CISSP Final Examination   Score:

1 **Proper separation of duties involves which of the following?**

A Operators are not permitted modify the system time.

B Programmers are permitted to use the system console.

C Console operators are permitted to mount tapes and disks.

D Tape operators are permitted to use the system console.

2 **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?**

A DAC

B MAC

C Access control matrix

D TACACS

3 **What is Kerberos?**

A A three-headed dog from Egyptian mythology.

B A trusted third-party authentication protocol.

C A security model.

D A remote authentication dial in user server.

4 **What is called an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics?**

A Biometrics

B Micrometrics

C Macrometrics

D MicroBiometrics

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

A Iris scan

B Hand geometry

C Voice pattern

D Fingerprints

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

A Role-based access control

B Mandatory access control

C Lattice-based access control

D Discretionary access control

7 **Legacy Single Sign On (SSO) is:**

A 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.

B Technology to manage passwords consistently across multiple platforms, enforcing policies such as password change intervals.

C A mechanism where users can authenticate themselves once, and a central repository of their credentials are used to launch various legacy applications.

D Another way of referring to SESAME and KryptoKnight, now that Kerberos is the de-facto industry standard single sign on mechanism.

8 **What does the Clark-Wilson security model focus on?**

A Confidentiality

B Integrity

C Accountability

D Availability

9 **Identification and authentication are the keystones of most access control systems. Identification establishes:**

A User accountability for the actions on the system.

B Top management accountability for the actions on the system.

C EDP department accountability for the actions of users on the system.

D Authentication for actions on the system

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

A 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.

B The initial logon process is cumbersome to discourage potential intruders.

C Once a user obtains access to the system through the initial log-on, they only need to logon to some applications.

D Once a user obtains access to the system through the initial log-on, he has to logout from all other systems

11 **When a biometric system is used, which error type deals with the possibility of GRANTING access to impostors who should be REJECTED?**

A Type I error

B Type II error

C Type III error

D Crossover error

12 **Which of the following statements pertaining to the use of passwords is correct?**

A Passwords cannot be compromised and need not be protected.

B In the ideal situation, a password should only be used once.

C In the ideal situation, a password should not be used not more than twice.

D In the ideal situation, a password should not be used more than three times.

13 **Administrative controls include which of the following?**

A Policies and procedures, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

B Policies and objectives of such policies, security awareness training, background checks, work habit checks, a review of vacation history, and increased supervision.

C Policies and procedures, security hacking training, background checks, work habit checks, a review of vacation history, and increased supervision.

D Policies and procedures, security awareness training, background checks, work habit checks, a review of personal family history, and increased supervision.

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

A A capacity table

B An access control list

C An access control matrix

D A capability table

15 **Controls are implemented to:**

A Eliminate risk and reduce the potential for loss

B Mitigate risk and eliminate the potential for loss

C Mitigate risk and reduce the potential for loss

D Eliminate risk and eliminate the potential for loss

16 **Access Control techniques do not include which of the following choices?**

A Relevant Access Controls

B Discretionary Access Control

C Mandatory Access Control

D Lattice Based Access Control

17 **Because all the secret keys are held and authentication is performed on the Kerberos TGS and the authentication servers, these servers are vulnerable to:**

A Neither physical attacks nor attacks from malicious code.

B Physical attacks only

C Both physical attacks and attacks from malicious code.

D Physical attacks but not attacks from malicious code.

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

A Discretionary Access

B Least Privilege

C Mandatory Access

D Separation of Duties

19 **Which of the following best describes an exploit?**

A An intentional hidden message or feature in an object such as a piece of software or a movie.

B 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

C An anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer

D 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

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

A Holiday

B Christmas12

C Jenny

D GyN19Za!

21 **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?**

A Clark and Wilson Model

B Harrison-Ruzzo-Ullman Model

C Rivest and Shamir Model

D Bell-LaPadula Model

22 **Behavioral-based systems are also known as?**

A Profile-based systems

B Pattern matching systems

C Misuse detective systems

D Rule-based IDS

23 **Which authentication technique best protects against hijacking?**

A Static authentication

B Continuous authentication

C Robust authentication

D Strong authentication

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

A A preventive control.

B A deterrent control.

C A recovery control.

D A directive control.

25 **Which of the following is a type of non-discretionary access control?**

A Role-based access control.

B Mandatory access control.

C User-directed access control.

D Ladder-based access control.

26 **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):**

A Active attack.

B Outside attack.

C Inside attack.

D Passive attack.

27 **Using clipping levels refers to:**

A Setting allowable thresholds on a reported activity

B Limiting access to top management staff

C Setting personnel authority limits based on need-to-know basis

D Encryption of data so that it cannot be stolen

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

A Access control lists

B Discretionary access control

C Role-based access control

D Non-mandatory access control

29 **Which of the following is most relevant to determining the maximum effective cost of access control?**

A The value of information that is protected.

B Management’s perceptions regarding data importance.

C Budget planning related to base versus incremental spending.

D The cost to replace lost data.

30 **Which of the following is a preventive control?**

A Motion detectors

B Guard dogs

C Audit logs

D Intrusion detection systems

31 **Which type of password token involves time synchronization?**

A Static password tokens

B Synchronous dynamic password tokens

C Asynchronous dynamic password tokens

D Challenge-response tokens

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

A Deterrent controls

B Detective controls

C Preventive controls

D Compensating controls

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

A Clark-Wilson model

B Biba model

C Non-interference model

D Sutherland model

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

A Server farm

B Client farm

C Cluster farm

D Host farm

35 **Which type of attack involves the alteration of a packet at the IP level to convince a system that it is communicating with a known entity in order to gain access to a system?**

A TCP sequence number attack

B IP spoofing attack

C Piggybacking attack

D Teardrop attack

36 **What is the framing specification used for transmitting digital signals at 1.544 Mbps on a T1 facility?**

A DS-0

B DS-1

C DS-2

D DS-3

37 **Which of the following Common Data Network Services is used to share a printer or a print queue/spooler?**

A Mail services.

B Print services.

C Client/Server services.

D Domain Name Service.

38 **A Packet Filtering Firewall system is considered a:**

A First generation firewall.

B Second-generation firewall.

C Third generation firewall.

D Fourth generation firewall.

39 **Which of the following tape format types offer the largest capacity?**

A Digital Audio Tape (DAT)

B Quarter inch Cartridge (QIC)

C 8mm tape

D Digital Linear Tape (DLT)

40 **How long are IPv4 addresses?**

A 32 bits long.

B 64 bits long.

C 128 bits long.

D 16 bits long.

41 **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:**

A Netware Architecture.

B Network Architecture.

C WAN Architecture.

D Multiprotocol Architecture.

42 **Which of the following is true of network security?**

A A firewall is a not a necessity in today's connected world.

B A firewall is a necessity in today's connected world.

C A whitewall is a necessity in today's connected world.

D A black firewall is a necessity in today's connected world.

43 **Which layer of the TCP/IP protocol model ensures error-free delivery and packet sequencing?**

A Internet layer

B Network access layer

C Host-to-host transport layer

D Application layer

44 **A Wide Area Network (WAN) is basically everything outside of a(n):**

A Local Area Network (LAN).

B Campus Area Network (CAN).

C Metropolitan Area Network (MAN).

D Internet.

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

A Session layer

B Transport layer

C Network layer

D Data link layer

46 **Which of the following is an example of connectionless communication?**

A UDP

B X.25

C Packet switching

D TCP

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

A A SYN scan.

B A half-port scan.

C A buffer overflow attack.

D A packet destined for the network's broadcast address.

48 **Which of the following is the simplest type of firewall?**

A Stateful packet filtering firewall

B Packet filtering firewall

C Dual-homed host firewall

D Application gateway

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

A 110

B 109

C 139

D 119

50 **Which of the following does NOT allow for a workstation to get an IP address assigned?**

A BOOTP

B RARP

C DHCP

D ICMP

51 **This type of RAID implementation uses its own Central Processing Unit (CPU) for calculations on an intelligent controller card by:**

A Hardware implementation.

B Software implementation.

C Network implementation.

D Call implementation.

52 **Which of the following backup methods makes a complete backup of every file on the server every time it is run?**

A Full backup method.

B Incremental backup method.

C Differential backup method.

D Tape backup method.

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

A Network access layer

B Application layer

C Host-to-host transport layer

D Internet layer

54 **Which OSI/ISO layer does a SOCKS server operate at?**

A Session layer

B Transport layer

C Network layer

D Data link layer

55 **Which of the following is often not an aspect of Incident Response Management?**

A Coordinating the notification and distribution of information pertaining to the incident to the appropriate parties (those with a need to know) through a predefined escalation path

B Mitigating risk to the enterprise by minimizing the disruptions to normal business activities and the costs associated with remediating the incident (including public relations)

C Assembling teams of technical personnel to investigate the potential vulnerabilities and to resolve specific intrusions

D Assembling a team of legal personnel to investigate the tort implications of computer systems being unavailable.

56 **Communications and network security relate to which of the following?**

A Voice

B Voice and multimedia

C Data and multimedia

D Voice, data and multimedia

57 **Network cabling comes in three flavors, they are:**

A Twisted pair, coaxial, and fiber optic.

B Tagged pair, coaxial, and fiber optic.

C Trusted pair, coaxial, and fiber optic.

D Twisted pair, control, and fiber optic.

58 **The basic function of a Failure Resistant Disk System (FRDS) is which of the following?**

A Protect file servers from data loss and a loss of availability due to disk failure.

B Persistent file servers from data gain and a gain of availability due to disk failure.

C Prudent file servers from data loss and a loss of acceptability due to disk failure.

D Packet file servers from data loss and a loss of accountability due to disk failure.

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

A Switch

B Bridge

C Hub

D Router

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

A Data link layer

B Physical layer

C Transport layer

D Network layer

61 **Before the advent of classless addressing, the address 128.192.168.16 would have been considered part of a:**

A Class A network.

B Class B network.

C Class C network.

D Class D network.

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

A 172.12.42.5

B 172.140.42.5

C 172.31.42.5

D 172.15.42.5

63 **Which of the following layers of the ISO/OSI model do packet-filtering firewalls operate at?**

A Application layer

B Session layer

C Network layer

D Presentation layer

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

A Very expensive, resulting in the highest cost per megabyte of data capacity.

B Very inexpensive, resulting in the lowest cost per megabyte of data capacity.

C Very unreliable resulting in a greater risk of losing data.

D Very reliable resulting in a lower risk of losing data.

65 **Which of the following rules appearing in an Internet firewall policy is inappropriate?**

A The firewall software shall run on a dedicated computer.

B Appropriate firewall documentation shall be maintained on off-line storage at all times.

C The firewall shall be configured to deny all services not expressly permitted.

D The firewall should be tested on-line to validate proper configuration changes.

66 **The session layer provides a logical persistent connection between peer hosts. Which of the following is one of the modes used in the session layer to establish this connection?**

A Full duplex

B Synchronous

C Asynchronous

D Half simplex

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

A 80 meters

B 100 meters

C 185 meters

D 500 meters

68 **Which of the following is a device that is used to amplify the received signals?**

A Bridge

B Router

C Repeater

D Brouter

69 **Packet Filtering Firewalls examines both the source and destination address of the:**

A Incoming and outgoing data packets.

B Outgoing data packets only.

C Incoming Data packets only.

D User data packet.

70 **Application Layer Firewalls operate at the:**

A OSI protocol Layer seven, the Application Layer.

B OSI protocol Layer six, the Presentation Layer.

C OSI protocol Layer five, the Session Layer.

D OSI protocol Layer four, the Transport Layer.

71 **Upon which of the following ISO/OSI layers does network address translation operate?**

A Transport layer

B Session layer

C Data link layer

D Network layer

72 **Combining which of the following creates RAID Level 15?**

A Level 1 (mirroring) with level 5 (interleave).

B Level 0 (striping) with level 5 (interleave).

C Level 2 (hamming) with level 5 (interleave).

D Level 10 (striping and mirroring) with level 5 (interleave).

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

A Token Link.

B Token system.

C Token Ring.

D Duplicate ring.

74 **What is the main difference between a Smurf and a Fraggle attack?**

A A Smurf attack is ICMP-based and a Fraggle attack is UDP-based.

B A Smurf attack is UDP-based and a Fraggle attack is TCP-based.

C Smurf attack packets cannot be spoofed.

D A Smurf attack is UDP-based and a Fraggle attack is ICMP-based.

75 **Which of the following is NOT an advantage of coaxial cabling over twisted pair?**

A It is more resistant to EMI.

B It provides a higher bandwidth.

C It provides for longer cable lengths.

D It is less expensive.

76 **How many bits compose an IPv6 address?**

A 32 bits

B 64 bits

C 96 bits

D 128 bits

77 **Which of the following elements of telecommunications is not used in assuring confidentiality?**

A Network security protocols

B Network authentication services

C Data encryption services

D Passwords

78 **Which of the following is NOT a task normally performed by a Computer Incident Response Team (CIRT)?**

A Develop an information security policy.

B Coordinate the distribution of information pertaining to the incident to the appropriate parties.

C Mitigate risk to the enterprise.

D Assemble teams to investigate the potential vulnerabilities.

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

A Signature-based IDS and statistical anomaly-based IDS, respectively.

B Signature-based IDS and dynamic anomaly-based IDS, respectively.

C Anomaly-based IDS and statistical-based IDS, respectively.

D Signature-based IDS and motion anomaly-based IDS, respectively.

80 **Which cable technology refers to CAT3 and CAT5 categories?**

A Coaxial cables

B Fiber Optic cables

C Axial cables

D Twisted Pair cables

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

A Application Layer

B Presentation Layer

C Data Link Layer

D Network Layer

82 **DNS, FTP, TFTP, SNMP are provided at which level of the Open Systems Interconnect (OSI) Reference Model?**

A Application

B Network

C Presentation

D Transport

83 **Which RAID implementation creates one large disk by using several disks?**

A RAID level 0

B RAID level 1

C RAID level 2

D RAID level 10

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

A Message non-repudiation.

B Message confidentiality.

C Message interleave checking.

D Message integrity.

85 **Advanced Research Projects Agency Network (ARPANET), Department of Defense Research Projects Agency Network (DARPANET), Defense Data Network (DDN), or DoD Internets are referred to as which of the following?**

A The Internet.

B The Intranet.

C The Extranet.

D The Ethernet.

86 **Which device is used to connect two networks or applications at the higher level of the ISO/OSI framework?**

A Bridge

B Brouter

C Router

D Gateway

87 **What is a packet sniffer?**

A It tracks network connections to off-site locations.

B It monitors network traffic for illegal packets.

C It scans network segments for cabling faults.

D It captures network traffic for later analysis.

88 **Which of the following is the core of fiber optic cables made of?**

A PVC

B Glass fibers

C Kevlar

D Teflon

89 **A DMZ is also known as a**

A Screened subnet

B Three legged firewall

C Place to attract hackers

D Bastion host

90 **Which of the following statements pertaining to Asynchronous Transfer Mode (ATM) is false?**

A It can be used for voice

B It can be used for data

C It carries various sizes of packets

D It can be used for video

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

A Striping

B Mirroring

C Integrating

D Clustering

92 **Why are coaxial cables called "coaxial"?**

A It includes two physical channels that carry the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis.

B It includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis

C It includes two physical channels that carry the signal surrounded (after a layer of insulation) by another two concentric physical channel, both running along the same axis.

D It includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running perpendicular and along the different axis

93 **Which of the following takes the concept of RAID 1 (mirroring) and applies it to a pair of servers?**

A A redundant server implementation

B A redundant client implementation

C A redundant guest implementation

D A redundant host implementation

94 **Which of the following is the protocol that provides for the collection of network information by polling the devices on the network from a management station?**

A File Transfer Protocol (FTP).

B Trivial File Transfer Protocol (TFTP).

C Simple Mail Transfer Protocol (SMTP).

D Simple Network Management Protocol (SNMP).

95 **Which of the following tapes is only 0.498 inches in size, yet the compression techniques and head scanning process make it a large capacity and fast tape?**

A Digital Audio Tape (DAT).

B Analog Linear Tape (ALT).

C Digital Signal Tape (DST).

D Digital Linear Tape (DLT).

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

A Full backup method

B Incremental backup method

C Fast backup method

D Differential backup method

97 **Which of the following layers does IPSEC OPERATE at?**

A Session

B Transport

C Network

D Data Link

98 **In which layer are connection-oriented protocols in the TCP/IP suite implemented?**

A Transport layer

B Application layer

C Physical layer

D Network layer

99 **The structures, transmission methods, transport formats, and security measures that are used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media includes:**

A The Telecommunications and Network Security domain

B The Telecommunications and Netware Security domain

C The Technical communications and Network Security domain

D The Telnet and Network Security domain

100 **What is defined as the rules for communicating between computers on a LAN?**

A LAN transmission protocols

B LAN topologies

C LAN transmission methods

D LAN media access methods

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

A IP address.

B MAC address.

C TCP address.

D Datagram address.

102 **Which of the following is the biggest concern with wireless technologies?**

A Availability

B Confidentiality

C Reliability

D Integrity

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

A By convention it uses 's-http://' instead of 'http://'.

B Is the predecessor to Transport Layer Security (TLS)?

C Netscape developed it.

D It is used for transmitting private documents over the Internet.

104 **In the UTP category rating, the tighter the wind:**

A The higher the rating and its resistance against interference and attenuation.

B The slower the rating and its resistance against interference and attenuation.

C The shorter the rating and its resistance against interference and attenuation.

D The longer the rating and its resistance against interference and attenuation.

105 **Which of the following protocols does the Internet use?**

A SNA.

B DECnet.

C TCP/IP.

D MAP.

106 **What is also known as 10Base5?**

A Thinnet

B Thicknet

C ARCnet

D UTP

107 **What is the role of IKE within the IPSec protocol?**

A Peer authentication and key exchange

B Data encryption

C Data signature

D Enforcing quality of service

108 **Which protocol's primary function is to facilitate file and directory transfer between two machines?**

A Telnet.

B File Transfer Protocol (FTP).

C Trivial File Transfer Protocol (TFTP).

D Simple Mail Transfer Protocol (SMTP)

109 **The DMZ does not normally contain a(n):**

A Encryption server

B Web server

C External DNS server

D Mail relay

110 **What is a hub used for?**

A Connecting two LANs using different protocols

B Connecting two segments of a single LAN

C Connecting a LAN with a WAN

D Connecting a LAN with a MAN

111 **In SSL/TLS protocol, what kind of authentication is supported?**

A Peer-to-peer authentication

B Only server authentication (optional)

C Server authentication (mandatory) and client authentication (optional)

D Role based authentication scheme

112 **Which of the following would best define the "Gap in the WAP" security issue that existed prior to the WAP 2.0 specifications?**

A The processing capability shows a serious gap between wireless devices and PCs.

B The fact that WTLS transmissions have to be decrypted at the carrier's WAP gateway to be re-encrypted with SSL for use over wired networks.

C The fact that Wireless communications are far easier to intercept than wired communications.

D The inability of wireless devices to implement strong encryption algorithms.

113 **Behavior-based ID systems are less common than:**

A Client-based ID systems.

B Network-based ID systems.

C Host-based ID systems.

D Knowledge-based ID systems.

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

A Server cluster.

B Client cluster.

C Guest cluster.

D Host cluster.

115 **How is Annualized Loss Expectancy (ALE) derived from a threat?**

A ARO x (SLE - EF)

B SLE x ARO

C SLE/EF

D AV x EF

116 **Which of the following would best classify as a management control?**

A Review of security controls

B Personnel security

C Physical and environmental protection

D Documentation

117 **Which of the following is NOT a common integrity goal?**

A Prevent unauthorized users from making modifications.

B Maintain internal and external consistency.

C Prevent authorized users from making improper modifications.

D Prevent paths that could lead to inappropriate disclosure.

118 **A weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks is called a(n)?**

A Vulnerability

B Risk

C Threat

D Overflow

119 **Whose role is it to assign a classification level to information?**

A Security manager

B User

C Owner

D Auditor

120 **In a properly segregated environment, which of the following tasks is compatible with the task of security administrator?**

A Applications programming

B Quality assurance

C Systems programming

D Data entry

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

A A risk

B A threat

C A vulnerability

D A weakness

122 **Which of the following is BEST defined as a physical control?**

A Monitoring of system activity

B Environmental controls

C Identification and authentication methods

D Logical access control mechanisms

123 **What can be described as a measure of the magnitude of loss or impact on the value of an asset?**

A Probability

B Exposure factor

C Vulnerability

D Threat

124 **Which of the following would BEST be defined as the absence or weakness of safeguard that could be exploited?**

A A threat

B A vulnerability

C A risk

D An exposure

125 **Related to information security, the guarantee that the message sent is the message received is an example of which of the following?**

A Integrity

B Confidentiality

C Availability

D Identity

126 **Which of the following is an advantage of a qualitative over a quantitative risk analysis?**

A It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.

B It provides specific quantifiable measurements of the magnitude of the impacts.

C It makes a cost-benefit analysis of recommended controls easier.

D It can easily be automated.

127 **What are the three FUNDAMENTAL principles of security?**

A Accountability, confidentiality and integrity

B Confidentiality, integrity and availability

C Integrity, availability and accountability

D Availability, accountability and confidentiality

128 **What would be the Annualized Rate of Occurrence (ARO) of the threat "user input error", in the case where a company employs 100 data entry clerks and every one of them makes one input error each month?**

A 100

B 120

C 1

D 1,200

129 **Making sure that the data has not been changed unintentionally due to an accident or malice is:**

A Integrity.

B Confidentiality.

C Availability.

D Auditability.

130 **All risks must be:**

A Transferred

B Eliminated

C Identified

D Insured

131 **What is the goal of the Maintenance phase in a common development process of a security policy?**

A To review of the document on the specified review date

B Publication within the organization

C To write a proposal to management that states the objectives of the policy

D To present the document to an approving body

132 **What is an event or activity that has the potential to cause harm to the information systems or networks?**

A Vulnerability

B Threat agent

C Weakness

D Threat

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

A Hackers.

B Industrial saboteurs.

C Foreign intelligence officers.

D Employees.

134 **What is the main responsibility of the information (data) owner?**

A Determining the data sensitivity or classification level

B Running regular data backups

C Audit the data users

D Periodically check the validity and accuracy of the data

135 **Which of the following choices is NOT part of a security policy?**

A Definition of overall steps of information security and the importance of security

B Statement of management intent, supporting the goals and principles of information security

C Definition of general and specific responsibilities for information security management

D Description of specific technologies used in the field of information security

136 **Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?**

A Confidentiality

B Integrity

C Availability

D Capability

137 **Which one of the following represents an ALE calculation?**

A Single loss expectancy x annualized rate of occurrence.

B Gross loss expectancy x loss frequency.

C Actual replacement cost - proceeds of salvage.

D Asset value x loss expectancy.

138 **Which of the following statements pertaining to quantitative risk analysis is false?**

A Portion of it can be automated

B It involves complex calculations

C It requires a high volume of information

D It requires little experience to apply

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

A Attributes

B Records or tuples

C Record retention

D Relation

140 **In what way could Java applets pose a security threat?**

A Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP

B Java interpreters do not provide the ability to limit system access that an applet could have on a client system.

C Executables from the Internet may attempt an intentional attack when they are downloaded on a client system.

D Java does not check the byte code at runtime or provide other safety mechanisms for program isolation from the client system.

141 **Which of the following can be defined as an attribute in one relation that has values matching the primary key in another relation?**

A Foreign key

B Candidate key

C Primary key

D Secondary key

142 **Which of the following phases of a system development life cycle is most concerned with establishing a sound policy as the foundation for design?**

A Development/acquisition

B Implementation

C Initiation

D Maintenance

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

A Computer-aided develop and imaging.

B Computer-aided duplexing and imaging.

C Computer-aided processing and imaging.

D Computer-aided design and imaging.

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

A Normalization

B Assimilation

C Reduction

D Compaction

145 **Which of the following tests ensure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems?**

A Recovery testing

B Security testing

C Stress/volume testing

D Interface testing

146 **Which of the following is one of the oldest and most common problems in software development and programming and is still very prevalent today?**

A Buffer Overflow

B Social Engineering

C Code injection for machine language

D Unassembled reversible DOS instructions.

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

A Bind variables

B Assimilation variables

C Reduction variables

D Resolution variables

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

A A translator

B An interpreter

C A compiler

D An assembler

149 **Risk reduction in a system development life-cycle should be applied:**

A Mostly to the initiation phase.

B Mostly to the development phase.

C Mostly to the disposal phase.

D Equally to all phases.

150 **Which of the following is NOT true concerning Application Control?**

A It limits end users use of applications in such a way that only particular screens are visible.

B Only specific records can be requested through the application controls

C Particular usage of the application can be recorded for audit purposes

D It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved

151 **Which uses a key of the same length as the message?**

A Running key cipher

B One-time pad

C Steganography

D Cipher block chaining

152 **Which type of Encryption technology does VeriSign's SSL utilize?**

A Secret key

B Hybrid: Symmetric and asymmetric cryptography

C Public Key

D Asymmetric key

153 **Which of the following statements related to a private key cryptosystem is FALSE?**

A The encryption key should be secure.

B Data Encryption Standard (DES) is a typical private key cryptosystem.

C The key used for decryption is known to the sender

D Two different keys are used for the encryption and decryption.

154 **Which kind of certificate is used to validate a user identity?**

A Public key certificate

B Attribute certificate

C Root certificate

D Code signing certificate

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

A Encryption

B Integrity

C Digital signature

D Authentication

156 **Which of the following is a symmetric encryption algorithm?**

A RSA

B Elliptic Curve

C RC5

D El Gamal

157 **The DES algorithm is an example of which type of cryptography?**

A Secret Key.

B Two-key.

C Asymmetric Key.

D Public Key.

158 **What is the primary role of smartcards in a PKI?**

A Transparent renewal of user keys

B Easy distribution of the certificates between the users

C Fast hardware encryption of the raw data

D Tamperproof, mobile storage and application of private keys of the users

159 **Which of the following are suitable protocols for securing VPN connections at the lower layers of the OSI model?**

A S/MIME and SSH

B TLS and SSL

C IPSec and L2TP

D PKCS#10 and X.509

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

A Registration authority

B Certification authority

C Issuing authority

D Vouching authority

161 **Which is NOT a suitable method for distributing certificate revocation information?**

A CA revocation mailing list

B Delta CRL

C OCSP (online certificate status protocol)

D Distribution point CRL

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

A Confidentiality

B Key exchange

C Integrity

D Non-repudiation

163 **Cryptography does not concern itself with:**

A Availability

B Integrity

C Confidentiality

D Authenticity

164 **Which of the following protocols that provide integrity and authentication for IPSec can also provide non-repudiation in IPSec?**

A Authentication Header (AH)

B Encapsulating Security Payload (ESP)

C Secure Sockets Layer (SSL)

D Secure Shell (SSH-2)

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

A Cipher block chaining

B Electronic code book

C Input feedback

D Cipher feedback

166 **Which principle involves encryption keys being separated into two components, each of which does not reveal the other?**

A Dual control

B Separation of duties

C Split knowledge

D Need to know

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

A ISAKMP

B Diffie-Hellman

C Cryptology

D KEA

168 **What is the length of an MD5 message digest?**

A 128 bits

B 160 bits

C 256 bits

D Varies depending upon the message size.

169 **Which of the following mail standards relies on a "Web of Trust"?**

A Secure Multipurpose Internet Mail Extensions (S/MIME)

B Pretty Good Privacy (PGP)

C MIME Object Security Services (MOSS)

D Privacy Enhanced Mail (PEM)

170 **The Secure Hash Algorithm (SHA-1) creates:**

A A fixed length message digest from a fixed length input message

B A variable length message digest from a variable length input message

C A fixed length message digest from a variable length input message

D A variable length message digest from a fixed length input message

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

A Asymmetric Key.

B Symmetric Key.

C Secret Key.

D Private Key.

172 **Which of the following encryption methods is unbreakable?**

A Symmetric ciphers.

B DES codebooks.

C One-time pads.

D Elliptic Curve Cryptography.

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

A Secure Electronic Transaction (SET)

B MONDEX

C Secure Shell (SSH-2)

D Secure Hypertext Transfer Protocol (S-HTTP)

174 **Which of the following statements pertaining to link encryption is false?**

A It encrypts all the data along a specific communication path.

B It provides protection against packet sniffers and eavesdroppers.

C Information stays encrypted from one end of its journey to the other.

D User information, header, trailers, addresses and routing data that are part of the packets are encrypted.

175 **Which of the following algorithms does NOT provide hashing?**

A SHA-1

B MD2

C RC4

D MD5

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

A A known-plaintext attack

B A known-algorithm attack

C A chosen-cipher text attack

D A chosen-plaintext attack

177 **Which of the following is NOT related to a Public key infrastructure (PKI)?**

A A Certificate authority

B A Ticket Granting Service

C A Registration authority

D A X.509 certificate

178 **Which of the following ASYMMETRIC encryption algorithms is based on the difficulty of FACTORING LARGE NUMBERS?**

A El Gamal

B Elliptic Curve Cryptosystems (ECCs)

C RSA

D International Data Encryption Algorithm (IDEA)

179 **What would BEST define a covert channel?**

A An undocumented backdoor that has been left by a programmer in an operating system

B An open system port that should be closed.

C A communication channel that allows transfer of information in a manner that violates the system's security policy.

D A Trojan horse.

180 **Which Orange book security rating introduces security labels?**

A C2

B B1

C B2

D B3

181 **The Orange Book does NOT cover:**

A Integrity

B Assurance

C Accountability

D Confidentiality

182 **Which of the following statements pertaining to protection rings is false?**

A They provide strict boundaries and definitions on what the processes that work within each ring can access.

B Programs operating in inner rings are usually referred to as existing in a privileged mode.

C They support the CIA triad requirements of multitasking operating systems.

D They provide users with a direct access to peripherals

183 **Which of the following is the lowest TCSEC class wherein the system must protect against covert storage channels (but not necessarily covert timing channels)?**

A B2

B B1

C B3

D A1

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

A No write up

B No read up

C No write down

D No read down

185 **Which of the following did the National Computer Security Center (NCSC) develop?**

A TCSEC

B ITSEC

C DIACAP

D NIACAP

186 **Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system?**

A Fail proof

B Fail soft

C Fail safe

D Fail resilient

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

A Authorization, Identification, authentication

B Identification, accountability, authorization

C Identification, authentication, authorization

D Authentication, Authorization, Identification

188 **The biggest difference between System High Security Mode and Dedicated Security Mode is:**

A The clearance required

B Object classification

C Subjects cannot access all objects

D Need-to-know

189 **Which of the following models does NOT include data integrity?**

A Biba

B Clark-Wilson

C Bell-LaPadula

D Brewer-Nash

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

A D

B C

C B

D A

191 **Which security model introduces access to objects only through programs?**

A The Biba model

B The Bell-LaPadula model

C The Clark-Wilson model

D The information flow model

192 **Which access control model uses a directed graph to specify rights that can be transferred from a subject to an object?**

A The Clark-Wilson model

B The Biba Integrity model

C The Take-Grant model

D The Non-interference model

193 **What can best be defined as the sum of protection mechanisms inside the computer, including hardware, firmware and software?**

A Trusted system

B Security kernel

C Trusted computing base

D Security perimeter

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

A A and B.

B B and C.

C A, B, and C.

D B and D.

195 **Physically securing backup tapes from unauthorized access is an obvious security concern and is considered a function of the:**

A Operations Security Domain.

B Operations Security Domain Analysis.

C Telecommunications and Network Security Domain.

D Business Continuity Planning and Disaster Recovery Planning.

196 **Operation security requires the implementation of physical security to control which of the following?**

A Unauthorized personnel access

B Incoming hardware

C Contingency conditions

D Evacuation procedures

197 **The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?**

A Clipping level

B Acceptance level

C Forgiveness level

D Logging level

198 **Which of the following logical access exposures INVOLVES CHANGING data before, or as it is entered into the computer?**

A Data diddling

B Salami techniques

C Trojan horses

D Viruses

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

A Trusted recovery

B Hot swappable

C Redundancy

D Secure boot

200 **What is the main objective of proper separation of duties?**

A To prevent employees from disclosing sensitive information.

B To ensure access controls are in place.

C To ensure that no single individual can compromise a system.

D To ensure that audit trails are not tampered with.

201 **Which of the following is not concerned with configuration management?**

A Hardware

B Software

C Documentation

D They all are concerned with configuration management.

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

A When to make backups

B Where to keep backups

C What records to backup

D How to store backups

203 **Which of the following refers to the data left on the media after the media has been erased?**

A Remnants

B Recovery

C Sticky bits

D Semi-hidden

204 **Which of the following is NOT a countermeasure to traffic analysis?**

A Padding messages.

B Eavesdropping.

C Sending noise.

D Covert channel analysis.

205 **What is NOT one of the drawbacks of hot sites?**

A Need Security controls, as it usually contain mirrored copies of live production data

B Full redundancy in hardware, software, communication lines and applications is very expensive

C The hot sites are available immediately or within maximum tolerable downtime (MTD)

D They are administratively resource intensive, as transaction redundancy controls need to be implemented to keep data up-to-date

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

A Non-mobile hot site.

B Mobile hot site.

C Warm site.

D Cold site.

207 **Which of the following is an ADVANTAGE of the use of hot sites as a backup alternative?**

A The costs associated with hot sites are low.

B Hot sites can be made ready for operation within a short period of time.

C Hot sites can be used for an extended amount of time.

D Hot sites do not require that equipment and systems software be compatible with the primary installation being backed up.

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

A Inscribed, printed and Written documents

B Manuscripts

C Accounts Receivable

D Money and Securities

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

A It is unlikely to be affected by the same contingency.

B It is close enough to become operational quickly.

C It is close enough to serve its users.

D It is convenient to airports and hotels.

210 **Which of the following is the most complete disaster recovery plan test type after completing the Parallel test?**

A Full Interruption test

B Checklist test

C Simulation test

D Structured walk-through test

211 **What is the most correct choice when talking about the steps to resume normal operation?**

A Most critical operations are moved from alternate site to primary site before others

B Operation may be carried by a completely different team than disaster recovery team

C Non critical systems are moved first from alternate site to the primary business location

D Business operations cannot be moved back, until green light is given by the salvage team that primary site is ready

212 **What is a hot-site facility?**

A A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.

B A site in which space is reserved with pre-installed wiring and raised floors.

C A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.

D A site with ready-made work space with telecommunications equipment, LANs, PCs, and terminals for work groups.

213 **Which of the following specifically addresses cyber attacks against an organization's IT systems?**

A Continuity of support plan

B Business continuity plan

C Incident response plan

D Continuity of operations plan

214 **Which is not one of the primary goals of BIA?**

A Criticality Prioritization

B Down time estimation

C Determining requirements for critical business functions

D Deciding on various test to be performed to validate Business Continuity Plan

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

A Simulation test

B Checklist test

C Parallel test

D Structured walk-through test

216 **Which of the following tasks is NOT usually part of a Business Impact Analysis (BIA)?**

A Identify the type and quantity of resources required for the recovery.

B Identify critical business processes and the dependencies between them.

C Identify organizational risks.

D Develop a mission statement.

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

A It should have the same amount of physical access restrictions as the primary processing site.

B It should be located in proximity to the originating site so that it can quickly be made operational.

C It should be easily identified from the outside so in the event of an emergency it can be easily found.

D Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

218 **System reliability is increased by:**

A A lower MTBF and a lower MTTR.

B A higher MTBF and a lower MTTR.

C A lower MTBF and a higher MTTR.

D A higher MTBF and a higher MTTR.

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

A Personnel turnover

B Large plans can take a lot of work to maintain

C Continuous auditing makes a Disaster Recovery plan irrelevant

D Infrastructure and environment changes

220 **What is the PRIMARY reason to maintain the chain of custody on evidence that has been collected?**

A To ensure that no evidence is lost.

B To ensure that all possible evidence is gathered.

C To ensure that the evidence is trustworthy

D To ensure that incidents were handled with due care and due diligence.

221 **The Internet Architecture Board (IAB) characterizes which of the following as unethical behavior for Internet users?**

A Writing computer viruses.

B Monitoring data traffic.

C Wasting computer resources.

D Concealing unauthorized accesses.

222 **Which of the following is biggest factor that makes Computer Crimes possible?**

A The fraudster obtaining advanced training & special knowledge.

B Victim carelessness.

C Collusion with others in information processing.

D System design flaws.

223 **Which of the following is an example of an active attack?**

A Traffic analysis

B Masquerading

C Eavesdropping

D Shoulder surfing

224 **Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the _____ Amendment. Private citizens are not subject to protecting these amendment rules of others unless they are acting as police agents.**

A First.

B Second.

C Third.

D Fourth.

225 **Once evidence is seized, a law enforcement officer should emphasize which of the following?**

A Chain of command.

B Chain of custody.

C Chain of control.

D Chain of communications.

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

A Because it is used to demonstrate the truth of the contents.

B Because it is used to identify the state of the system.

C Because the state of the memory cannot be used as evidence.

D Because of the exclusionary rule.

227 **After an intrusion has been contained and the compromised systems been reinstalled, which of the following need not be reviewed before bringing the system back to service?**

A Access control lists

B System services and their configuration

C Audit trails

D User accounts

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

A Relevant.

B Decrypted.

C Edited.

D Incriminating.

229 **Which category of law is also referenced as a Tort law?**

A Civil law

B Criminal law

C Administrative law

D Public law

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

A An organization that provides a secure channel for receiving reports about suspected security incidents.

B An organization that ensures that security incidents are reported to the authorities.

C An organization that coordinates and supports the response to security incidents.

D An organization that disseminates incident-related information to its constituency and other involved parties.

231 **Which of the following would be LESS likely to prevent an employee from reporting an incident?**

A They are afraid of being pulled into something they don't want to be involved with.

B The process of reporting incidents is centralized.

C They are afraid of being accused of something they didn't do.

D They are unaware of the company's security policies and procedures.

232 **In addition to Human Resources, with what company function must the collection of physical evidence be coordinated if an employee is suspected?**

A Legal.

B Industrial Security.

C Public relations.

D Computer security.

233 **When should a post-mortem review meeting be held after an intrusion has been properly taken care of?**

A Within the first three months after the investigation of the intrusion is completed.

B Within the first week after prosecution of intruders have taken place, whether successful or not.

C Within the first month after the investigation of the intrusion is completed.

D Within the first week of completing the investigation of the intrusion.

234 **Which of the following would best describe secondary evidence?**

A Oral testimony by a non-expert witness

B Oral testimony by an expert witness

C A copy of a piece of evidence

D Evidence that proves a specific act

235 **Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breaches if:**

A The company is not a multi-national company.

B They have not exercised due care protecting computing resources.

C They have failed to properly insure computer resources against loss.

D The company does not prosecute the hacker that caused the breach.

236 **Which type of attack would a competitive intelligence attack best classify as?**

A Business attack

B Intelligence attack

C Financial attack

D Grudge attack

237 **Which of the following is NOT part of the (ISC)2 Code of Ethics?**

A Not use a computer to harm people or interfere with other people's computer work.

B Execute responsibilities in a manner consistent with the highest standards of their profession,

C Appropriately report activity related to the profession that they believe to be unlawful and shall cooperate with resulting investigations.

D Not misuse the information in which they come into contact during the course of their duties, and they shall maintain the confidentiality of all information in their possession that is so identified.

238 **What category of law deals with regulatory standards that regulate performance and conduct? Government agencies create these standards, which are usually applied to companies and individuals within those companies?**

A Standards law.

B Conduct law.

C Compliance law.

D Administrative law.

239 **Evidence life cycle does not include which of the following?**

A Protection

B Identification

C Recording

D Destruction

240 **On November 23, 2001, what did thirty countries including Canada, the United States and China ratify?**

A International Computer Abuse Treaty.

B Internet Protection Convention.

C Cybercrime Anti-Terrorist Group.

D Cybercrime Convention.

241 **The recording or viewing of events after the fact using a closed-circuit TV camera is considered a:**

A Preventative control.

B Detective control.

C Compensating control.

D Corrective control.

242 **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?**

A Administrative control mechanisms

B Integrity control mechanisms

C Technical control mechanisms

D Physical control mechanisms

243 **A prolonged high voltage is a:**

A Spike

B Blackout

C Surge

D Fault

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

A Are sensitive data files encrypted on all portable systems?

B Are deposits and withdrawals of tapes and other storage media from the library authorized and logged?

C Are computer monitors located to eliminate viewing by unauthorized persons?

D Are procedures in place to determine compliance with password policies?

245 **A momentary low voltage, from 1 cycle to a few seconds, is a:**

A Spike

B Blackout

C Sag

D Fault

246 **Critical areas should be lighted:**

A Eight feet high and two feet out.

B Eight feet high and four feet out.

C Ten feet high and four feet out.

D Ten feet high and six feet out.

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

A Preaction

B Wet pipe

C Dry pipe

D Deluge

248 **A prolonged complete loss of electric power is a:**

A Brownout

B Blackout

C Surge

D Fault

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

A CO2

B CO2, soda acid, or Halon

C Water or soda acid

D ABC Rated Dry Chemical

250 **Which type of fire extinguisher is most appropriate for an information processing facility?**

A Type A

B Type B

C Type C

D Type D