# Information Security Final Exam - Questions and Answers

**1. What encryption algorithm uses the same pre-shared key to encrypt and decrypt data?**Answer: C. Symmetric

**2. What name is given to a amateur hacker?**Answer: C. Script kiddie

**3. Pick three types of records that cyber criminals would be interested in stealing from organization.**Answer: C. Employment, E. Education, G. Medical

**4. What is the workforce framework category that includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence?**Answer: D. Analyze

**5. What two methods help to ensure system availability?**Answer: B. System backups, C. System resiliency

**6. What does the term BYOD represent?**Answer: D. Bring your own device

**7. What does the term vulnerability mean?**Answer: E. A weakness that makes a target susceptible to an attack

**8. Thwarting cyber criminals includes which of the following?**Answer: A. Establishing early warning systems, E. Sharing cyber intelligence information

**9. What are two common hash functions?**Answer: C. SHA, E. MD5

**10. What service determines which resources a user can access along with the operations that a user can perform?**Answer: D. Authorization

**11. What type of cybersecurity laws protect you from an organization that might want to share your sensitive data?**Answer: D. Privacy

**12. For the purpose of authentication, what three methods are used to verify identity?**Answer: B. Something you know, C. Something you are, E. Something you have

**13. What is a secure virtual network called that uses the public network?**Answer: C. VPN

**14. What is a method of sending information from one device to another using removable media?**Answer: E. Sneaker net

**15. The three foundational principles of the cybersecurity domain.**Answer: C. Integrity, E. Availability, F. Confidentiality

**16. What are three access control security services?**Answer: A. Authentication, C. Authorization, E. Accounting

**17. Which two methods help to ensure data integrity?**Answer: C. Data consistency checks, E. Hashing

**18. There are three states of data**Answer: B. At rest, D. In-transit, E. In-process

**19. What is identified by the first dimension of the cybersecurity cube?**Answer: D. Goals

**20. Which two reasons describe why WEP is a weak protocol?**Answer: B. The key is static and repeats on a congested network, E. The key is transmitted in clear text

**21. What type of an attack can disable a computer by forcing it to use memory or by overworking its CPU?**Answer: D. DDOS

**22. What is a vulnerability that allows criminals to inject scripts into web pages viewed by users?**Answer: F. Cross-site scripting

**23. What are three validation criteria used for a validation rule?**Answer: B. Format, C. Range, E. Type

**24. What is the danger in proceeding with a transaction on a site with no lock in the browser?**Answer: D. The site is not using a digital certificate to secure the transaction, with the result that everything is in the clear

**25. Which integrity requirement is implemented by ensuring primary keys are unique and not null?**Answer: A. Entity integrity

**26. What three questions should be asked when creating a disaster recovery plan?**Answer: D. Who is responsible for the process, E. What is the process?, F. Does the process require approval?

**27. What are three types of attacks that are preventable through the use of salting?**Answer: A. Lookup tables, C. Reverse lookup tables, D. Rainbow tables

**28. What security tool can ensure integrity and authenticity using SHA-1 in IPsec?**Answer: D. HMAC

**29. Which three devices represent examples of physical access controls?**Answer: A. Swipe cards, C. Locks, F. Video cameras

**30. What are the three steps to configure a scan?**Answer: A. Configure a scan policy, C. Vulnerability scan, F. Launch the scan

**31. Which two statements characterize DoS attacks?**Answer: B. They attempt to compromise the availability of a network, host, or application, E. Examples include smurf attacks and ping of death attacks

**32. Which two network security solutions can be used to mitigate DoS attacks?**Answer: C. Antispoofing technologies, D. Intrusion protection systems

**33. What is the primary method for mitigating malware?**Answer: B. Installing antivirus software on all hosts

**34. Which statement accurately characterizes the evolution of threats to network security?**Answer: A. Internal threats can cause even greater damage than external threats

**35. What is an objective of a state-sponsored attack?**Answer: A. To right a perceived wrong

**36. What service or protocol does the Secure Copy Protocol rely on?**Answer: A. AAA

**37. What can be determined from a syslog message from 172.16.45.1?**Answer: D. The message informs the administrator that a user with an IP address of 172.16.45.1 configured this device remotely.

**38. What is the purpose of AAA accounting?**Answer: A. To collect and report data usage

**39. What are two protocols used by AAA to authenticate users?**Answer: B. TACACS+, E. RADIUS

**40. What are two attributes of TACACS+ authentication?**Answer: B. Encryption for all communication, C. Separate processes for authentication and authorization

**41. How many bits does DES use for encryption?**Answer: B. 56 bits

**42. Which encryption algorithm is asymmetric?**Answer: A. DH

**43. Which algorithm can ensure data confidentiality?**Answer: B. AES

**44. What is the purpose of a digital certificate?**Answer: D. It authenticates a website and establishes a secure connection to exchange confidential data

**45. What type of encryption algorithm uses the same key to encrypt and decrypt data?**Answer: B. Shared-secret