



CISSP.exam.715q

CISSP

CISSP

Certified Information Systems Security Professional

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (715 questions)

Question 1

How often should tests and disaster recovery drills be performed?

- ☐ At least once a quarter
- ☐ At least once every 6 months
- ☐ At least once a year
- ☐ At least once every 2 years

Question 2

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 3

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

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

Question 4

Which access control model would a lattice-based access control model be an example of?

- ☐ Mandatory access control.
- ☐ Discretionary access control.
- ☐ Non-discretionary access control.
- ☐ Rule-based access control.

Question 5

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 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

Which of the following will a Business Impact Analysis NOT identify?

- ☐ Areas that would suffer the greatest financial or operational loss in the event of a disaster.
- ☐ Systems critical to the survival of the enterprise.
- ☐ The names of individuals to be contacted during a disaster.
- ☐ The outage time that can be tolerated by the enterprise as a result of a disaster.

Question 8

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 9

Which of the following services relies on UDP?

- ☐ FTP
- ☐ Telnet
- ☐ DNS
- ☐ SMTP

Question 10

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 11

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 12

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 13

Which of the following encryption algorithms does NOT deal with discrete logarithms?

- ☐ El Gamal
- ☐ Diffie-Hellman
- ☐ RSA
- ☐ Elliptic Curve

Question 14

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 15

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 16

Which of the following media is MOST resistant to EMI interference?

- ☐ microwave
- ☐ fiber optic
- ☐ twisted pair
- ☐ coaxial cable

Question 17

Which of the following statements pertaining to using Kerberos without any extension is FALSE?

- ☐ A client can be impersonated by password-guessing.
- ☐ Kerberos is mostly a third-party authentication protocol.
- ☐ Kerberos uses public key cryptography.
- ☐ Kerberos provides robust authentication.

Question 18

Which type of password token involves time synchronization?

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

Question 19

At which of the OSI/ISO model layer is IP implemented?

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

Question 20

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 21

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 22

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

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

Question 23

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 24

Access Control techniques do NOT include which of the following?

- ☐ Relevant Access Controls
- ☐ Discretionary Access Control
- ☐ Mandatory Access Control
- ☐ Lattice Based Access Control

Question 25

In an 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 26

Which key agreement scheme uses implicit signatures?

- ☐ MQV
- ☐ DH
- ☐ ECC
- ☐ RSA

Question 27

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

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

Question 28

One of the following statements about the differences between PPTP and L2TP is NOT true

- ☐ PPTP can run only on top of IP networks.
- ☐ PPTP is an encryption protocol and L2TP is not.
- ☐ L2TP works well with all firewalls and network devices that perform NAT.
- ☐ L2TP supports AAA servers

Question 29

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 30

Which of the following is the most complete disaster recovery plan test type, to be performed after successfully completing the Parallel test?

- ☐ Full Interruption test
- ☐ Checklist test
- ☐ Simulation test
- ☐ Structured walk-through test

Question 31

What would you call a microchip installed on the motherboard of modern computers and is dedicated to carrying out security functions that involve the storage and processing of symmetric and asymmetric keys, hashes, and digital certificates.

- ☐ Trusted Platform Module (TPM)
- ☐ Trusted BIOS Module (TBM)
- ☐ Central Processing Unit (CPU)
- ☐ Arithmetic Logical Unit (ALU)

Question 32

Which of the following transmission media would NOT be affected by cross talk or interference?

- ☐ Copper cable
- ☐ Radio System
- ☐ Satellite radiolink
- ☐ Fiber optic cables

Question 33

What is called the number of columns in a table?

- ☐ Schema
- ☐ Relation
- ☐ Degree
- ☐ Cardinality

Question 34

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 35

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 36

Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?

- ☐ Message non-repudiation.
- ☐ Message confidentiality.
- ☐ Message interleave checking.
- ☐ Message integrity.

Question 37

What is the main focus of the Bell-LaPadula security model?

- ☐ Accountability
- ☐ Integrity
- ☐ Confidentiality
- ☐ Availability

Question 38

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 39

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 40

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 41

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 42

An Intrusion Detection System (IDS) is what type of control?

- ☐ A preventive control.
- ☐ A detective control.
- ☐ A recovery control.
- ☐ A directive control.

Question 43

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 44

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 45

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 46

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 47

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 48

Which of the following suppresses combustion by disrupting a chemical reaction, by doing so it kills the fire?

- ☐ Halon
- ☐ CO2
- ☐ water
- ☐ soda acid

Question 49

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 50

You have been tasked with developing a Business Continuity Plan/Disaster Recovery (BCP/DR) plan. After several months of researching the various areas of the organization, you are ready to present the plan to Senior Management.

During the presentation meeting, the plan that you have dutifully created is not received positively. Senior Management is convinced that they need to enact your plan, nor are they prepared to invest any money in the plan.

What is the BEST reason, as to why Senior Management is not willing to enact your plan?

- ☐ The business case was not initially made and thus did not secure their support.
- ☐ They were not included in any of the Risk Assessment meetings.
- ☐ They were not included in any of the Business Impact Assessment meetings.
- ☐ A Business Impact Assessment was not performed.

Question 51

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 52

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 53

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 54

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

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

Question 55

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 56

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

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

Question 57

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 58

Which of the following statements pertaining to message digests is NOT true?

- ☐ The original file cannot be created from the message digest.
- ☐ Two different files should not have the same message digest.
- ☐ The message digest should be calculated using at least 128 bytes of the file.
- ☐ Message digests are usually of fixed size.

Question 59

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 60

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 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

During a business impact analysis it is concluded that a system has maximum tolerable downtime of 2 hours. What would this system be classified as?

- ☐ Important
- ☐ Urgent
- ☐ Critical
- ☐ Vital

Question 63

What is the minimum static charge able to cause disk drive data loss?

- ☐ 550 volts
- ☐ 1000 volts
- ☐ 1500 volts
- ☐ 2000 volts

Question 64

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 65

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 66

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 67

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

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

Question 68

This OSI layer has a service that negotiates transfer syntax and translates data to and from the transfer syntax for users, which may represent data using different syntaxes. At which of the following layers would you find such service?

- ☐ Session
- ☐ Transport
- ☐ Presentation
- ☐ Application

Question 69

Which OSI/OSI layer defines the X.24, V.35, X.21 and HSSI standard interfaces?

- ☐ Transport layer
- ☐ Network layer
- ☐ Data link layer
- ☐ Physical layer

Question 70

Which access control model achieves data integrity through well-formed transactions and separation of duties?

- ☐ Clark-Wilson model
- ☐ Biba model
- ☐ Non-interference model
- ☐ Sutherland model

Question 71

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 72

Degaussing is used to clear data from all of the following media except:

- ☐ Floppy Disks
- ☐ Read-Only Media
- ☐ Video Tapes
- ☐ Magnetic Hard Disks

Question 73

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 74

What does the * (star) integrity axiom mean in the Biba model?

- ☐ No read up
- ☐ No write down
- ☐ No read down
- ☐ No write up

Question 75

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 76

Rule-Based Access Control (RuBAC) access is determined by rules. Such rules would fit within what category of access control?

- ☐ Discretionary Access Control (DAC)
- ☐ Mandatory Access control (MAC)
- ☐ Non-Discretionary Access Control (NDAC)
- ☐ Lattice-based Access control

Question 77

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 78

Kerberos can prevent which one of the following attacks?

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

Question 79

What algorithm has been selected as the AES algorithm, replacing the DES algorithm?

- ☐ RC6
- ☐ Twofish
- ☐ Rijndael
- ☐ Blowfish

Question 80

In the Bell-LaPadula model, the *-property (Star-property) is also called:

- ☐ The simple security property
- ☐ The confidentiality property
- ☐ The confinement property
- ☐ The tranquility property

Question 81

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 82

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 83

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 84

According to Requirement 3 of the Payment Card Industry's Data Security Standard (PCI DSS) there is a requirement to "protect stored cardholder data." Which of the following items cannot be stored by the merchant?

- ☐ Primary Account Number
- ☐ Cardholder Name
- ☐ Expiration Date
- ☐ The Card Validation Code (CVV2)

Question 85

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 86

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 87

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

- ☐ B
- ☐ A
- ☐ C
- ☐ D

Question 88

Which of the following statements pertaining to RAID technologies is incorrect?

- ☐ RAID-5 has a higher performance in read/write speeds than the other levels.
- ☐ RAID-3 uses byte-level striping with dedicated parity.
- ☐ RAID-0 relies solely on striping.
- ☐ RAID-4 uses dedicated parity.

Question 89

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 90

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 91

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

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

Question 92

Which of the following services is provided by S-RPC?

- ☐ Availability
- ☐ Accountability
- ☐ Integrity
- ☐ Authentication

Question 93

What security model implies a central authority that defines rules and sometimes global rules, dictating what subjects can have access to what objects?

- ☐ Flow Model
- ☐ Discretionary access control
- ☐ Mandatory access control
- ☐ Non-discretionary access control

Question 94

Which of the following are well known ports assigned by the IANA?

- ☐ Ports 0 to 255
- ☐ Ports 0 to 1024
- ☐ Ports 0 to 1023
- ☐ Ports 0 to 127

Question 95

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 96

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 97

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 98

Which of the following is NOT an asymmetric key algorithm?

- ☐ RSA
- ☐ Elliptic Curve Cryptosystem (ECC)
- ☐ El Gamal
- ☐ Data Encryption Standard (DES)

Question 99

What is the MOST critical characteristic of a biometric identifying system?

- ☐ Perceived intrusiveness
- ☐ Storage requirements
- ☐ Accuracy
- ☐ Scalability

Question 100

Which of the following is NOT part of the Kerberos authentication protocol?

- ☐ Symmetric key cryptography
- ☐ Authentication service (AS)
- ☐ Principals
- ☐ Public Key

Question 101

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 102

Which port does the Post Office Protocol Version 3 (POP3) make use of?

- ☐ 110
- ☐ 109
- ☐ 139
- ☐ 119

Question 103

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 104

What does the simple integrity axiom mean in the Biba model?

- ☐ No write down
- ☐ No read down
- ☐ No read up
- ☐ No write up

Question 105

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 106

Which of the following statements pertaining to key management is NOT true?

- ☐ The more a key is used, the shorter its lifetime should be.
- ☐ When not using the full keyspace, the key should be extremely random.
- ☐ Keys should be backed up or escrowed in case of emergencies.
- ☐ A key's lifetime should correspond with the sensitivity of the data it is protecting.

Question 107

Transport Layer Security (TLS) is a two-layered socket layer security protocol that contains the TLS Record Protocol and the:

- ☐ Transport Layer Security (TLS) Internet Protocol.
- ☐ Transport Layer Security (TLS) Data Protocol.
- ☐ Transport Layer Security (TLS) Link Protocol.
- ☐ Transport Layer Security (TLS) Handshake Protocol.

Question 108

What can be defined as a batch process dumping backup data through communications lines to a server at an alternate location?

- ☐ Remote journaling
- ☐ Electronic vaulting
- ☐ Data clustering
- ☐ Database shadowing

Question 109

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 110

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 111

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

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

Question 112

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 113

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 114

What is the essential difference between a self-audit and an independent audit?

- ☐ Tools used
- ☐ Results
- ☐ Objectivity
- ☐ Competence

Question 115

Which of the following access control models requires security clearance for subjects?

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

Question 116

Which of the following questions is LESS likely to help in assessing identification and authentication controls?

- ☐ Is a current list maintained and approved of authorized users and their access?
- ☐ Are passwords changed at least every ninety days or earlier if needed?
- ☐ Are inactive user identifications disabled after a specified period of time?
- ☐ Is there a process for reporting incidents?

Question 117

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 118

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

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

Question 119

What size is an MD5 message digest (hash)?

- ☐ 128 bits
- ☐ 160 bits
- ☐ 256 bits
- ☐ 128 bytes

Question 120

A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:

- ☐ Mandatory Access Control
- ☐ Discretionary Access Control
- ☐ Non-Discretionary Access Control
- ☐ Rule-based Access control

Question 121

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

- ☐ 168
- ☐ 128
- ☐ 56
- ☐ 64

Question 122

Which of the following was NOT designed to be a proprietary encryption algorithm?

- ☐ RC2
- ☐ RC4
- ☐ Blowfish
- ☐ Skipjack

Question 123

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 124

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 125

When attempting to establish liability, which of the following would be described as performing the ongoing maintenance necessary to keep something in proper working order, updated, effective, or to abide by what is commonly expected in a situation?

- ☐ Due care
- ☐ Due concern
- ☐ Due diligence
- ☐ Due practice

Question 126

SQL commands do not include which of the following?

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

Question 127

The equation used to calculate the total number of symmetric keys (K) needed for a group of users (N) to communicate securely with each other is given by which of the following?

- ☐ $K(N - 1) / 2$
- ☐ $N(K - 1) / 2$
- ☐ $K(N + 1) / 2$
- ☐ $N(N - 1) / 2$

Question 128

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 129

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

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

Question 130

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 131

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 132

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 133

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 134

Of the following, which is NOT a specific loss criteria that should be considered while developing a BIA?

- ☐ Loss of skilled workers knowledge
- ☐ Loss in revenue
- ☐ Loss in profits
- ☐ Loss in reputation

Question 135

What can be defined as a list of subjects along with their access rights that are authorized to access a specific object?

- ☐ A capability table
- ☐ An access control list
- ☐ An access control matrix
- ☐ A role-based matrix

Question 136

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 137

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 138

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 139

Which of the following is NOT a type of motion detector?

- ☐ Photoelectric sensor
- ☐ Passive infrared sensors
- ☐ Microwave Sensor.
- ☐ Ultrasonic Sensor.

Question 140

In which LAN transmission method is a source packet copied and sent to specific multiple destinations but not ALL of the destinations on the network?

- ☐ Overcast
- ☐ Unicast
- ☐ Multicast
- ☐ Broadcast

Question 141

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 142

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

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

Question 143

What are the four basic elements of Fire?

- ☐ Heat, Fuel, Oxygen, and Chain Reaction
- ☐ Heat, Fuel, CO2, and Chain Reaction
- ☐ Heat, Wood, Oxygen, and Chain Reaction
- ☐ Flame, Fuel, Oxygen, and Chain Reaction

Question 144

MOST access violations are:

- ☐ Accidental
- ☐ Caused by internal hackers
- ☐ Caused by external hackers
- ☐ Related to Internet

Question 145

Which of the following service is not provided by a public key infrastructure (PKI)?

- ☐ Access control
- ☐ Integrity
- ☐ Authentication
- ☐ Reliability

Question 146

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 147

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 148

Which fire class can water be most appropriate for?

- ☐ Class A fires
- ☐ Class B fires
- ☐ Class C fires
- ☐ Class D fires

Question 149

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 150

The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers 6 is which of the following?

- ☐ Application Layer
- ☐ Presentation Layer
- ☐ Data Link Layer
- ☐ Network Layer

Question 151

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 152

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 153

What is called the type of access control where there are pairs of elements that have the least upper bound of values and greatest lower bound of values?

- ☐ Mandatory model
- ☐ Discretionary model
- ☐ Lattice model
- ☐ Rule model

Question 154

For maximum security design, what type of fence is most effective and cost-effective method (Foot is being used as measurement unit below)?

- ☐ 3' to 4' high.
- ☐ 6' to 7' high.
- ☐ 8' high and above with strands of barbed wire.
- ☐ Double fencing

Question 155

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 156

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 157

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 158

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 159

Which of the following is used to monitor network traffic or to monitor host audit logs in real time to determine violations of system security policy that have taken place?

- ☐ Intrusion Detection System
- ☐ Compliance Validation System
- ☐ Intrusion Management System (IMS)
- ☐ Compliance Monitoring System

Question 160

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 161

In which layer of the OSI Model are connection-oriented protocols located in the TCP/IP suite of protocols?

- ☐ Transport layer
- ☐ Application layer
- ☐ Physical layer
- ☐ Network layer

Question 162

Which ISO/OSI layer establishes the communications link between individual devices over a physical link or channel?

- ☐ Transport layer
- ☐ Network layer
- ☐ Data link layer
- ☐ Physical layer

Question 163

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 164

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 165

The Information Technology Security Evaluation Criteria (ITSEC) was written to address which of the following that the Orange Book did not address?

- ☐ integrity and confidentiality
- ☐ confidentiality and availability
- ☐ integrity and availability
- ☐ none of the above

Question 166

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 167

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 168

Which of the following is NOT an encryption algorithm?

- ☐ Skipjack
- ☐ SHA-1
- ☐ Twofish
- ☐ DEA

Question 169

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 170

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

- ☐ PPP
- ☐ RARP
- ☐ L2F
- ☐ ICMP

Question 171

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 172

What is the maximum allowable key size of the Rijndael encryption algorithm?

- ☐ 128 bits
- ☐ 192 bits
- ☐ 256 bits
- ☐ 512 bits

Question 173

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 174

Behavioral-based systems are also known as?

- ☐ Profile-based systems
- ☐ Pattern matching systems
- ☐ Misuse detective systems
- ☐ Rule-based IDS

Question 175

Which Orange book security rating is the FIRST to be concerned with covert channels?

- ☐ A1
- ☐ B3
- ☐ B2
- ☐ B1

Question 176

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 177

Which access control model provides upper and lower bounds of access capabilities for a subject?

- ☐ Role-based access control
- ☐ Lattice-based access control
- ☐ Biba access control
- ☐ Content-dependent access control

Question 178

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

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

Question 179

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 180

Which of the following is the MOST secure form of triple-DES encryption?

- ☐ DES-EDE3
- ☐ DES-EDE1
- ☐ DES-EEE4
- ☐ DES-EDE2

Question 181

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 182

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 183

Which of the following virus types changes some of its characteristics as it spreads?

- ☐ Boot Sector
- ☐ Parasitic
- ☐ Stealth
- ☐ Polymorphic

Question 184

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 185

Readable is to unreadable just as plain text is to:

- ☐ Cipher Text
- ☐ Encryption
- ☐ Unplain Text
- ☐ Digitally Signed

Question 186

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

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

Question 187

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 188

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 189

Complete the following sentence. A message can be encrypted, which provides:

- ☐ confidentiality.
- ☐ non-repudiation.
- ☐ authentication.
- ☐ integrity.

Question 190

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 191

Which OSI/ISO layer is the Media Access Control (MAC) sublayer part of?

- ☐ Transport layer
- ☐ Network layer
- ☐ Data link layer
- ☐ Physical layer

Question 192

What security model is dependent on security labels?

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

Question 193

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 194

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 195

What IDS approach relies on a database of known attacks?

- ☐ Signature-based intrusion detection
- ☐ Statistical anomaly-based intrusion detection
- ☐ Behavior-based intrusion detection
- ☐ Network-based intrusion detection

Question 196

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 197

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 198

Which of the following does NOT concern itself with key management?

- ☐ Internet Security Association Key Management Protocol (ISAKMP)
- ☐ Diffie-Hellman (DH)
- ☐ Cryptology (CRYPTO)
- ☐ Key Exchange Algorithm (KEA)

Question 199

What is the maximum key size for the RC5 algorithm?

- ☐ 128 bits
- ☐ 256 bits
- ☐ 1024 bits
- ☐ 2040 bits

Question 200

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 201

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 202

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 203

Which Orange book security rating introduces the object reuse protection?

- ☐ C1
- ☐ C2
- ☐ B1
- ☐ B2

Question 204

Which access model is most appropriate for companies with a high employee turnover?

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

Question 205

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 206

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 207

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

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

Question 208

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 209

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 210

Which of the following classes is defined in the TCSEC (Orange Book) as discretionary protection?

- ☐ C
- ☐ B
- ☐ A
- ☐ D

Question 211

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 212

The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers does NOT have which of the following characteristics?

- ☐ Standard model for network communications
- ☐ Used to gain information from network devices such as count of packets received and routing tables
- ☐ Enables dissimilar networks to communicate
- ☐ Defines 7 protocol layers (a.k.a. protocol stack)

Question 213

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 214

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 215

Which device acting as a translator is used to connect two networks or applications from Layer 4 up to Layer 7 of the ISO/OSI Model?

- ☐ Bridge
- ☐ Repeater
- ☐ Router
- ☐ Gateway

Question 216

In telephony different types of connections are being used. The connection from the phone company's branch office to local customers is referred to as which of the following choices?

- ☐ new loop
- ☐ local loop
- ☐ loopback
- ☐ indigenous loop

Question 217

Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

- ☐ Palm Scan
- ☐ Hand Geometry
- ☐ Fingerprint
- ☐ Retina scan

Question 218

Of the three types of alternate sites: hot, warm or cold, which is BEST described by the following facility description?

Configured and functional facility
Available with a few hours
Requires constant maintenance
Is expensive to maintain

- ☐ Hot Site
- ☐ Warm Site
- ☐ Cold Site
- ☐ Remote Site

Question 219

Which of the following BEST ensures accountability of users for the actions taken within a system or domain?

- ☐ Identification
- ☐ Authentication
- ☐ Authorization
- ☐ Credentials

Question 220

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 221

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 222

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 223

A business continuity plan is an example of which of the following?

- ☐ Corrective control
- ☐ Detective control
- ☐ Preventive control
- ☐ Compensating control

Question 224

Suppose that you are the COMSEC - Communications Security custodian for a large, multinational corporation. Susie, from Finance approaches you in the break room saying that she lost her smart ID card that she uses to digitally sign and encrypt emails in the PKI.

What happens to the certificates contained on the smart card after the security officer takes appropriate action?

- ☐ They are added to the CRL
- ☐ They are reissued to the user
- ☐ New certificates are issued to the user
- ☐ The user may no longer have certificates

Question 225

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 226

The US-EU Safe Harbor process has been created to address which of the following?

- ☐ Integrity of data transferred between U.S. and European companies
- ☐ Confidentiality of data transferred between U.S and European companies
- ☐ Protection of personal data transferred between U.S and European companies
- ☐ Confidentiality of data transferred between European and international companies

Question 227

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 228

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 229

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 230

What is the difference between the OCSP (Online Certificate Status Protocol) and a Certificate Revocation List (CRL)?

- ☐ The OCSP (Online Certificate Status Protocol) provides real-time certificate checks and a Certificate Revocation List (CRL) has a delay in the updates.
- ☐ The OCSP (Online Certificate Status Protocol) is a proprietary certificate mechanism developed by Microsoft and a Certificate Revocation List (CRL) is an open standard.
- ☐ The OCSP (Online Certificate Status Protocol) is used only by Active Directory and a Certificate Revocation List (CRL) is used by Certificate Authorities
- ☐ The OCSP (Online Certificate Status Protocol) is a way to check the attributes of a certificate and a Certificate Revocation List (CRL) is used by Certificate Authorities.

Question 231

During which phase of an IT system life cycle are security requirements developed?

- ☐ Operation
- ☐ Initiation
- ☐ Functional design analysis and Planning
- ☐ Implementation

Question 232

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

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

Question 233

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 234

Which of the following offers confidentiality to an e-mail message?

- ☐ The sender encrypting it with its private key.
- ☐ The sender encrypting it with its public key.
- ☐ The sender encrypting it with the receiver's public key.
- ☐ The sender encrypting it with the receiver's private key.

Question 235

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 236

Which of the following focuses on sustaining an organization's business functions during and after a disruption?

- ☐ Business continuity plan
- ☐ Business recovery plan
- ☐ Continuity of operations plan
- ☐ Disaster recovery plan

Question 237

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 238

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 239

Which of the following is responsible for MOST of the security issues?

- ☐ Outside espionage
- ☐ Hackers
- ☐ Personnel
- ☐ Equipment failure

Question 240

Which of the following is a class A fire?

- ☐ common combustibles
- ☐ liquid
- ☐ electrical
- ☐ Halon

Question 241

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

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

Question 242

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 243

Which security model uses division of operations into different parts and requires different users to perform each part?

- ☐ Bell-LaPadula model
- ☐ Biba model
- ☐ Clark-Wilson model
- ☐ Non-interference model

Question 244

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

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

Question 245

Complete the blanks. When using PKI, I digitally sign a message using my _____ key. The recipient verifies my signature using my _____ key.

- ☐ Private / Public
- ☐ Public / Private
- ☐ Symmetric / Asymmetric
- ☐ Private / Symmetric

Question 246

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 247

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 248

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 249

Which of the following statements pertaining to access control is FALSE?

- ☐ Users should only access data on a need-to-know basis.
- ☐ If access is not explicitly denied, it should be implicitly allowed.
- ☐ Access rights should be granted based on the level of trust a company has on a subject.
- ☐ Roles can be an efficient way to assign rights to a type of user who performs certain tasks.

Question 250

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 251

You are an information systems security officer at a mid-sized business and are called upon to investigate a threat conveyed in an email from one employee to another. You gather the evidence from both the email server transaction logs and from the computers of the two individuals involved in the incident and prepare an executive summary. You find that a threat was sent from one user to the other in a digitally signed email. The sender of the threat says he didn't send the email in question.

What concept of PKI - Public Key Infrastructure will implicate the sender?

- ☐ Non-repudiation
- ☐ The digital signature of the recipient
- ☐ Authentication
- ☐ Integrity

Question 252

Which of the following statements pertaining to block ciphers is NOT true?

- ☐ It operates on fixed-size blocks of plaintext.
- ☐ It is more suitable for software than hardware implementations.
- ☐ Plain text is encrypted with a public key and decrypted with a private key.
- ☐ Some Block ciphers can operate internally as a stream.

Question 253

When we encrypt or decrypt data there is a basic operation involving ones and zeros where they are compared in a process that looks something like this:

0101 0001 Plain text
0111 0011 Key stream
0010 0010 Output

What is this cryptographic operation called?

- ☐ Exclusive-OR
- ☐ Bit Swapping
- ☐ Logical-NOR
- ☐ Decryption

Question 254

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 255

Which of the following is TRUE related to network sniffing?

- ☐ Sniffers allow an attacker to monitor data passing across a network.
- ☐ Sniffers alter the source address of a computer to disguise and exploit weak authentication methods.
- ☐ Sniffers take over network connections.
- ☐ Sniffers send IP fragments to a system that overlap with each other.

Question 256

The steps of an access control model should follow which logical flow:

- ☐ Authorization, Identification, authentication
- ☐ Identification, accountability, authorization
- ☐ Identification, authentication, authorization
- ☐ Authentication, Authorization, Identification

Question 257

How many rounds are used by DES?

- ☐ 16
- ☐ 32
- ☐ 64
- ☐ 48

Question 258

What is the effective key size of DES?

- ☐ 56 bits
- ☐ 64 bits
- ☐ 128 bits
- ☐ 1024 bits

Question 259

Which of the following security-focused protocols has confidentiality services operating at a layer different from the others?

- ☐ Secure HTTP (S-HTTP)
- ☐ FTP Secure (FTPS)
- ☐ Secure socket layer (SSL)
- ☐ Sequenced Packet Exchange (SPX)

Question 260

Which of the following is electromagnetic interference (EMI) that is noise from the radiation generated by the difference between the hot and ground wires?

- ☐ traverse-mode noise
- ☐ common-mode noise
- ☐ crossover-mode noise
- ☐ transversal-mode noise

Question 261

Which of the following is the preferred way to suppress an electrical fire in an information center?

- ☐ CO2
- ☐ CO2, soda acid, or Halon
- ☐ water or soda acid
- ☐ ABC Rated Dry Chemical

Question 262

Which of the following is not a property of the Rijndael block cipher algorithm?

- ☐ It employs a round transformation that is comprised of three layers of distinct and invertible transformations.
- ☐ It is suited for high speed chips with no area restrictions.
- ☐ It operates on 64-bit plaintext blocks and uses a 128 bit key.
- ☐ It could be used on a smart card.

Question 263

What is the RESULT of a hash algorithm being applied to a message?

- ☐ A digital signature
- ☐ A ciphertext
- ☐ A message digest
- ☐ A plaintext

Question 264

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 265

Which of the following is most concerned with personnel security?

- ☐ Management controls
- ☐ Operational controls
- ☐ Technical controls
- ☐ Human resources controls

Question 266

What is the maximum length of cable that can be used for a twisted-pair, Category 5 10Base-T cable?

- ☐ 80 meters
- ☐ 100 meters
- ☐ 185 meters
- ☐ 500 meters

Question 267

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 268

A contingency plan should address:

- ☐ Potential risks.
- ☐ Residual risks.
- ☐ Identified risks.
- ☐ All answers are correct.

Question 269

Failure of a contingency plan is usually:

- ☐ A technical failure.
- ☐ A management failure.
- ☐ Because of a lack of awareness.
- ☐ Because of a lack of training.

Question 270

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 271

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 272

Which of the following models does NOT include data integrity or conflict of interest?

- ☐ Biba
- ☐ Clark-Wilson
- ☐ Bell-LaPadula
- ☐ Brewer-Nash

Question 273

What is a hot-site facility?

- ☐ A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.
- ☐ A site in which space is reserved with pre-installed wiring and raised floors.
- ☐ A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.
- ☐ A site with readymade work space with telecommunications equipment, LANs, PCs, and terminals for work groups.

Question 274

An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:

- ☐ Netware availability
- ☐ Network availability
- ☐ Network acceptability
- ☐ Network accountability

Question 275

In what LAN topology do all the transmissions of the network travel the full length of cable and are received by all other stations?

- ☐ Bus topology
- ☐ Ring topology
- ☐ Star topology
- ☐ FDDI topology

Question 276

Which backup type run at regular intervals would take the least time to complete?

- ☐ Full Backup
- ☐ Differential Backup
- ☐ Incremental Backup
- ☐ Disk Mirroring

Question 277

Which of the following is NOT an example of a detective control?

- ☐ System Monitor
- ☐ IDS
- ☐ Motion detector
- ☐ Backup data restore

Question 278

What is the MOST important step in business continuity planning?

- ☐ Risk Assessment
- ☐ Due Care
- ☐ Business Impact Analysis (BIA)
- ☐ Due Diligence

Question 279

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 280

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 281

What physical characteristic does a retinal scan biometric device measure?

- ☐ The amount of light reaching the retina
- ☐ The amount of light reflected by the retina
- ☐ The pattern of light receptors at the back of the eye
- ☐ The pattern of blood vessels at the back of the eye

Question 282

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 283

Which of the following is not a DES mode of operation?

- ☐ Cipher block chaining
- ☐ Electronic code book
- ☐ Input feedback
- ☐ Cipher feedback

Question 284

Which of the following best describes remote journaling?

- ☐ Send hourly tapes containing transactions off-site.
- ☐ Send daily tapes containing transactions off-site.
- ☐ Real-time capture of transactions to multiple storage devices.
- ☐ Real time transmission of copies of the entries in the journal of transactions to an alternate site.

Question 285

Which of the following is NOT a proper component of Media Viability Controls?

- ☐ Storage
- ☐ Writing
- ☐ Handling
- ☐ Marking

Question 286

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

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

Question 287

Which of the following protocols offers native encryption?

- ☐ IPSEC, SSH, PPTP, SSL, MPLS, L2F, and L2TP
- ☐ IPSEC, SSH, SSL, TFTP
- ☐ IPSEC, SSH, SSL, TLS
- ☐ IPSEC, SSH, PPTP, SSL, MPLS, and L2TP

Question 288

Which of the following statements pertaining to Kerberos is TRUE?

- ☐ Kerberos uses public key cryptography.
- ☐ Kerberos uses X.509 certificates.
- ☐ Kerberos is a credential-based authentication system.
- ☐ Kerberos was developed by Microsoft.

Question 289

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 290

Which layer defines how packets are routed between end systems?

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

Question 291

A business impact assessment is one element in business continuity planning. What are the three primary goals of a BIA?

- ☐ Data processing continuity planning, data recovery plan maintenance, and testing the disaster recovery plan.
- ☐ Scope and plan initiation, business continuity plan development, and plan approval and implementation.
- ☐ Facility requirements planning, facility security management, and administrative personnel controls.
- ☐ Criticality prioritization, downtime estimation, and resource requirements.

Question 292

Another name for a VPN is a:

- ☐ tunnel
- ☐ one-time password
- ☐ pipeline
- ☐ bypass

Question 293

Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?

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

Question 294

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 295

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 296

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 297

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

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

Question 298

Which of the following binds a subject name to a public key value?

- ☐ A public-key certificate
- ☐ A public key infrastructure
- ☐ A secret key infrastructure
- ☐ A private key certificate

Question 299

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 300

Which encryption algorithm is BEST suited for communication with handheld wireless devices?

- ☐ ECC (Elliptic Curve Cryptosystem)
- ☐ RSA
- ☐ SHA
- ☐ RC4

Question 301

Which of the following backup sites is the most effective for disaster recovery?

- ☐ Time brokers
- ☐ Hot sites
- ☐ Cold sites
- ☐ Reciprocal Agreement

Question 302

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 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 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 305

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 306

Which of the following would be an example of the BEST password?

- ☐ golf001
- ☐ Elizabeth
- ☐ T1me4g0lF
- ☐ password

Question 307

Cryptography does NOT concern itself with which of the following choices?

- ☐ Availability
- ☐ Integrity
- ☐ Confidentiality
- ☐ Validation

Question 308

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 309

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 310

Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT) by ensuring the message comes from its claimed originator and that it has not been altered in transmission?

- ☐ Secure Electronic Transaction (SET)
- ☐ Message Authentication Code (MAC)
- ☐ Cyclic Redundancy Check (CRC)
- ☐ Secure Hash Standard (SHS)

Question 311

The "vulnerability of a facility" to damage or attack may be assessed by all of the following EXCEPT:

- ☐ Inspection
- ☐ History of losses
- ☐ Security controls
- ☐ security budget

Question 312

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

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

Question 313

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 314

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 315

Which of the following is NOT an example of an operational control?

- ☐ Backup and recovery
- ☐ Auditing
- ☐ Contingency planning
- ☐ Operations procedures

Question 316

The typical computer fraudsters are usually persons with which of the following characteristics?

- ☐ They have had previous contact with law enforcement
- ☐ They conspire with others
- ☐ They hold a position of trust
- ☐ They deviate from the accepted norms of society

Question 317

An Ethernet address is composed of how many bits?

- ☐ 48-bit address
- ☐ 32-bit address.
- ☐ 64-bit address
- ☐ 128-bit address

Question 318

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 319

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 320

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 321

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

- ☐ ISDN
- ☐ SLIP
- ☐ xDSL
- ☐ T1

Question 322

Smart cards are an example of which type of control?

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

Question 323

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

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

Question 324

Which of the following is BEST provided by symmetric cryptography?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Non-repudiation

Question 325

Which of the following represents the rows of the table in a relational database?

- ☐ attributes
- ☐ records or tuples
- ☐ record retention
- ☐ relation

Question 326

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 327

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 328

Cryptography does NOT help in:

- ☐ detecting fraudulent insertion.
- ☐ detecting fraudulent deletion.
- ☐ detecting fraudulent modification.
- ☐ detecting fraudulent disclosure.

Question 329

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 330

Which of the following is addressed by Kerberos?

- ☐ Confidentiality and Integrity
- ☐ Authentication and Availability
- ☐ Validation and Integrity
- ☐ Auditability and Integrity

Question 331

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 332

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 333

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 334

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 335

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 336

Which layer deals with Media Access Control (MAC) addresses?

- ☐ Data link layer
- ☐ Physical layer
- ☐ Transport layer
- ☐ Network layer

Question 337

Which of the following IEEE standards defines the token ring media access method?

- ☐ 802.3
- ☐ 802.11
- ☐ 802.5
- ☐ 802.2

Question 338

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

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

Question 339

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 340

Which of the following would be used to implement Mandatory Access Control (MAC)?

- ☐ Clark-Wilson Access Control
- ☐ Role-based access control
- ☐ Lattice-based access control
- ☐ User dictated access control

Question 341

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

- ☐ VDSL
- ☐ SDSL
- ☐ ADSL
- ☐ HDSL

Question 342

Which of the following organizations PRODUCES and PUBLISHES the Federal Information Processing Standards (FIPS)?

- ☐ The National Computer Security Center (NCSC)
- ☐ The National Institute of Standards and Technology (NIST)
- ☐ The National Security Agency (NSA)
- ☐ The American National Standards Institute (ANSI)

Question 343

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 344

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 345

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 346

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 347

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 348

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 349

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 350

Which IPSec operational mode encrypts the entire data packet (including header and data) into an IPSec packet?

- ☐ Authentication mode
- ☐ Tunnel mode
- ☐ Transport mode
- ☐ Safe mode

Question 351

To control access by a subject (an active entity such as individual or process) to an object (a passive entity such as a file) involves setting up:

- ☐ Access Rules
- ☐ Access Matrix
- ☐ Identification controls
- ☐ Access terminal

Question 352

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 353

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 354

Which of the following is not a one-way hashing algorithm?

- ☐ MD2
- ☐ RC4
- ☐ SHA-1
- ☐ HAVAL

Question 355

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 356

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 357

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 358

Why would a database be denormalized?

- ☐ To ensure data integrity
- ☐ To increase processing efficiency
- ☐ To prevent duplication of data
- ☐ To save storage space

Question 359

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 360

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

- ☐ Static electricity
- ☐ Electro-plating
- ☐ Energy-plating
- ☐ Element-plating

Question 361

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 362

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 363

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 364

Which of the following was developed by the National Computer Security Center (NCSC) for the US Department of Defense?

- ☐ TCSEC
- ☐ ITSEC
- ☐ DIACAP
- ☐ NIACAP

Question 365

In which mode of DES, will a block of plaintext and a key always give the same ciphertext?

- ☐ Electronic Code Book (ECB)
- ☐ Output Feedback (OFB)
- ☐ Counter Mode (CTR)
- ☐ Cipher Feedback (CFB)

Question 366

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 367

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 368

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 369

What works as an E-mail message transfer agent?

- ☐ SMTP
- ☐ SNMP
- ☐ S-RPC
- ☐ S/MIME

Question 370

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 371

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 372

What is electronic vaulting?

- ☐ Information is backed up to tape on a hourly basis and is stored in an on-site vault.
- ☐ Information is backed up to tape on a daily basis and is stored in an on-site vault.
- ☐ Transferring electronic journals or transaction logs to an off-site storage facility
- ☐ A transfer of bulk information to a remote central backup facility.

Question 373

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 374

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 375

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 376

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 377

Which of the following statements relating to the Bell-LaPadula security model is FALSE (assuming the Strong Star property is not being used)?

- ☐ A subject is not allowed to read up.
- ☐ The *- property restriction can be escaped by temporarily downgrading a high level subject.
- ☐ A subject is not allowed to read down.
- ☐ It is restricted to confidentiality.

Question 378

Which of the following keys has the SHORTEST lifespan?

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

Question 379

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 380

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

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

Question 381

Which of the following type of cryptography is used when both parties use the same key to communicate securely with each other?

- ☐ Symmetric Key Cryptography
- ☐ PKI - Public Key Infrastructure
- ☐ Diffie-Hellman
- ☐ DSS - Digital Signature Standard

Question 382

Which of the following access control techniques BEST gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure?

- ☐ Access control lists
- ☐ Discretionary access control
- ☐ Role-based access control
- ☐ Non-mandatory access control

Question 383

In non-discretionary access control using Role Based Access Control (RBAC), a central authority determines what subjects can have access to certain objects based on the organizational security policy. The access controls may be based on:

- ☐ The society's role in the organization
- ☐ The individual's role in the organization
- ☐ The group-dynamics as they relate to the individual's role in the organization
- ☐ The group-dynamics as they relate to the master-slave role in the organization

Question 384

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 385

Which of the following is an example of discretionary access control?

- ☐ Identity-based access control
- ☐ Task-based access control
- ☐ Role-based access control
- ☐ Rule-based access control

Question 386

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 387

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 388

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 389

Packet Filtering Firewalls can also enable access for:

- ☐ only authorized application port or service numbers.
- ☐ only unauthorized application port or service numbers.
- ☐ only authorized application port or ex-service numbers.
- ☐ only authorized application port or service integers.

Question 390

Which of the following offers security to wireless communications?

- ☐ S-WAP
- ☐ WTLS
- ☐ WSP
- ☐ WDP

Question 391

All of the following can be considered essential business functions that should be identified when creating a Business Impact Analysis (BIA) except one. Which of the following would be considered an essential element of the BIA but an important topic to include within the BCP plan?

- ☐ IT Network Support
- ☐ Accounting
- ☐ Public Relations
- ☐ Purchasing

Question 392

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 393

Which of the following monitors network traffic in real time?

- ☐ network-based IDS
- ☐ host-based IDS
- ☐ application-based IDS
- ☐ firewall-based IDS

Question 394

What is RAD?

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

Question 395

Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?

- ☐ Preventive/Administrative Pairing
- ☐ Preventive/Technical Pairing
- ☐ Preventive/Physical Pairing
- ☐ Detective/Technical Pairing

Question 396

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 397

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.

Question 398

Which of the following term BEST describes a weakness that could potentially be exploited?

- ☐ Vulnerability
- ☐ Risk
- ☐ Threat
- ☐ Target of evaluation (TOE)

Question 399

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 400

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 401

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 402

Which access control type has a central authority that determine to what objects the subjects have access to and it is based on role or on the organizational security policy?

- ☐ Mandatory Access Control
- ☐ Discretionary Access Control
- ☐ Non-Discretionary Access Control
- ☐ Rule-based Access control

Question 403

Which authentication technique BEST protects against hijacking?

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

Question 404

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 405

The Computer Security Policy Model the Orange Book is based on is which of the following?

- ☐ Bell-LaPadula
- ☐ Data Encryption Standard
- ☐ Kerberos
- ☐ Tempest

Question 406

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 407

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 408

Which of the following is NOT a precaution you can take to reduce static electricity?

- ☐ power line conditioning
- ☐ anti-static sprays
- ☐ maintain proper humidity levels
- ☐ anti-static flooring

Question 409

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 410

Which of following is NOT a service provided by AAA servers (Radius, TACACS and DIAMETER)?

- ☐ Authentication
- ☐ Administration
- ☐ Accounting
- ☐ Authorization

Question 411

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 412

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 413

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 414

The type of discretionary access control (DAC) that is based on an individual's identity is also called:

- ☐ Identity-based Access control
- ☐ Rule-based Access control
- ☐ Non-Discretionary Access Control
- ☐ Lattice-based Access control

Question 415

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

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

Question 416

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 417

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 418

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 419

Which of the following control helps to identify an incident's activities and potentially an intruder?

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

Question 420

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 421

Which of the following is NOT a disadvantage of symmetric cryptography when compared with asymmetric ciphers?

- ☐ Provides Limited security services
- ☐ Has no built in Key distribution
- ☐ Speed
- ☐ Large number of keys are needed

Question 422

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 423

Address Resolution Protocol (ARP) interrogates the network by sending out a?

- ☐ broadcast.
- ☐ multicast.
- ☐ unicast.
- ☐ semicast.

Question 424

One of the following assertions is NOT a characteristic of Internet Protocol Security (IPSec)

- ☐ Data cannot be read by unauthorized parties
- ☐ The identity of all IPsec endpoints are confirmed by other endpoints
- ☐ Data is delivered in the exact order in which it is sent
- ☐ The number of packets being exchanged can be counted.

Question 425

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 426

Which of the following statements pertaining to the Bell-LaPadula model is TRUE if you are NOT making use of the strong star property?

- ☐ It allows "read up."
- ☐ It addresses covert channels.
- ☐ It addresses management of access controls.
- ☐ It allows "write up."

Question 427

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 428

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 429

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 430

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

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

Question 431

Which of the following is NOT a characteristic of a host-based intrusion detection system?

- ☐ A HIDS does not consume large amounts of system resources
- ☐ A HIDS can analyze system logs, processes and resources
- ☐ A HIDS looks for unauthorized changes to the system
- ☐ A HIDS can notify system administrators when unusual events are identified

Question 432

Which OSI/ISO layer defines how to address the physical devices on the network?

- ☐ Session layer
- ☐ Data Link layer
- ☐ Application layer
- ☐ Transport layer

Question 433

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 434

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

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

Question 435

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 436

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 437

Which Orange book security rating introduces security labels?

- ☐ C2
- ☐ B1
- ☐ B2
- ☐ B3

Question 438

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 439

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 440

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

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

Question 441

Communications and network security relates to transmission of which of the following?

- ☐ voice
- ☐ voice and multimedia
- ☐ data and multimedia
- ☐ voice, data and multimedia

Question 442

In what way can violation of clipping levels assist in violation tracking and analysis?

- ☐ Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.
- ☐ Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.
- ☐ Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status.
- ☐ Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations.

Question 443

Who should direct short-term recovery actions immediately following a disaster?

- ☐ Chief Information Officer.
- ☐ Chief Operating Officer.
- ☐ Disaster Recovery Manager.
- ☐ Chief Executive Officer.

Question 444

What is the key size of the International Data Encryption Algorithm (IDEA)?

- ☐ 64 bits
- ☐ 128 bits
- ☐ 160 bits
- ☐ 192 bits

Question 445

Which of the following is true about a "dry pipe" sprinkler system?

- ☐ It is a substitute for carbon dioxide systems.
- ☐ It maximizes chances of accidental discharge of water.
- ☐ It reduces the likelihood of the sprinkler system pipes freezing.
- ☐ It uses less water than "wet pipe" systems.

Question 446

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

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

Question 447

Which of the following is BEST at defeating frequency analysis?

- ☐ Substitution cipher
- ☐ Polyalphabetic cipher
- ☐ Transposition cipher
- ☐ Caesar cipher

Question 448

Which of the following is NOT a common backup method?

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

Question 449

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 450

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 451

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 452

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

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

Question 453

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

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

Question 454

Which layer of the TCP/IP protocol model would BEST correspond to the OSI/ISO model's network layer?

- ☐ Network access layer
- ☐ Application layer
- ☐ Host-to-host transport layer
- ☐ Internet layer

Question 455

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 456

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

- ☐ B1
- ☐ B2
- ☐ F6
- ☐ C2

Question 457

Which of the following statements pertaining to link encryption is FALSE?

- ☐ It encrypts all the data along a specific communication path.
- ☐ It provides protection against packet sniffers and eavesdroppers.
- ☐ Information stays encrypted from one end of its journey to the other.
- ☐ User information, header, trailers, addresses and routing data that are part of the packets are encrypted.

Question 458

What is the name for a substitution cipher that shifts the alphabet by 13 places?

- ☐ Caesar cipher
- ☐ Polyalphabetic cipher
- ☐ ROT13 cipher
- ☐ Transposition cipher

Question 459

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 460

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 461

What is the name of the protocol use to set up and manage Security Associations (SA) for IP Security (IPSec)?

- ☐ Internet Key Exchange (IKE)
- ☐ Secure Key Exchange Mechanism
- ☐ Oakley
- ☐ Internet Security Association and Key Management Protocol

Question 462

What is the main issue with media reuse?

- ☐ Degaussing
- ☐ Data remanence
- ☐ Media destruction
- ☐ Purging

Question 463

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 464

Which access control model is BEST suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

- ☐ DAC
- ☐ MAC
- ☐ Access control matrix
- ☐ TACACS

Question 465

Which of the following issues is not addressed by digital signatures?

- ☐ nonrepudiation
- ☐ authentication
- ☐ data integrity
- ☐ denial-of-service

Question 466

Java is not:

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

Question 467

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 468

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 469

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 470

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 471

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 472

Which of the following would BEST describe a Concealment cipher?

- ☐ Permutation is used, meaning that letters are scrambled.
- ☐ Every X number of words within a text, is a part of the real message.
- ☐ Replaces bits, characters, or blocks of characters with different bits, characters or blocks.
- ☐ Hiding data in another message so that the very existence of the data is concealed.

Question 473

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 474

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 475

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 476

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 477

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 478

Like the Kerberos protocol, SESAME is also subject to which of the following?

- ☐ timeslot replay
- ☐ password guessing
- ☐ symmetric key guessing
- ☐ asymmetric key guessing

Question 479

Which of the following is a Hashing Algorithm?

- ☐ SHA
- ☐ RSA
- ☐ Diffie Hellman (DH)
- ☐ Elliptic Curve Cryptography (ECC)

Question 480

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 481

Which of the following is NOT a VPN communications protocol standard?

- ☐ Point-to-point tunneling protocol (PPTP)
- ☐ Challenge Handshake Authentication Protocol (CHAP)
- ☐ Layer 2 tunneling protocol (L2TP)
- ☐ IP Security

Question 482

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 483

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 484

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 485

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 486

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 487

Which of the following is NOT an example of preventive control?

- ☐ Physical access control like locks and door
- ☐ User login screen which allows only authorize user to access website
- ☐ Encrypt the data so that only authorize user can view the same
- ☐ Duplicate checking of a calculation

Question 488

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 489

Which of the following is a class C fire?

- ☐ electrical
- ☐ liquid
- ☐ common combustibles
- ☐ soda acid

Question 490

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 491

Business Continuity Planning (BCP) is defined as a preparation that facilitates:

- ☐ the rapid recovery of mission-critical business operations
- ☐ the continuation of critical business functions
- ☐ the monitoring of threat activity for adjustment of technical controls
- ☐ the reduction of the impact of a disaster

Question 492

Public key infrastructure (PKI) consists of programs, data formats, procedures, communication protocols, security policies, and public key cryptographic mechanisms working in a comprehensive manner to enable a wide range of dispersed people to communicate in a secure and predictable fashion.

This infrastructure is based upon which of the following Standard?

- ☐ X.509
- ☐ X.500
- ☐ X.400
- ☐ X.25

Question 493

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 494

What kind of encryption technology does SSL utilize?

- ☐ Secret or Symmetric key
- ☐ Hybrid (both Symmetric and Asymmetric)
- ☐ Public Key
- ☐ Private Key

Question 495

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 496

What is a decrease in amplitude as a signal propagates along a transmission medium BEST known as?

- ☐ Crosstalk
- ☐ Noise
- ☐ Delay distortion
- ☐ Attenuation

Question 497

Which of the following security models does NOT concern itself with the flow of data?

- ☐ The information flow model
- ☐ The Biba model
- ☐ The Bell-LaPadula model
- ☐ The noninterference model

Question 498

Which of the following statements relating to the Biba security model is FALSE?

- ☐ It is a state machine model.
- ☐ A subject is not allowed to write up.
- ☐ Integrity levels are assigned to subjects and objects.
- ☐ Programs serve as an intermediate layer between subjects and objects.

Question 499

Which of the following is more suitable for a hardware implementation?

- ☐ Stream ciphers
- ☐ Block ciphers
- ☐ Cipher block chaining
- ☐ Electronic code book

Question 500

Which of the following is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length?

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

Question 501

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 502

Which of the following is not a physical control for physical security?

- ☐ lighting
- ☐ fences
- ☐ training
- ☐ facility construction materials

Question 503

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 504

Which of the following attacks could capture network user passwords?

- ☐ Data diddling
- ☐ Sniffing
- ☐ IP Spoofing
- ☐ Smurfing

Question 505

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 506

In the context of access control, locks, gates, guards are examples of which of the following?

- ☐ Administrative controls
- ☐ Technical controls
- ☐ Physical controls
- ☐ Logical controls

Question 507

Which of the following is most affected by denial-of-service (DoS) attacks?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Accountability
- ☐ Availability

Question 508

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 509

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 510

What is the difference between Access Control Lists (ACLs) and Capability Tables?

- ☐ Access control lists are related/attached to a subject whereas capability tables are related/attached to an object.
- ☐ Access control lists are related/attached to an object whereas capability tables are related/attached to a subject.
- ☐ Capability tables are used for objects whereas access control lists are used for users.
- ☐ They are basically the same.

Question 511

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 512

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 513

What is the PRIMARY use of a password?

- ☐ Allow access to files.
- ☐ Identify the user.
- ☐ Authenticate the user.
- ☐ Segregate various users' accesses.

Question 514

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 515

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 516

The International Organization for Standardization / Open Systems Interconnection (ISO/OSI) Layer 7 does NOT include which of the following?

- ☐ SMTP (Simple Mail Transfer Protocol)
- ☐ TCP (Transmission Control Protocol)
- ☐ SNMP (Simple Network Management Protocol)
- ☐ HTTP (Hypertext Transfer Protocol)

Question 517

A one-way hash provides which of the following?

- ☐ Confidentiality
- ☐ Availability
- ☐ Integrity
- ☐ Authentication

Question 518

The US department of Health, Education and Welfare developed a list of fair information practices focused on privacy of individually, personal identifiable information. Which one of the following is incorrect?

- ☐ There must be a way for a person to find out what information about them exists and how it is used.
- ☐ There must be a personal data record-keeping system whose very existence shall be kept secret.
- ☐ There must be a way for a person to prevent information about them, which was obtained for one purpose, from being used or made available for another purpose without their consent.
- ☐ Any organization creating, maintaining, using, or disseminating records of personal identifiable information must ensure reliability of the data for their intended use and must make precautions to prevent misuses of that data.

Question 519

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 520

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 521

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 522

Which of the following is NOT a basic component of security architecture?

- ☐ Motherboard
- ☐ Central Processing Unit (CPU)
- ☐ Storage Devices
- ☐ Peripherals (input/output devices)

Question 523

Which of the following is NOT an example of a block cipher?

- ☐ Skipjack
- ☐ IDEA
- ☐ Blowfish
- ☐ RC4

Question 524

Which of the following protects Kerberos against replay attacks?

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

Question 525

Which Orange Book evaluation level is described as "Verified Design"?

- ☐ A1.
- ☐ B3.
- ☐ B2.
- ☐ B1.

Question 526

Which of the following can prevent hijacking of a web session?

- ☐ RSA
- ☐ SET
- ☐ SSL
- ☐ PPP

Question 527

Of the reasons why a Disaster Recovery plan gets outdated, which of the following is not true?

- ☐ Personnel turnover
- ☐ Large plans can take a lot of work to maintain
- ☐ Continuous auditing makes a Disaster Recovery plan irrelevant
- ☐ Infrastructure and environment changes

Question 528

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 529

Which of the following statements pertaining to disaster recovery is incorrect?

- ☐ A recovery team's primary task is to get the pre-defined critical business functions at the alternate backup processing site.
- ☐ A salvage team's task is to ensure that the primary site returns to normal processing conditions.
- ☐ The disaster recovery plan should include how the company will return from the alternate site to the primary site.
- ☐ When returning to the primary site, the most critical applications should be brought back first.

Question 530

Which layer of the TCP/IP protocol model defines the IP datagram and handles the routing of data across networks?

- ☐ Application layer
- ☐ Host-to-host transport layer
- ☐ Internet layer
- ☐ Network access layer

Question 531

According to the Orange Book, which security level is the first to require a system to protect against covert timing channels?

- ☐ A1
- ☐ B3
- ☐ B2
- ☐ B1

Question 532

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 533

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 534

Which of the following is currently the most recommended water system for a computer room?

- ☐ preaction
- ☐ wet pipe
- ☐ dry pipe
- ☐ deluge

Question 535

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 536

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 537

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 538

Individual accountability does not include which of the following?

- ☐ unique identifiers
- ☐ policies and procedures
- ☐ access rules
- ☐ audit trails

Question 539

What algorithm was DES derived from?

- ☐ Twofish.
- ☐ Skipjack.
- ☐ Brooks-Aldeman.
- ☐ Lucifer.

Question 540

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 541

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 542

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 543

The owner of a system should have the confidence that the system will behave according to its specifications. This is termed as:

- ☐ Integrity
- ☐ Accountability
- ☐ Assurance
- ☐ Availability

Question 544

Which of the following assertions is NOT true about pattern matching and anomaly detection in intrusion detection?

- ☐ Anomaly detection tends to produce more data
- ☐ A pattern matching IDS can only identify known attacks
- ☐ Stateful matching scans for attack signatures by analyzing individual packets instead of traffic streams
- ☐ An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines

Question 545

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 546

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 547

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:

- ☐ through access control mechanisms that require identification and authentication and through the audit function.
- ☐ through logical or technical controls involving the restriction of access to systems and the protection of information.
- ☐ through logical or technical controls but not involving the restriction of access to systems and the protection of information.
- ☐ through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Question 548

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 549

For competitive reasons, the customers of a large shipping company called the "Integrated International Secure Shipping Containers Corporation" (IISSCC) like to keep private the various cargos that they ship. IISSCC 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 IISSCC 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 550

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 551

Which of the following BEST describes a function relying on a shared secret key that is used along with a hashing algorithm to verify the integrity of the communication content as well as the sender?

- ☐ Message Authentication Code - MAC
- ☐ PAM - Pluggable Authentication Module
- ☐ NAM - Negative Acknowledgement Message
- ☐ Digital Signature Certificate

Question 552

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 553

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 554

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 555

Which of the following questions is LEAST likely to help in assessing controls covering audit trails?

- ☐ Does the audit trail provide a trace of user actions?
- ☐ Are incidents monitored and tracked until resolved?
- ☐ Is access to online logs strictly controlled?
- ☐ Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Question 556

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 557

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 558

Which of the following statements pertaining to stream ciphers is TRUE?

- ☐ A stream cipher is a type of asymmetric encryption algorithm.
- ☐ A stream cipher generates what is called a keystream.
- ☐ A stream cipher is slower than a block cipher.
- ☐ A stream cipher is not appropriate for hardware-based encryption.

Question 559

What is the Biba security model concerned with?

- ☐ Confidentiality
- ☐ Reliability
- ☐ Availability
- ☐ Integrity

Question 560

Which of the following standards concerns digital certificates?

- ☐ X.400
- ☐ X.25
- ☐ X.509
- ☐ X.75

Question 561

What level of assurance for a digital certificate verifies a user's name, address, social security number, and other information against a credit bureau database?

- ☐ Level 1/Class 1
- ☐ Level 2/Class 2
- ☐ Level 3/Class 3
- ☐ Level 4/Class 4

Question 562

Which of the following is 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 563

Which of the following is required in order to provide accountability?

- ☐ Authentication
- ☐ Integrity
- ☐ Confidentiality
- ☐ Audit trails

Question 564

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 565

Which access control model was proposed for enforcing access control in government and military applications?

- ☐ Bell-LaPadula model
- ☐ Biba model
- ☐ Sutherland model
- ☐ Brewer-Nash model

Question 566

A periodic review of user account management should NOT determine:

- ☐ conformity with the concept of least privilege.
- ☐ whether active accounts are still being used.
- ☐ strength of user-chosen passwords.
- ☐ whether management authorizations are up-to-date.

Question 567

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 568

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

- ☐ 81
- ☐ 80
- ☐ 8080
- ☐ 8180

Question 569

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 570

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 571

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

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

Question 572

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

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

Question 573

Which of the following is the SIMPLEST type of firewall?

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

Question 574

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 575

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 576

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 577

Which of the following biometric devices offers the LOWEST CER?

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

Question 578

What is the main concern with single sign-on?

- ☐ Maximum unauthorized access would be possible if a password is disclosed.
- ☐ The security administrator's workload would increase.
- ☐ The users' password would be too hard to remember.
- ☐ User access rights would be increased.

Question 579

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 580

When planning for disaster recovery it is important to know a chain of command should one or more people become missing, incapacitated or otherwise available to lead the organization.

Which of the following terms BEST describes this process?

- ☐ Succession Planning
- ☐ Continuity of Operations
- ☐ Business Impact Analysis
- ☐ Business Continuity Planning

Question 581

Which of the following is not an EPA-approved replacement for Halon?

- ☐ Bromine
- ☐ Inergen
- ☐ FM-200
- ☐ FE-13

Question 582

In an organization where there are frequent personnel changes, non-discretionary access control using Role Based Access Control (RBAC) is useful because:

- ☐ people need not use discretion
- ☐ the access controls are based on the individual's role or title within the organization.
- ☐ the access controls are not based on the individual's role or title within the organization
- ☐ the access controls are often based on the individual's role or title within the organization

Question 583

Which of the following plan provides procedures for sustaining essential business operations while recovering from significant disruption?

- ☐ Business Continuity Plan
- ☐ Occupant Emergency Plan
- ☐ Cyber Incident Response Plan
- ☐ Disaster Recovery Plan

Question 584

Which of the following is the lowest TCSEC class wherein the systems must support separate operator and system administrator roles?

- ☐ B2
- ☐ B1
- ☐ A1
- ☐ A2

Question 585

Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?

- ☐ Risk assessment
- ☐ Residual risks
- ☐ Security controls
- ☐ Business units

Question 586

Which of the following protocols operates at the session layer (layer 5)?

- ☐ RPC
- ☐ IGMP
- ☐ LPD
- ☐ SPX

Question 587

How many bits compose an IPv6 address?

- ☐ 32 bits
- ☐ 64 bits
- ☐ 96 bits
- ☐ 128 bits

Question 588

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 589

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 590

Which of the following modes of DES is MOST likely used for Database Encryption?

- ☐ Electronic Code Book (ECB)
- ☐ Cipher Block Chaining (CBC)
- ☐ Cipher Feedback (CFB)
- ☐ Output Feedback (OFB)

Question 591

Complete the following sentence. A digital signature is a:

- ☐ hash value that has been encrypted with the sender's private key
- ☐ hash value that has been encrypted with the sender's public key
- ☐ hash value that has been encrypted with the senders Session key
- ☐ senders signature signed and scanned in a digital format

Question 592

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 593

The Diffie-Hellman algorithm is primarily used to provide which of the following?

- ☐ Confidentiality
- ☐ Key Agreement
- ☐ Integrity
- ☐ Non-repudiation

Question 594

Which of the following statements pertaining to disaster recovery planning is incorrect?

- ☐ Every organization must have a disaster recovery plan
- ☐ A disaster recovery plan contains actions to be taken before, during and after a disruptive event.
- ☐ The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.
- ☐ A disaster recovery plan should cover return from alternate facilities to primary facilities.

Question 595

What can be defined as a table of subjects and objects indicating what actions individual subjects can take upon individual objects?

- ☐ A capacity table
- ☐ An access control list
- ☐ An access control matrix
- ☐ A capability table

Question 596

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 597

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 598

Similar to Secure Shell (SSH-2), Secure Sockets Layer (SSL) uses symmetric encryption for encrypting the bulk of the data being sent over the session and it uses asymmetric or public key cryptography for:

- ☐ Peer Authentication
- ☐ Peer Identification
- ☐ Server Authentication
- ☐ Name Resolution

Question 599

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 600

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

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

Question 601

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

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

Question 602

Which one of the following is used to provide authentication and confidentiality for e-mail messages?

- ☐ Digital signature
- ☐ PGP
- ☐ IPSEC AH
- ☐ MD4

Question 603

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

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

Question 604

What is defined as the rules for communicating between computers on a Local Area Network (LAN)?

- ☐ LAN Media Access methods
- ☐ LAN topologies
- ☐ LAN transmission methods
- ☐ Contention Access Control

Question 605

Which layer of the DoD TCP/IP model controls the communication flow between hosts?

- ☐ Internet layer
- ☐ Host-to-host transport layer
- ☐ Application layer
- ☐ Network access layer

Question 606

Which of the following is NOT a property of the Rijndael block cipher algorithm?

- ☐ The key sizes must be a multiple of 32 bits
- ☐ Maximum block size is 256 bits
- ☐ Maximum key size is 512 bits
- ☐ The key size does not have to match the block size

Question 607

Which of the following is NOT a critical security aspect of Operations Controls?

- ☐ Controls over hardware.
- ☐ Data media used.
- ☐ Operators using resources.
- ☐ Environmental controls.

Question 608

Which of the following is a LAN transmission method?

- ☐ Broadcast
- ☐ Carrier-sense multiple access with collision detection (CSMA/CD)
- ☐ Token ring
- ☐ Fiber Distributed Data Interface (FDDI)

Question 609

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 610

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 611

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 612

Which of the following is NOT an example of an asymmetric key algorithm?

- ☐ Elliptic curve cryptosystem (ECC)
- ☐ Diffie-Hellman
- ☐ Advanced Encryption Standard (AES)
- ☐ Merkle-Hellman Knapsack

Question 613

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 614

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 615

Which of the following category of UTP cables is specified to be able to handle gigabit Ethernet (1 Gbps) according to the EIA/TIA-568-B standards?

- ☐ Category 5e UTP
- ☐ Category 2 UTP
- ☐ Category 3 UTP
- ☐ Category 1e UTP

Question 616

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

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

Question 617

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 618

In a Public Key Infrastructure, how are public keys published?

- ☐ They are sent via e-mail.
- ☐ Through digital certificates.
- ☐ They are sent by owners.
- ☐ They are not published.

Question 619

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 620

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 621

An X.509 public key certificate with the key usage attribute "non-repudiation" can be used for which of the following?

- ☐ encrypting messages
- ☐ signing messages
- ☐ verifying signed messages
- ☐ decrypting encrypted messages

Question 622

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 623

Which of the following is NOT a form of detective technical control?

- ☐ Audit trails
- ☐ Access control software
- ☐ Honeypot
- ☐ Intrusion detection system

Question 624

For which areas of the enterprise are business continuity plans required?

- ☐ All areas of the enterprise.
- ☐ The financial and information processing areas of the enterprise.
- ☐ The operating areas of the enterprise.
- ☐ The marketing, finance, and information processing areas.

Question 625

The Diffie-Hellman algorithm is used for:

- ☐ Encryption
- ☐ Digital signature
- ☐ Key agreement
- ☐ Non-repudiation

Question 626

What does the * (star) property mean in the Bell-LaPadula model?

- ☐ No write up
- ☐ No read up
- ☐ No write down
- ☐ No read down

Question 627

Which of the following statements pertaining to VPN protocol standards is false?

- ☐ L2TP is a combination of PPTP and L2F.
- ☐ L2TP and PPTP were designed for single point-to-point client to server communication.
- ☐ L2TP operates at the network layer.
- ☐ PPTP uses native PPP authentication and encryption services.

Question 628

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 629

Kerberos depends upon what encryption method?

- ☐ Public Key cryptography.
- ☐ Secret Key cryptography.
- ☐ El Gamal cryptography.
- ☐ Blowfish cryptography.

Question 630

Which of the following is a transaction redundancy implementation?

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

Question 631

Tim is a network administrator of Acme Inc. He is responsible for configuring the network devices. John the new security manager reviews the configuration of the Firewall configured by Tim and identifies an issue.

This specific firewall is configured in failover mode with another firewall. A sniffer on a PC connected to the same switch as the firewalls can decipher the credentials, used by Tim while configuring the firewalls.

Which of the following should be used by Tim to ensure that no one can eavesdrop on the communication?

- ☐ SSH
- ☐ SFTP
- ☐ SCP
- ☐ RSH

Question 632

Business Impact Analysis (BIA) is about:

- ☐ Technology
- ☐ Supporting the mission of the organization
- ☐ Due Care
- ☐ Risk Assessment

Question 633

After a company is out of an emergency state, what should be moved back to the original site first?

- ☐ Executives
- ☐ Least critical components
- ☐ IT support staff
- ☐ Most critical components

Question 634

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 635

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 636

How many layers are defined within the US Department of Defense (DoD) TCP/IP Model?

- ☐ 7
- ☐ 5
- ☐ 4
- ☐ 3

Question 637

Logical or technical controls involve the restriction of access to systems and the protection of information. Which of the following statements pertaining to these types of controls is TRUE?

- ☐ Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks but do not include a review of vacation history, and also do not include increased supervision.
- ☐ Examples of these types of controls do not include encryption, smart cards, access lists, and transmission protocols.
- ☐ Examples of these types of controls are encryption, smart cards, access lists, and transmission protocols.
- ☐ Examples of these types of controls include policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

Question 638

Which of the following statements pertaining to Secure Sockets Layer (SSL) is FALSE?

- ☐ The SSL protocol was developed by Netscape to secure Internet client-server transactions.
- ☐ The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.
- ☐ Web pages using the SSL protocol start with HTTPS
- ☐ SSL can be used with applications such as Telnet, FTP and email protocols.

Question 639

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 640

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 641

During a test of a disaster recovery plan the IT systems are concurrently set up at the alternate site. The results are compared to the results of regular processing at the original site. What kind of testing has taken place?

- ☐ Simulation
- ☐ Parallel
- ☐ Checklist
- ☐ Full interruption

Question 642

Which type of attack involves hijacking a session between a host and a target by predicting the target's choice of an initial TCP sequence number?

- ☐ IP spoofing attack
- ☐ SYN flood attack
- ☐ TCP sequence number attack
- ☐ Smurf attack

Question 643

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 644

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 645

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 646

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 647

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

- ☐ TCP
- ☐ PPP
- ☐ ICMP
- ☐ SMTP

Question 648

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 649

Which of the following should be performed by an operator?

- ☐ Changing profiles
- ☐ Approving changes
- ☐ Adding and removal of users
- ☐ Installing system software

Question 650

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 651

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 652

Which service usually runs on port 25?

- ☐ File Transfer Protocol (FTP)
- ☐ Telnet
- ☐ Simple Mail Transfer Protocol (SMTP)
- ☐ Domain Name Service (DNS)

Question 653

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

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

Question 654

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 655

Where in a PKI infrastructure is a list of revoked certificates stored?

- ☐ CRL
- ☐ Registration Authority
- ☐ Recovery Agent
- ☐ Key escrow

Question 656

Which of the following elements is NOT included in a Public Key Infrastructure (PKI)?

- ☐ Timestamping
- ☐ Repository
- ☐ Certificate revocation
- ☐ Internet Key Exchange (IKE)

Question 657

Which of the following is NOT a known type of Message Authentication Code (MAC)?

- ☐ Keyed-hash message authentication code (HMAC)
- ☐ DES-CBC
- ☐ Signature-based MAC (SMAC)
- ☐ Universal Hashing Based MAC (UMAC)

Question 658

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 659

Which of the following are additional access control objectives?

- ☐ Consistency and utility
- ☐ Reliability and utility
- ☐ Usefulness and utility
- ☐ Convenience and utility

Question 660

What kind of certificate is used to validate a user identity?

- ☐ Public key certificate
- ☐ Attribute certificate
- ☐ Root certificate
- ☐ Code signing certificate

Question 661

The Orange Book is founded upon which security policy model?

- ☐ The Biba Model
- ☐ The Bell LaPadula Model
- ☐ Clark-Wilson Model
- ☐ TEMPEST

Question 662

Which of the following is most appropriate to notify an external user that session monitoring is being conducted?

- ☐ Logon Banners
- ☐ Wall poster
- ☐ Employee Handbook
- ☐ Written agreement

Question 663

What can be defined as secret communications where the very existence of the message is hidden?

- ☐ Clustering
- ☐ Steganography
- ☐ Cryptology
- ☐ Vernam cipher

Question 664

At which layer of ISO/OSI does the fiber optics work?

- ☐ Network layer
- ☐ Transport layer
- ☐ Data link layer
- ☐ Physical layer

Question 665

What is the maximum number of different keys that can be used when encrypting with Triple DES?

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4

Question 666

While using IPsec, the ESP and AH protocols both provide integrity services. However, when using AH, some special attention needs to be paid if one of the peers uses NAT for address translation service. Which of the items below would affect the use of AH and its Integrity Check Value (ICV) the MOST?

- ☐ Key session exchange
- ☐ Packet Header Source or Destination address
- ☐ VPN cryptographic key size
- ☐ Cryptographic algorithm used

Question 667

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 668

What key size is used by the Clipper Chip?

- ☐ 40 bits
- ☐ 56 bits
- ☐ 64 bits
- ☐ 80 bits

Question 669

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 670

Which of the following algorithms is a stream cipher?

- ☐ RC2
- ☐ RC4
- ☐ RC5
- ☐ RC6

Question 671

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 672

Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

- ☐ Differential cryptanalysis
- ☐ Differential linear cryptanalysis
- ☐ Birthday attack
- ☐ Statistical attack

Question 673

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 674

Which of the following is NOT a symmetric key algorithm?

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

Question 675

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 676

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

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

Question 677

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

- ☐ A1
- ☐ B3
- ☐ B2
- ☐ B1

Question 678

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 679

Which of the following would best describe certificate path validation?

- ☐ Verification of the validity of all certificates of the certificate chain to the root certificate
- ☐ Verification of the integrity of the associated root certificate
- ☐ Verification of the integrity of the concerned private key
- ☐ Verification of the revocation status of the concerned certificate

Question 680

What layer of the OSI/ISO model does Point-to-point tunneling protocol (PPTP) work at?

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

Question 681

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 682

A code, as is pertains to cryptography:

- ☐ is a generic term for encryption.
- ☐ is specific to substitution ciphers.
- ☐ deals with linguistic units.
- ☐ is specific to transposition ciphers.

Question 683

What does the Clark-Wilson security model focus on?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Accountability
- ☐ Availability

Question 684

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 685

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 686

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 687

What is the name of the FIRST mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?

- ☐ Clark and Wilson Model
- ☐ Harrison-Ruzzo-Ullman Model
- ☐ Rivest and Shamir Model
- ☐ Bell-LaPadula Model

Question 688

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 689

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 690

Which of the following is a symmetric encryption algorithm?

- ☐ RSA
- ☐ Elliptic Curve
- ☐ RC5
- ☐ El Gamal

Question 691

What does the simple security (ss) property mean in the Bell-LaPadula model?

- ☐ No read up
- ☐ No write down
- ☐ No read down
- ☐ No write up

Question 692

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 693

Which answer BEST describes a secure cryptoprocessor that can be used to store cryptographic keys, passwords or certificates in a component located on the motherboard of a computer?

- ☐ TPM - Trusted Platform Module
- ☐ TPM - Trusted Procedure Module
- ☐ Smart Card
- ☐ Enigma Machine

Question 694

Secure Sockets Layer (SSL) is very heavily used for protecting which of the following?

- ☐ Web transactions.
- ☐ EDI transactions.
- ☐ Telnet transactions.
- ☐ Electronic Payment transactions.

Question 695

Which of the following is the WEAKEST authentication mechanism?

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

Question 696

Which of the following statements do apply to a hot site?

- ☐ It is expensive.
- ☐ There are cases of common overselling of processing capabilities by the service provider.
- ☐ It provides a false sense of security.
- ☐ It is accessible on a first come first serve basis. In case of large disaster it might Be accessible.

Question 697

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 698

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 699

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 700

What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?

- ☐ SYN Flood attack
- ☐ Smurf attack
- ☐ Ping of Death attack
- ☐ Denial of Service (DoS) attack

Question 701

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

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

Question 702

Which type of encryption is considered to be unbreakable if the stream is truly random and is as large as the plaintext and never reused in whole or part?

- ☐ One Time Pad (OTP)
- ☐ One time Cryptopad (OTC)
- ☐ Cryptanalysis
- ☐ Pretty Good Privacy (PGP)

Question 703

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 704

Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

- ☐ Alternative routing
- ☐ Diverse routing
- ☐ Long haul network diversity
- ☐ Last mile circuit protection

Question 705

What is the Maximum Tolerable Downtime (MTD)?

- ☐ Maximum elapsed time required to complete recovery of application data
- ☐ Minimum elapsed time required to complete recovery of application data
- ☐ Maximum elapsed time required to move back to primary site after a major disruption
- ☐ It is maximum delay businesses can tolerate and still remain viable

Question 706

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

- ☐ D
- ☐ C
- ☐ B
- ☐ A

Question 707

Which access control model is also called Non-Discretionary Access Control (NDAC)?

- ☐ Lattice based access control
- ☐ Mandatory access control
- ☐ Role-based access control
- ☐ Label-based access control

Question 708

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 709

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 710

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 711

What protocol is used on the Local Area Network (LAN) to obtain an IP address from its known MAC address?

- ☐ Reverse address resolution protocol (RARP)
- ☐ Address resolution protocol (ARP)
- ☐ Data link layer
- ☐ Network address translation (NAT)

Question 712

Which of the following best describes signature-based detection?

- ☐ Compare source code, looking for events or sets of events that could cause damage to a system or network.
- ☐ Compare system activity for the behavior patterns of new attacks.
- ☐ Compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack.
- ☐ Compare network nodes looking for objects or sets of objects that match a predefined pattern of objects that may describe a known attack.

Question 713

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 714

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 715

In which of the following models are Subjects and Objects identified and the permissions applied to each subject/object combination are specified? Such a model can be used to quickly summarize what permissions a subject has for various system objects.

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