

Question 1

Which of the following security concerns falls into the administrative type for access controls?

- A. Fire management
- B. Monitoring
- C. System Access
- D. Asset management

Question 2

What are the essential practices for identification?

- A. Confidentiality, integrity, and availability
- B. Authentication, authorization, and accounting
- C. Uniqueness, nondescriptive, and issuance
- D. Access, monitor, and control

Question 3

When using smart cards to aid in the authentication process, which integrated circuit design requires ultraviolet light to erase the memory of the circuit?

- A. EPROM
- B. EEPROM
- C. RAM
- D. PROM

Question 4

When routers are used to filter packets through access lists, which type of access list will allow the filtering to be based on upper-layer session information and allow the temporary connection to be opened for IP traffic?

- A. Extended
- B. Lock-and-Key
- C. Standard
- D. Reflexive

Question 5

What is the most basic form of the Data Encryption Standard?

- A. Cipher Feedback Mode
- B. Output Feedback Mode
- C. Electronic Codebook Mode
- D. Cipher Block Chaining Mode

Question 6

Traffic on the network is directed using which of the following perimeter devices?

- A. Firewalls
- B. Routers
- C. IDS/IPS
- D. Hubs

Question 7

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

- A. Honeypot
- B. Demilitarized Zone
- C. Screened Subnet
- D. Defense-in-Depth

Question 8

What is the hierarchical tree structure used in DNS called?

- A. Domain namespace
- B. Domain name
- C. Queries
- D. DNS Domain

Question 9

What is the term used to recognize the function of a DNS server designated to handle queries for resolving external DNS domain names by sending the request to another DNS server?

- A. DNS Router
- B. DNS Forwarder
- C. DNS Client
- D. No term exists

Question 10

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

- A. OCTAVE
- B. CRAMM
- C. Failure Modes and Effect Analysis
- D. NIST SP 800-66

Question 11

What IEEE standard covers the requirements for providing wireless support from 1-30 miles, typically in MANs?

- A. 802.11
- B. 802.16

- C. 802.15.1
- D. 17001

Question 12

Which of the following is not a phase of the data life cycle?

- A. Generation
- B. **Initiation**
- C. Transfer
- D. Transformation

Question 13

What is the primary model for creating security policies?

- A. Allow everything unless specifically denied
- B. Only create enforceable policies
- C. All policies are essentially unenforceable
- D. **Deny everything unless specifically allowed**

Question 14

What is the insecure area between a trusted network and untrusted network called?

- A. **DMZ**
- B. Subnet
- C. Supernet
- D. VPN

Question 15

Which of the following is not a responsibility of facility **security**?

- A. Building materials
- B. **Computer and network**
- C. Facility age
- D. Health and safety concerns

Question 16

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

- A. RSA
- B. EL Gamal
- C. **CAST**
- D. Diffie-Hellmann

Question 17

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

- A. Packet Filter
- B. Screened Subnet
- C. Application Proxy
- D. Stateful Inspection

Question 18

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

- A. Something a person knows
- B. Something a person does
- C. Something a person is
- D. Something a person has

Question 19

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

- A. RADIUS
- B. TACACS
- C. Kerberos
- D. All of the above

Question 20

Which of the following is not an access control characteristic?

- A. Corrective
- B. Monitoring
- C. Preventative
- D. Compensation

Question 21

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

- A. Something the user has
- B. Something the user is
- C. Something the user knows
- D. All of the above

Question 22

Which of the following job functions should not be identified from an individual's network id?

- A. Manager
- B. Finance

- C. Administrator
- D. Webmaster

Question 23

Which ISO standard provides the required radio frequency power for proximity integrated circuit card?

- A. 802.11
- B. 14442
- C. 12000
- D. 802.15

Question 24

What is the purpose of cryptography?

- A. Protect users from identification
- B. Protect connections from intrusion
- C. Protect information from unauthorized access
- D. All of the above

Question 25

Which key standard was developed for financial institutions to transmit securities across electronic mediums?

- A. ANSI X9.17
- B. PKI
- C. X.509
- D. None of the above

Question 26

Which of the following is not considered a layer of a Defense-in-Depth solution?

- A. Routers and firewalls
- B. Antivirus software
- C. Proxy servers
- D. Application servers

Question 27

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

- A. Asterisk
- B. Question mark
- C. Hyphen
- D. Ampersand

Question 28

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

- A. Forwarding
- B. Caching
- C. Zoning
- D. Namespace

Question 29

What risk analysis program is a strategic assessment and planning technique used for understanding security?

- A. COBRA
- B. DELPHI
- C. RADIUS
- D. OCTAVE

Question 30

What type of incident is cyberstalking considered to be?

- A. Reconnaissance
- B. Extortion
- C. Harassment
- D. Repudiation

Question 31

In decision tree analysis, which node is the start of the decision tree?

- A. Root node
- B. End node
- C. Event node
- D. Decision node

Question 32

What is the analysis method used by IDS solutions identifies unacceptable behavior based on deviations from standards set by RFC documents?

- A. Pattern matching
- B. Protocol anomaly
- C. Statistical anomaly
- D. Stateful matching

Question 33

What is the resource records used in DNS to list IP addresses for the DNS root servers called?

- A. Domain namespace
- B. Root trees

- C. Root hints
- D. Queries

Question 34

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

- A. Star
- B. Mesh
- C. Hub
- D. All of the above

Question 35

What suite of protocols is used by Virtual Private Networks?

- A. IPSec
- B. IP
- C. LADP
- D. RIP

Question 36

Hash functions are used to provide what security requirement?

- A. Confidentiality
- B. Availability
- C. Integrity
- D. Accountability

Question 37

Which of the following is a behavioral form of biometrics?

- A. Voice patterns and recognition
- B. Keystroke pattern analysis
- C. Retina and iris scans
- D. Hand geometry and fingerprints

Question 38

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

- A. A dictionary password of 15 characters
- B. An alphanumeric password of 10 characters
- C. A combination password of 12 characters
- D. A complex password of 8 characters

Question 39

Which of the following attributes of an access control system describes the verification of available actions to a user in the network environment?

- A. Accountability
- B. Identification
- C. Authorization
- D. Authentication

Question 40

What type of control is used to compensate for incidents with the intent to return the business to normal operations?

- A. Recovery
- B. Corrective
- C. Compensation
- D. Detective

Question 41

In what type of threat do technically skilled people, including perpetrators of major fraud, industry competitors, organized crime figures, and government intelligence agencies, attempt to gain access to your network?

- A. Unstructured
- B. External
- C. Structured
- D. DDoS

Question 42

What security vulnerability category would include using a password of "cisco"?

- A. Policies
- B. Technology
- C. Administration and configuration
- D. Access

Question 43

What type of attack is used to learn information about your network?

- A. Footprint analysis
- B. Access
- C. DoS
- D. Session

Question 44

What is the most effective type of network reconnaissance attack?

- A. DNS
- B. Phishing
- C. Packet sniffing
- D. Social engineering

Question 45

What type of attack redirects traffic from one web site to another, where the attack either changes the hosts file on a user's PC or exploits a vulnerability on a DNS server to send back a spoofed DNS reply?

- A. Phishing
- B. Pharming
- C. Emanations capturing
- D. Dumpster driving

Question 46

What type of attack conceals data inside another object, like an image or a sound file?

- A. Steganography
- B. Overt channel
- C. Covert channel
- D. ICMP tunneling

Question 47

In a brute-force password attack, about what percentage of passwords have to be guessed by a password cracking program before the password is cracked?

- A. 25
- B. 50
- C. 75
- D. 100

Question 48

What is the most common type of application access attack?

- A. Social engineering
- B. Trojan horse
- C. E-mail attachment
- D. Buffer overflow

Question 49

What would be used to mitigate TCP SYN flood attacks?

- A. TCP setup controls
- B. Java and ActiveX filtering

- C. RFC 2827 filtering
- D. uRPF

Question 50

Which of the following is not used in a Smurf attack?

- A. uRPF
- B. ICMP
- C. Directed broadcast addresses
- D. Reflectors

Question 51

Your company's traveling sales force use modems in their laptop systems to dial remotely into your network each night to update the company's order processing database. Given that they are using a dial-up connection over the public switched telephone network (PSTN), what's the fastest data rate these users can achieve?

- A. 56 Kbps
- B. 256 Kbps
- C. 512 Kbps
- D. 1.5 Mbps

Question 52

What components make up a North American Primary Rate Interface (PRI) ISDN connection?

- A. 30, 64 Kbps B channels
- B. One, 64 Kbps D channel
- C. Two, 64 Kbps B channels
- D. One, 16 Kbps D channel

Question 53

Which type of ISDN devices manage data link and network layer functions, such as routing, in ISDN networks with multiple devices?

- A. Terminal adapter (TA)
- B. Terminal equipment 1 (TE1)
- C. Network terminator 2 (NT2)
- D. Network terminator 1 (NT1)

Question 54

Which of the following is true regarding the SLIP remote access protocol?

- A. It supports the NetBEUI protocol.

- B. It does not support TCP/IP.
- C. It does not support password encryption.
- D. It supports data encryption during transmission.

Question 55

You are implementing an RAS and routing solution. The network to which remote clients will connect contains a Windows server and a Linux server that communicate using TCP/IP. It also contains a legacy NetWare 4.2 server running a custom mission-critical application for your organization that uses the IPX/SPX protocol. Given that the clients' systems that will connect to the network through the RAS server, as well as the RAS server itself, already have TCP/IP configured, what should you do? (Choose two.)

- A. Configure the IPX/SPX protocol on the client workstations.
- B. Implement TCP/IP on the NetWare server.
- C. Migrate the NetWare server data to a Windows Server 2008 system.
- D. Configure the RAS server to support SLIP connections to enable TCP/IP and IPX/SPX to be used simultaneously by remote connections.

Question 56

Which PPP component is responsible for encapsulating data for transmission over a PPP connection?

- A. Network Control Protocols (NCPs)
- B. Link Control Protocol (LCP)
- C. High-Level Data Link Control (HDLC)
- D. Internet Protocol Control Protocol (IPCP)

Question 57

7. A PPP connection is being established between your Windows 7 workstation and a Windows Server 2008 RAS server. The connection is started when your workstation sends LCP frames to establish, configure, and then test the link. What happens next?

- A. The authentication protocols to be used in the connection are negotiated.
- B. Your workstation sends NCP frames to setup the network layer protocols to be used in the connection.
- C. HDLC is used to encapsulate the data stream and transmits it through the PPP connection.
- D. The configured network protocols pass data through the PPP connection.

Question 58

You are configuring a RAS implementation using a Windows Server 2008 system. You want to enhance security by using a RADIUS server for authentication. What should you do?

- A. Configure the RAS server to use PAP for authentication.
- B. Configure the RAS server to use EAP for authentication.

- C. Configure the RAS server to use CHAP for authentication.
- D. Configure the RAS server to use MS-CHAPv2 for authentication.

Question 59

You need to establish a remote connection to a Linux server from a Linux workstation using the Secure Shell (SSH) protocol. You are currently logged into your workstation as the `rbutler` user. You need to access the Linux server as the `dbadmin` user to update the data in the MySQL database service. Given that the hostname of the Linux server is `db1`, what should you do?

- A. Enter **ssh db1** at the shell prompt of your Linux workstation, and then log in as `dbadmin`.
- B. Enter **ssh -l dbadmin db1** at the shell prompt of your Linux workstation.
- C. Enter **ssh -u mysqladmin db1** at the shell prompt of your Linux workstation.
- D. Enter **telnet db1** at the shell prompt of your Linux workstation, and then authenticate as the `dbadmin` user.

Question 60

Which of the following are functions of the Point-to-Point Protocol over Ethernet (PPPoE) protocol?

- A. It encapsulates PPP frames within traditional Ethernet frames.
- B. It establishes a PPP connection through a traditional Ethernet network.
- C. It enables data transfers from a remote client to a server by creating a VPN.
- D. It encrypts VPN traffic using the IPsec protocol.

Question 61

You need to access an application running in a Citrix server farm from your Windows workstation. You need to configure your workstation's firewall to allow this type of traffic. What should you do? (Choose two.)

- A. Open port 80 in the firewall.
- B. Open port 636 in the firewall.
- C. Open port 1494 in the firewall.
- D. Open port 1293 in the firewall.

Question 62

You want to be able to access the desktop of a Windows Server 2003 system in your data center remotely from a Windows workstation at your desk. What do you need to do? (Choose two.)

- A. Enable the Remote Desktop option on the Remote tab in the properties of My Computer on the workstation.
- B. Open TCP port 5800 in the firewall of the server and the desktop system.

- C. Add your user account to the list of allowed remote users on the Remote tab in the properties of My Computer on the workstation.
- D. Enable the Remote Desktop option on the Remote tab in the properties of My Computer on the server.

Question 63

Which authentication protocol authenticates both the client and the server when setting up a PPP connection?

- A. PAP
- B. CHAP
- C. MS-CHAP
- D. MS-CHAPv2

Question 64

You are establishing a VPN connection over the Internet to your organization's home network from your hotel room. Which protocols could be used to create a VPN tunnel through the Internet, depending upon how your VPN server and client software are configured? (Choose two.)

- A. PPP
- B. SLIP
- C. PPTP
- D. L2TP

Question 65

You want to establish a VPN connection from your laptop at home to your company's internal network through the Internet. Your company's VPN server uses L2TP to create the tunnel. You need to configure your workstation's firewall to allow the VPN traffic through. What must you do? (Choose two.)

- A. Open TCP port 1723 in the firewall.
- B. Open UDP port 1701 in the firewall.
- C. Open TCP port 80 in the firewall.
- D. Open TCP port 1677 in the firewall

Question 66

You are establishing a VPN connection from your home computer to your office network through the Internet. Your VPN server and client are configured to use L2TP/IPSec to create and secure the tunnel. What is the first process that occurs during the establishment of the connection?

- A. A security association (SA) is negotiated between the client and the server using Internet key exchange (IKE).
- B. Encapsulating Security Payload (ESP) communication is established between the client and the server.
- C. An L2TP tunnel is established between the client and the server.
- D. L2TP packets are encapsulated by IPSec and transmitted between the client and the server.

Question 67

What security protocol is used by IKE to establish a security association between endpoints during the setup of an L2TP/IPSec VPN connection?

- A. Internet Protocol Security (IPSec)
- B. Transport Layer Security (TLS)
- C. Internet Security Association and Key Management Protocol (ISAKMP)
- D. Secure Shell (SSH)

Question 68

Which of the following are advantages of using an SSL VPN instead of a traditional VPN? (Choose two.)

- A. An SSL VPN requires fewer open ports in the firewall.
- B. An SSL VPN uses IKE to establish a security association between endpoints in the tunnel.
- C. An SSL VPN doesn't require special client software.
- D. An SSL VPN doesn't require digital certificates to authenticate users..

Question 69

Your VPN is configured to use PPTP to establish VPN tunnels between the VPN server and clients. Which security protocol is used to encrypt the traffic transmitted through the tunnel?

- A. IPSec
- B. MPPE
- C. TLS
- D. MS-CHAP

Question 70

Your organization is composed of a main office and three remote branch offices. An L2TP/IPSec VPN tunnel is used to connect the network at each branch office to the network at the main office through the Internet. When a branch office user accesses a resource, such as a shared folder on a server, on the main office network, her network request goes to the local branch office network first, then through the appropriate VPN

tunnel to the main office network, and finally reaches the desired resource on the main office network. What type of VPN is in use in this scenario?

- A. Client-to-site
- B. Point-to-point
- C. Client-server
- D. Site-to-site

Question 71

Which of the following is not true of 3DES?

- A. It encrypts blocks of 64-bit data.
- B. It uses ECB and CBC modes.
- C. It runs DES three times.
- D. It uses a substitution cipher.

Question 72

Which of the following ciphers operates on small chunks of data, typically in bit sizes?

- A. Block
- B. Stream
- C. Transposition
- D. Polyalphabetic

Question 73

A(n) _____ is where small changes in the input data create large changes in the resulting output data.

- A. Asymmetric key
- B. Avalanche effect
- C. Electronic code book
- D. Cipher-block chaining

Question 74

What takes variable-length input, along with a key, and creates a fixed-length output?

- A. Encryption algorithm
- B. HMAC function
- C. IDEA
- D. RC4

Question 75

How long are MD5 signatures?

- A. 64 bits
- B. 112 bits
- C. 128 bits
- D. 160 bits

Question 76

Which of the following is an example of an HMAC function?

- A. Skipjack
- B. RC2
- C. DH
- D. SHA-1