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 from 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 polices?

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 if 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 patters 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 1

Answer: B

Reasoning: The administrative controls involve the actions, policies, and management of the control system, and include procedures, hiring, security policies, monitoring, user management, and privilege management. The other types are physical and technical.

Question 2

Answer: C

Reasoning: The essential practices of identification process are uniqueness, nondescriptive, and issuance.

Question 3

Answer: A

Reasoning: EPROM (Erasable programmable read-only memory) must use ultraviolet to erase memory. EEPROM improves the process by using electricity instead of ultraviolet. PROM cannot be erased. RAM supports memory retention by an independent power source.

Question 4

Answer: D

Reasoning: A standard access list will use the source IP address to perform packet filtering. Both the source and destination IP addresses are used in an extended access list. Lock-andkey access lists will automatically create lists to allow traffic from authenticated sources. Reflexive lists will allow IP packets to be filtered based on upper-layer session information. A temporary connection can be opened for IP traffic.

Question 5

Answer: C

Reasoning: Electronic Codebook Mode (ECB) is the most basic form of DES. Each 640bit block of text is encrypted independently. It is generally used for very short messages.

Question 6

Answer: B

Reasoning: Router can be used on the perimeter to direct traffic between the trusted and untrusted network. Firewalls will typically block traffic, while IDS/IPS devices will monitor traffic and make decisions based on traffic types. Hubs are not considered perimeter devices.

Question 7

Answer: D

Reasoning: Defense-in-Depth solutions are used to delay an attack instead of preventing the attack. The purpose of delaying the attack is to allow time to effectively apply countermeasures.

Question 8

Answer: A

Reasoning: The domain namespace is a hierarchy naming tree structured use din DNS. The root of the tree is managed by the InterNIC. Domains are any tree or subtree within the overall domain namespace.

Question 9

Answer: B

Reasoning: DNS Servers which send queries to other servers to resolve external or offsite DNs domain names is called a forwarder.

Question 10

Answer: C

Reasoning: Risk assessments are either qualitative or quantitative. Quantitative assessments include Spanning Tree Analysis and Failure Modes and Effect Analysis.

Question 11

Answer: B

Reasoning: IEEE 802.16 is the official standard for WiMAX which is commonly used as a ‘last mile’ technology with a range of 1-10 miles and found commonly in MANs.

Question 12

Answer: B

Reasoning: The data life cycle have seven phases: Information generation, use, transfer, transformation, storage, archival, and destruction.

Question 13

Answer: D

Reasoning: The primary model for developing security policies is to deny everything unless specifically allowed.

Question 14

Answer: A

Reasoning: A demilitarized zone (DMZ) is a prescribed insecure area between a trusted network and an untrusted network. Corporations use the DMZ to manage customer relations using the Internet, without allowing the general public access to the internal network. The DMZ can also be used to provide interrelationship support between corporate partnerships and alliances.

Question 15

Answer: B

Reasoning: The physical security responsibilities revolve around site layout, building materials, building age, provision of the infrastructure, and requirements for health and safety.

Question 16

Answer: C

Reasoning: Symmetric Algorithms utilize a single cryptographic key to encrypt and decrypt a message. The most popular types are DES, AES, and CAST.

Question 17

Answer: A

Reasoning: A packet filter firewall is the most commonly implemented firewall between trusted and untrusted networks. They are often used in conjunction with other firewall types to provide a diverse solution.

Question 18

Answer: D

Reasoning: Smart cards are physical items that a person will possess to prove their identity to the network or computer system: They are something a person will have.

Question 19

Answer: C

Reasoning: Single sign on capabilities allow a user to login in once and utilize the same login for all systems managed by the authentication tool. Kerberos is recognized as a single sing on tool.

Question 20

Answer: B

Reasoning: The six primary access control characteristics are preventative, deterrent, detective, corrective, recovery, and compensation. All controls involve some form of monitoring, but monitoring is not a distinguished characteristic.

Question 21

Answer: D

Reasoning: User controls related to access can be single-factor, two-factor, or three-factor solutions. The three factors are related to what the user knows, has, or is and does.

Question 22

Answer: A

Reasoning: Some roles on the network have greater access and are more sensitive than others. Because of this, it is imperative not to be able to distinguish the network id of those individuals who possess these roles, namely admin, administrator, webmaster, fiancé, root. The role of manager is too vague to make a general rule for its exclusion.

Question 23

Answer: B

Reasoning: ISO 14442 defines the physical characteristics, radio frequency power, signal interface, and initialization for transmission contactless cards, or proximity integrated circuit cards (PICC).

Question 24

Answer: C

Reasoning: Cryptography is used to protect information from unauthorized access, whether that information is stored or transmitted. The technique will encrypt the data and decrypt it when required.

Question 25

Answer: A

Reasoning: ANSI X9.17 was developed for financial institutions. It uses a hierarchical approach to ensure keys are secure.

Question 26

Answer: D

Reasoning: Application servers are not themselves a component of the Defense-in-Depth solution, however, software such as host-based IDS may be installed on the server which would be considered a Defense-in-Depth component of the solution.

Question 27

Answer: C

Reasoning: DNS names can consist of upper and lower case letters, numbers and hyphens. Invalid characters are replaced by hyphens.

Question 28

Answer: B

Reasoning: Caching is the technique used to store information temporarily which has been recently accessed.

Question 29

Answer: D

Reasoning: RADIUS is an authentication tool, not a risk analysis. Operationally Critical Treat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk-based strategic assessments and planning technique.

Question 30

Answer: C

Reasoning: Cyberstalking is a form of harassment which uses electronic devices to track a person’s activities.

Question 31

Answer: A

Reasoning: The root node is the start of the decision tree in decision tree analysis.

Question 32

Answer: B

Reasoning: Protocol anomaly-based IDS solutions identify deviations from RFC standards, as well as attacks not having signatures. Well-defined protocols will reduce the number of false-positive results.

Question 33

Answer: C

Reasoning: Root hints are resource records used in DNS solutions to list the IP addresses for the DNS root servers.

Question 34

Answer: D

Reasoning: The two network topologies commonly used in VPN solutions are mesh and star. A hub configuration is another name for the star topology.

Question 35

Answer: A

Reasoning: IP Security, or IPSec, is a suite of protocols that allow VPNS to be established securely across an untrusted network.

Question 36

Answer: C

Reasoning: Hash functions are used to ensure that the received data matches the data that was sent. This verifies the integrity of a message.

Question 37

Answer: B

Reasoning: Biometric solutions can either be physiological or behavior. The two most popular forms of behavior biometrics are keystroke pattern analysis and signature dynamics.

Question 38

Answer: D

Reasoning: When speaking strictly in terms of password length, the longer the character string of the password, the more difficult the password would be to hack. However, the greater variety of characters used can make the password even more difficult: therefore a shorter password using alphanumeric and special characters would be more difficult to hack then a longer password using only the alphabet. A standard, or dictionary, password uses only the alphabet. A combination, or alphanumeric, passwords adds numbers to the password string. Complex password add special characters to the available selection and are typically the most difficult to hack.

Question 39

Answer: C

Reasoning: The core attributes of access control architectures are identification, authentication, authorization, and accountability. The related actions provide providing identity, verifying identity, limited actions, and tracking activities. Authorization techniques determine the actions available to an authenticated user.

Question 40

Answer: A

Reasoning: A recovery control is used to return conditions to normal. Corrective controls are used to apply remedies and compensation controls and provide alternatives to controlling the environment.