as input to an algorithm, which then transforms plaintext into ciphertext (and vice versa for decryption). A key, which is essentially a random string of bits, serves as an input parameter for symmetric and asymmetric cryptographic algorithms and selected hash algorithms. | |