Q1. How many keys are needed for symmetric key encryption?

1. 1 C.3
2. 2 D. 4

Q2.Which of the following key lengths would be considered uncrackable? (Choose all that apply.)

1. 512 C. 128
2. 256 D. 64

Q3. What algorithm outputs a 128-bit message digest regardless of the length of the input?

1. SHA C. RC4
2. MD5 D. RC6

Q4. Which algorithm is used in the digital signature process?

1. RC4 C.Blowfish
2. RC5 D. MD5

Q5. Data encrypted with the server's public key can be decrypted with which key?

1. The server's public key
2. The server's private key
3. The client's public key
4. The client's private key

Q6. What is the goal of a known–plain text attack?

1. To read the encrypted data
2. To gain access to the public key
3. To discover the encryption key
4. To validate the sender of the data

Q7. What is the standard format for digital certificates?

1. x.500 C. x.25
2. x.509 D. XOR

Q8. What are two components of a PKI?

1. User passwords
2. Digital certificates
3. Encrypted data
4. CA

Q9. What element of the CIA triad ensures that the data sent is the same data received?

1. Confidentiality
2. Integrity
3. Authentication

Q10. What is the purpose of a hash?

1. To ensure confidentiality when using a public network such as the Internet
2. To ensure integrity of a transferred file
3. To ensure only authorized users are accessing a file
4. To ensure the data is available to authorized users

Q11. Which cryptographic attack attempts to crack the code by looking for patterns and using statistical analysis?

1. Cipher text–only attack
2. Chosen–plain text attack
3. Chosen–cipher text attack
4. Brute-force attack

Q12. Which program is useful in ensuring the integrity of a file that has been downloaded from the Internet?

1. Tripwire
2. Norton Internet Security
3. Snort
4. WinMD5

Q13. Which of the following is true concerning IPSec?

1. It provides authentication, confidentiality, packet integrity, and encapsulation functions, but not antireplay capabilities.
2. IKE is used to securely share keys between IPSec peers during Phase 1.
3. Cisco routers use transform sets to define interesting traffic.
4. It supports IPv4 and IPv6.

Q14. What is an example of a packet-filtering firewall?

1. Websense
2. Router ACLs
3. ASA state table
4. Cut-through proxy

Q15. What kind of firewall terminates users' connections and establishes new connections to the actual destination?

1. Application inspection firewall
2. Stateful firewall
3. Packet-filtering firewall
4. Application gateway firewall

Q16. What information is found in a state table of a stateful filtering firewall? (Choose two.)

1. TCP flags
2. Protocol numbers or names
3. MAC addresses
4. FTP commands executed by a user

Q17. What traffic should you typically be denying inbound into your network? (Choose two.)

1. SMTP
2. DNS
3. ICMP
4. SNMP

Q18. You have a router with two interfaces: FA0/0 and FA0/1. FA0/0 has networks 10.0.1.0/24, 10.0.2.0/24, and 192.168.1.0/24 associated with it. FA0/1 has networks 10.0.3.0/24, 192.168.2.0/24, and 192.168.3.0/24 associated with it. Users associated with FA0/1 need to connect to servers to FA0/0. In this situation, what addresses should you drop to prevent spoofing attacks?

1. Source addresses from 192.168.2.0/24
2. Destination addresses from 192.168.1.0/24
3. Destination addresses of 192.168.2.0/24
4. Source addresses from 192.168.3.0/24
5. Source addresses from 10.0.1.0/24

Q19. Which of the following is a quantitative assessment used in risk management?

1. OCTAVE
2. CRAMM
3. Failure Modes and Effect Analysis
4. NIST SP 800-66

Q20. What is the primary model for creating security polices?

1. Allow everything unless specifically denied
2. Only create enforceable policies
3. All policies are essentially unenforceable
4. Deny everything unless specifically allowed

Q21. Which of the following is a symmetric algorithms used in encrypting information?

1. RSA
2. EL Gamal
3. CAST
4. Diffie-Hellmann

Q22. What type of firewall is the most commonly implemented between a trusted and untrusted network?

1. Packet Filter
2. Screened Subnet
3. Application Proxy
4. Stateful Inspection

Q23. Smart cards are authentication tools which fulfill which type of authentication characteristic?

1. Something a person knows
2. Something a person does
3. Something a person is
4. Something a person has

Q24.Which of the following authentication systems provide single sign on capabilities?

1. RADIUS
2. TACACS
3. Kerberos
4. All of the above

Q25.Which of the following is not an access control characteristic?

1. Corrective
2. Monitoring
3. Preventative
4. Compensation

Q26.Which of the following is a factor of authentication related to user controls?

1. Something the user has
2. Something the user is
3. Something the user knows
4. All of the above

Q27. What character is used to represent an invalid character in DNS names?

1. Asterisk
2. Question mark
3. Hyphen
4. Ampersand

Q28. What type if incident is cyberstalking considered to be?

1. Reconnaissance
2. Extortion
3. Harassment
4. Repudiation

Q29. What type of network topology is commonly used by VPN solutions?

1. Star
2. Mesh
3. Hub
4. All of the above

Q30.What suite of protocols is used by Virtual Private Networks?

1. IPSec C. LADP
2. IP D. RIP

Q31. Which of the following is a behavioral form of biometrics?

1. Voice patters and recognition
2. Keystroke pattern analysis
3. Retina and iris scans
4. Hand geometry and fingerprints

Q32. Which of the following passwords would be the most difficult to hack?

1. A dictionary password of 15 characters
2. An alphanumeric password of 10 characters
3. A combination password of 12 characters
4. A complex password of 8 characters

Q33. What is the technique used to store accessed information temporarily called?

1. Forwarding
2. Caching
3. Zoning
4. Namespace

Q34. What security implementation is used to delay an attack rather than prevent it?

1. Honeypot
2. Demilitarized Zone
3. Screened Subnet
4. Defense-in-Depth

Q35.What is the hierarchical tree structure used in DNS called?

1. Domain namespace
2. Domain name
3. Queries
4. DNS Domain