



CISSP.exam.724q

CISSP

CISSP

Certified Information Systems Security Professional

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (724 questions)

Question 1

Which conceptual approach to intrusion detection system is the MOST common?

- ☐ Behavior-based intrusion detection
- ☐ Knowledge-based intrusion detection
- ☐ Statistical anomaly-based intrusion detection
- ☐ Host-based intrusion detection

Question 2

Which of the following is used to create and modify the structure of your tables and other objects in the database?

- ☐ SQL Data Definition Language (DDL)
- ☐ SQL Data Manipulation Language (DML)
- ☐ SQL Data Relational Language (DRL)
- ☐ SQL Data Identification Language (DIL)

Question 3

An employee ensures all cables are shielded, builds concrete walls that extend from the true floor to the true ceiling and installs a white noise generator. What attack is the employee trying to protect against?

- ☐ Emanation Attacks
- ☐ Social Engineering
- ☐ Object reuse
- ☐ Wiretapping

Question 4

Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?

- ☐ Simulation test
- ☐ Checklist test
- ☐ Parallel test
- ☐ Structured walk-through test

Question 5

Communications devices must operate:

- ☐ at different speeds to communicate.
- ☐ at the same speed to communicate.
- ☐ at varying speeds to interact.
- ☐ at high speed to interact.

Question 6

Which of the following are placeholders for literal values in a Structured Query Language (SQL) query being sent to the database on a server?

- ☐ Bind variables
- ☐ Assimilation variables
- ☐ Reduction variables
- ☐ Resolution variables

Question 7

The authenticator within Kerberos provides a requested service to the client after validating which of the following?

- ☐ timestamp
- ☐ client public key
- ☐ client private key
- ☐ server public key

Question 8

Electrical systems are the lifeblood of computer operations. The continued supply of clean, steady power is required to maintain the proper personnel environment as well as to sustain data operations. Which of the following is not an element that can threaten power systems?

- ☐ Transient Noise
- ☐ Faulty Ground
- ☐ Brownouts
- ☐ UPS

Question 9

Which type of fire extinguisher is MOST appropriate for a digital information processing facility?

- ☐ Type A
- ☐ Type B
- ☐ Type C
- ☐ Type D

Question 10

Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?

- ☐ Interface errors are detected earlier.
- ☐ Errors in critical modules are detected earlier.
- ☐ Confidence in the system is achieved earlier.
- ☐ Major functions and processing are tested earlier.

Question 11

Legacy single sign on (SSO) is:

- ☐ Technology to allow users to authenticate to every application by entering the same user ID and password each time, thus having to remember only a single password.
- ☐ Technology to manage passwords consistently across multiple platforms, enforcing policies such as password change intervals.
- ☐ A mechanism where users can authenticate themselves once, and then a central repository of their credentials is used to launch various legacy applications.
- ☐ Another way of referring to SESAME and KryptoKnight, now that Kerberos is the de-facto industry standard single sign on mechanism.

Question 12

At which OSI/ISO layer is an encrypted authentication between a client software package and a firewall performed?

- ☐ Network layer
- ☐ Session layer
- ☐ Transport layer
- ☐ Data link layer

Question 13

Which of the following would best define a digital envelope?

- ☐ A message that is encrypted and signed with a digital certificate.
- ☐ A message that is signed with a secret key and encrypted with the sender's private key.
- ☐ A message encrypted with a secret key attached with the message. The secret key is encrypted with the public key of the receiver.
- ☐ A message that is encrypted with the recipient's public key and signed with the sender's private key.

Question 14

Which of the following is a tool often used to reduce the risk to a local area network (LAN) that has external connections by filtering Ingress and Egress traffic?

- ☐ A firewall.
- ☐ Dial-up.
- ☐ Passwords.
- ☐ Fiber optics.

Question 15

Domain Name Service is a distributed database system that is used to map:

- ☐ Domain Name to IP addresses.
- ☐ MAC addresses to domain names.
- ☐ MAC Address to IP addresses.
- ☐ IP addresses to MAC Addresses.

Question 16

Which of the following would best describe the difference between white-box testing and black-box testing?

- ☐ White-box testing is performed by an independent programmer team.
- ☐ Black-box testing uses the bottom-up approach.
- ☐ White-box testing examines the program internal logical structure.
- ☐ Black-box testing involves the business units

Question 17

Examples of types of physical access controls include all EXCEPT which of the following?

- ☐ badges
- ☐ locks
- ☐ guards
- ☐ passwords

Question 18

Which of the following can best be defined as a key recovery technique for storing knowledge of a cryptographic key by encrypting it with another key and ensuring that only certain third parties can perform the decryption operation to retrieve the stored key?

- ☐ Key escrow
- ☐ Fair cryptography
- ☐ Key encapsulation
- ☐ Zero-knowledge recovery

Question 19

Which of the following testing method examines internal structure or working of an application?

- ☐ White-box testing
- ☐ Parallel Test
- ☐ Regression Testing
- ☐ Pilot Testing

Question 20

This type of backup management provides a continuous on-line backup by using optical or tape "jukeboxes," similar to WORMs (Write Once, Read Many):

- ☐ Hierarchical Storage Management (HSM).
- ☐ Hierarchical Resource Management (HRM).
- ☐ Hierarchical Access Management (HAM).
- ☐ Hierarchical Instance Management (HIM).

Question 21

Identity Management solutions include such technologies as Directories services, Single Sign-On and Web Access management. There are many reasons for management to choose an identity management solution.

Which of the following is a key management challenge regarding identity management solutions?

- ☐ Increasing the number of points of failures.
- ☐ Users will no longer be able to “recycle” their password for different applications.
- ☐ Costs increase as identity management technologies require significant resources.
- ☐ It must be able to scale to support high volumes of data and peak transaction rates.

Question 22

What is the verification that the user's claimed identity is valid called and is usually implemented through a user password at log-on time?

- ☐ Authentication
- ☐ Identification
- ☐ Integrity
- ☐ Confidentiality

Question 23

Which of the following controls related to physical security is NOT an administrative control?

- ☐ Personnel controls
- ☐ Alarms
- ☐ Training
- ☐ Emergency response and procedures

Question 24

Which of the following is NOT a two-factor authentication mechanism?

- ☐ Something you have and something you know.
- ☐ Something you do and a password.
- ☐ A smartcard and something you are.
- ☐ Something you know and a password.

Question 25

Which of the following represents the best programming?

- ☐ Low cohesion, low coupling
- ☐ Low cohesion, high coupling
- ☐ High cohesion, low coupling
- ☐ High cohesion, high coupling

Question 26

When an outgoing request is made on a port number greater than 1023, this type of firewall creates an ACL to allow the incoming reply on that port to pass:

- ☐ packet filtering
- ☐ Circuit level proxy
- ☐ Dynamic packet filtering
- ☐ Application level proxy

Question 27

To be in compliance with the Montreal Protocol, which of the following options can be taken to refill a Halon flooding system in the event that Halon is fully discharged in the computer room?

- ☐ Order an immediate refill with Halon 1201 from the manufacturer.
- ☐ Contact a Halon recycling bank to make arrangements for a refill.
- ☐ Order a Non-Hydrochlorofluorocarbon compound from the manufacturer.
- ☐ Order an immediate refill with Halon 1301 from the manufacturer.

Question 28

Critical areas should be lighted:

- ☐ Eight feet high and two feet out.
- ☐ Eight feet high and four feet out.
- ☐ Ten feet high and four feet out.
- ☐ Ten feet high and six feet out.

Question 29

The primary service provided by Kerberos is which of the following?

- ☐ non-repudiation
- ☐ confidentiality
- ☐ authentication
- ☐ authorization

Question 30

A momentary high voltage is a:

- ☐ spike
- ☐ blackout
- ☐ surge
- ☐ fault

Question 31

The high availability of multiple all-inclusive, easy-to-use hacking tools that do NOT require much technical knowledge has brought a growth in the number of which type of attackers?

- ☐ Black hats
- ☐ White hats
- ☐ Script kiddies
- ☐ Phreakers

Question 32

Which of the following is the most reliable authentication method for remote access?

- ☐ Variable callback system
- ☐ Synchronous token
- ☐ Fixed callback system
- ☐ Combination of callback and caller ID

Question 33

Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?

- ☐ It is unlikely to be affected by the same disaster.
- ☐ It is close enough to become operational quickly.
- ☐ It is close enough to serve its users.
- ☐ It is convenient to airports and hotels.

Question 34

Which of the following groups represents the leading source of computer crime losses?

- ☐ Hackers
- ☐ Industrial saboteurs
- ☐ Foreign intelligence officers
- ☐ Employees

Question 35

Organizations should not view disaster recovery as which of the following?

- ☐ Committed expense.
- ☐ Discretionary expense.
- ☐ Enforcement of legal statutes.
- ☐ Compliance with regulations.

Question 36

Which of the following Common Data Network Services is used to send and receive email internally or externally through an email gateway device?

- ☐ File services.
- ☐ Mail services.
- ☐ Print services.
- ☐ Client/Server services.

Question 37

Which of the following was developed to address some of the weaknesses in Kerberos and uses public key cryptography for the distribution of secret keys and provides additional access control support?

- ☐ SESAME
- ☐ RADIUS
- ☐ KryptoKnight
- ☐ TACACS+

Question 38

In which of the following security models is the subject's clearance compared to the object's classification such that specific rules can be applied to control how the subject-to-object interactions take place?

- ☐ Bell-LaPadula model
- ☐ Biba model
- ☐ Access Matrix model
- ☐ Take-Grant model

Question 39

Which of the following is commonly used for retrofitting multilevel security to a database management system?

- ☐ trusted front-end
- ☐ trusted back-end
- ☐ controller
- ☐ kernel

Question 40

Which term BEST describes a practice used to detect fraud for users or a user by forcing them to be away from the workplace for a while?

- ☐ Mandatory Vacations
- ☐ Least Privilege Principle
- ☐ Obligatory Separation
- ☐ Job Rotation

Question 41

Which of the following protocols does not operate at the data link layer (layer 2)?

- ☐ PPP
- ☐ RARP
- ☐ L2F
- ☐ ICMP

Question 42

Which backup method usually resets the archive bit on the files after they have been backed up?

- ☐ Incremental backup method.
- ☐ Differential backup method.
- ☐ Partial backup method.
- ☐ Tape backup method.

Question 43

Which of the following statements regarding an off-site information processing facility is TRUE?

- ☐ It should have the same amount of physical access restrictions as the primary processing site.
- ☐ It should be located in proximity to the originating site so that it can quickly be made operational.
- ☐ It should be easily identified from the outside so in the event of an emergency it can be easily found.
- ☐ Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Question 44

Which protocol is used to send email?

- ☐ File Transfer Protocol (FTP).
- ☐ Post Office Protocol (POP).
- ☐ Network File System (NFS).
- ☐ Simple Mail Transfer Protocol (SMTP).

Question 45

What is RAD?

- ☐ A development methodology
- ☐ A project management technique
- ☐ A measure of system complexity
- ☐ Risk-assessment diagramming

Question 46

A smart Card that has two chips with the Capability of utilizing both Contact and Contactless formats is called:

- ☐ Contact Smart Cards
- ☐ Contactless Smart Cards
- ☐ Hybrid Cards
- ☐ Combi Cards

Question 47

A persistent collection of interrelated data items can be defined as which of the following?

- ☐ database
- ☐ database management system
- ☐ database security
- ☐ database shadowing

Question 48

Which of the following attack is MOSTLY performed by an attacker to steal the identity information of a user such as credit card number, passwords, etc?

- ☐ Smurf attack
- ☐ Traffic analysis
- ☐ Pharming
- ☐ Interrupt attack

Question 49

Which of the following represents a relation, which is the basis of a relational database?

- ☐ One-dimensional table
- ☐ Two-dimensional table
- ☐ Three-dimensional table
- ☐ Four-dimensional table

Question 50

Which of the following is NOT a property of a one-way hash function?

- ☐ It converts a message of a fixed length into a message digest of arbitrary length.
- ☐ It is computationally infeasible to construct two different messages with the same digest.
- ☐ It converts a message of arbitrary length into a message digest of a fixed length.
- ☐ Given a digest value, it is computationally infeasible to find the corresponding message.

Question 51

Which is the last line of defense in a physical security sense?

- ☐ people
- ☐ interior barriers
- ☐ exterior barriers
- ☐ perimeter barriers

Question 52

Which of the following questions is less likely to help in assessing physical and environmental protection?

- ☐ Are entry codes changed periodically?
- ☐ Are appropriate fire suppression and prevention devices installed and working?
- ☐ Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
- ☐ Is physical access to data transmission lines controlled?

Question 53

Why does compiled code pose more of a security risk than interpreted code?

- ☐ Because malicious code can be embedded in compiled code and be difficult to detect.
- ☐ If the executed compiled code fails, there is a chance it will fail insecurely.
- ☐ Because compilers are not reliable.
- ☐ There is no risk difference between interpreted code and compiled code.

Question 54

A momentary power outage is a:

- ☐ spike
- ☐ blackout
- ☐ surge
- ☐ fault

Question 55

Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?

- ☐ Business and functional managers
- ☐ IT Security practitioners
- ☐ System and information owners
- ☐ Chief information officer

Question 56

Which of the following can be defined as THE unique attribute used as a unique identifier within a given table to identify a tuple?

- ☐ primary key
- ☐ candidate key
- ☐ foreign key
- ☐ secondary key

Question 57

An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?

- ☐ Discretionary Access
- ☐ Least Privilege
- ☐ Mandatory Access
- ☐ Separation of Duties

Question 58

A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:

- ☐ server cluster.
- ☐ client cluster.
- ☐ guest cluster.
- ☐ host cluster.

Question 59

Which of the following would describe a type of biometric error refers to as FASLE rejection rate?

- ☐ Type I error
- ☐ Type II error
- ☐ Type III error
- ☐ CER error

Question 60

What are cognitive passwords?

- ☐ Passwords that can be used only once.
- ☐ Fact or opinion-based information used to verify an individual's identity.
- ☐ Password generators that use a challenge response scheme.
- ☐ Passphrases.

Question 61

Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is NOT a component that achieves this type of security?

- ☐ Administrative control mechanisms
- ☐ Integrity control mechanisms
- ☐ Technical control mechanisms
- ☐ Physical control mechanisms

Question 62

Layer 2 of the OSI model has two sublayers. What are those sublayers, and what are two IEEE standards that describe technologies at that layer?

- ☐ LLC and MAC; IEEE 802.2 and 802.3
- ☐ LLC and MAC; IEEE 802.1 and 802.3
- ☐ Network and MAC; IEEE 802.1 and 802.3
- ☐ LLC and MAC; IEEE 802.2 and 802.3

Question 63

Which of the following is not classified as "Security and Audit Frameworks and Methodologies"?

- ☐ Bell LaPadula
- ☐ Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- ☐ IT Infrastructure Library (ITIL)
- ☐ Control Objectives for Information and related Technology (COBIT)

Question 64

Which of the following statements pertaining to PPTP (Point-to-Point Tunneling Protocol) is NOT true?

- ☐ PPTP allows the tunneling of any protocols that can be carried within PPP.
- ☐ PPTP does not provide strong encryption.
- ☐ PPTP does not support any token-based authentication method for users.
- ☐ PPTP is derived from L2TP.

Question 65

Which of the following does not address Database Management Systems (DBMS) Security?

- ☐ Perturbation
- ☐ Cell suppression
- ☐ Padded cells
- ☐ Partitioning

Question 66

Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?

- ☐ OAKLEY
- ☐ Internet Security Association and Key Management Protocol (ISAKMP)
- ☐ Simple Key-management for Internet Protocols (SKIP)
- ☐ IPsec Key exchange (IKE)

Question 67

This type of supporting evidence is used to help prove an idea or a point, however it cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?

- ☐ Circumstantial evidence
- ☐ Corroborative evidence
- ☐ Opinion evidence
- ☐ Secondary evidence

Question 68

Which of the following is not an element of a relational database model?

- ☐ Relations, tuples, attributes and domains
- ☐ Data Manipulation Language (DML) on how the data will be accessed and manipulated
- ☐ Constraints to determine valid ranges and values
- ☐ Security structures called referential validation within tables

Question 69

Which of the following is NOT a security characteristic we need to consider while choosing a biometric identification system?

- ☐ data acquisition process
- ☐ cost
- ☐ enrollment process
- ☐ speed and user interface

Question 70

Devices that supply power when the commercial utility power system fails are called which of the following?

- ☐ power conditioners
- ☐ uninterruptible power supplies
- ☐ power filters
- ☐ power dividers

Question 71

Which of the following is a NOT a guideline necessary to enhance security in the critical Heating Ventilation Air Conditioning (HVAC) aspect of facility operations?

- ☐ Restrict access to main air intake points to persons who have a work-related reason to be there
- ☐ Maintain access rosters of maintenance personnel who are not authorized to work on the system
- ☐ Escort all contractors with access to the system while on site
- ☐ Ensure that all air intake points are adequately secured with locking devices

Question 72

Which security model uses an access control triple and also requires separation of duty?

- ☐ DAC
- ☐ Lattice
- ☐ Clark-Wilson
- ☐ Bell-LaPadula

Question 73

Which of the following statements pertaining to firewalls is NOT true?

- ☐ Firewalls create bottlenecks between the internal and external network.
- ☐ Firewalls allow for centralization of security services in machines optimized and dedicated to the task.
- ☐ Firewalls protect a network at all layers of the OSI models.
- ☐ Firewalls are used to create security checkpoints at the boundaries of private networks.

Question 74

During the initial stage of configuration of your firewall, which of the following rules appearing in an Internet firewall policy is inappropriate?

- ☐ The firewall software shall run on a dedicated computer.
- ☐ Appropriate firewall documentation and a copy of the rulebase shall be maintained on offline storage at all times.
- ☐ The firewall shall be configured to deny all services not expressly permitted.
- ☐ The firewall should be tested online first to validate proper configuration.

Question 75

For competitive reasons, the customers of a large shipping company called the "Integrated International Secure Shipping Containers Corporation" (IISCC) like to keep private the various cargos that they ship. IISCC uses a secure database system based on the Bell-LaPadula access control model to keep this information private. Different information in this database is classified at different levels. For example, the time and date a ship departs is labeled Unclassified, so customers can estimate when their cargos will arrive, but the contents of all shipping containers on the ship are labeled Top Secret to keep different shippers from viewing each other's cargos.

An unscrupulous fruit shipper, the "Association of Private Fruit Exporters, Limited" (APFEL) wants to learn whether or not a competitor, the "Fruit Is Good Corporation" (FIGCO), is shipping pineapples on the ship "S.S. Cruise Pacific" (S.S. CP). APFEL can't simply read the top secret contents in the IISCC database because of the access model. A smart APFEL worker, however, attempts to insert a false, unclassified record in the database that says that FIGCO is shipping pineapples on the S.S. CP, reasoning that if there is already a FIGCO-pineapple-SSCP record then the insertion attempt will fail. But the attempt does not fail, so APFEL can't be sure whether or not FIGCO is shipping pineapples on the S.S. CP.

What is the name of the access control model property that prevented APFEL from reading FIGCO's cargo information? What is a secure database technique that could explain why, when the insertion attempt succeeded, APFEL was still unsure whether or not FIGCO was shipping pineapples?

- ☐ *-Property and Polymorphism
- ☐ Strong *-Property and Polyinstantiation
- ☐ Simple Security Property and Polymorphism
- ☐ Simple Security Property and Polyinstantiation

Question 76

It is a violation of the "separation of duties" principle when which of the following individuals access the software on systems implementing security?

- ☐ security administrator
- ☐ security analyst
- ☐ systems auditor
- ☐ systems programmer

Question 77

Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

- ☐ Steganography
- ☐ Digital watermarking
- ☐ Digital enveloping
- ☐ Digital signature

Question 78

Which of the following technologies has been developed to support TCP/IP networking over low-speed serial interfaces?

- ☐ ISDN
- ☐ SLIP
- ☐ xDSL
- ☐ T1

Question 79

The control of communications test equipment should be clearly addressed by security policy for which of the following reasons?

- ☐ Test equipment is easily damaged.
- ☐ Test equipment can be used to browse information passing on a network.
- ☐ Test equipment is difficult to replace if lost or stolen.
- ☐ Test equipment must always be available for the maintenance personnel.

Question 80

The act of requiring two of the three factors to be used in the authentication process refers to:

- ☐ Two-Factor Authentication
- ☐ One-Factor Authentication
- ☐ Bi-Factor Authentication
- ☐ Double Authentication

Question 81

Which of the following statements pertaining to ethical hacking is NOT true?

- ☐ An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services.
- ☐ Testing should be done remotely to simulate external threats.
- ☐ Ethical hacking should not involve writing to or modifying the target systems negatively.
- ☐ Ethical hackers never use tools that have the potential of affecting servers or services.

Question 82

The IP header contains a protocol field. If this field contains the value of 1, what type of data is contained within the IP datagram?

- ☐ TCP.
- ☐ ICMP.
- ☐ UDP.
- ☐ IGMP.

Question 83

Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

- ☐ Accountability of biometrics systems
- ☐ Acceptability of biometrics systems
- ☐ Availability of biometrics systems
- ☐ Adaptability of biometrics systems

Question 84

An application layer firewall is also called a:

- ☐ Proxy
- ☐ A Presentation Layer Gateway.
- ☐ A Session Layer Gateway.
- ☐ A Transport Layer Gateway.

Question 85

The Domain Name System (DNS) is a global network of:

- ☐ servers that provide these Domain Name Services.
- ☐ clients that provide these Domain Name Services.
- ☐ hosts that provide these Domain Name Services.
- ☐ workstations that provide these Domain Name Services.

Question 86

There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?

- ☐ public keys
- ☐ private keys
- ☐ public-key certificates
- ☐ private-key certificates

Question 87

Which one of the following is usually not a benefit resulting from the use of firewalls?

- ☐ Reduces the risks of external threats from malicious hackers.
- ☐ Prevents the spread of viruses.
- ☐ Reduces the threat level on internal system.
- ☐ Allows centralized management and control of services.

Question 88

With regard to databases, which of the following has characteristics of ease of reusing code and analysis and reduced maintenance?

- ☐ Object-Oriented Databases (OODB)
- ☐ Object-Relational Databases (ORDB)
- ☐ Relational Databases
- ☐ Database management systems (DBMS)

Question 89

Which of the following is often implemented by a one-for-one disk to disk ratio?

- ☐ RAID Level 1
- ☐ RAID Level 0
- ☐ RAID Level 2
- ☐ RAID Level 5

Question 90

A public key algorithm that does both encryption and digital signature is which of the following?

- ☐ RSA
- ☐ DES
- ☐ IDEA
- ☐ Diffie-Hellman

Question 91

What is Kerberos?

- ☐ A three-headed dog from the Egyptian mythology.
- ☐ A trusted third-party authentication protocol.
- ☐ A security model.
- ☐ A remote authentication dial-in user server.

Question 92

Which of the following places the Orange Book classifications in order from MOST secure to LEAST secure?

- ☐ A, B, C, D
- ☐ D, C, B, A
- ☐ D, B, A, C
- ☐ C, D, B, A

Question 93

Which of the following is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes?

- ☐ The Software Capability Maturity Model (CMM)
- ☐ The Spiral Model
- ☐ The Waterfall Model
- ☐ Expert Systems Model

Question 94

What can be defined as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate?

- ☐ A public-key certificate
- ☐ An attribute certificate
- ☐ A digital certificate
- ☐ A descriptive certificate

Question 95

Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?

- ☐ 192.168.42.5
- ☐ 192.166.42.5
- ☐ 192.175.42.5
- ☐ 192.1.42.5

Question 96

What is the 802.11 standard related to?

- ☐ Public Key Infrastructure (PKI)
- ☐ Wireless network communications
- ☐ Packet-switching technology
- ☐ The OSI/ISO model

Question 97

Which of the following is TRUE regarding Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)?

- ☐ TCP is connection-oriented, UDP is not.
- ☐ UDP provides for Error Correction, TCP does not.
- ☐ UDP is useful for longer messages, rather than TCP.
- ☐ TCP does not guarantee delivery of data, while UDP does guarantee data delivery.

Question 98

A server farm consisting of multiple similar servers seen as a single IP address from users interacting with the group of servers is an example of which of the following?

- ☐ Server clustering
- ☐ Redundant servers
- ☐ Multiple servers
- ☐ Server fault tolerance

Question 99

The Orange Book requires auditing mechanisms for any systems evaluated at which of the following levels?

- ☐ C1 and above.
- ☐ C2 and above.
- ☐ B1 and above.
- ☐ B2 and above.

Question 100

Which of the following computer crime is MORE often associated with INSIDERS?

- ☐ IP spoofing
- ☐ Password sniffing
- ☐ Data diddling
- ☐ Denial of service (DoS)

Question 101

Which of the following can BEST eliminate dial-up access through a Remote Access Server as a hacking vector?

- ☐ Using a TACACS+ server.
- ☐ Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
- ☐ Setting modem ring count to at least 5
- ☐ Only attaching modems to non-networked hosts.

Question 102

Which of the following services relies on UDP?

- ☐ FTP
- ☐ Telnet
- ☐ DNS
- ☐ SMTP

Question 103

Which of the following is TRUE of network security?

- ☐ A firewall is a not a necessity in today's connected world.
- ☐ A firewall is a necessity in today's connected world.
- ☐ A whitewall is a necessity in today's connected world.
- ☐ A black firewall is a necessity in today's connected world.

Question 104

Which of the following is NOT true of the Kerberos protocol?

- ☐ Only a single login is required per session.
- ☐ The initial authentication steps are done using public key algorithm.
- ☐ The KDC is aware of all systems in the network and is trusted by all of them
- ☐ It performs mutual authentication

Question 105

Which of the following is NOT a security goal for remote access?

- ☐ Reliable authentication of users and systems
- ☐ Protection of confidential data
- ☐ Easy to manage access control to systems and network resources
- ☐ Automated login for remote users

Question 106

This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

- ☐ Checkpoint level
- ☐ Ceiling level
- ☐ Clipping level
- ☐ Threshold level

Question 107

Which of the following services is NOT provided by the digital signature standard (DSS)?

- ☐ Encryption
- ☐ Integrity
- ☐ Digital signature
- ☐ Authentication

Question 108

Which virus category has the capability of changing its own code, making it harder to detect by anti-virus software?

- ☐ Stealth viruses
- ☐ Polymorphic viruses
- ☐ Trojan horses
- ☐ Logic bombs

Question 109

Which type of password provides maximum security because a new password is required for each new log-on?

- ☐ One-time or dynamic password
- ☐ Cognitive password
- ☐ Static password
- ☐ Passphrase

Question 110

Physically securing backup tapes from unauthorized access is obviously a security concern and is considered a function of the:

- ☐ Operations Security Domain.
- ☐ Operations Security Domain Analysis.
- ☐ Telecommunications and Network Security Domain.
- ☐ Business Continuity Planning and Disaster Recovery Planning.

Question 111

Single Sign-on (SSO) is characterized by which of the following advantages?

- ☐ Convenience
- ☐ Convenience and centralized administration
- ☐ Convenience and centralized data administration
- ☐ Convenience and centralized network administration

Question 112

Which RAID implementation stripes data and parity at block level across all the drives?

- ☐ RAID level 1
- ☐ RAID level 2
- ☐ RAID level 4
- ☐ RAID level 5

Question 113

What best describes a scenario when an employee has been shaving off pennies from multiple accounts and depositing the funds into his own bank account?

- ☐ Data fiddling
- ☐ Data diddling
- ☐ Salami techniques
- ☐ Trojan horses

Question 114

What is NOT true about a one-way hashing function?

- ☐ It provides authentication of the message
- ☐ A hash cannot be reverse to get the message used to create the hash
- ☐ The results of a one-way hash is a message digest
- ☐ It provides integrity of the message

Question 115

In biometric identification systems, the parts of the body conveniently available for identification are:

- ☐ neck and mouth
- ☐ hands, face, and eyes
- ☐ feet and hair
- ☐ voice and neck

Question 116

Which of the following are additional terms used to describe knowledge-based IDS and behavior-based IDS?

- ☐ Signature-based IDS and statistical anomaly-based IDS, respectively.
- ☐ Signature-based IDS and dynamic anomaly-based IDS, respectively.
- ☐ Anomaly-based IDS and statistical-based IDS, respectively.
- ☐ Signature-based IDS and motion anomaly-based IDS, respectively.

Question 117

When considering an IT System Development Life-cycle, security should be:

- ☐ Mostly considered during the initiation phase.
- ☐ Mostly considered during the development phase.
- ☐ Treated as an integral part of the overall system design.
- ☐ Added once the design is completed.

Question 118

What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?

- ☐ The most critical operations are moved from alternate site to primary site before others
- ☐ Operation may be carried by a completely different team than disaster recovery team
- ☐ The least critical functions should be moved back first
- ☐ You move items back in the same order as the categories document in your plan or exactly in the same order as you did on your way to the alternate site

Question 119

Which of the following components are considered part of the Trusted Computing Base?

- ☐ Trusted hardware and firmware.
- ☐ Trusted hardware and software.
- ☐ Trusted hardware, software and firmware.
- ☐ Trusted computer operators and system managers.

Question 120

Which of the following is defined as a key establishment protocol based on the Diffie-Hellman algorithm proposed for IPsec but superseded by IKE?

- ☐ Diffie-Hellman Key Exchange Protocol
- ☐ Internet Security Association and Key Management Protocol (ISAKMP)
- ☐ Simple Key-management for Internet Protocols (SKIP)
- ☐ OAKLEY

Question 121

Application Layer Firewalls operate at the:

- ☐ OSI protocol Layer seven, the Application Layer.
- ☐ OSI protocol Layer six, the Presentation Layer.
- ☐ OSI protocol Layer five, the Session Layer.
- ☐ OSI protocol Layer four, the Transport Layer.

Question 122

All hosts on an IP network have a logical ID called a(n):

- ☐ IP address.
- ☐ MAC address.
- ☐ TCP address.
- ☐ Datagram address.

Question 123

What is the most effective means of determining that controls are functioning properly within an operating system?

- ☐ Interview with computer operator
- ☐ Review of software control features and/or parameters
- ☐ Review of operating system manual
- ☐ Interview with product vendor

Question 124

If an organization were to deploy only one Intrusion Detection System (IDS) sensor to protect its information system from the Internet:

- ☐ It should be host-based and installed on the most critical system in the DMZ, between the external router and the firewall.
- ☐ It should be network-based and installed in the DMZ, between the external router and the firewall.
- ☐ It should be network-based and installed between the firewall to the DMZ and the intranet.
- ☐ It should be host-based and installed between the external router and the Internet.

Question 125

Which of the following offers security to wireless communications?

- ☐ S-WAP
- ☐ WTLS
- ☐ WSP
- ☐ WDP

Question 126

Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?

- ☐ System development activity
- ☐ Help-desk function
- ☐ System Imaging
- ☐ Risk management process

Question 127

What type of key would you find within a browser's list of trusted root CAs?

- ☐ Private key
- ☐ Symmetric key
- ☐ Recovery key
- ☐ Public key

Question 128

Which of the following tools is less likely to be used by a hacker?

- ☐ l0phtcrack
- ☐ Tripwire
- ☐ OphCrack
- ☐ John the Ripper

Question 129

Which of the following is NOT true concerning Application Control?

- ☐ It limits end users use of applications in such a way that only particular screens are visible.
- ☐ Only specific records can be requested through the application controls
- ☐ Particular usage of the application can be recorded for audit purposes
- ☐ It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved

Question 130

Which of the following is NOT a technique used to perform a penetration test?

- ☐ traffic padding
- ☐ scanning and probing
- ☐ war dialing
- ☐ sniffing

Question 131

A DMZ is located:

- ☐ right behind your first Internet facing firewall
- ☐ right in front of your first Internet facing firewall
- ☐ right behind your first network active firewall
- ☐ right behind your first network passive Internet http firewall

Question 132

A Differential backup process will:

- ☐ Backs up data labeled with archive bit 1 and leaves the data labeled as archive bit 1
- ☐ Backs up data labeled with archive bit 1 and changes the data label to archive bit 0
- ☐ Backs up data labeled with archive bit 0 and leaves the data labeled as archive bit 0
- ☐ Backs up data labeled with archive bit 0 and changes the data label to archive bit 1

Question 133

Which of the following is the primary security feature of a proxy server?

- ☐ Virus Detection
- ☐ URL blocking
- ☐ Route blocking
- ☐ Content filtering

Question 134

Which of the following is NOT true about IPSec Tunnel mode?

- ☐ Fundamentally an IP tunnel with encryption and authentication
- ☐ Works at the Transport layer of the OSI model
- ☐ Have two sets of IP headers
- ☐ Established for gateway service

Question 135

What setup should an administrator use for regularly testing the strength of user passwords?

- ☐ A networked workstation so that the live password database can easily be accessed by the cracking program.
- ☐ A networked workstation so the password database can easily be copied locally and processed by the cracking program.
- ☐ A standalone workstation on which the password database is copied and processed by the cracking program.
- ☐ A password-cracking program is unethical; therefore it should not be used.

Question 136

The DES algorithm is an example of what type of cryptography?

- ☐ Secret Key
- ☐ Two-key
- ☐ Asymmetric Key
- ☐ Public Key

Question 137

Which of the following is the MOST secure firewall implementation?

- ☐ Dual-homed host firewalls
- ☐ Screened-subnet firewalls
- ☐ Screened-host firewalls
- ☐ Packet-filtering firewalls

Question 138

What is used to hide data from unauthorized users by allowing a relation in a database to contain multiple tuples with the same primary keys with each instance distinguished by a security level?

- ☐ Data mining
- ☐ Polyinstantiation
- ☐ Cell suppression
- ☐ Noise and perturbation

Question 139

Which of the following ciphers is a subset on which the Vigenere polyalphabetic cipher was based on?

- ☐ Caesar
- ☐ The Jefferson disks
- ☐ Enigma
- ☐ SIGABA

Question 140

The basic language of modems and dial-up remote access systems is:

- ☐ Asynchronous Communication.
- ☐ Synchronous Communication.
- ☐ Asynchronous Interaction.
- ☐ Synchronous Interaction.

Question 141

What can be defined as an event that could cause harm to the information systems?

- ☐ A risk
- ☐ A threat
- ☐ A vulnerability
- ☐ A weakness

Question 142

Which of the following was developed as a simple mechanism for allowing simple network terminals to load their operating system from a server over the LAN?

- ☐ DHCP
- ☐ BootP
- ☐ DNS
- ☐ ARP

Question 143

Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?

- ☐ Estimating the cost of the changes requested
- ☐ Recreating and analyzing the problem
- ☐ Determining the interface that is presented to the user
- ☐ Establishing the priorities of requests

Question 144

Business Continuity and Disaster Recovery Planning (Primarily) addresses the:

- ☐ Availability of the CIA triad
- ☐ Confidentiality of the CIA triad
- ☐ Integrity of the CIA triad
- ☐ Availability, Confidentiality and Integrity of the CIA triad

Question 145

What can be defined as a momentary low voltage?

- ☐ spike
- ☐ blackout
- ☐ sag
- ☐ fault

Question 146

This is a common security issue that is extremely hard to control in large environments. It occurs when a user has more computer rights, permissions, and access than what is required for the tasks the user needs to fulfill. What BEST describes this scenario?

- ☐ Excessive Rights
- ☐ Excessive Access
- ☐ Excessive Permissions
- ☐ Excessive Privileges

Question 147

Which answer BEST describes a computer software attack that takes advantage of a previously unpublished vulnerability?

- ☐ Zero-Day Attack
- ☐ Exploit Attack
- ☐ Vulnerability Attack
- ☐ Software Crack

Question 148

Which of the following NAT firewall translation modes allows a large group of internal clients to share a single or small group of ROUTABLE IP addresses for the purpose of hiding their identities when communicating with external hosts?

- ☐ Static translation
- ☐ Load balancing translation
- ☐ Network redundancy translation
- ☐ Dynamic translation

Question 149

Which of the following biometric devices offers the LOWEST CER?

- ☐ Keystroke dynamics
- ☐ Voice verification
- ☐ Iris scan
- ☐ Fingerprint

Question 150

At which of the basic phases of the System Development Life Cycle are security requirements formalized?

- ☐ Disposal
- ☐ System Design Specifications
- ☐ Development and Implementation
- ☐ Functional Requirements Definition

Question 151

Which of the following devices enables more than one signal to be sent out simultaneously over one physical circuit?

- ☐ Router
- ☐ Multiplexer
- ☐ Channel service unit/Data service unit (CSU/DSU)
- ☐ Wan switch

Question 152

The spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on the server in which of the following scenarios?

- ☐ system is up and running
- ☐ system is quiesced but operational
- ☐ system is idle but operational
- ☐ system is up and in single-user-mode

Question 153

The National Institute of Standards and Technology (NIST) standard pertaining to perimeter protection states that critical areas should be illuminated up to?

- ☐ Illuminated at nine feet high with at least three foot-candles
- ☐ Illuminated at eight feet high with at least three foot-candles
- ☐ Illuminated at eight feet high with at least two foot-candles
- ☐ Illuminated at nine feet high with at least two foot-candles

Question 154

Which of the following NAT firewall translation modes offers no protection from hacking attacks to an internal host using this functionality?

- ☐ Network redundancy translation
- ☐ Load balancing translation
- ☐ Dynamic translation
- ☐ Static translation

Question 155

During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?

- ☐ Damage mitigation
- ☐ Install LAN communications network and servers
- ☐ Assess damage to LAN and servers
- ☐ Recover equipment

Question 156

What is the percentage of invalid subjects that are falsely accepted by a Biometric authentication system called?

- ☐ False Rejection Rate (FRR) or Type I Error
- ☐ False Acceptance Rate (FAR) or Type II Error
- ☐ Crossover Error Rate (CER)
- ☐ True Acceptance Rate (TAR) or Type III Error

Question 157

Which of the following would MOST likely ensure that a system development project meets business objectives?

- ☐ Development and tests are run by different individuals
- ☐ User involvement in system specification and acceptance
- ☐ Development of a project plan identifying all development activities
- ☐ Strict deadlines and budgets

Question 158

What are the four domains that make up CobiT?

- ☐ Plan and Organize, Maintain and Implement, Deliver and Support, and Monitor and Evaluate
- ☐ Plan and Organize, Acquire and Implement, Support and Purchase, and Monitor and Evaluate
- ☐ Acquire and Implement, Deliver and Support, Monitor, and Evaluate
- ☐ Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate

Question 159

Who is responsible for implementing user clearances in computer-based information systems at the B3 level of the TCSEC rating?

- ☐ Security administrators
- ☐ Operators
- ☐ Data owners
- ☐ Data custodians

Question 160

Which of the following is NOT a disadvantage of Single Sign On (SSO)?

- ☐ Support for all major operating system environment is difficult
- ☐ The cost associated with SSO development can be significant
- ☐ SSO could be single point of failure and total compromise of an organization asset
- ☐ SSO improves an administrator's ability to manage user's account and authorization to all associated system

Question 161

Which of the following describes the major disadvantage of many Single Sign-On (SSO) implementations?

- ☐ Once an individual obtains access to the system through the initial log-on, they have access to all resources within the environment that the account has access to.
- ☐ The initial logon process is cumbersome to discourage potential intruders.
- ☐ Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.
- ☐ Once a user obtains access to the system through the initial log-on, he has to logout from all other systems

Question 162

Which of the following is the marriage of object-oriented and relational technologies combining the attributes of both?

- ☐ object-relational database
- ☐ object-oriented database
- ☐ object-linking database
- ☐ object-management database

Question 163

What is the most secure way to dispose of information on a CD-ROM?

- ☐ Sanitizing
- ☐ Physical damage
- ☐ Degaussing
- ☐ Physical destruction

Question 164

Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?

- ☐ SSL
- ☐ FTP
- ☐ SSH
- ☐ S/MIME

Question 165

Operations Security seeks to PRIMARILY protect against which of the following?

- ☐ object reuse
- ☐ facility disaster
- ☐ compromising emanations
- ☐ asset threats

Question 166

To be admissible in court, computer evidence must be which of the following?

- ☐ Relevant
- ☐ Decrypted
- ☐ Edited
- ☐ Incriminating

Question 167

Which of the following is an extension to Network Address Translation that permits multiple devices providing services on a local area network (LAN) to be mapped to a single public IP address?

- ☐ IP Spoofing
- ☐ IP subnetting
- ☐ Port address translation
- ☐ IP Distribution

Question 168

Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?

- ☐ Test environment using test data.
- ☐ Test environment using sanitized live workloads data.
- ☐ Production environment using test data.
- ☐ Production environment using sanitized live workloads data.

Question 169

What would BEST define a covert channel?

- ☐ An undocumented backdoor that has been left by a programmer in an operating system
- ☐ An open system port that should be closed.
- ☐ A communication channel that allows transfer of information in a manner that violates the system's security policy.
- ☐ A Trojan horse.

Question 170

The RSA Algorithm uses which mathematical concept as the basis of its encryption?

- ☐ Geometry
- ☐ 16-round ciphers
- ☐ PI (3.14159...)
- ☐ Two large prime numbers

Question 171

Which of the following computer recovery sites is the least expensive and the most difficult to test?

- ☐ non-mobile hot site.
- ☐ mobile hot site.
- ☐ warm site.
- ☐ cold site.

Question 172

Which of the following is NOT a system-sensing wireless proximity card?

- ☐ magnetically striped card
- ☐ passive device
- ☐ field-powered device
- ☐ transponder

Question 173

In the physical security context, a security door equipped with an electronic lock configured to ignore the unlock signals sent from the building emergency access control system in the event of an issue (fire, intrusion, power failure) would be in which of the following configuration?

- ☐ Fail Soft
- ☐ Fail Open
- ☐ Fail Safe
- ☐ Fail Secure

Question 174

Which of the following determines that the product developed meets the projects goals?

- ☐ verification
- ☐ validation
- ☐ concurrence
- ☐ accuracy

Question 175

What is a password called that is the same for each log-on session?

- ☐ one-time password
- ☐ two-time password
- ☐ static password
- ☐ dynamic password

Question 176

In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?

- ☐ Known-plaintext attack
- ☐ Ciphertext-only attack
- ☐ Chosen-Ciphertext attack
- ☐ Plaintext-only attack

Question 177

What uses a key of the same length as the message where each bit or character from the plaintext is encrypted by a modular addition?

- ☐ Running key cipher
- ☐ One-time pad
- ☐ Steganography
- ☐ Cipher block chaining

Question 178

What is the primary reason why some sites choose not to implement Trivial File Transfer Protocol (TFTP)?

- ☐ It is too complex to manage user access restrictions under TFTP
- ☐ Due to the inherent security risks
- ☐ It does not offer high level encryption like FTP
- ☐ It cannot support the Lightweight Directory Access Protocol (LDAP)

Question 179

Which type of control is concerned with avoiding occurrences of risks?

- ☐ Deterrent controls
- ☐ Detective controls
- ☐ Preventive controls
- ☐ Compensating controls

Question 180

What mechanism does a system use to compare the security labels of a subject and an object?

- ☐ Validation Module.
- ☐ Reference Monitor.
- ☐ Clearance Check.
- ☐ Security Module.

Question 181

Which of the following is a fraud detection method whereby employees are moved from position to position?

- ☐ Job Rotation
- ☐ Mandatory Rotation
- ☐ Mandatory Vacations
- ☐ Mandatory Job Duties

Question 182

The standard server port number for HTTP is which of the following?

- ☐ 81
- ☐ 80
- ☐ 8080
- ☐ 8180

Question 183

Which of the following would constitute the BEST example of a password to use for access to a system by a network administrator?

- ☐ holiday
- ☐ Christmas12
- ☐ Jenny
- ☐ GyN19Za!

Question 184

Which xDSL flavor, appropriate for home or small offices, delivers more bandwidth downstream than upstream and over longer distance?

- ☐ VDSL
- ☐ SDSL
- ☐ ADSL
- ☐ HDSL

Question 185

Frame relay and X.25 networks are part of which of the following?

- ☐ Circuit-switched services
- ☐ Cell-switched services
- ☐ Packet-switched services
- ☐ Dedicated digital services

Question 186

What is the MAIN objective of proper separation of duties?

- ☐ To prevent employees from disclosing sensitive information.
- ☐ To ensure access controls are in place.
- ☐ To ensure that no single individual can compromise a system.
- ☐ To ensure that audit trails are not tampered with.

Question 187

Which of the following statements pertaining to Kerberos is TRUE?

- ☐ Kerberos does not address availability
- ☐ Kerberos does not address integrity
- ☐ Kerberos does not make use of Symmetric Keys
- ☐ Kerberos cannot address confidentiality of information

Question 188

Which of the following Common Data Network Services is used to print documents to a shared printer or a print queue/spooler?

- ☐ Mail services.
- ☐ Print services.
- ☐ Client/Server services.
- ☐ Domain Name Service.

Question 189

Which of the following protects Kerberos against replay attacks?

- ☐ Tokens
- ☐ Passwords
- ☐ Cryptography
- ☐ Time stamps

Question 190

The absence of a safeguard, or a weakness in a system that may possibly be exploited is called a(n)?

- ☐ Threat
- ☐ Exposure
- ☐ Vulnerability
- ☐ Risk

Question 191

Regarding risk reduction, which of the following answers is BEST defined by the process of giving only just enough access to information necessary for them to perform their job functions?

- ☐ Least Privilege Principle
- ☐ Minimum Privilege Principle
- ☐ Mandatory Privilege Requirement
- ☐ Implicit Information Principle

Question 192

Which of the following is NOT appropriate in addressing object reuse?

- ☐ Degaussing magnetic tapes when they're no longer needed.
- ☐ Deleting files on disk before reusing the space.
- ☐ Clearing memory blocks before they are allocated to a program or data.
- ☐ Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.

Question 193

Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

- ☐ SSH (Secure Shell)
- ☐ S/MIME (Secure MIME)
- ☐ SET (Secure Electronic Transaction)
- ☐ SSL (Secure Sockets Layer)

Question 194

Which authentication technique BEST protects against hijacking?

- ☐ Static authentication
- ☐ Continuous authentication
- ☐ Robust authentication
- ☐ Strong authentication

Question 195

Which of the following is NOT a characteristic or shortcoming of packet filtering gateways?

- ☐ The source and destination addresses, protocols, and ports contained in the IP packet header are the only information that is available to the router in making a decision whether or not to permit traffic access to an internal network.
- ☐ They don't protect against IP or DNS address spoofing.
- ☐ They do not support strong user authentication.
- ☐ They are appropriate for medium-risk environment.

Question 196

What is an IP routing table?

- ☐ A list of IP addresses and corresponding MAC addresses.
- ☐ A list of station and network addresses with corresponding gateway IP address.
- ☐ A list of host names and corresponding IP addresses.
- ☐ A list of current network interfaces on which IP routing is enabled.

Question 197

Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

- ☐ Extensible Authentication Protocol
- ☐ Challenge Handshake Authentication Protocol
- ☐ Remote Authentication Dial-In User Service
- ☐ Multilevel Authentication Protocol.

Question 198

Which of the following answers is directly related to providing High Availability to your users?

- ☐ Backup data circuits
- ☐ Good hiring practices
- ☐ Updated Antivirus Software
- ☐ Senior Executive Support

Question 199

Which of the following should NOT normally be allowed through a firewall?

- ☐ SNMP
- ☐ SMTP
- ☐ HTTP
- ☐ SSH

Question 200

What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?

- ☐ Certificate revocation list
- ☐ Certificate revocation tree
- ☐ Authority revocation list
- ☐ Untrusted certificate list

Question 201

Which of the following Kerberos components holds all users' and services' cryptographic keys?

- ☐ The Key Distribution Service
- ☐ The Authentication Service
- ☐ The Key Distribution Center
- ☐ The Key Granting Service

Question 202

Which of the following is NOT true of Secure Sockets Layer (SSL)?

- ☐ By convention it uses 's-http:/' instead of 'http:/'.
- ☐ Is the predecessor to the Transport Layer Security (TLS) protocol.
- ☐ It was developed by Netscape.
- ☐ It is used for transmitting private information, data, and documents over the Internet.

Question 203

A Packet Filtering Firewall system is considered a:

- ☐ first generation firewall.
- ☐ second generation firewall.
- ☐ third generation firewall.
- ☐ fourth generation firewall.

Question 204

Which of the following is NOT a true statement regarding the implementation of the 3DES modes?

- ☐ DES-EEE1 uses one key
- ☐ DES-EEE2 uses two keys
- ☐ DES-EEE3 uses three keys
- ☐ DES-EDE2 uses two keys

Question 205

Proxies work by transferring a copy of each accepted data packet from one network to another, thereby masking the:

- ☐ data's payload.
- ☐ data's details.
- ☐ data's owner.
- ☐ data's origin.

Question 206

You are part of a security staff at a highly profitable bank and each day, all traffic on the network is logged for later review. Every Friday when major deposits are made you're seeing a series of bits placed in the "Urgent Pointer" field of a TCP packet. This is only 16 bits which isn't much but it concerns you because:

- ☐ This could be a sign of covert channeling in bank network communications and should be investigated.
- ☐ It could be a sign of a damaged network cable causing the issue.
- ☐ It could be a symptom of malfunctioning network card or drivers and the source system should be checked for the problem.
- ☐ It is normal traffic because sometimes the previous fields 16 bit checksum value can over run into the urgent pointer's 16 bit field causing the condition.

Question 207

The BEST technique to authenticate to a system is to:

- ☐ establish biometric access through a secured server or Web site.
- ☐ ensure the person is authenticated by something he knows and something he has.
- ☐ maintain correct and accurate ACLs (access control lists) to allow access to applications.
- ☐ allow access only through user ID and password.

Question 208

Which of the following logical access exposures involves changing data before, or as it is entered into the computer?

- ☐ Data diddling
- ☐ Salami techniques
- ☐ Trojan horses
- ☐ Viruses

Question 209

Which of the following remote access authentication systems is the MOST robust?

- ☐ TACACS+
- ☐ RADIUS
- ☐ PAP
- ☐ TACACS

Question 210

Which type of algorithm is considered to have the highest strength per bit of key length of any of the asymmetric algorithms?

- ☐ Rivest, Shamir, Adleman (RSA)
- ☐ El Gamal
- ☐ Elliptic Curve Cryptography (ECC)
- ☐ Advanced Encryption Standard (AES)

Question 211

Which division of the Orange Book deals with discretionary protection (need-to-know)?

- ☐ D
- ☐ C
- ☐ B
- ☐ A

Question 212

What enables users to validate each other's certificate when they are certified under different certification hierarchies?

- ☐ Cross-certification
- ☐ Multiple certificates
- ☐ Redundant certification authorities
- ☐ Root certification authorities

Question 213

A packet containing a long string of NOP's followed by a command is usually indicative of what?

- ☐ A syn scan.
- ☐ A half-port scan.
- ☐ A buffer overflow attack.
- ☐ A packet destined for the network's broadcast address.

Question 214

What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?

- ☐ Key collision
- ☐ Key clustering
- ☐ Hashing
- ☐ Ciphertext collision

Question 215

Which backup method only copies files that have been recently added or changed and also leaves the archive bit unchanged?

- ☐ Full backup method
- ☐ Incremental backup method
- ☐ Fast backup method
- ☐ Differential backup method

Question 216

Within the OSI model, at what layer are some of the SLIP, CSLIP, PPP control functions provided?

- ☐ Data Link
- ☐ Transport
- ☐ Presentation
- ☐ Application

Question 217

What is the role of IKE within the IPsec protocol?

- ☐ peer authentication and key exchange
- ☐ data encryption
- ☐ data signature
- ☐ enforcing quality of service

Question 218

What is the percentage of valid subjects that are falsely rejected by a Biometric Authentication system called?

- ☐ False Rejection Rate (FRR) or Type I Error
- ☐ False Acceptance Rate (FAR) or Type II Error
- ☐ Crossover Error Rate (CER)
- ☐ True Rejection Rate (TRR) or Type III Error

Question 219

Which of the following access control models requires defining classification for objects?

- ☐ Role-based access control
- ☐ Discretionary access control
- ☐ Identity-based access control
- ☐ Mandatory access control

Question 220

When first analyzing an intrusion that has just been detected and confirming that it is a true positive, which of the following actions should be done as a first step if you wish to prosecute the attacker in court?

- ☐ Back up the compromised systems.
- ☐ Identify the attacks used to gain access.
- ☐ Capture and record system information.
- ☐ Isolate the compromised systems.

Question 221

Which of the following is a not a preventative control?

- ☐ Deny programmer access to production data.
- ☐ Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.
- ☐ Run a source comparison program between control and current source periodically.
- ☐ Establish procedures for emergency changes.

Question 222

Which of the following phases of a system development life-cycle is most concerned with establishing a good security policy as the foundation for design?

- ☐ Development/acquisition
- ☐ Implementation
- ☐ Initiation
- ☐ Maintenance

Question 223

Which of the following results in the most devastating business interruptions?

- ☐ Loss of Hardware/Software
- ☐ Loss of Data
- ☐ Loss of Communication Links
- ☐ Loss of Applications

Question 224

Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

- ☐ The Take-Grant model
- ☐ The Biba integrity model
- ☐ The Clark Wilson integrity model
- ☐ The Bell-LaPadula integrity model

Question 225

Kerberos can prevent which one of the following attacks?

- ☐ Tunneling attack.
- ☐ Playback (replay) attack.
- ☐ Destructive attack.
- ☐ Process attack.

Question 226

Which of the following can be defined as a unique identifier in the table that unambiguously points to an individual tuple or record in the table?

- ☐ primary key
- ☐ candidate key
- ☐ secondary key
- ☐ foreign key

Question 227

The RSA algorithm is an example of what type of cryptography?

- ☐ Asymmetric Key.
- ☐ Symmetric Key.
- ☐ Secret Key.
- ☐ Private Key.

Question 228

Which of the following type of traffic can easily be filtered with a stateful packet filter by enforcing the context or state of the request?

- ☐ ICMP
- ☐ TCP
- ☐ UDP
- ☐ IP

Question 229

Which cable technology refers to the CAT3 and CAT5 categories?

- ☐ Coaxial cables
- ☐ Fiber Optic cables
- ☐ Axial cables
- ☐ Twisted Pair cables

Question 230

Which of the following is NOT a common weakness of packet filtering firewalls?

- ☐ Vulnerability to denial-of-service and related attacks.
- ☐ Vulnerability to IP spoofing.
- ☐ Limited logging functionality.
- ☐ No support for advanced user authentication schemes.

Question 231

In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?

- ☐ Human Resources
- ☐ Industrial Security
- ☐ Public Relations
- ☐ External Audit Group

Question 232

CobiT was developed from the COSO framework. Which of the choices below best describe the COSO's main objectives and purpose?

- ☐ COSO main purpose is to help ensure fraudulent financial reporting cannot take place in an organization
- ☐ COSO main purpose is to define a sound risk management approach within financial companies.
- ☐ COSO addresses corporate culture and policy development.
- ☐ COSO is risk management system used for the protection of federal systems.

Question 233

What is a common problem when using vibration detection devices for perimeter control?

- ☐ They are vulnerable to non-adversarial disturbances.
- ☐ They can be defeated by electronic means.
- ☐ Signal amplitude is affected by weather conditions.
- ☐ They must be buried below the frost line.

Question 234

Which of the following establishes the minimal national standards for certifying and accrediting national security systems?

- ☐ NIACAP
- ☐ DIACAP
- ☐ HIPAA
- ☐ TCSEC

Question 235

How do you distinguish between a bridge and a router?

- ☐ A bridge simply connects multiple networks, a router examines each packet to determine which network to forward it to.
- ☐ "Bridge" and "router" are synonyms for equipment used to join two networks.
- ☐ The bridge is a specific type of router used to connect a LAN to the global Internet.
- ☐ The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.

Question 236

Which of the following security control is intended to avoid an incident from occurring?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Question 237

In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class C network?

- ☐ The first bit of the IP address would be set to zero.
- ☐ The first bit of the IP address would be set to one and the second bit set to zero.
- ☐ The first two bits of the IP address would be set to one, and the third bit set to zero.
- ☐ The first three bits of the IP address would be set to one.

Question 238

Which of the following statements pertaining to air conditioning for an information processing facility is TRUE?

- ☐ The AC units must be controllable from outside the area.
- ☐ The AC units must keep negative pressure in the room so that smoke and other gases are forced out of the room.
- ☐ The AC units must be on the same power source as the equipment in the room to allow for easier shutdown.
- ☐ The AC units must be dedicated to the information processing facility.

Question 239

Which of the following countermeasures would be the most appropriate to prevent possible intrusion or damage from wardialing attacks?

- ☐ Monitoring and auditing for such activity
- ☐ Require user authentication
- ☐ Making sure only necessary phone numbers are made public
- ☐ Using completely different numbers for voice and data accesses

Question 240

What attack involves the perpetrator sending spoofed packet(s) which contains the same destination and source IP address as the remote host, the same port for the source and destination, having the SYN flag, and targeting any open ports that are open on the remote host?

- ☐ Boink attack
- ☐ Land attack
- ☐ Teardrop attack
- ☐ Smurf attack

Question 241

The Data Encryption Algorithm performs how many rounds of substitution and permutation?

- ☐ 4
- ☐ 16
- ☐ 54
- ☐ 64

Question 242

The communications products and services, which ensure that the various components of a network (such as devices, protocols, and access methods) work together refers to:

- ☐ Netware Architecture.
- ☐ Network Architecture.
- ☐ WAN Architecture.
- ☐ Multiprotocol Architecture.

Question 243

What is considered the MOST important type of error to avoid for a biometric access control system?

- ☐ Type I Error
- ☐ Type II Error
- ☐ Combined Error Rate
- ☐ Crossover Error Rate

Question 244

What is the appropriate role of the security analyst in the application system development or acquisition project?

- ☐ policeman
- ☐ control evaluator & consultant
- ☐ data owner
- ☐ application user

Question 245

Which of the following biometric devices has the lowest user acceptance level?

- ☐ Retina Scan
- ☐ Fingerprint scan
- ☐ Hand geometry
- ☐ Signature recognition

Question 246

Which of the following is TRUE of two-factor authentication?

- ☐ It uses the RSA public-key signature based on integers with large prime factors.
- ☐ It requires two measurements of hand geometry.
- ☐ It does not use single sign-on technology.
- ☐ It relies on two independent proofs of identity.

Question 247

Which of the following best defines a Computer Security Incident Response Team (CSIRT)?

- ☐ An organization that provides a secure channel for receiving reports about suspected security incidents.
- ☐ An organization that ensures that security incidents are reported to the authorities.
- ☐ An organization that coordinates and supports the response to security incidents.
- ☐ An organization that disseminates incident-related information to its constituency and other involved parties.

Question 248

What is a sequence of characters that is usually longer than the allotted number for a password called?

- ☐ passphrase
- ☐ cognitive phrase
- ☐ anticipated phrase
- ☐ Real phrase

Question 249

Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

- ☐ B
- ☐ A
- ☐ C
- ☐ D

Question 250

Which of the following is defined as an Internet, IPsec, key-establishment protocol, partly based on OAKLEY, that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations?

- ☐ Internet Key exchange (IKE)
- ☐ Security Association Authentication Protocol (SAAP)
- ☐ Simple Key-management for Internet Protocols (SKIP)
- ☐ Key Exchange Algorithm (KEA)

Question 251

The object-relational and object-oriented models are better suited to managing complex data such as required for which of the following?

- ☐ computer-aided development and imaging
- ☐ computer-aided duplexing and imaging
- ☐ computer-aided processing and imaging
- ☐ computer-aided design and imaging

Question 252

There is no way to completely abolish or avoid risks, you can only manage them. A risk free environment does not exist. If you have risks that have been identified, understood and evaluated to be acceptable in order to conduct business operations. What is this this approach to risk management called?

- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk Transference
- ☐ Risk Mitigation

Question 253

What would you call the process that takes advantages of the security provided by a transmission protocol by carrying one protocol over another?

- ☐ Piggy Backing
- ☐ Steganography
- ☐ Tunneling
- ☐ Concealing

Question 254

You are a manager for a large international bank and periodically move employees between positions in your department. What is this process called?

- ☐ Job Rotation
- ☐ Separation of Duties
- ☐ Mandatory Vacation
- ☐ Dual Control

Question 255

What is called the use of technologies such as fingerprint, retina, and iris scans to authenticate the individuals requesting access to resources?

- ☐ Micrometrics
- ☐ Macrometrics
- ☐ Biometrics
- ☐ MicroBiometrics

Question 256

Which of the following can best be defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs?

- ☐ A known-plaintext attack
- ☐ A known-algorithm attack
- ☐ A chosen-ciphertext attack
- ☐ A chosen-plaintext attack

Question 257

PGP uses which of the following to encrypt data?

- ☐ An asymmetric encryption algorithm
- ☐ A symmetric encryption algorithm
- ☐ A symmetric key distribution system
- ☐ An X.509 digital certificate

Question 258

Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?

- ☐ External Hot site
- ☐ Warm Site
- ☐ Internal Hot Site
- ☐ Dual Data Center

Question 259

Which common backup method is the fastest on a daily basis?

- ☐ Full backup method
- ☐ Incremental backup method
- ☐ Fast backup method
- ☐ Differential backup method

Question 260

In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?

- ☐ Using a write blocker
- ☐ Made a full-disk image
- ☐ Created a message digest for log files
- ☐ Displayed the contents of a folder

Question 261

What is Dumpster Diving?

- ☐ Going through dust bin
- ☐ Running through another person's garbage for discarded document, information and other various items that could be used against that person or company
- ☐ Performing media analysis
- ☐ performing forensics on the deleted items

Question 262

Which of the following could be BEST defined as the likelihood of a threat agent taking advantage of a vulnerability?

- ☐ A risk.
- ☐ A residual risk.
- ☐ An exposure.
- ☐ A countermeasure.

Question 263

What is an error called that causes a system to be vulnerable because of the environment in which it is installed?

- ☐ Configuration error
- ☐ Environmental error
- ☐ Access validation error
- ☐ Exceptional condition handling error

Question 264

Which of the following is often the GREATEST challenge of distributed computing solutions?

- ☐ scalability
- ☐ security
- ☐ heterogeneity
- ☐ usability

Question 265

Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

- ☐ Direct evidence.
- ☐ Circumstantial evidence.
- ☐ Conclusive evidence.
- ☐ Corroborative evidence.

Question 266

Who developed one of the first mathematical models of a multilevel-security computer system?

- ☐ Diffie and Hellman.
- ☐ Clark and Wilson.
- ☐ Bell and LaPadula.
- ☐ Gasser and Lipner.

Question 267

Which of the following Common Data Network Services allocates computing power resources among workstations with some shared resources centralized on a server?

- ☐ Print services
- ☐ File services
- ☐ Client/Server services
- ☐ Domain Name Service

Question 268

Virus scanning and content inspection of S/MIME encrypted e-mail without doing any further processing is:

- ☐ Not possible
- ☐ Only possible with key recovery scheme of all user keys
- ☐ It is possible only if X509 Version 3 certificates are used
- ☐ It is possible only by "brute force" decryption

Question 269

Which of the following risk handling technique involves the practice of being proactive so that the risk in question is not realized?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Question 270

Which of the following is TRUE about Kerberos?

- ☐ It utilizes public key cryptography.
- ☐ It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
- ☐ It depends upon symmetric ciphers.
- ☐ It is a second party authentication system.

Question 271

Which of the following would not correspond to the number of primary keys values found in a table in a relational database?

- ☐ Degree
- ☐ Number of tuples
- ☐ Cardinality
- ☐ Number of rows

Question 272

In biometrics, "one-to-many" search against database of stored biometric images is done in:

- ☐ Authentication
- ☐ Identification
- ☐ Identities
- ☐ Identity-based access control

Question 273

Which of the following is the most costly countermeasure to reducing physical security risks?

- ☐ Procedural Controls
- ☐ Hardware Devices
- ☐ Electronic Systems
- ☐ Security Guards

Question 274

Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use Hybrid Encryption Methods. What does this mean?

- ☐ Use of public key encryption to secure a secret key, and message encryption using the secret key.
- ☐ Use of the recipient's public key for encryption and decryption based on the recipient's private key.
- ☐ Use of software encryption assisted by a hardware encryption accelerator.
- ☐ Use of elliptic curve encryption.

Question 275

Which of the following should be allowed through a firewall to easy communication and usage by users?

- ☐ RIP
- ☐ IGRP
- ☐ DNS
- ☐ OSPF

Question 276

Which of the following division is defined in the TCSEC (Orange Book) as minimal protection?

- ☐ Division D
- ☐ Division C
- ☐ Division B
- ☐ Division A

Question 277

Which of the following backup method must be made regardless of whether Differential or Incremental methods are used?

- ☐ Full Backup Method.
- ☐ Incremental backup method.
- ☐ Supplemental backup method.
- ☐ Tape backup method.

Question 278

A packet filtering firewall looks at the data packet to get information about the source and destination addresses of an incoming packet, the protocol (TCP, UDP, or ICMP), and the source and destination port for the:

- ☐ desired service.
- ☐ dedicated service.
- ☐ delayed service.
- ☐ distributed service.

Question 279

One drawback of Application Level Firewall is that it reduces network performance due to the fact that it must analyze every packet and:

- ☐ decide what to do with each application.
- ☐ decide what to do with each user.
- ☐ decide what to do with each port.
- ☐ decide what to do with each packet.

Question 280

Why would a memory dump be admissible as evidence in court?

- ☐ Because it is used to demonstrate the truth of the contents.
- ☐ Because it is used to identify the state of the system.
- ☐ Because the state of the memory cannot be used as evidence.
- ☐ Because of the exclusionary rule.

Question 281

Which of the following concerning the Rijndael block cipher algorithm is NOT true?

- ☐ The design of Rijndael was strongly influenced by the design of the block cipher Square.
- ☐ A total of 25 combinations of key length and block length are possible
- ☐ Both block size and key length can be extended to multiples of 64 bits.
- ☐ The cipher has a variable block length and key length.

Question 282

The main issue with RAID Level 1 is that the one-for-one ratio is:

- ☐ very expensive, resulting in the highest cost per megabyte of data capacity.
- ☐ very inexpensive, resulting in the lowest cost per megabyte of data capacity.
- ☐ very unreliable resulting in a greater risk of losing data.
- ☐ very reliable resulting in a lower risk of losing data.

Question 283

Which backup method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup?

- ☐ The differential backup method.
- ☐ The full backup method.
- ☐ The incremental backup method.
- ☐ The tape backup method.

Question 284

When a possible intrusion into your organization's information system has been detected, which of the following actions should be performed first?

- ☐ Eliminate all means of intruder access.
- ☐ Contain the intrusion.
- ☐ Determine to what extent systems and data are compromised.
- ☐ Communicate with relevant parties.

Question 285

An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):

- ☐ active attack.
- ☐ outside attack.
- ☐ inside attack.
- ☐ passive attack.

Question 286

When backing up an applications system's data, which of the following is a key question to be answered first?

- ☐ When to make backups.
- ☐ Where to keep backups.
- ☐ What records to backup.
- ☐ How to store backups.

Question 287

The main risks that physical security components combat are all of the following EXCEPT:

- ☐ SYN flood
- ☐ Physical damage
- ☐ Theft
- ☐ Tailgating

Question 288

Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?

- ☐ Composition
- ☐ Priorities
- ☐ Dependencies
- ☐ Service levels

Question 289

What is the MOST critical piece to disaster recovery and continuity planning?

- ☐ Security policy
- ☐ Management support
- ☐ Availability of backup information processing facilities
- ☐ Staff training

Question 290

IT security measures should:

- ☐ be complex.
- ☐ be tailored to meet organizational security goals.
- ☐ make sure that every asset of the organization is well protected.
- ☐ not be developed in a layered fashion.

Question 291

What security model is dependent on security labels?

- ☐ Discretionary access control
- ☐ Label-based access control
- ☐ Mandatory access control
- ☐ Non-discretionary access control

Question 292

Ding Ltd. is a firm specialized in intellectual property business. A new video streaming application needs to be installed for the purpose of conducting the annual awareness program as per the firm security program. The application will stream internally copyrighted computer based training videos. The requirements for the application installation are to use a single server, low cost technologies, high performance and no high availability capacities.

In regards to storage technology, what is the most suitable configuration for the server hard drives?

- ☐ Single hard disk (no RAID)
- ☐ RAID 0
- ☐ RAID 1
- ☐ RAID 10

Question 293

Which of the following is related to physical security and is NOT considered a technical control?

- ☐ Access control Mechanisms
- ☐ Intrusion Detection Systems
- ☐ Firewalls
- ☐ Locks

Question 294

Which of the following best describes the purpose of debugging programs?

- ☐ To generate random data that can be used to test programs before implementing them.
- ☐ To ensure that program coding flaws are detected and corrected.
- ☐ To protect, during the programming phase, valid changes from being overwritten by other changes.
- ☐ To compare source code versions before transferring to the test environment

Question 295

Which RAID level concept is considered more expensive and is applied to servers to create what is commonly known as server fault tolerance?

- ☐ RAID level 0
- ☐ RAID level 1
- ☐ RAID level 2
- ☐ RAID level 5

Question 296

Compared to RSA, which of the following is true of Elliptic Curve Cryptography (ECC)?

- ☐ It has been mathematically proved to be more secure.
- ☐ It has been mathematically proved to be less secure.
- ☐ It is believed to require longer key for equivalent security.
- ☐ It is believed to require shorter keys for equivalent security.

Question 297

Which of the following are required for Life-Cycle Assurance?

- ☐ System Architecture and Design specification
- ☐ Security Testing and Covert Channel Analysis
- ☐ Security Testing and Trusted distribution
- ☐ Configuration Management and Trusted Facility Management

Question 298

Which of the following is a cryptographic protocol and infrastructure developed to send encrypted credit card numbers over the Internet?

- ☐ Secure Electronic Transaction (SET)
- ☐ MONDEX
- ☐ Secure Shell (SSH-2)
- ☐ Secure Hypertext Transfer Protocol (S-HTTP)

Question 299

What refers to legitimate users accessing networked services that would normally be restricted to them?

- ☐ Spoofing
- ☐ Piggybacking
- ☐ Eavesdropping
- ☐ Logon abuse

Question 300

Which of the following Orange Book ratings represents the highest level of trust?

- ☐ B1
- ☐ B2
- ☐ F6
- ☐ C2

Question 301

The throughput rate is the rate at which individuals, once enrolled, can be processed and identified or authenticated by a biometric system. Acceptable throughput rates are in the range of:

- ☐ 100 subjects per minute.
- ☐ 25 subjects per minute.
- ☐ 10 subjects per minute.
- ☐ 50 subjects per minute.

Question 302

Because ordinary cable introduces a toxic hazard in the event of fire, special cabling is required in a separate area provided for air circulation for heating, ventilation, and air-conditioning (sometimes referred to as HVAC) and typically provided in the space between the structural ceiling and a drop-down ceiling. This area is referred to as the:

- ☐ smoke boundary area.
- ☐ fire detection area.
- ☐ plenum area.
- ☐ intergen area.

Question 303

Which of the following Common Data Network Services is used to share data files and subdirectories on file servers?

- ☐ File services.
- ☐ Mail services.
- ☐ Print services.
- ☐ Client/Server services.

Question 304

Which of the following is a Microsoft technology for communication among software components distributed across networked computers?

- ☐ DDE
- ☐ OLE
- ☐ ODBC
- ☐ DCOM

Question 305

In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?

- ☐ The transactions should be dropped from processing.
- ☐ The transactions should be processed after the program makes adjustments.
- ☐ The transactions should be written to a report and reviewed.
- ☐ The transactions should be corrected and reprocessed.

Question 306

Computer security should be first and foremost which of the following?

- ☐ Cover all identified risks
- ☐ Be cost-effective.
- ☐ Be examined in both monetary and non-monetary terms.
- ☐ Be proportionate to the value of IT systems.

Question 307

In a stateful inspection firewall, data packets are captured by an inspection engine that is operating at the:

- ☐ Network or Transport Layer.
- ☐ Application Layer.
- ☐ Inspection Layer.
- ☐ Data Link Layer.

Question 308

Which of the following ensures that security is NOT breached when a system crash or other system failure occurs?

- ☐ Trusted recovery
- ☐ Hot swappable
- ☐ Redundancy
- ☐ Secure boot

Question 309

A prolonged electrical power supply that is below normal voltage is a:

- ☐ brownout
- ☐ blackout
- ☐ surge
- ☐ fault

Question 310

Which of the following translates source code one command at a time for execution on a computer?

- ☐ A translator
- ☐ An interpreter
- ☐ A compiler
- ☐ An assembler

Question 311

Java is not:

- ☐ Object-oriented.
- ☐ Distributed.
- ☐ Architecture Specific.
- ☐ Multithreaded.

Question 312

Which of the following is NOT a symmetric key algorithm?

- ☐ Blowfish
- ☐ Digital Signature Standard (DSS)
- ☐ Triple DES (3DES)
- ☐ RC5

Question 313

The Loki attack exploits a covert channel using which network protocol?

- ☐ TCP
- ☐ PPP
- ☐ ICMP
- ☐ SMTP

Question 314

Which of the following biometrics devices has the highest Crossover Error Rate (CER)?

- ☐ Iris scan
- ☐ Hand geometry
- ☐ Voice pattern
- ☐ Fingerprints

Question 315

A 'Pseudo flaw' is which of the following?

- ☐ An apparent loophole deliberately implanted in an operating system program as a trap for intruders.
- ☐ An omission when generating Pseudo-code.
- ☐ Used for testing for bounds violations in application programming.
- ☐ A normally generated page fault causing the system to halt.

Question 316

In the Open Systems Interconnect (OSI) Reference Model, at what level are TCP and UDP provided?

- ☐ Transport
- ☐ Network
- ☐ Presentation
- ☐ Application

Question 317

Which of the following offers advantages such as the ability to use stronger passwords, easier password administration, one set of credential, and faster resource access?

- ☐ Smart cards
- ☐ Single Sign-On (SSO)
- ☐ Symmetric Ciphers
- ☐ Public Key Infrastructure (PKI)

Question 318

Which of the following is an advantage of proxies?

- ☐ Proxies provide a single point of access, control, and logging.
- ☐ Proxies must exist for each service.
- ☐ Proxies create a single point of failure.
- ☐ Proxies do not protect the base operating system.

Question 319

There are basic goals of Cryptography. Which of the following most benefits from the process of encryption?

- ☐ Confidentiality
- ☐ Authentication
- ☐ Integrity
- ☐ Non-Repudiation

Question 320

In order to enable users to perform tasks and duties without having to go through extra steps, it is important that the security controls and mechanisms that are in place have a degree of?

- ☐ Complexity
- ☐ Non-transparency
- ☐ Transparency
- ☐ Simplicity

Question 321

Which expert system operating mode allows determining if a given hypothesis is valid?

- ☐ Blackboard
- ☐ Lateral chaining
- ☐ Forward chaining
- ☐ Backward chaining

Question 322

Which of the following statements pertaining to IPSec is NOT true?

- ☐ A security association has to be defined between two IPSec systems in order for bi-directional communication to be established.
- ☐ Integrity and authentication for IP datagrams are provided by AH.
- ☐ ESP provides for integrity, authentication and encryption to IP datagrams.
- ☐ In transport mode, ESP only encrypts the data payload of each packet.

Question 323

If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a:

- ☐ server farm
- ☐ client farm
- ☐ cluster farm
- ☐ host farm

Question 324

A hardware RAID implementation is usually:

- ☐ platform-independent.
- ☐ platform-dependent.
- ☐ operating system dependent.
- ☐ software dependent.

Question 325

When RAID runs as part of the operating system on the file server, it is an example of a:

- ☐ software implementation.
- ☐ hardware implementation.
- ☐ network implementation.
- ☐ server implementation.

Question 326

Which of the following provides coordinated procedures for minimizing loss of life, injury, and property damage in response to a physical threat?

- ☐ Business continuity plan
- ☐ Incident response plan
- ☐ Disaster recovery plan
- ☐ Occupant emergency plan

Question 327

In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?

- ☐ Both client and server
- ☐ The client's browser
- ☐ The web server
- ☐ The merchant's Certificate Server

Question 328

During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?

- ☐ Measurement of accuracy
- ☐ Elapsed time for completion of critical tasks
- ☐ Quantitatively measuring the results of the test
- ☐ Evaluation of the observed test results

Question 329

Which of the following is covered under Crime Insurance Policy Coverage?

- ☐ Inscribed, printed and Written documents
- ☐ Manuscripts
- ☐ Accounts Receivable
- ☐ Money and Securities

Question 330

Which of the following fire extinguishing systems incorporating a detection system is currently the most recommended water system for a computer room?

- ☐ Wet pipe
- ☐ Dry pipe
- ☐ Deluge
- ☐ Preaction

Question 331

A Differential backup process:

- ☐ Backs up data labeled with archive bit 1 and leaves the data labeled as archive bit 1
- ☐ Backs up data labeled with archive bit 1 and changes the data label to archive bit 0
- ☐ Backs up data labeled with archive bit 0 and leaves the data labeled as archive bit 0
- ☐ Backs up data labeled with archive bit 0 and changes the data label to archive bit 1

Question 332

Which of the following was designed to support multiple network types over the same serial link?

- ☐ Ethernet
- ☐ SLIP
- ☐ PPP
- ☐ PPTP

Question 333

When considering all the reasons that buffer overflow vulnerabilities exist what is the real reason?

- ☐ Human error
- ☐ The Windows Operating system
- ☐ Insecure programming languages
- ☐ Insecure Transport Protocols

Question 334

To mitigate the risk of fire in your new data center, you plan to implement a heat-activated fire detector. Your requirement is to have the earliest warning possible of a fire outbreak. Which type of sensor would you select and where would you place it?

- ☐ Rate-of-rise temperature sensor installed on the side wall
- ☐ Variable heat sensor installed above the suspended ceiling
- ☐ Fixed-temperature sensor installed in the air vent
- ☐ Rate-of-rise temperature sensor installed below the raised floors

Question 335

In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class A network?

- ☐ The first bit of the IP address would be set to zero.
- ☐ The first bit of the IP address would be set to one and the second bit set to zero.
- ☐ The first two bits of the IP address would be set to one, and the third bit set to zero.
- ☐ The first three bits of the IP address would be set to one.

Question 336

A network-based vulnerability assessment is a type of test also referred to as:

- ☐ An active vulnerability assessment.
- ☐ A routing vulnerability assessment.
- ☐ A host-based vulnerability assessment.
- ☐ A passive vulnerability assessment.

Question 337

Which type of risk assessment is the formula $ALE = ARO \times SLE$ used for?

- ☐ Quantitative Analysis
- ☐ Qualitative Analysis
- ☐ Objective Analysis
- ☐ Expected Loss Analysis

Question 338

Which layer of the TCP/IP protocol stack corresponds to the ISO/OSI Network layer (layer 3)?

- ☐ Host-to-host layer
- ☐ Internet layer
- ☐ Network access layer
- ☐ Session layer

Question 339

Another type of access control is lattice-based access control. In this type of control a lattice model is applied. How is this type of access control concept applied?

- ☐ The pair of elements is the subject and object, and the subject has an upper bound equal or higher than the upper bound of the object being accessed.
- ☐ The pair of elements is the subject and object, and the subject has an upper bound lower than the upper bound of the object being accessed.
- ☐ The pair of elements is the subject and object, and the subject has no special upper or lower bound needed within the lattice.
- ☐ The pair of elements is the subject and object, and the subject has no access rights in relation to an object.

Question 340

Which of the following categories of hackers poses the greatest threat?

- ☐ Disgruntled employees
- ☐ Student hackers
- ☐ Criminal hackers
- ☐ Corporate spies

Question 341

Which security model introduces access to objects only through programs?

- ☐ The Biba model
- ☐ The Bell-LaPadula model
- ☐ The Clark-Wilson model
- ☐ The information flow model

Question 342

Which of the following is NOT a media viability control used to protect the viability of data storage media?

- ☐ clearing
- ☐ marking
- ☐ handling
- ☐ storage

Question 343

Why do buffer overflows happen? What is the main cause?

- ☐ Because buffers can only hold so much data
- ☐ Because of improper parameter checking within the application
- ☐ Because they are an easy weakness to exploit
- ☐ Because of insufficient system memory

Question 344

Which of the following is BEST practice to employ in order to reduce the risk of collusion?

- ☐ Least Privilege
- ☐ Job Rotation
- ☐ Separation of Duties
- ☐ Mandatory Vacations

Question 345

Which of the following computer recovery sites is only partially equipped with processing equipment?

- ☐ hot site.
- ☐ rolling hot site.
- ☐ warm site.
- ☐ cold site.

Question 346

A potential problem related to the physical installation of the Iris Scanner in regards to the usage of the iris pattern within a biometric system is:

- ☐ Concern that the laser beam may cause eye damage.
- ☐ The iris pattern changes as a person grows older.
- ☐ There is a relatively high rate of false accepts.
- ☐ The optical unit must be positioned so that the sun does not shine into the aperture.

Question 347

Which type of password token involves time synchronization?

- ☐ Static password tokens
- ☐ Synchronous dynamic password tokens
- ☐ Asynchronous dynamic password tokens
- ☐ Challenge-response tokens

Question 348

Which of the following is NOT a common backup method?

- ☐ Full backup method
- ☐ Daily backup method
- ☐ Incremental backup method
- ☐ Differential backup method

Question 349

Passwords can be required to change monthly, quarterly, or at other intervals:

- ☐ depending on the criticality of the information needing protection.
- ☐ depending on the criticality of the information needing protection and the password's frequency of use.
- ☐ depending on the password's frequency of use.
- ☐ not depending on the criticality of the information needing protection but depending on the password's frequency of use.

Question 350

Which of the following answers BEST describes the Bell La-Padula model of storage and access control of classified information?

- ☐ No read up and No write down
- ☐ No write up, no read down
- ☐ No read over and no write up
- ☐ No reading from higher classification levels

Question 351

Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?

- ☐ Digital Video Tape (DVT).
- ☐ Digital Analog Tape (DAT).
- ☐ Digital Voice Tape (DVT).
- ☐ Digital Audio Tape (DAT).

Question 352

RAID level 10 is created by combining which of the following?

- ☐ level 0 (striping) with level 1 (mirroring).
- ☐ level 0 (striping) with level 2 (hamming).
- ☐ level 0 (striping) with level 1 (clustering).
- ☐ level 0 (striping) with level 1 (hamming).

Question 353

Which of the following backup methods is most appropriate for off-site archiving?

- ☐ Incremental backup method
- ☐ Off-site backup method
- ☐ Full backup method
- ☐ Differential backup method

Question 354

When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

- ☐ Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
- ☐ Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
- ☐ They both involve rewriting the media.
- ☐ Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Question 355

Which Network Address Translation (NAT) is the MOST convenient and secure solution?

- ☐ Hiding Network Address Translation
- ☐ Port Address Translation
- ☐ Dedicated Address Translation
- ☐ Static Address Translation

Question 356

Which of the following is used to create parity information?

- ☐ a hamming code
- ☐ a clustering code
- ☐ a mirroring code
- ☐ a striping code

Question 357

Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

- ☐ Degaussing
- ☐ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Question 358

ICMP and IGMP belong to which layer of the OSI model?

- ☐ Datagram Layer.
- ☐ Network Layer.
- ☐ Transport Layer.
- ☐ Data Link Layer.

Question 359

A DMZ is also known as a:

- ☐ screened subnet.
- ☐ three legged firewall.
- ☐ place to attract hackers.
- ☐ bastion host.

Question 360

At which temperature does damage start occurring to magnetic media?

- ☐ 100 degrees Fahrenheit or 37.7 degrees Celsius
- ☐ 125 degrees Fahrenheit or 51.66 degrees Celsius
- ☐ 150 degrees Fahrenheit or 65.5 degrees Celsius
- ☐ 175 degrees Fahrenheit or 79.4 degrees Celsius

Question 361

Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

- ☐ IS security specialists
- ☐ Senior Management
- ☐ Senior security analysts
- ☐ systems Auditors

Question 362

Which of the following was designed as a more fault-tolerant topology than Ethernet, and very resilient when properly implemented?

- ☐ Token Link.
- ☐ Token system.
- ☐ Token Ring.
- ☐ Duplicate ring.

Question 363

Which of the following allows two computers to coordinate in executing software?

- ☐ RSH
- ☐ RPC
- ☐ NFS
- ☐ SNMP

Question 364

Which of the following keys has the SHORTEST lifespan?

- ☐ Secret key
- ☐ Public key
- ☐ Session key
- ☐ Private key

Question 365

In regards to relational database operations using the Structure Query Language (SQL), which of the following is a value that can be bound to a placeholder declared within an SQL statement?

- ☐ A bind value
- ☐ An assimilation value
- ☐ A reduction value
- ☐ A resolution value

Question 366

RADIUS incorporates which of the following services?

- ☐ Authentication server and PIN codes.
- ☐ Authentication of clients and static passwords generation.
- ☐ Authentication of clients and dynamic passwords generation.
- ☐ Authentication server as well as support for Static and Dynamic passwords.

Question 367

How can an individual/person BEST be identified or authenticated to prevent local masquerading attacks?

- ☐ User Id and password
- ☐ Smart card and PIN code
- ☐ Two-factor authentication
- ☐ Biometrics

Question 368

Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard?

- ☐ Twofish
- ☐ Serpent
- ☐ RC6
- ☐ Rijndael

Question 369

Which of the following biometric parameters are better suited for authentication use over a long period of time?

- ☐ Iris pattern
- ☐ Voice pattern
- ☐ Signature dynamics
- ☐ Retina pattern

Question 370

In Mandatory Access Control, sensitivity labels attached to objects contain what information?

- ☐ The item's classification
- ☐ The item's classification and category set
- ☐ The item's category
- ☐ The items' need to know

Question 371

When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?

- ☐ Executive management staff
- ☐ Senior business unit management
- ☐ BCP committee
- ☐ Functional business units

Question 372

The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?

- ☐ 64 bits of data input results in 56 bits of encrypted output
- ☐ 128 bit key with 8 bits used for parity
- ☐ 64 bit blocks with a 64 bit total key length
- ☐ 56 bits of data input results in 56 bits of encrypted output

Question 373

What is the process that RAID Level 0 uses as it creates one large disk by using several disks?

- ☐ striping
- ☐ mirroring
- ☐ integrating
- ☐ clustering

Question 374

Which of the following cable types is limited in length to 185 meters?

- ☐ 10BaseT
- ☐ RG8
- ☐ RG58
- ☐ 10Base5

Question 375

Which of the following is a transaction redundancy implementation?

- ☐ On-site mirroring
- ☐ Electronic Vaulting
- ☐ Remote Journaling
- ☐ Database Shadowing

Question 376

Which one of the following is a key agreement protocol used to enable two entities to agree and generate a session key (secret key used for one session) over an insecure medium without any prior secrets or communications between the entities? The negotiated key will subsequently be used for message encryption using Symmetric Cryptography.

- ☐ RSA
- ☐ PKI
- ☐ Diffie_Hellmann
- ☐ 3DES

Question 377

At which OSI layer does SSL reside in?

- ☐ Application
- ☐ Session
- ☐ Transport
- ☐ Network

Question 378

Controls such as job rotation, the sharing of responsibilities, and reviews of audit records are associated with:

- ☐ preventive/physical.
- ☐ detective/technical.
- ☐ detective/physical.
- ☐ detective/administrative.

Question 379

A site that is owned by the company and mirrors the original production site is referred to as a _____?

- ☐ Hot site.
- ☐ Warm Site.
- ☐ Reciprocal site.
- ☐ Redundant Site.

Question 380

Which of the following phases of a software development life cycle normally incorporates the security specifications, determines access controls, and evaluates encryption options?

- ☐ Detailed design
- ☐ Implementation
- ☐ Product design
- ☐ Software plans and requirements

Question 381

Which of the following is LESS likely to be used today in creating a Virtual Private Network?

- ☐ L2TP
- ☐ PPTP
- ☐ IPSec
- ☐ L2F

Question 382

Which of the following protocols would BEST mitigate threats of sniffing attacks on web application traffic?

- ☐ SSL or TLS
- ☐ 802.1X
- ☐ ARP Cache Security
- ☐ SSH - Secure Shell

Question 383

Which of the following is an advantage of using a high-level programming language?

- ☐ It decreases execution times for programs
- ☐ It allows programmers to define syntax
- ☐ It requires programmer-controlled storage management
- ☐ It enforces coding standards

Question 384

In a known plaintext attack, the cryptanalyst has knowledge of which of the following?

- ☐ the ciphertext and the key
- ☐ the plaintext and the secret key
- ☐ both the plaintext and the associated ciphertext of several messages
- ☐ the plaintext and the algorithm

Question 385

Who vouches for the binding between the data items in a digital certificate?

- ☐ Registration authority
- ☐ Certification authority
- ☐ Issuing authority
- ☐ Vouching authority

Question 386

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It does not permit management to:

- ☐ specify what users can do.
- ☐ specify which resources they can access.
- ☐ specify how to restrain hackers.
- ☐ specify what operations they can perform on a system.

Question 387

The security of a computer application is MOST effective and economical in which of the following cases?

- ☐ The system is optimized prior to the addition of security.
- ☐ The system is procured off-the-shelf.
- ☐ The system is customized to meet the specific security threat.
- ☐ The system is originally designed to provide the necessary security.

Question 388

Which of the following statements pertaining to fire suppression systems is TRUE?

- ☐ Halon is today the most common choice as far as agents are concerned because it is highly effective in the way that it interferes with the chemical reaction of the elements within a fire.
- ☐ Gas masks provide an effective protection against use of CO2 systems. They are recommended for the protection of the employees within data centers.
- ☐ CO2 systems are NOT effective because they suppress the oxygen supply required to sustain the fire.
- ☐ Water Based extinguishers are NOT an effective fire suppression method for class C (electrical) fires.

Question 389

Knowledge-based Intrusion Detection Systems (IDS) are more common than:

- ☐ Network-based IDS
- ☐ Host-based IDS
- ☐ Behavior-based IDS
- ☐ Application-Based IDS

Question 390

According to ISC2, what should be the fire rating for the internal walls of an information processing facility?

- ☐ All walls must have a one-hour minimum fire rating.
- ☐ All internal walls must have a one-hour minimum fire rating, except for walls to adjacent rooms where records such as paper and media are stored, which should have a two-hour minimum fire rating.
- ☐ All walls must have a two-hour minimum fire rating.
- ☐ All walls must have a two-hour minimum fire rating, except for walls to adjacent rooms where records such as paper and media are stored, which should have a three-hour minimum fire rating.

Question 391

The Orange Book states that "Hardware and software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB [Trusted Computing Base]." This statement is the formal requirement for:

- ☐ Security Testing.
- ☐ Design Verification.
- ☐ System Integrity.
- ☐ System Architecture Specification.

Question 392

Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered. There are two basic IDS analysis methods that exist.

Which of the basic method is more prone to false positive?

- ☐ Pattern Matching (also called signature analysis)
- ☐ Anomaly Detection
- ☐ Host-based intrusion detection
- ☐ Network-based intrusion detection

Question 393

Which of the following is the most critical item from a disaster recovery point of view?

- ☐ Data
- ☐ Hardware/Software
- ☐ Communication Links
- ☐ Software Applications

Question 394

What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity?

- ☐ A digital envelope
- ☐ A cryptographic hash
- ☐ A Message Authentication Code
- ☐ A digital signature

Question 395

Which of the following is the most reliable, secure means of removing data from magnetic storage media such as a magnetic tape, or a cassette?

- ☐ Degaussing
- ☐ Parity Bit Manipulation
- ☐ Zeroization
- ☐ Buffer overflow

Question 396

The Logical Link Control sub-layer is a part of which of the following?

- ☐ The ISO/OSI Data Link layer.
- ☐ The Reference monitor.
- ☐ The Transport layer of the TCP/IP stack model.
- ☐ Change management control.

Question 397

The Orange Book describes four hierarchical levels to categorize security systems. Which of the following levels require mandatory protection?

- ☐ A and B.
- ☐ B and C.
- ☐ A, B, and C.
- ☐ B and D.

Question 398

Which of the following are the three classifications of RAID identified by the RAID Advisory Board?

- ☐ Failure Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems.
- ☐ Foreign Resistant Disk Systems (FRDSs), Failure Tolerant Disk Systems, and Disaster Tolerant Disk Systems.
- ☐ Failure Resistant Disk Systems (FRDSs), File Transfer Disk Systems, and Disaster Tolerant Disk Systems.
- ☐ Federal Resistant Disk Systems (FRDSs), Fault Tolerant Disk Systems, and Disaster Tolerant Disk Systems.

Question 399

The ideal operating humidity range is defined as 40 percent to 60 percent. High humidity (greater than 60 percent) can produce what type of problem on computer parts?

- ☐ Static electricity
- ☐ Corrosion
- ☐ Energy-plating
- ☐ Element-plating

Question 400

The Clipper Chip utilizes which concept in public key cryptography?

- ☐ Substitution
- ☐ Key Escrow
- ☐ An undefined algorithm
- ☐ Super strong encryption

Question 401

How many bits is the effective length of the key of the Data Encryption Standard algorithm?

- ☐ 168
- ☐ 128
- ☐ 56
- ☐ 64

Question 402

A confidential number used as an authentication factor to verify a user's identity is called a:

- ☐ PIN
- ☐ User ID
- ☐ Password
- ☐ Challenge

Question 403

The BIGGEST difference between System High Security Mode and Dedicated Security Mode is:

- ☐ The clearance required
- ☐ Object classification
- ☐ Subjects cannot access all objects
- ☐ Need-to-know

Question 404

Which one of the following is NOT one of the outcomes of a vulnerability assessment?

- ☐ Quantative loss assessment
- ☐ Qualitative loss assessment
- ☐ Formal approval of BCP scope and initiation document
- ☐ Defining critical support areas

Question 405

Normalizing data within a database could include all or some of the following except which one?

- ☐ Eliminate duplicative columns from the same table.
- ☐ Eliminates functional dependencies on a partial key by putting the fields in a separate table from those that are dependent on the whole key
- ☐ Eliminates Functional dependencies on non-key fields by putting them in a separate table. At this level, all non-key fields are dependent on the primary key.
- ☐ Eliminating duplicate key fields by putting them into separate tables.

Question 406

Which of the following is the WEAKEST authentication mechanism?

- ☐ Passphrases
- ☐ Passwords
- ☐ One-time passwords
- ☐ Token devices

Question 407

Which of the following LAN devices only operates at the physical layer of the OSI/ISO model?

- ☐ Switch
- ☐ Bridge
- ☐ Hub
- ☐ Router

Question 408

Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

- ☐ Wave pattern motion detectors
- ☐ Capacitance detectors
- ☐ Field-powered devices
- ☐ Audio detectors

Question 409

A prolonged complete loss of electric power is a:

- ☐ brownout
- ☐ blackout
- ☐ surge
- ☐ fault

Question 410

Which of the following should NOT be performed by an operator?

- ☐ Implementing the initial program load
- ☐ Monitoring execution of the system
- ☐ Data entry
- ☐ Controlling job flow

Question 411

SQL commands do not include which of the following?

- ☐ Select, Update
- ☐ Grant, Revoke
- ☐ Delete, Insert
- ☐ Add, Relist

Question 412

SMTP can best be described as:

- ☐ a host-to-host email protocol.
- ☐ an email retrieval protocol.
- ☐ a web-based e-mail reading protocol.
- ☐ a standard defining the format of e-mail messages.

Question 413

Asynchronous Communication transfers data by sending:

- ☐ bits of data sequentially
- ☐ bits of data sequentially in irregular timing patterns
- ☐ bits of data in sync with a heartbeat or clock
- ☐ bits of data simultaneously

Question 414

Which of the following is not a defined maturity level within the Software Capability Maturity Model?

- ☐ Repeatable
- ☐ Defined
- ☐ Managed
- ☐ Oriented

Question 415

When a station communicates on the network for the first time, which of the following protocol would search for and find the Internet Protocol (IP) address that matches with a known Ethernet address?

- ☐ Address Resolution Protocol (ARP).
- ☐ Reverse Address Resolution Protocol (RARP).
- ☐ Internet Control Message protocol (ICMP).
- ☐ User Datagram Protocol (UDP).

Question 416

When referring to the data structures of a packet, the term Protocol Data Unit (PDU) is used, what is the proper term to refer to a single unit of TCP data at the transport layer?

- ☐ TCP segment.
- ☐ TCP datagram.
- ☐ TCP frame.
- ☐ TCP packet.

Question 417

Which Orange Book evaluation level is described as "Structured Protection"?

- ☐ A1
- ☐ B3
- ☐ B2
- ☐ B1

Question 418

Common Criteria 15408 generally outlines assurance and functional requirements through a security evaluation process concept of _____, _____, _____ for Evaluated Assurance Levels (EALs) to certify a product or system.

- ☐ EAL, Security Target, Target of Evaluation
- ☐ SFR, Protection Profile, Security Target
- ☐ Protection Profile, Target of Evaluation, Security Target
- ☐ SFR, Security Target, Target of Evaluation

Question 419

When submitting a passphrase for authentication, the passphrase is converted into:

- ☐ a virtual password by the system.
- ☐ a new passphrase by the system.
- ☐ a new passphrase by the encryption technology
- ☐ a real password by the system which can be used forever.

Question 420

Which backup method is used if backup time is critical and tape space is at an extreme premium?

- ☐ Incremental backup method.
- ☐ Differential backup method.
- ☐ Full backup method.
- ☐ Tape backup method.

Question 421

Common Criteria has assurance level from EAL 1 to EAL 7 regarding the depth of design and testing. Which of following assure the Target of Evaluation (or TOE) is methodically designed, tested and reviewed?

- ☐ EAL 3
- ☐ EAL 4
- ☐ EAL 5
- ☐ EAL 6

Question 422

What is the PRIMARY goal of incident handling?

- ☐ Successfully retrieve all evidence that can be used to prosecute
- ☐ Improve the company's ability to be prepared for threats and disasters
- ☐ Improve the company's disaster recovery plan
- ☐ Contain and repair any damage caused by an event.

Question 423

The information security staff's participation in which of the following system development life cycle phases provides maximum benefit to the organization?

- ☐ project initiation and planning phase
- ☐ system design specifications phase
- ☐ development and documentation phase
- ☐ in parallel with every phase throughout the project

Question 424

Which of the following is the SIMPLEST type of firewall?

- ☐ Stateful packet filtering firewall
- ☐ Packet filtering firewall
- ☐ Dual-homed host firewall
- ☐ Application gateway

Question 425

Which of the following is a large hardware/software backup system that uses the RAID technology?

- ☐ Tape Array.
- ☐ Scale Array.
- ☐ Crimson Array
- ☐ Table Array.

Question 426

Referential Integrity requires that for any foreign key attribute, the referenced relation must have a tuple with the same value for which of the following?

- ☐ primary key
- ☐ secondary key
- ☐ foreign key
- ☐ candidate key

Question 427

Which of the following algorithms does NOT provide hashing?

- ☐ SHA-1
- ☐ MD2
- ☐ RC4
- ☐ MD5

Question 428

Smart cards are an example of which type of control?

- ☐ Detective control
- ☐ Administrative control
- ☐ Technical control
- ☐ Physical control

Question 429

What is the greatest danger from DHCP?

- ☐ An intruder on the network impersonating a DHCP server and thereby misconfiguring the DHCP clients.
- ☐ Having multiple clients on the same LAN having the same IP address.
- ☐ Having the wrong router used as the default gateway.
- ☐ Having the organization's mail server unreachable.

Question 430

Which of the following floors would be MOST appropriate to locate information processing facilities in a 6-stories building?

- ☐ Basement
- ☐ Ground floor
- ☐ Third floor
- ☐ Sixth floor

Question 431

What is a characteristic of using the Electronic Code Book mode of DES encryption?

- ☐ A given block of plaintext and a given key will always produce the same ciphertext.
- ☐ Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
- ☐ Individual characters are encoded by combining output from earlier encryption routines with plaintext.
- ☐ The previous DES output is used as input.

Question 432

In which phase of Internet Key Exchange (IKE) protocol is peer authentication performed?

- ☐ Pre Initialization Phase
- ☐ Phase 1
- ☐ Phase 2
- ☐ No peer authentication is performed

Question 433

How should a doorway of a manned facility with automatic locks be configured?

- ☐ It should be configured to be fail-secure.
- ☐ It should be configured to be fail-safe.
- ☐ It should have a door delay cipher lock.
- ☐ It should not allow piggybacking.

Question 434

An electrical device (AC or DC) which can generate coercive magnetic force for the purpose of reducing magnetic flux density to zero on storage media or other magnetic media is called:

- ☐ a magnetic field.
- ☐ a degausser.
- ☐ magnetic remanence.
- ☐ magnetic saturation.

Question 435

Which of the following is one of the oldest and most common problem in software development that is still very prevalent today?

- ☐ Buffer Overflow
- ☐ Social Engineering
- ☐ Code injection for machine language
- ☐ Unassembled reversible DOS instructions.

Question 436

Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?

- ☐ The use of good key generators.
- ☐ The use of session keys.
- ☐ Nothing can defend you against a brute force crypto key attack.
- ☐ Algorithms that are immune to brute force key attacks.

Question 437

In the UTP category rating, the tighter the wind:

- ☐ the higher the rating and its resistance against interference and crosstalk.
- ☐ the slower the rating and its resistance against interference and attenuation.
- ☐ the shorter the rating and its resistance against interference and attenuation.
- ☐ the longer the rating and its resistance against interference and attenuation.

Question 438

The Secure Hash Algorithm (SHA-1) creates:

- ☐ a fixed length message digest from a fixed length input message.
- ☐ a variable length message digest from a variable length input message.
- ☐ a fixed length message digest from a variable length input message.
- ☐ a variable length message digest from a fixed length input message.

Question 439

What attribute is included in a X.509-certificate?

- ☐ Distinguished name of the subject
- ☐ Telephone number of the department
- ☐ secret key of the issuing CA
- ☐ the key pair of the certificate holder

Question 440

Organizations should consider which of the following first before allowing external access to their LANs via the Internet?

- ☐ Plan for implementing workstation locking mechanisms.
- ☐ Plan for protecting the modem pool.
- ☐ Plan for providing the user with his account usage information.
- ☐ Plan for considering proper authentication options.

Question 441

What is NOT true with pre shared key authentication within IKE / IPsec protocol?

- ☐ Pre shared key authentication is normally based on simple passwords
- ☐ Needs a Public Key Infrastructure (PKI) to work
- ☐ IKE is used to setup Security Associations
- ☐ IKE builds upon the Oakley protocol and the ISAKMP protocol.

Question 442

Which of the following answers presents the MOST significant threat to network based IDS or IPS systems?

- ☐ Encrypted Traffic
- ☐ Complex IDS/IPS Signature Syntax
- ☐ Digitally Signed Network Packets
- ☐ Segregated VLANs

Question 443

Which of the following is an important part of database design that ensures that attributes in a table depend only on the primary key?

- ☐ Normalization
- ☐ Assimilation
- ☐ Reduction
- ☐ Compaction

Question 444

Secure Electronic Transaction (SET) and Secure HTTP (S-HTTP) operate at which layer of the OSI model?

- ☐ Application Layer.
- ☐ Transport Layer.
- ☐ Session Layer.
- ☐ Network Layer.

Question 445

A message can be encrypted and digitally signed, which provides:

- ☐ Confidentiality, Authentication, Non-repudiation, and Integrity.
- ☐ Confidentiality and Authentication
- ☐ Confidentiality and Non-repudiation
- ☐ Confidentiality and Integrity.

Question 446

Which of the following statements is NOT true of IPSec Transport mode?

- ☐ It is required for gateways providing access to internal systems
- ☐ Set-up when end-point is host or communications terminates at end-points
- ☐ If used in gateway-to-host communication, gateway must act as host
- ☐ When ESP is used for the security protocol, the hash is only applied to the upper layer protocols contained in the packet

Question 447

Which of the following DoD Model layer provides non-repudiation services?

- ☐ Network layer.
- ☐ Application layer.
- ☐ Transport layer.
- ☐ Data link layer.

Question 448

Covert Channel Analysis is FIRST introduced at what level of the TCSEC rating?

- ☐ C2 and above.
- ☐ B1 and above.
- ☐ B2 and above.
- ☐ B3 and above.

Question 449

Which of the following is the BIGGEST concern with firewall security?

- ☐ Internal hackers
- ☐ Complex configuration rules leading to misconfiguration
- ☐ Buffer overflows
- ☐ Distributed denial of service (DDoS) attacks

Question 450

Password management falls into which control category?

- ☐ Compensating
- ☐ Detective
- ☐ Preventive
- ☐ Technical

Question 451

The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

- ☐ Clipping level
- ☐ Acceptance level
- ☐ Forgiveness level
- ☐ Logging level

Question 452

A circuit level proxy is _____ when compared to an application level proxy.

- ☐ lower in processing overhead.
- ☐ more difficult to maintain.
- ☐ more secure.
- ☐ slower.

Question 453

Which of the following answers BEST indicates the most important part of a data backup plan?

- ☐ Testing the backups with restore operations
- ☐ An effective backup plan
- ☐ A reliable network infrastructure
- ☐ Expensive backup hardware

Question 454

Which of the following statements pertaining to software testing is incorrect?

- ☐ Unit testing should be addressed and considered when the modules are being designed.
- ☐ Test data should be part of the specifications.
- ☐ Testing should be performed with live data to cover all possible situations.
- ☐ Test data generators can be used to systematically generate random test data that can be used to test programs.

Question 455

Which of the following would be an example of the BEST password?

- ☐ golf001
- ☐ Elizabeth
- ☐ T1me4g0lF
- ☐ password

Question 456

In Mandatory Access Control, sensitivity labels attached to object contain what information?

- ☐ The item's classification
- ☐ The item's classification and category set
- ☐ The item's category
- ☐ The item's need to know

Question 457

Which of the following type of lock uses a numeric keypad or dial to gain entry?

- ☐ Bolting door locks
- ☐ Cipher lock
- ☐ Electronic door lock
- ☐ Biometric door lock

Question 458

Which of the following best describes what would be expected at a "hot site"?

- ☐ Computers, climate control, cables and peripherals
- ☐ Computers and peripherals
- ☐ Computers and dedicated climate control systems.
- ☐ Dedicated climate control systems

Question 459

What is a limitation of TCP Wrappers?

- ☐ It cannot control access to running UDP services.
- ☐ It stops packets before they reach the application layer, thus confusing some proxy servers.
- ☐ The hosts.* access control system requires a complicated directory tree.
- ☐ They are too expensive.

Question 460

Which of the following can be defined as an attribute in one relation that has values matching the primary key in another relation?

- ☐ foreign key
- ☐ candidate key
- ☐ primary key
- ☐ secondary key

Question 461

What is the access protection system that limits connections by calling back the number of a previously authorized location called?

- ☐ Sendback systems
- ☐ Callback forward systems
- ☐ Callback systems
- ☐ Sendback forward systems

Question 462

Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys? This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?

- ☐ Internet Security Association and Key Management Protocol (ISAKMP)
- ☐ Simple Key-management for Internet Protocols (SKIP)
- ☐ Diffie-Hellman Key Distribution Protocol
- ☐ IPsec Key exchange (IKE)

Question 463

Who should measure the effectiveness of Information System security related controls in an organization?

- ☐ The local security specialist
- ☐ The business manager
- ☐ The systems auditor
- ☐ The central security manager

Question 464

Which of the following is addressed by Kerberos?

- ☐ Confidentiality and Integrity
- ☐ Authentication and Availability
- ☐ Validation and Integrity
- ☐ Auditability and Integrity

Question 465

Who should DECIDE how a company should approach security and what security measures should be implemented?

- ☐ Senior management
- ☐ Data owner
- ☐ Auditor
- ☐ The information security specialist

Question 466

RAID Level 1 mirrors the data from one disk or set of disks using which of the following techniques?

- ☐ Duplicating the data onto another disk or set of disks.
- ☐ Moving the data onto another disk or set of disks.
- ☐ Establishing dual connectivity to another disk or set of disks.
- ☐ Establishing dual addressing to another disk or set of disks.

Question 467

During an IS audit, auditor has observed that authentication and authorization steps are split into two functions and there is a possibility to force the authorization step to be completed before the authentication step. Which of the following technique an attacker could use to force authorization step before authentication?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Race Condition

Question 468

Which of the following defines when RAID separates the data into multiple units and stores it on multiple disks?

- ☐ striping
- ☐ scanning
- ☐ screening
- ☐ shadowing

Question 469

Which of the following is a method of multiplexing data where a communication channel is divided into an arbitrary number of variable bit-rate digital channels or data streams. This method allocates bandwidth dynamically to physical channels having information to transmit?

- ☐ Time-division multiplexing
- ☐ Asynchronous time-division multiplexing
- ☐ Statistical multiplexing
- ☐ Frequency division multiplexing

Question 470

You have been approached by one of your clients. They are interested in doing some security re-engineering. The client is looking at various information security models. It is a highly secure environment where data at high classifications cannot be leaked to subjects at lower classifications. Of primary concern to them, is the identification of potential covert channel. As an Information Security Professional, which model would you recommend to the client?

- ☐ Information Flow Model combined with Bell LaPadula
- ☐ Bell LaPadula
- ☐ Biba
- ☐ Information Flow Model

Question 471

Which of the following is NOT a component of IPSec?

- ☐ Authentication Header
- ☐ Encapsulating Security Payload
- ☐ Key Distribution Center
- ☐ Internet Key Exchange

Question 472

What can be defined as secret communications where the very existence of the message is hidden?

- ☐ Clustering
- ☐ Steganography
- ☐ Cryptology
- ☐ Vernam cipher

Question 473

Of the multiple methods of handling risks which we must undertake to carry out business operations, which one involves using controls to reduce the risk?

- ☐ Mitigation
- ☐ Avoidance
- ☐ Acceptance
- ☐ Transference

Question 474

What are user interfaces that limit the functions that can be selected by a user called?

- ☐ Constrained user interfaces
- ☐ Limited user interfaces
- ☐ Mini user interfaces
- ☐ Unlimited user interfaces

Question 475

In order to ensure the privacy and integrity of the data, connections between firewalls over public networks should use:

- ☐ Screened subnets
- ☐ Digital certificates
- ☐ An encrypted Virtual Private Network
- ☐ Encryption

Question 476

Which of the following would be LESS likely to prevent an employee from reporting an incident?

- ☐ They are afraid of being pulled into something they don't want to be involved with.
- ☐ The process of reporting incidents is centralized.
- ☐ They are afraid of being accused of something they didn't do.
- ☐ They are unaware of the company's security policies and procedures.

Question 477

Which of the following statements pertaining to packet switching is NOT true?

- ☐ Most data sent today uses digital signals over network employing packet switching.
- ☐ Messages are divided into packets.
- ☐ All packets from a message travel through the same route.
- ☐ Each network node or point examines each packet for routing.

Question 478

Which of the following are suitable protocols for securing VPN connections at the lower layers of the OSI model?

- ☐ S/MIME and SSH
- ☐ TLS and SSL
- ☐ IPsec and L2TP
- ☐ PKCS#10 and X.509

Question 479

What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?

- ☐ Central station alarm
- ☐ Proprietary alarm
- ☐ A remote station alarm
- ☐ An auxiliary station alarm

Question 480

What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?

- ☐ DS-0
- ☐ DS-1
- ☐ DS-2
- ☐ DS-3

Question 481

What algorithm was DES derived from?

- ☐ Twofish.
- ☐ Skipjack.
- ☐ Brooks-Aldeman.
- ☐ Lucifer.

Question 482

Pin, Password, Passphrases, Tokens, smart cards, and biometric devices are all items that can be used for Authentication. When one of these items listed above in conjunction with a second factor to validate authentication, it provides robust authentication of the individual by practicing which of the following?

- ☐ Multi-party authentication
- ☐ Two-factor authentication
- ☐ Mandatory authentication
- ☐ Discretionary authentication

Question 483

Which one of the following is used to provide authentication and confidentiality for e-mail messages?

- ☐ Digital signature
- ☐ PGP
- ☐ IPSEC AH
- ☐ MD4

Question 484

Under what conditions would the use of a Class C fire extinguisher be preferable to a Class A extinguisher?

- ☐ When the fire involves paper products
- ☐ When the fire is caused by flammable products
- ☐ When the fire involves electrical equipment
- ☐ When the fire is in an enclosed area

Question 485

Which of the following statements pertaining to secure information processing facilities is NOT true?

- ☐ Walls should have an acceptable fire rating.
- ☐ Windows should be protected with bars.
- ☐ Doors must resist forcible entry.
- ☐ Location and type of fire suppression systems should be known.

Question 486

Which of the following issues is not addressed by digital signatures?

- ☐ nonrepudiation
- ☐ authentication
- ☐ data integrity
- ☐ denial-of-service

Question 487

What is the maximum number of different keys that can be used when encrypting with Triple DES?

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4

Question 488

John is the product manager for an information system. His product has undergone under security review by an IS auditor. John has decided to apply appropriate security controls to reduce the security risks suggested by an IS auditor. Which of the following technique is used by John to treat the identified risk provided by an IS auditor?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Question 489

The copyright law ("original works of authorship") protects the right of the owner in all of the following except?

- ☐ The public distribution of the idea
- ☐ Reproduction of the idea
- ☐ The idea itself
- ☐ Display of the idea

Question 490

Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?

- ☐ Message non-repudiation.
- ☐ Message confidentiality.
- ☐ Message interleave checking.
- ☐ Message integrity.

Question 491

Matches between which of the following are important because they represent references from one relation to another and establish the connections among these relations?

- ☐ foreign key to primary key
- ☐ foreign key to candidate key
- ☐ candidate key to primary key
- ☐ primary key to secondary key

Question 492

What is the primary difference between FTP and TFTP?

- ☐ Speed of negotiation
- ☐ Authentication
- ☐ Ability to automate
- ☐ TFTP is used to transfer configuration files to and from network equipment.

Question 493

The description of the database is called a schema. The schema is defined by which of the following?

- ☐ Data Control Language (DCL).
- ☐ Data Manipulation Language (DML).
- ☐ Data Definition Language (DDL).
- ☐ Search Query Language (SQL).

Question 494

What is the PRIMARY reason to maintain the chain of custody on evidence that has been collected?

- ☐ To ensure that no evidence is lost.
- ☐ To ensure that all possible evidence is gathered.
- ☐ To ensure that it will be admissible in court
- ☐ To ensure that incidents were handled with due care and due diligence.

Question 495

Which of the following virus types changes some of its characteristics as it spreads?

- ☐ Boot Sector
- ☐ Parasitic
- ☐ Stealth
- ☐ Polymorphic

Question 496

Which of the following is a Wide Area Network that was originally funded by the Department of Defense, which uses TCP/IP for data interchange?

- ☐ The Internet.
- ☐ The Intranet.
- ☐ The extranet.
- ☐ The Ethernet.

Question 497

Which of the following protocols that provide integrity and authentication for IPSec, can also provide non-repudiation in IPSec?

- ☐ Authentication Header (AH)
- ☐ Encapsulating Security Payload (ESP)
- ☐ Secure Sockets Layer (SSL)
- ☐ Secure Shell (SSH-2)

Question 498

Complex applications involving multimedia, computer aided design, video, graphics, and expert systems are more suited to which of the following database type?

- ☐ Object-Oriented Databases (OODB)
- ☐ Object-Relational Databases
- ☐ Relational Databases
- ☐ Database management systems (DBMS)

Question 499

Which of the following cryptographic attacks describes when the attacker has a copy of the plaintext and the corresponding ciphertext?

- ☐ known plaintext
- ☐ brute force
- ☐ ciphertext only
- ☐ chosen plaintext

Question 500

Which of the following access control models introduces user security clearance and data classification?

- ☐ Role-based access control
- ☐ Discretionary access control
- ☐ Non-discretionary access control
- ☐ Mandatory access control

Question 501

Which of the following specifically addresses cyber-attacks against an organization's IT systems?

- ☐ Continuity of support plan
- ☐ Business continuity plan
- ☐ Incident response plan
- ☐ Continuity of operations plan

Question 502

Which of the following risk handling technique involves the practice of passing on the risk to another entity, such as an insurance company?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Question 503

Which of the following would be the MOST serious risk where a systems development life cycle methodology is inadequate?

- ☐ The project will be completed late.
- ☐ The project will exceed the cost estimates.
- ☐ The project will be incompatible with existing systems.
- ☐ The project will fail to meet business and user needs.

Question 504

What is the PRIMARY purpose of using redundant array of inexpensive disks (RAID) level zero?

- ☐ To improve system performance.
- ☐ To maximize usage of hard disk space.
- ☐ To provide fault tolerance and protection against file server hard disk crashes.
- ☐ To implement integrity.

Question 505

Which of the following terms can be described as the process to conceal data into another file or media in a practice known as security through obscurity?

- ☐ Steganography
- ☐ ADS - Alternate Data Streams
- ☐ Encryption
- ☐ NTFS ADS

Question 506

Which of the following statements is TRUE about data encryption as a method of protecting data?

- ☐ It should sometimes be used for password files
- ☐ It is usually easily administered
- ☐ It makes few demands on system resources
- ☐ It requires careful key management

Question 507

A server cluster looks like a:

- ☐ single server from the user's point of view.
- ☐ dual server from the user's point of view.
- ☐ triple server from the user's point of view.
- ☐ quadruple server from the user's point of view.

Question 508

Which of the following BEST defines add-on security?

- ☐ Physical security complementing logical security measures.
- ☐ Protection mechanisms implemented as an integral part of an information system.
- ☐ Layer security.
- ☐ Protection mechanisms implemented after an information system has become operational.

Question 509

In regards to the query function of relational database operations, which of the following represent implementation procedures that correspond to each of the low-level operations in the query?

- ☐ query plan
- ☐ relational plan
- ☐ database plan
- ☐ structuring plan

Question 510

Which of the following is biggest factor that makes Computer Crimes possible?

- ☐ The fraudster obtaining advanced training & special knowledge.
- ☐ Victim carelessness.
- ☐ Collusion with others in information processing.
- ☐ System design flaws.

Question 511

What can be defined as: It confirms that users' needs have been met by the supplied solution?

- ☐ Accreditation
- ☐ Certification
- ☐ Assurance
- ☐ Acceptance

Question 512

Which of the following can best define the "revocation request grace period"?

- ☐ The period of time allotted within which the user must make a revocation request upon a revocation reason
- ☐ Minimum response time for performing a revocation by the CA
- ☐ Maximum response time for performing a revocation by the CA
- ☐ Time period between the arrival of a revocation request and the publication of the revocation information

Question 513

Which of the following BEST ensures accountability of users for the actions taken within a system or domain?

- ☐ Identification
- ☐ Authentication
- ☐ Authorization
- ☐ Credentials

Question 514

In Synchronous dynamic password tokens:

- ☐ The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
- ☐ The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
- ☐ The unique password is not entered into a system or workstation along with an owner's PIN.
- ☐ The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.

Question 515

Address Resolution Protocol (ARP) interrogates the network by sending out a?

- ☐ broadcast.
- ☐ multicast.
- ☐ unicast.
- ☐ semicast.

Question 516

The primary purpose for using one-way hashing of user passwords within a password file is which of the following?

- ☐ It prevents an unauthorized person from trying multiple passwords in one logon attempt.
- ☐ It prevents an unauthorized person from reading the password.
- ☐ It minimizes the amount of storage required for user passwords.
- ☐ It minimizes the amount of processing time used for encrypting passwords.

Question 517

Which of the following defines the software that maintains and provides access to the database?

- ☐ database management system (DBMS)
- ☐ relational database management system (RDBMS)
- ☐ database identification system (DBIS)
- ☐ Interface Definition Language system (IDLS)

Question 518

Which of the following is implemented through scripts or smart agents that replay the users multiple log-ins against authentication servers to verify a user's identity which permit access to system services?

- ☐ Single Sign-On
- ☐ Dynamic Sign-On
- ☐ Smart cards
- ☐ Kerberos

Question 519

Which of the following ensures that a TCB is designed, developed, and maintained with formally controlled standards that enforces protection at each stage in the system's life cycle?

- ☐ Life cycle assurance
- ☐ Operational assurance
- ☐ Covert timing assurance
- ☐ Covert storage assurance

Question 520

Which RAID implementation is commonly called mirroring?

- ☐ RAID level 2
- ☐ RAID level 3
- ☐ RAID level 5
- ☐ RAID level 1

Question 521

What is the primary goal of setting up a honey pot?

- ☐ To lure hackers into attacking unused systems
- ☐ To entrap and track down possible hackers
- ☐ To set up a sacrificial lamb on the network
- ☐ To know when certain types of attacks are in progress and to learn about attack techniques so the network can be fortified.

Question 522

Which of the following access control models is based on sensitivity labels?

- ☐ Discretionary access control
- ☐ Mandatory access control
- ☐ Rule-based access control
- ☐ Role-based access control

Question 523

The MAIN issue with Level 1 of RAID is which of the following?

- ☐ It is very expensive.
- ☐ It is difficult to recover.
- ☐ It causes poor performance.
- ☐ It is relatively unreliable.

Question 524

The Physical Security domain focuses on three areas that are the basis to physically protecting enterprise's resources and sensitive information. Which of the following is NOT one of these areas?

- ☐ Threats
- ☐ Countermeasures
- ☐ Vulnerabilities
- ☐ Risks

Question 525

The viewing of recorded events after the fact using a closed-circuit TV camera is considered a

- ☐ Preventative control.
- ☐ Detective control
- ☐ Compensating control
- ☐ Corrective control

Question 526

Which of the following statements pertaining to IPSec is NOT true?

- ☐ IPSec can help in protecting networks from some of the IP network attacks.
- ☐ IPSec provides confidentiality and integrity to information transferred over IP networks through transport layer encryption and authentication.
- ☐ IPSec protects against man-in-the-middle attacks.
- ☐ IPSec protects against spoofing.

Question 527

Once evidence is seized, a law enforcement officer should emphasize which of the following?

- ☐ Chain of command
- ☐ Chain of custody
- ☐ Chain of control
- ☐ Chain of communications

Question 528

Why would a database be denormalized?

- ☐ To ensure data integrity
- ☐ To increase processing efficiency
- ☐ To prevent duplication of data
- ☐ To save storage space

Question 529

Which of the following is defined as the most recent point in time to which data must be synchronized without adversely affecting the organization (financial or operational impacts)?

- ☐ Recovery Point Objective
- ☐ Recovery Time Objective
- ☐ Point of Time Objective
- ☐ Critical Time Objective

Question 530

Which of the following is NOT a correct notation for an IPv6 address?

- ☐ 2001:0db8:0:0:0:0:1428:57ab
- ☐ ABCD:EF01:2345:6789:
- ☐ ABCD:EF01:2345:6789::1
- ☐ 2001:DB8::8:800::417A

Question 531

Which of the following packets should NOT be dropped at a firewall protecting an organization's internal network?

- ☐ Inbound packets with Source Routing option set
- ☐ Router information exchange protocols
- ☐ Inbound packets with an internal address as the source IP address
- ☐ Outbound packets with an external destination IP address

Question 532

Which of the following statements pertaining to biometrics is FALSE?

- ☐ User can be authenticated based on behavior.
- ☐ User can be authenticated based on unique physical attributes.
- ☐ User can be authenticated by what he knows.
- ☐ A biometric system's accuracy is determined by its crossover error rate (CER).

Question 533

Fault tolerance countermeasures are designed to combat threats to which of the following?

- ☐ an uninterruptible power supply.
- ☐ backup and retention capability.
- ☐ design reliability.
- ☐ data integrity.

Question 534

Sensitivity labels are an example of what application control type?

- ☐ Preventive security controls
- ☐ Detective security controls
- ☐ Compensating administrative controls
- ☐ Preventive accuracy controls

Question 535

At which layer of ISO/OSI does the fiber optics work?

- ☐ Network layer
- ☐ Transport layer
- ☐ Data link layer
- ☐ Physical layer

Question 536

When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?

- ☐ Type I error
- ☐ Type II error
- ☐ Type III error
- ☐ Crossover error

Question 537

Which of the following describes the sequence of steps required for a Kerberos session to be established between a user (Principal P1), and an application server (Principal P2)?

- ☐ Principals P1 and Principals P2 authenticate to the Key Distribution Center (KDC),
- ☐ Principal P1 receives a Ticket Granting Ticket (TGT), and then Principal P2 requests a service ticket from the KDC.
- ☐ Principal P1 authenticates to the Key Distribution Center (KDC), Principal P1 receives a Ticket Granting Ticket (TGT), and Principal P1 requests a service ticket from the Ticket Granting Service (TGS) in order to access the application server P2
- ☐ Principal P1 authenticates to the Key Distribution Center (KDC),
- ☐ Principal P1 requests a Ticket Granting Ticket (TGT) from the authentication server, and then Principal P1 requests a service ticket from the application server P2
- ☐ Principals P1 and P2 authenticate to the Key Distribution Center (KDC), Principal P1 requests a Ticket Granting Ticket (TGT) from the authentication server, and application server P2 requests a service ticket from P1

Question 538

Which of the following backup methods makes a complete backup of every file on the server every time it is run?

- ☐ The full backup method.
- ☐ The incremental backup method.
- ☐ The differential backup method.
- ☐ The tape backup method.

Question 539

Which of the following statements relating to Distributed Computing Environment (DCE) is FALSE?

- ☐ It is a layer of software that sits on the top of the network layer and provides services to the applications above it.
- ☐ It uses a Universal Unique Identifier (UUID) to uniquely identify users, resources and components.
- ☐ It provides the same functionality as DCOM, but it is more proprietary than DCOM.
- ☐ It is a set of management services with a communication layer based on RPC.

Question 540

Which of the following is NOT a way to secure a wireless network?

- ☐ Disable broadcast of SSID within AP's configuration
- ☐ Change AP's default values
- ☐ Put the access points (AP) in a location protected by a firewall
- ☐ Give AP's descriptive names

Question 541

The Diffie-Hellman algorithm is primarily used to provide which of the following?

- ☐ Confidentiality
- ☐ Key Agreement
- ☐ Integrity
- ☐ Non-repudiation

Question 542

What is the percentage at which the False Rejection Rate equals the False Acceptance Rate called?

- ☐ False Rejection Rate (FRR) or Type I Error
- ☐ False Acceptance Rate (FAR) or Type II Error
- ☐ Crossover Error Rate (CER)
- ☐ Failure to enroll rate (FTE or FER)

Question 543

In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on physical attributes of a person. This raised the necessity of answering two questions:

- ☐ What was the sex of a person and his age?
- ☐ What part of body to be used and how to accomplish identification that is viable?
- ☐ What was the age of a person and his income level?
- ☐ What was the tone of the voice of a person and his habits?

Question 544

In which phase of the System Development Lifecycle (SDLC) is Security Accreditation Obtained?

- ☐ Functional Requirements Phase
- ☐ Testing and evaluation control
- ☐ Acceptance Phase
- ☐ Postinstallation Phase

Question 545

Which of the following best describes the Secure Electronic Transaction (SET) protocol?

- ☐ Originated by VISA and MasterCard as an Internet credit card protocol using Message Authentication Code.
- ☐ Originated by VISA and MasterCard as an Internet credit card protocol using digital signatures.
- ☐ Originated by VISA and MasterCard as an Internet credit card protocol using the transport layer.
- ☐ Originated by VISA and American Express as an Internet credit card protocol using SSL.

Question 546

What can be BEST defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?

- ☐ Risk management
- ☐ Risk analysis
- ☐ Threat analysis
- ☐ Due diligence

Question 547

Unshielded Twisted Pair cabling is a:

- ☐ four-pair wire medium that is used in a variety of networks.
- ☐ three-pair wire medium that is used in a variety of networks.
- ☐ two-pair wire medium that is used in a variety of networks.
- ☐ one-pair wire medium that is used in a variety of networks.

Question 548

In SSL/TLS protocol, what kind of authentication is supported when you establish a secure session between a client and a server?

- ☐ Peer-to-peer authentication
- ☐ Only server authentication (optional)
- ☐ Server authentication (mandatory) and client authentication (optional)
- ☐ Role based authentication scheme

Question 549

In the context of Biometric authentication, there is a quick way to compare the accuracy of devices. In general, the devices that have the lowest value would be the most accurate. Which of the following would be used to compare accuracy of devices?

- ☐ the CER is used.
- ☐ the FRR is used
- ☐ the FAR is used
- ☐ the FER is used

Question 550

Which of the following is NOT an asymmetric key algorithm?

- ☐ RSA
- ☐ Elliptic Curve Cryptosystem (ECC)
- ☐ El Gamal
- ☐ Data Encryption Standard (DES)

Question 551

What is called the number of columns in a table?

- ☐ Schema
- ☐ Relation
- ☐ Degree
- ☐ Cardinality

Question 552

What is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?

- ☐ Polyinstantiation
- ☐ Inference
- ☐ Aggregation
- ☐ Data mining

Question 553

What is the proper term to refer to a single unit of IP data?

- ☐ IP segment.
- ☐ IP datagram.
- ☐ IP frame.
- ☐ IP fragment.

Question 554

What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

- ☐ A
- ☐ D
- ☐ E
- ☐ F

Question 555

Tim's day to day responsibilities include monitoring health of devices on the network. He uses a Network Monitoring System supporting SNMP to monitor the devices for any anomalies or high traffic passing through the interfaces.

Which of the protocols would be BEST to use if some of the requirements are to prevent easy disclosure of the SNMP strings and authentication of the source of the packets?

- ☐ UDP
- ☐ SNMP V1
- ☐ SNMP V3
- ☐ SNMP V2

Question 556

Which of the following would be MOST important to guarantee that the computer evidence will be admissible in court?

- ☐ It must prove a fact that is immaterial to the case.
- ☐ Its reliability must be proven.
- ☐ The process for producing it must be documented and repeatable.
- ☐ The chain of custody of the evidence must show who collected, secured, controlled, handled, transported the evidence, and that it was not tampered with.

Question 557

Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

- ☐ The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.
- ☐ The channels through which the information flows are secure.
- ☐ The recipient's identity can be positively verified by the sender.
- ☐ The sender of the message is the only other person with access to the recipient's private key.

Question 558

In which of the following phases of system development life cycle (SDLC) is contingency planning most important?

- ☐ Initiation
- ☐ Development/acquisition
- ☐ Implementation
- ☐ Operation/maintenance

Question 559

Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer in a network. Within which OSI/ISO layer is RPC implemented?

- ☐ Session layer
- ☐ Transport layer
- ☐ Data link layer
- ☐ Network layer

Question 560

What is the PRIMARY use of a password?

- ☐ Allow access to files.
- ☐ Identify the user.
- ☐ Authenticate the user.
- ☐ Segregate various users' accesses.

Question 561

What is the length of an MD5 message digest?

- ☐ 128 bits
- ☐ 160 bits
- ☐ 256 bits
- ☐ varies depending upon the message size.

Question 562

A demilitarized zone is:

- ☐ a part of a network perfectly safe from hackers
- ☐ a militarized network segment
- ☐ a firewall
- ☐ the network segment between the Internet and a private network

Question 563

Which of the following should be used as a replacement for Telnet for secure remote login over an insecure network?

- ☐ S-Telnet
- ☐ SSL
- ☐ Rlogin
- ☐ SSH

Question 564

In this type of attack, the intruder re-routes data traffic from a network device to a personal machine. This diversion allows an attacker to gain access to critical resources and user credentials, such as passwords, and to gain unauthorized access to critical systems of an organization. Pick the BEST choice below.

- ☐ Network Address Translation
- ☐ Network Address Hijacking
- ☐ Network Address Supernetting
- ☐ Network Address Sniffing

Question 565

Why is infrared generally considered to be more secure to eavesdropping than multidirectional radio transmissions?

- ☐ Because infrared eavesdropping requires more sophisticated equipment.
- ☐ Because infrared operates only over short distances.
- ☐ Because infrared requires direct line-of-sight paths.
- ☐ Because infrared operates at extra-low frequencies (ELF).

Question 566

Which of the following is most concerned with personnel security?

- ☐ Management controls
- ☐ Operational controls
- ☐ Technical controls
- ☐ Human resources controls

Question 567

In computing what is the name of a non-self-replicating type of malware program containing malicious code that appears to have some useful purpose but also contains code that has a malicious or harmful purpose imbedded in it, when executed, carries out actions that are unknown to the person installing it, typically causing loss or theft of data, and possible system harm.

- ☐ virus
- ☐ worm
- ☐ Trojan horse
- ☐ trapdoor

Question 568

Which of the following represents the rows of the table in a relational database?

- ☐ attributes
- ☐ records or tuples
- ☐ record retention
- ☐ relation

Question 569

A database view is the results of which of the following operations?

- ☐ Join and Select.
- ☐ Join, Insert, and Project.
- ☐ Join, Project, and Create.
- ☐ Join, Project, and Select.

Question 570

Which of the following would be true about Static password tokens?

- ☐ The owner identity is authenticated by the token
- ☐ The owner will never be authenticated by the token.
- ☐ The owner will authenticate himself to the system.
- ☐ The token does not authenticates the token owner but the system.

Question 571

In terms of Risk Analysis and dealing with risk, which of the four common ways listed below seek to eliminate involvement with the risk being evaluated?

- ☐ Avoidance
- ☐ Acceptance
- ☐ Transference
- ☐ Mitigation

Question 572

Which of the following would be the best reason for separating the test and development environments?

- ☐ To restrict access to systems under test.
- ☐ To control the stability of the test environment.
- ☐ To segregate user and development staff.
- ☐ To secure access to systems under development.

Question 573

Frame relay uses a public switched network to provide:

- ☐ Local Area Network (LAN) connectivity.
- ☐ Metropolitan Area Network (MAN) connectivity.
- ☐ Wide Area Network (WAN) connectivity.
- ☐ World Area Network (WAN) connectivity.

Question 574

MOST access violations are:

- ☐ Accidental
- ☐ Caused by internal hackers
- ☐ Caused by external hackers
- ☐ Related to Internet

Question 575

Which of the following should be performed by an operator?

- ☐ Changing profiles
- ☐ Approving changes
- ☐ Adding and removal of users
- ☐ Installing system software

Question 576

Which answer BEST describes information access permissions where, unless the user is specifically given access to certain data they are denied any access by default?

- ☐ Implicit Deny
- ☐ Explicit Deny
- ☐ Implied Permissions
- ☐ Explicit Permit

Question 577

Kerberos depends upon what encryption method?

- ☐ Public Key cryptography.
- ☐ Secret Key cryptography.
- ☐ El Gamal cryptography.
- ☐ Blowfish cryptography.

Question 578

Which of the following attacks could capture network user passwords?

- ☐ Data diddling
- ☐ Sniffing
- ☐ IP Spoofing
- ☐ Smurfing

Question 579

Which of the following stripes the data and the parity information at the block level across all the drives in the set?

- ☐ RAID Level 5
- ☐ RAID Level 0
- ☐ RAID Level 2
- ☐ RAID Level 1

Question 580

Which of the following European Union (EU) principles pertaining to the protection of information on private individuals is incorrect?

- ☐ Data collected by an organization can be used for any purpose and for as long as necessary, as long as it is never communicated outside of the organization by which it was collected.
- ☐ Individuals have the right to correct errors contained in their personal data.
- ☐ Transmission of personal information to locations where "equivalent" personal data protection cannot be assured is prohibited.
- ☐ Records kept on an individual should be accurate and up to date.

Question 581

Which RAID Level often implements a one-for-one disk to disk ratio?

- ☐ RAID Level 1
- ☐ RAID Level 0
- ☐ RAID Level 2
- ☐ RAID Level 5

Question 582

This type of attack is generally most applicable to public-key cryptosystems, what type of attack am I?

- ☐ Chosen-Ciphertext attack
- ☐ Ciphertext-only attack
- ☐ Plaintext Only Attack
- ☐ Adaptive-Chosen-Plaintext attack

Question 583

Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

- ☐ TCP
- ☐ SSL
- ☐ UDP
- ☐ SSH

Question 584

Which Orange Book evaluation level is described as "Verified Design"?

- ☐ A1.
- ☐ B3.
- ☐ B2.
- ☐ B1.

Question 585

Which of the following backup sites is the most effective for disaster recovery?

- ☐ Time brokers
- ☐ Hot sites
- ☐ Cold sites
- ☐ Reciprocal Agreement

Question 586

Hierarchical Storage Management (HSM) is commonly employed in:

- ☐ very large data retrieval systems.
- ☐ very small data retrieval systems.
- ☐ shorter data retrieval systems.
- ☐ most data retrieval systems.

Question 587

Which of the following RAID levels is not used in practice and was quickly superseded by the more flexible levels?

- ☐ RAID Level 0
- ☐ RAID Level 1
- ☐ RAID Level 2
- ☐ RAID Level 7

Question 588

If an employee's computer has been used by a fraudulent employee to commit a crime, the hard disk may be seized as evidence and once the investigation is complete it would follow the normal steps of the Evidence Life Cycle. In such case, the Evidence life cycle would not include which of the following steps listed below?

- ☐ Acquisition collection and identification
- ☐ Analysis
- ☐ Storage, preservation, and transportation
- ☐ Destruction

Question 589

Which of the following is an advantage of prototyping?

- ☐ Prototype systems can provide significant time and cost savings.
- ☐ Change control is often less complicated with prototype systems.
- ☐ It ensures that functions or extras are not added to the intended system.
- ☐ Strong internal controls are easier to implement.

Question 590

The older coaxial cable has been widely replaced with twisted pair, which is extremely easy to work with, inexpensive, and also resistant to multiple host failure at once, especially when used in one of the following topology:

- ☐ Token Passing Configuration.
- ☐ Star Configuration.
- ☐ Ring Configuration.
- ☐ Point to Point Configuration.

Question 591

A prolonged high voltage is a:

- ☐ spike
- ☐ blackout
- ☐ surge
- ☐ fault

Question 592

Kerberos is vulnerable to replay in which of the following circumstances?

- ☐ When a private key is compromised within an allotted time window.
- ☐ When a public key is compromised within an allotted time window.
- ☐ When a ticket is compromised within an allotted time window.
- ☐ When the KSD is compromised within an allotted time window.

Question 593

Which of the following encryption methods is known to be unbreakable?

- ☐ Symmetric ciphers.
- ☐ DES codebooks.
- ☐ One-time pads.
- ☐ Elliptic Curve Cryptography.

Question 594

The only difference between RAID 3 and RAID 4 is that level 3 is implemented at the byte level while level 4 is usually implemented at which of the following?

- ☐ Block level.
- ☐ Bridge level.
- ☐ Channel level.
- ☐ Buffer level.

Question 595

Which of the following items is NOT a benefit of cold sites?

- ☐ No resource contention with other organization
- ☐ Quick Recovery
- ☐ A secondary location is available to reconstruct the environment
- ☐ Low Cost

Question 596

In a database management system (DBMS), what is the "cardinality"?

- ☐ The number of rows in a relation.
- ☐ The number of columns in a relation.
- ☐ The set of allowable values that an attribute can take.
- ☐ The number of relations in a database.

Question 597

Another name for a VPN is a:

- ☐ tunnel
- ☐ one-time password
- ☐ pipeline
- ☐ bypass

Question 598

Which of the following statements pertaining to biometrics is FALSE?

- ☐ Increased system sensitivity can cause a higher false rejection rate
- ☐ The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
- ☐ False acceptance rate is also known as Type II error.
- ☐ Biometrics are based on the Type 2 authentication mechanism.

Question 599

Which of the following is most affected by denial-of-service (DoS) attacks?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Accountability
- ☐ Availability

Question 600

Which software development model is actually a meta-model that incorporates a number of the software development models?

- ☐ The Waterfall model
- ☐ The modified Waterfall model
- ☐ The Spiral model
- ☐ The Critical Path Model (CPM)

Question 601

An intranet provides more security and control than which of the following:

- ☐ private posting on the Internet.
- ☐ public posting on the Ethernet.
- ☐ public posting on the Internet.
- ☐ public posting on the Extranet.

Question 602

A security evaluation report and an accreditation statement are produced in which of the following phases of the system development life cycle?

- ☐ project initiation and planning phase
- ☐ system design specification phase
- ☐ development & documentation phase
- ☐ acceptance phase

Question 603

Which of the following pairings uses technology to enforce access control policies?

- ☐ Preventive/Administrative
- ☐ Preventive/Technical
- ☐ Preventive/Physical
- ☐ Detective/Administrative

Question 604

What are the three MOST important functions that Digital Signatures perform?

- ☐ Integrity, Confidentiality and Authorization
- ☐ Integrity, Authentication and Nonrepudiation
- ☐ Authorization, Authentication and Nonrepudiation
- ☐ Authorization, Detection and Accountability

Question 605

Which of the following answers best describes the type of penetration testing where the analyst has full knowledge of the network on which he is going to perform his test?

- ☐ White-Box Penetration Testing
- ☐ Black-Box Pen Testing
- ☐ Penetration Testing
- ☐ Gray-Box Pen Testing

Question 606

Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

- ☐ Palm Scan
- ☐ Hand Geometry
- ☐ Fingerprint
- ☐ Retina scan

Question 607

What security problem is most likely to exist if an operating system permits objects to be used sequentially by multiple users without forcing a refresh of the objects?

- ☐ Disclosure of residual data.
- ☐ Unauthorized obtaining of a privileged execution state.
- ☐ Data leakage through covert channels.
- ☐ Denial of service through a deadly embrace.

Question 608

Which of the following refers to the data left on the media after the media has been erased?

- ☐ remanence
- ☐ recovery
- ☐ sticky bits
- ☐ semi-hidden

Question 609

Which of the following is true of biometrics?

- ☐ It is used for identification in physical controls and it is not used in logical controls.
- ☐ It is used for authentication in physical controls and for identification in logical controls.
- ☐ It is used for identification in physical controls and for authentication in logical controls.
- ☐ Biometrics has no role in logical controls.

Question 610

What algorithm has been selected as the AES algorithm, replacing the DES algorithm?

- ☐ RC6
- ☐ Twofish
- ☐ Rijndael
- ☐ Blowfish

Question 611

Which of the following statements pertaining to packet filtering is NOT true?

- ☐ It is based on ACLs.
- ☐ It is not application dependent.
- ☐ It operates at the network layer.
- ☐ It keeps track of the state of a connection.

Question 612

What is the main problem of the renewal of a root CA certificate?

- ☐ It requires key recovery of all end user keys
- ☐ It requires the authentic distribution of the new root CA certificate to all PKI participants
- ☐ It requires the collection of the old root CA certificates from all the users
- ☐ It requires issuance of the new root CA certificate

Question 613

In a dry pipe system, there is no water standing in the pipe - it is being held back by what type of valve?

- ☐ Relief valve
- ☐ Emergency valve
- ☐ Release valve
- ☐ Clapper valve

Question 614

What does "System Integrity" mean?

- ☐ The software of the system has been implemented as designed.
- ☐ Users can't tamper with processes they do not own.
- ☐ Hardware and firmware have undergone periodic testing to verify that they are functioning properly.
- ☐ Design specifications have been verified against the formal top-level specification.

Question 615

RAID Level 1 is commonly called which of the following?

- ☐ mirroring
- ☐ striping
- ☐ clustering
- ☐ hamming

Question 616

Which of the following rules is LEAST likely to support the concept of least privilege?

- ☐ The number of administrative accounts should be kept to a minimum.
- ☐ Administrators should use regular accounts when performing routine operations like reading mail.
- ☐ Permissions on tools that are likely to be used by hackers should be as restrictive as possible.
- ☐ Only data to and from critical systems and applications should be allowed through the firewall.

Question 617

What is NOT an authentication method within IKE and IPsec?

- ☐ CHAP
- ☐ Pre shared key
- ☐ certificate based authentication
- ☐ Public key authentication

Question 618

Which of the following is a drawback of fiber optic cables?

- ☐ It is affected by electromagnetic interference (EMI).
- ☐ It can easily be tapped.
- ☐ The expertise needed to install it.
- ☐ The limited distance at high speeds.

Question 619

Which of the following backup methods is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets?

- ☐ full backup method.
- ☐ incremental backup method.
- ☐ differential backup method.
- ☐ tape backup method.

Question 620

Which of the following media is MOST resistant to tapping?

- ☐ Microwave.
- ☐ Twisted pair.
- ☐ Coaxial cable.
- ☐ Fiber optic.

Question 621

Which of the following is NOT an advantage that TACACS+ has over TACACS?

- ☐ Event logging
- ☐ Use of two-factor password authentication
- ☐ User has the ability to change his password
- ☐ Ability for security tokens to be resynchronized

Question 622

Which access control model enables the OWNER of the resource to specify what subjects can access specific resources based on their identity?

- ☐ Discretionary Access Control
- ☐ Mandatory Access Control
- ☐ Sensitive Access Control
- ☐ Role-based Access Control

Question 623

Which one of the following factors is NOT one on which Authentication is based?

- ☐ Type 1 Something you know, such as a PIN or password
- ☐ Type 2 Something you have, such as an ATM card or smart card
- ☐ Type 3 Something you are (based upon one or more intrinsic physical or behavioral traits), such as a fingerprint or retina scan
- ☐ Type 4 Something you are, such as a system administrator or security administrator

Question 624

Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Accuracy

Question 625

Which of the following protocols operates at the session layer (layer 5)?

- ☐ RPC
- ☐ IGMP
- ☐ LPD
- ☐ SPX

Question 626

When you update records in multiple locations or you make a copy of the whole database at a remote location as a way to achieve the proper level of fault-tolerance and redundancy, it is known as?

- ☐ Shadowing
- ☐ Data mirroring
- ☐ Backup
- ☐ Archiving

Question 627

What is the primary role of smartcards in a PKI?

- ☐ Transparent renewal of user keys
- ☐ Easy distribution of the certificates between the users
- ☐ Fast hardware encryption of the raw data
- ☐ Tamper resistant, mobile storage and application of private keys of the users

Question 628

Authentication Headers (AH) and Encapsulating Security Payload (ESP) protocols are the driving force of IPSec. Authentication Headers (AH) provides the following service except:

- ☐ Authentication
- ☐ Integrity
- ☐ Replay resistance and non-repudiations
- ☐ Confidentiality

Question 629

Network-based Intrusion Detection systems:

- ☐ commonly reside on a discrete network segment and monitor the traffic on that network segment.
- ☐ commonly will not reside on a discrete network segment and monitor the traffic on that network segment.
- ☐ commonly reside on a discrete network segment and does not monitor the traffic on that network segment.
- ☐ commonly reside on a host and monitor the traffic on that specific host.

Question 630

RAID levels 3 and 5 run:

- ☐ faster on hardware.
- ☐ slower on hardware.
- ☐ faster on software.
- ☐ at the same speed on software and hardware.

Question 631

The IP header contains a protocol field. If this field contains the value of 2, what type of data is contained within the IP datagram?

- ☐ TCP.
- ☐ ICMP.
- ☐ UDP.
- ☐ IGMP.

Question 632

During an IS audit, one of your auditors has observed that some of the critical servers in your organization can be accessed ONLY by using a shared/common user name and password. What should be the auditor's PRIMARY concern be with this approach?

- ☐ Password sharing
- ☐ Accountability
- ☐ Shared account management
- ☐ Difficulty in auditing shared account

Question 633

Which of the following is NOT a countermeasure to traffic analysis?

- ☐ Padding messages.
- ☐ Eavesdropping.
- ☐ Sending noise.
- ☐ Faraday Cage

Question 634

Which of the following is NOT a preventive login control?

- ☐ Last login message
- ☐ Password aging
- ☐ Minimum password length
- ☐ Account expiration

Question 635

Sam is the security Manager of a financial institute. Senior management has requested he performs a risk analysis on all critical vulnerabilities reported by an IS auditor. After completing the risk analysis, Sam has observed that for a few of the risks, the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred. What kind of a strategy should Sam recommend to the senior management to treat these risks?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Question 636

Individual accountability does not include which of the following?

- ☐ unique identifiers
- ☐ policies and procedures
- ☐ access rules
- ☐ audit trails

Question 637

If an organization were to monitor their employees' e-mail, it should not:

- ☐ Monitor only a limited number of employees.
- ☐ Inform all employees that e-mail is being monitored.
- ☐ Explain who can read the e-mail and how long it is backed up.
- ☐ Explain what is considered an acceptable use of the e-mail system.

Question 638

Which one of the following authentication mechanisms creates a problem for mobile users?

- ☐ Mechanisms based on IP addresses
- ☐ Mechanism with reusable passwords
- ☐ One-time password mechanism.
- ☐ Challenge response mechanism.

Question 639

FIPS-140 is a standard for the security of which of the following?

- ☐ Cryptographic service providers
- ☐ Smartcards
- ☐ Hardware and software cryptographic modules
- ☐ Hardware security modules

Question 640

Which of the following activities would not be included in the contingency planning process phase?

- ☐ Prioritization of applications
- ☐ Development of test procedures
- ☐ Assessment of threat impact on the organization
- ☐ Development of recovery scenarios

Question 641

Guards are appropriate whenever the function required by the security program involves which of the following?

- ☐ The use of discriminating judgment
- ☐ The use of physical force
- ☐ The operation of access control devices
- ☐ The need to detect unauthorized access

Question 642

Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of its internals?

- ☐ Black-box testing
- ☐ Parallel Test
- ☐ Regression Testing
- ☐ Pilot Testing

Question 643

Under what conditions would the use of a "Class C" hand-held fire extinguisher be preferable to the use of a "Class A" hand-held fire extinguisher?

- ☐ When the fire is in its incipient stage.
- ☐ When the fire involves electrical equipment.
- ☐ When the fire is located in an enclosed area.
- ☐ When the fire is caused by flammable products.

Question 644

What kind of certificate is used to validate a user identity?

- ☐ Public key certificate
- ☐ Attribute certificate
- ☐ Root certificate
- ☐ Code signing certificate

Question 645

Which of following is NOT a service provided by AAA servers (Radius, TACACS and DIAMETER)?

- ☐ Authentication
- ☐ Administration
- ☐ Accounting
- ☐ Authorization

Question 646

Prior to a live disaster test also called a Full Interruption test, which of the following is most important?

- ☐ Restore all files in preparation for the test.
- ☐ Document expected findings.
- ☐ Arrange physical security for the test site.
- ☐ Conduct of a successful Parallel Test

Question 647

Which of the following is responsible for MOST of the security issues?

- ☐ Outside espionage
- ☐ Hackers
- ☐ Personnel
- ☐ Equipment failure

Question 648

The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:

- ☐ preventive/physical.
- ☐ detective/technical.
- ☐ detective/physical.
- ☐ detective/administrative.

Question 649

Looking at the choices below, which ones would be the most suitable protocols/tools for securing e-mail?

- ☐ PGP and S/MIME
- ☐ IPsec and IKE
- ☐ TLS and SSL
- ☐ SSH

Question 650

Which of the following statements is MOST accurate regarding a digital signature?

- ☐ It is a method used to encrypt confidential data.
- ☐ It is the art of transferring handwritten signature to electronic media.
- ☐ It allows the recipient of data to prove the source and integrity of data.
- ☐ It can be used as a signature system and a cryptosystem.

Question 651

Complete the following sentence. A message can be encrypted, which provides:

- ☐ Confidentiality
- ☐ Non-Repudiation
- ☐ Authentication
- ☐ Integrity

Question 652

Which of the following questions is LESS likely to help in assessing physical access controls?

- ☐ Does management regularly review the list of persons with physical access to sensitive facilities?
- ☐ Is the operating system configured to prevent circumvention of the security software and application controls?
- ☐ Are keys or other access devices needed to enter the computer room and media library?
- ☐ Are visitors to sensitive areas signed in and escorted?

Question 653

Which of the following is a symmetric encryption algorithm?

- ☐ RSA
- ☐ Elliptic Curve
- ☐ RC5
- ☐ El Gamal

Question 654

In IPSec, if the communication is to be gateway-to-gateway or host-to-gateway:

- ☐ Tunnel mode of operation is required
- ☐ Only transport mode can be used
- ☐ Encapsulating Security Payload (ESP) authentication must be used
- ☐ Both tunnel and transport mode can be used

Question 655

Which backup method does not reset the archive bit on files that are backed up?

- ☐ Full backup method
- ☐ Incremental backup method
- ☐ Differential backup method
- ☐ Additive backup method

Question 656

Which of the following is a proximity identification device that does not require action by the user and works by responding with an access code to signals transmitted by a reader?

- ☐ A passive system sensing device
- ☐ A transponder
- ☐ A card swipe
- ☐ A magnetic card

Question 657

Which of the following items is NOT primarily used to ensure integrity?

- ☐ Cyclic Redundancy Check (CRC)
- ☐ Redundant Array of Inexpensive Disks (RAID) system
- ☐ Hashing Algorithms
- ☐ The Biba Security model

Question 658

Which is NOT a suitable method for distributing certificate revocation information?

- ☐ CA revocation mailing list
- ☐ Delta CRL
- ☐ OCSP (online certificate status protocol)
- ☐ Distribution point CRL

Question 659

Which of the following classes is defined in the TCSEC (Orange Book) as discretionary protection?

- ☐ C
- ☐ B
- ☐ A
- ☐ D

Question 660

Which of the following security models introduced the idea of mutual exclusivity which generates dynamically changing permissions?

- ☐ Biba
- ☐ Brewer & Nash
- ☐ Graham-Denning
- ☐ Clark-Wilson

Question 661

What is the primary role of cross certification?

- ☐ Creating trust between different PKIs
- ☐ Build an overall PKI hierarchy
- ☐ set up direct trust to a second root CA
- ☐ Prevent the nullification of user certificates by CA certificate revocation

Question 662

Risk reduction in a system development life-cycle should be applied:

- ☐ Mostly to the initiation phase.
- ☐ Mostly to the development phase.
- ☐ Mostly to the disposal phase.
- ☐ Equally to all phases.

Question 663

In order to be able to successfully prosecute an intruder:

- ☐ A point of contact should be designated to be responsible for communicating with law enforcement and other external agencies.
- ☐ A proper chain of custody of evidence has to be preserved.
- ☐ Collection of evidence has to be done following predefined procedures.
- ☐ Whenever possible, analyze a replica of the compromised resource, not the original, thereby avoiding inadvertently tampering with evidence.

Question 664

During which phase of an IT system life cycle are security requirements developed?

- ☐ Operation
- ☐ Initiation
- ☐ Functional design analysis and Planning
- ☐ Implementation

Question 665

Which of the following was the FIRST mathematical model of a multilevel security policy used to define the concepts of a security state and mode of access, and to outline rules of access?

- ☐ Biba
- ☐ Bell-LaPadula
- ☐ Clark-Wilson
- ☐ State machine

Question 666

Which of the following effectively doubles the amount of hard drives needed but also provides redundancy?

- ☐ RAID Level 0
- ☐ RAID Level 1
- ☐ RAID Level 2
- ☐ RAID Level 5

Question 667

Which protocol's primary function is to facilitate file and directory transfer between two machines?

- ☐ Telnet.
- ☐ File Transfer Protocol (FTP).
- ☐ Trivial File Transfer Protocol (TFTP).
- ☐ Simple Mail Transfer Protocol (SMTP)

Question 668

Ensuring that printed reports reach proper users and that receipts are signed before releasing sensitive documents are examples of:

- ☐ Deterrent controls
- ☐ Output controls
- ☐ Information flow controls
- ☐ Asset controls

Question 669

Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?

- ☐ Development/acquisition
- ☐ Implementation
- ☐ Operation/Maintenance
- ☐ Initiation

Question 670

The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as " _____," RSA is quite feasible for computer use.

- ☐ computing in Galois fields
- ☐ computing in Gladden fields
- ☐ computing in Gallipoli fields
- ☐ computing in Galbraith fields

Question 671

Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?

- ☐ Implementation
- ☐ System feasibility
- ☐ Product design
- ☐ Software plans and requirements

Question 672

Which of the following is NOT a valid reason to use external penetration service firms rather than corporate resources?

- ☐ They are more cost-effective
- ☐ They offer a lack of corporate bias
- ☐ They use highly talented ex-hackers
- ☐ They ensure a more complete reporting

Question 673

The most prevalent cause of computer center fires is which of the following?

- ☐ AC equipment
- ☐ Electrical distribution systems
- ☐ Heating systems
- ☐ Natural causes

Question 674

The Telecommunications Security Domain of information security is also concerned with the prevention and detection of the misuse or abuse of systems, which poses a threat to the tenets of:

- ☐ Confidentiality, Integrity, and Entity (C.I.E.).
- ☐ Confidentiality, Integrity, and Authenticity (C.I.A.).
- ☐ Confidentiality, Integrity, and Availability (C.I.A.).
- ☐ Confidentiality, Integrity, and Liability (C.I.L.).

Question 675

Which of the following security controls is intended to bring an environment back to regular operation?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Question 676

The environment that must be protected includes all personnel, equipment, data, communication devices, power supply and wiring. The necessary level of protection depends on the value of the data, the computer systems, and the company assets within the facility. The value of these items can be determined by what type of analysis?

- ☐ Critical-channel analysis
- ☐ Covert channel analysis
- ☐ Critical-path analysis
- ☐ Critical-conduit analysis

Question 677

What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?

- ☐ Accountability controls
- ☐ Mandatory access controls
- ☐ Assurance procedures
- ☐ Administrative controls

Question 678

Like the Kerberos protocol, SESAME is also subject to which of the following?

- ☐ timeslot replay
- ☐ password guessing
- ☐ symmetric key guessing
- ☐ asymmetric key guessing

Question 679

Which of the following asymmetric encryption algorithms is based on the difficulty of factoring LARGE numbers?

- ☐ El Gamal
- ☐ Elliptic Curve Cryptosystems (ECCs)
- ☐ RSA
- ☐ International Data Encryption Algorithm (IDEA)

Question 680

Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?

- ☐ hot site.
- ☐ warm site.
- ☐ cold site.
- ☐ reciprocal agreement.

Question 681

Which of the following protocols is designed to send individual messages securely?

- ☐ Kerberos
- ☐ Secure Electronic Transaction (SET).
- ☐ Secure Sockets Layer (SSL).
- ☐ Secure HTTP (S-HTTP).

Question 682

Which of the following is an IP address that is private (i.e. reserved for internal networks, and not a valid address to use on the Internet)?

- ☐ 10.0.42.5
- ☐ 11.0.42.5
- ☐ 12.0.42.5
- ☐ 13.0.42.5

Question 683

Which of the following is a CHARACTERISTIC of a decision support system (DSS) in regards to Threats and Risks Analysis?

- ☐ DSS is aimed at solving highly structured problems.
- ☐ DSS emphasizes flexibility in the decision making approach of users.
- ☐ DSS supports only structured decision-making tasks.
- ☐ DSS combines the use of models with non-traditional data access and retrieval functions.

Question 684

Which of the following BEST describes an exploit?

- ☐ An intentional hidden message or feature in an object such as a piece of software or a movie.
- ☐ A chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software.
- ☐ An anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer.
- ☐ A condition where a program (either an application or part of the operating system) stops performing its expected function and also stops responding to other parts of the system.

Question 685

The DMZ does not normally contain:

- ☐ encryption server
- ☐ web server
- ☐ external DNS server
- ☐ mail relay

Question 686

Which layer of the OSI/ISO model handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control?

- ☐ Physical
- ☐ Data link
- ☐ Network
- ☐ Session

Question 687

Who should direct short-term recovery actions immediately following a disaster?

- ☐ Chief Information Officer.
- ☐ Chief Operating Officer.
- ☐ Disaster Recovery Manager.
- ☐ Chief Executive Officer.

Question 688

How would nonrepudiation be BEST classified as?

- ☐ A preventive control
- ☐ A logical control
- ☐ A corrective control
- ☐ A compensating control

Question 689

An incremental backup process

- ☐ Backs up all the files that have changed since the last full or incremental backup and sets the archive bit to 0.
- ☐ Backs up the files that been modified since the last full backup. It does not change the archive bit value.
- ☐ Backs up all the data and changes the archive bit to 0.
- ☐ Backs up all the data and changes the archive bit to 1.

Question 690

What kind of encryption technology does SSL utilize?

- ☐ Secret or Symmetric key
- ☐ Hybrid (both Symmetric and Asymmetric)
- ☐ Public Key
- ☐ Private Key

Question 691

Which of the following is the act of performing tests and evaluations to test a system's security level to see if it complies with the design specifications and security requirements?

- ☐ Validation
- ☐ Verification
- ☐ Assessment
- ☐ Accuracy

Question 692

Controls like guards and general steps to maintain building security, securing of server rooms or laptops, the protection of cables, and usage of magnetic switches on doors and windows are some of the examples of:

- ☐ administrative controls.
- ☐ logical controls.
- ☐ technical controls.
- ☐ physical controls.

Question 693

Which of the following protects a password from eavesdroppers and supports the encryption of communication?

- ☐ Challenge Handshake Authentication Protocol (CHAP)
- ☐ Challenge Handshake Identification Protocol (CHIP)
- ☐ Challenge Handshake Encryption Protocol (CHEP)
- ☐ Challenge Handshake Substitution Protocol (CHSP)

Question 694

Which of the following does NOT apply to system-generated passwords?

- ☐ Passwords are harder to remember for users.
- ☐ If the password-generating algorithm gets to be known, the entire system is in jeopardy.
- ☐ Passwords are more vulnerable to brute force and dictionary attacks.
- ☐ Passwords are harder to guess for attackers.

Question 695

An Ethernet address is composed of how many bits?

- ☐ 48-bit address
- ☐ 32-bit address.
- ☐ 64-bit address
- ☐ 128-bit address

Question 696

What kind of encryption is realized in the S/MIME-standard?

- ☐ Asymmetric encryption scheme
- ☐ Password based encryption scheme
- ☐ Public key based, hybrid encryption scheme
- ☐ Elliptic curve based encryption

Question 697

A copy of evidence or oral description of its contents; which is not as reliable as best evidence is what type of evidence?

- ☐ Direct evidence
- ☐ Circumstantial evidence
- ☐ Hearsay evidence
- ☐ Secondary evidence

Question 698

Which of the following term BEST describes a weakness that could potentially be exploited?

- ☐ Vulnerability
- ☐ Risk
- ☐ Threat
- ☐ Target of evaluation (TOE)

Question 699

Which of the following is BEST defined as a physical control?

- ☐ Monitoring of system activity
- ☐ Fencing
- ☐ Identification and authentication methods
- ☐ Logical access control mechanisms

Question 700

Which of the following recovery plan test results would be most useful to management?

- ☐ elapsed time to perform various activities.
- ☐ list of successful and unsuccessful activities.
- ☐ amount of work completed.
- ☐ description of each activity.

Question 701

Which of the following would BEST be defined as an absence or weakness of safeguard that could be exploited?

- ☐ A threat.
- ☐ A vulnerability.
- ☐ A risk.
- ☐ An exposure.

Question 702

Which of the following is TRUE about link encryption?

- ☐ Each entity has a common key with the destination node.
- ☐ Encrypted messages are only decrypted by the final node.
- ☐ This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
- ☐ Only secure nodes are used in this type of transmission.

Question 703

Which of the following BEST explains why computerized information systems frequently fail to meet the needs of users?

- ☐ Inadequate quality assurance (QA) tools.
- ☐ Constantly changing user needs.
- ☐ Inadequate user participation in defining the system's requirements.
- ☐ Inadequate project management.

Question 704

While referring to physical security, what does positive pressurization means?

- ☐ The pressure inside your sprinkler system is greater than zero.
- ☐ The air goes out of a room when a door is opened and outside air does not go into the room.
- ☐ Causes the sprinkler system to go off.
- ☐ A series of measures that increase pressure on employees in order to make them more productive.

Question 705

Which of the following can be defined as the set of allowable values that an attribute can take?

- ☐ domain of a relation
- ☐ domain name service of a relation
- ☐ domain analysis of a relation
- ☐ domains, in database of a relation

Question 706

What works as an E-mail message transfer agent?

- ☐ SMTP
- ☐ SNMP
- ☐ S-RPC
- ☐ S/MIME

Question 707

Controlling access to information systems and associated networks is necessary for the preservation of their:

- ☐ Authenticity, confidentiality and availability
- ☐ Confidentiality, integrity, and availability.
- ☐ Integrity and availability.
- ☐ Authenticity, confidentiality, integrity and availability.

Question 708

Why does fiber optic communication technology have significant security advantage over other transmission technology?

- ☐ Higher data rates can be transmitted.
- ☐ Interception of data traffic is more difficult.
- ☐ Traffic analysis is prevented by multiplexing.
- ☐ Single and double-bit errors are correctable.

Question 709

In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?

- ☐ Subordinate CA
- ☐ Top Level CA
- ☐ Big CA
- ☐ Master CA

Question 710

You've decided to authenticate the source who initiated a particular transfer while ensuring integrity of the data being transferred. You can do this by:

- ☐ having the sender encrypt the message with his private key.
- ☐ having the sender encrypt the hash with his private key.
- ☐ having the sender encrypt the message with his symmetric key.
- ☐ having the sender encrypt the hash with his public key.

Question 711

What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?

- ☐ Evidence Circumstance Doctrine
- ☐ Exigent Circumstance Doctrine
- ☐ Evidence of Admissibility Doctrine
- ☐ Exigent Probable Doctrine

Question 712

Within Crime prevention through Environmental Design (CPTED) the concept of territoriality is BEST described as:

- ☐ ownership.
- ☐ protecting specific areas with different measures.
- ☐ localized emissions.
- ☐ compromise of the perimeter.

Question 713

What is the name of a one way transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string? Such a transformation cannot be reversed.

- ☐ One-way hash
- ☐ DES
- ☐ Transposition
- ☐ Substitution

Question 714

Which of the following is TRUE about digital certificate?

- ☐ It is the same as digital signature proving Integrity and Authenticity of the data
- ☐ Electronic credential proving that the person the certificate was issued to is who they claim to be.
- ☐ You can only get digital certificate from Verisign, RSA if you wish to prove the key belong to a specific user.
- ☐ Can't contain geography data such as country for example.

Question 715

What is the MOST critical characteristic of a biometric identifying system?

- ☐ Perceived intrusiveness
- ☐ Storage requirements
- ☐ Accuracy
- ☐ Scalability

Question 716

What is the RESULT of a hash algorithm being applied to a message?

- ☐ A digital signature
- ☐ A ciphertext
- ☐ A message digest
- ☐ A plaintext

Question 717

What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?

- ☐ Authentication
- ☐ Identification
- ☐ Authorization
- ☐ Confidentiality

Question 718

You are a security consultant who is required to perform penetration testing on a client's network. During penetration testing, you are required to use a compromised system to attack other systems on the network to avoid network restrictions like firewalls.

Which method would you use in this scenario:

- ☐ Black box Method
- ☐ Pivoting method
- ☐ White Box Method.
- ☐ Grey Box Method

Question 719

Buffer overflow and boundary condition errors are subsets of which of the following?

- ☐ Race condition errors.
- ☐ Access validation errors.
- ☐ Exceptional condition handling errors.
- ☐ Input validation errors.

Question 720

Which BEST describes a tool (i.e. keyfob, calculator, memory card or smart card) used to supply dynamic passwords?

- ☐ Tickets
- ☐ Tokens
- ☐ Token passing networks
- ☐ Coupons

Question 721

Which encryption algorithm is BEST suited for communication with handheld wireless devices?

- ☐ ECC (Elliptic Curve Cryptosystem)
- ☐ RSA
- ☐ SHA
- ☐ RC4

Question 722

The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:

- ☐ you need.
- ☐ you read.
- ☐ you are.
- ☐ you do.

Question 723

Which of the following choices is a valid Public Key Cryptography Standard (PKCS) addressing RSA?

- ☐ PKCS #17799
- ☐ PKCS-RSA
- ☐ PKCS#1
- ☐ PKCS#11

Question 724

An intranet is an Internet-like logical network that uses:

- ☐ a firm's internal, physical network infrastructure.
- ☐ a firm's external, physical network infrastructure.
- ☐ a firm's external, physical netBIOS infrastructure.
- ☐ a firm's internal, physical netBIOS infrastructure.