Advanced Cybersecurity Knowledge

Cybersecurity · Practice Test · 25 Questions

1. Which specific NIST publication serves as the primary framework for improving critical infrastructure cybersecurity?

A) NIST SP 800-53
B) NIST CSF 1.1
C) NIST SP 800-171
D) FIPS 140-2

2. What is the primary function of the 'salt' in cryptographic password hashing?

A) To increase the entropy of the input
B) To prevent rainbow table attacks
C) To encrypt the plaintext password
D) To authenticate the user's IP address

3. In the context of the OSI model, which layer does a traditional packet-filtering firewall primarily operate at?

A) Application Layer
B) Transport Layer
C) Network Layer
D) Data Link Layer

4. Which algorithm is defined by the IEEE 802.11i standard as the mandatory encryption protocol for WPA2?

A) TKIP
B) WEP
C) AES-CCMP
D) RC4

5. What does the 'P' stand for in the context of the HSTS security mechanism?

A) Protocol
B) Policy
C) Public
D) Protection

6. Which cyberattack technique involves exploiting the way a browser handles the 'Same-Origin Policy'?

A) Cross-Site Request Forgery (CSRF)
B) SQL Injection
C) Buffer Overflow
D) Heap Spraying

7. What is the maximum key length supported by the AES-256 encryption standard?

A) 128 bits
B) 192 bits
C) 256 bits
D) 512 bits

8. Which standard defines the requirements for an Information Security Management System (ISMS)?

A) ISO/IEC 27001
B) ISO/IEC 9001
C) ISO/IEC 31000
D) ISO/IEC 20000

9. What is the primary purpose of a 'honeytoken' in a decoy-based detection system?

A) To encrypt network traffic
B) To act as a canary for unauthorized data access
C) To authenticate administrative users
D) To block malicious IP addresses

10. Which cryptographic primitive is primarily used to ensure data integrity rather than confidentiality?

A) RSA
B) AES
C) SHA-256
D) ECC

11. What is the primary vulnerability targeted by 'Return-Oriented Programming' (ROP) attacks?

A) SQL injection
B) Cross-site scripting
C) Buffer overflow with non-executable memory
D) Denial of service

12. Which port is assigned by the IANA for secure LDAP (LDAPS) traffic?

A) 389
B) 636
C) 443
D) 80

13. In asymmetric encryption, what is the role of the Private Key in a digital signature operation?

A) To encrypt the document for confidentiality
B) To decrypt the sender's public key
C) To sign the hash of the data
D) To compress the message file

14. What does the acronym 'DLP' stand for in enterprise data security?

A) Data Link Protocol
B) Data Loss Prevention
C) Digital Logic Protection
D) Distributed Layer Processing

15. Which attack specifically targets the exhaustion of server resources by sending incomplete TCP handshakes?

A) SYN Flood
B) Ping of Death
C) Smurf Attack
D) DNS Amplification

16. Which cryptographic protocol was officially deprecated by IETF in RFC 7568?

A) TLS 1.2
B) SSL 3.0
C) TLS 1.3
D) DTLS 1.0

17. What is the core function of an HSM (Hardware Security Module)?

A) To act as a physical firewall
B) To store and manage cryptographic keys securely
C) To provide high-speed network routing
D) To monitor hardware temperature

18. Which specific type of attack uses a series of commands to manipulate the back-end database of a web application?

A) XSS
B) SQL Injection
C) CSRF
D) Directory Traversal

19. What is the significance of the 'entropy' value in a random number generator used for cryptography?

A) High entropy means predictable patterns
B) Low entropy means higher security
C) High entropy means greater unpredictability
D) Entropy is unrelated to security

20. Which security standard specifically addresses the protection of cardholder data?

A) GDPR
B) HIPAA
C) PCI-DSS
D) SOX

21. In access control models, what does 'RBAC' stand for?

A) Role-Based Access Control
B) Remote-Based Access Control
C) Resource-Based Access Control
D) Router-Based Access Control

22. What is the primary goal of the 'Zero Trust' security model?

A) To trust all internal devices
B) To remove all authentication
C) To never trust, always verify
D) To allow open access to all users

23. Which Linux file typically stores the hashed passwords for user accounts?

A) /etc/passwd
B) /etc/shadow
C) /etc/group
D) /etc/profile

24. What is a 'Rootkit' primarily designed to do?

A) To encrypt user files for ransom
B) To provide unauthorized root-level access while remaining hidden
C) To crash the operating system
D) To redirect network traffic to a proxy

25. Which type of malware replicates by infecting other files on a host system?

A) Worm
B) Trojan Horse
C) Virus
D) Spyware