Q1. The certificate authority signs the digital certificate with
a. User's public key
b. User's private key
c. It's own public key
d. It's own private key

Q2. Which of the following principle violated if computer system is not accessible?
a. Confidentiality
b. Availability
c. Access Control
d. Authentication

Q3. Which of the following is digital certificate standard
a. X.509
b. X.508
c. X.507
d. None of the above

Q.4 It is a program or hardware device that filters the information coming through an Internet connection to a network or a computer system.
a. antivirus
b. cookies
c. Firewall
d. cyber safety

Q.5 Trojan horses are very similar to virus in the matter that they are computer program that replicates copies of themselves.
a. true
b. false

Q.6 _____ monitors users activity on internet and transmit that information in the background to someone else.
a. Malware
b. Spyware
c. Adware
d. None of these

Q.7 viruses are_____
a. man made
b. naturally occur
c. machine
d. All of the above

Q.8 Unauthorized Access and viruses are dealing with network _____
a. Performance

b. Reliability
c. Security
d. None of the above

Q.9 Encryption is required
i. To play protect business information from never stopping when it is transmitted on internet.
ii. efficiently use the bandwidth available in PSTN
iii. To protect the information stored in companies Database from retrieval
iv. To preserve security of information stored in database if an unauthorised person retrieved it.
a. i and ii
b. ii and iii
c. iii and iv
d. i and iv

Q.10 By symmetric key encryption we mean
a. one private key is used for both encryption and decryption
b. private and public key used as symmetric
c. only public keys are used for encryption
d. only symmetric key is used for encryption

Q.11 The following is independent malicious program that need not any host program
a. trap doors
b. Trojan Horse
c. virus
d. worms

Q12. In tunnel mode IPsec protects the
a Entire IP packet
b IP header
c ip payload
d none of the mentioned

Q.13 which of the following is known as malicious software?
a. illegalware
b. badwear
c. Malware
d. maliciousware

Q14. which of the following is not an example of Smart Card?
a credit card which can be used to operate mobile phone
b electronic money card example monodex
c a driver license containing current information about bookings
d. an access control card containing a digitised photo

Q15. If DOS – Denial of Service then DDoS – ?

a. Dynamic Denial of Service
b. Distributed Denial of Service
c. Dynomic Denial of Service
d. None of the above

Q16. A program that copies itself.
a. Worm
b. Virus
c. Trojan
d. Bomb

Q.17 An attack in which the site is not capable of answering valid request
a. Smurfing
b. Ping strom
c. Denial of Service
d. E mail bombing

Q.18 Encryption is the study of creating and using decryption techniques.
a. True
b. False

Q.19 In public key cryptography, a key that decrypts the message.
a. Public key
b. Unique key
c. Security key
d. Private key

Q.20 An electronic document that establishes your credentials when you are performing transactions.
a. Digital code
b. OTP
c. E-mail
d. Digital certificate

Q.21 Which of the following is not a factor in securing the environment against an attack on security?
a. System configuration
b. The business strategy of the company
c. Education of the attacker
d. The network architecture

Q.22 The first phase of hacking and it system is compliments of which foundation of security?
a. Availability
b. Confidentiality
c. Integrity

d. Authentication

Q.23 what is the most important activity in system hacking?
a. information gathering
b. cracking passwords
c. Escalating privileges
d. covering tracks

Q.24 Phishing is a form of
a. Impersonation
b. Spamming
c. Identify Theft
d. Scanning

Q.25 Keyloggers are a form of
a. Spyware
b. Should surfing
c. Trojan
d. Social Engineering

Q.26 which of the following is a class of computer thread
a. DoS Attacks
b. Phishing
c. stocking
d.soliciting

Q.27 To hide information inside a picture what technology is used?
a.rootkits
b.Bitmapping
c. Steganography
d. Image rendering

Q.28 Which phase of hacking performs actual attack on a network of a system?
a. Reconnaissance
b.maintaining access
c. scanning
d. gaining access

Q.29 What is the purpose of Denial of Service attack?
a exploiting a weakness in TCP IP stack
b. To execute Trojan on a system
c. To overload a system so it is no longer operational
d. To shutdown services by tuning them off

Q30. what are some of the most common vulnerabilities that exist in a network of a system?

a. changing manufacturer or recommended settings of a newly installed application.
b. Additional unused features on a commercial software packages.
c. Utilizing open source application code
d. Balancing security concerns with functionality and ease of use of a system

Q31. How is IP address spoofing detected?
a. Installing and configuring a ideas that can read the IP header
b. Comparing the TTL values of the actual and spoofed addresses
c. Implementing a farewell to the network
d. Identifying all the TCP stations that are initiated but does not complete successfully

Q32. Which port does Telnet use?
a. 22
b. 80
c. 20
d. 23

Q.33 Sniffing is used to perform _____ fingerprinting
a. Passive stack
b. Active stack
c. passive banner grabbing
d. Scanned

Q.34 what are hybrid attacks?
a. An attempt to crack password using words that can be found in a dictionary.
b. An attempt to crack password by replacing characters of a dictionary word with the numbers and symbols
c. An attempt to crack password using a combination of characters numbers and symbols
d. An attempt to crack password by replacing characters with the numbers and symbols

Q.35 what is the best statement for taking advantage of a weakness in a security of an IT system?
a. Threat
b. Attack
c. Exploit
d. vulnerabilities

Q.36 what does the acronym VIRUS stands for?
a. Vital Information Resource Under Siege
b. Vital Informative Resourceful Under Siege
c. Virtual information Resource under Siege
d. None of the above

Q.37 Bom Thomas working at BBN Rote Program X which infected ARPANET. he later wrote program why to destroy X. What are X and Y?
a. X- Creeper, Y- Reaper
b. X- Reaper, Y- Creeper
c. X- Rabit, Y – Reaper
d. None of the above

Q.38 Which of the following are Threads for electronic payment systems
a. Computer worms

b. computer virus
c. Trojan horse
d. all the above

Q.39 Authentication is
a. modification
b. Insertion
c. hard to assure identity of user on a remote system
d. None of the above

Q.40 a virus that mitigates freely within a large population of unauthorised email user is called as
a. flameware
b. Worm
c. macro
d. plagiarism

Q41. What do most VPNs use to protect transmitted data?
a. Obscurity
b. Encryption
c. Encapsulation
d. Transmission logging

Q42. In addition to maintaining an updated system and controlling physical access, which of the following is the most effective countermeasure against PBX fraud and abuse?
a. Encrypting communications
b. Changing default passwords
c. Using transmission logs
d. Taping and archiving all conversations

Q43.Which of the following is not a VPocol?
a. PPTP
b. L2F
c. SLIP
d. IPSec

Q44. Which of the following model is more secured?
a. Lollipop model
b. Onion model
c. both a and b
d. None of the above

Q45. Which of the following is not a denial of service attack?
a. Exploiting a flaw in a program to consume 100 percent of the CPU
b. Sending malformed packets to a system, causing it to freeze
c. Performing a brute force attack against a known user account
d. Sending thousands of e-mails to a single address

Q.46 A person who illegally gain access to information they are not authorized to access commits ?
a. Fraud
b. Hijacking
c. Espionage
d. Theft

Q.47 _____ is the risk of loss of information
a. Exposure
b. Data leakage
c. Forwarding
d. Theft

Q.48 _____ refers to accuracy and consistency of data.
a. Confidentiality
b. Integrity
c. Availability
d. Risk remediation

Q.49 To protect the data, it should be _____?
a. Secure
b. Backup
c. Encrypted
d. Decrypted

Q.50 On windows based operating systems, which file system offers any level of file system security.
a. FAT
b. FAT32
c. NTFS
d. NTFS 32

Q.51 An extranet is defined as the network that restricts access to company files and folders from unknown people.
a. True
b. False
c. Can't say
d. May be
Q.52 Intranet is a network that is not available to outside word.
a. True
b. False
c. May be
d. Can't say

Q.53 Internetworking protocol used today is known as
a. TCP/IP
b. FTP
c. SMTP
d. None of above

Q.54 ARP stands for:
a. Address Resolution Phase
b. ARP Resolution Protocol
c. Address Recall Protocol
d. Address Resolution Protocol

Q.55 IPV4 and IPV6 addresses are
a. 32 bits and 64bits

b. 64 bits and 32 bits
c. 128bits and 32 bits
d. 32bits and 128 bits

Q.56 Identify the 3 Network layer protocols?
a. NetBios
b. RARP,ARP,IP
c. ARP
d. None of the above

Q.57 What is the function of the Transport layer and which protocols reside there?
a. MAC addressing – IP
b. Interhost communication - SQL, NFS
c. Best effort Packet delivery - TCP, UDP
d. End-to-end connections - TCP, UDP

Q.58 Ping command is used to:
a. Share routing information with a neighbor router
b. Transmit user data when buffers are full
c. Test connectivity
d. Test entire protocol stack

Q.59. Following statements are true for MAC address
a. Contains a network portion and host portion
b. Always assigned by System Administrator
c. 48 bits long and Contains a vendor code and serial number
d. None of the above

Q60. A SYN flood is an example of what type of attack?
a. Malicious code
b. Denial of service
c. Man-in-the-middle
d. Spoofing

Q61. An attack in which the attacker simply listens for all traffic being transmitted across a network, in the hope of viewing something such as a userid and password combination, is known as
a. man-in-the-middle attack
b. denial of service attack
c. sniffing attack
d. backdoor attack

Q62. Which attack takes advantage of a trusted relationship that exists between two systems?
a. Spoofing
b. Password guessing
c. Sniffing
d. Brute force

Q63. In what type of attack does an attacker resend the series of commands and codes used in a financial transaction in order to cause the transaction to be conducted multiple times?
a. Spoofing
b. Man-in-the-middle
c. Replay

d. Backdoor

Q64. The first step in an attack on a computer system consists of
a. Gathering as much information about the target system as possible.
b. Obtaining as much information about the organization in which the target lies as possible.
c. Searching for possible exploits that can be used against known vulnerabilities.
d. Searching for specific vulnerabilities that may exist in the target's operating system or software applications.

Q65. Malicious code that is set to execute its payload on a specific date or at a specific time is known as
a. logic bomb
b. A Trojan horse
c. A virus
d. A time bomb

Q66.Authentication is typically based upon
a. Something a user possesses
b. Something a user knows
c. Something measured on a user, such as a fingerprint
d. All of the above

Q67. Passwords are an example of
a. Something you have
b. Something you know
c. A shared secret
d. None of the above

Q68. What is the most common form of authentication used?
a. Biometrics
b. Tokens
c. Access-card
d. Username/password

Q69. What was the basis for authentication used in Kerberos?
a. Token
b. Certificate
c. Ticket
d. Biometrics

Q70. Information security places the focus of security efforts on:
a. The system hardware
b. The software
c. The user
d. The data

Q71.CHAP is the
a. Certificate Handling Application Program
b. Challenge Handshake Authentication Protocol
c. Controlling Hierarchical Access Protocol
d. Confidentiality Handling Application Protocol

Q72. The CIA of security includes
a. Confidentiality, integrity, authentication
b. Certificates, integrity, availability
c. Confidentiality, inspection, authentication
d. Confidentiality, integrity, availability

Q73. What are the two main types of intrusion detection systems?
a. Network-based and host-based
b. Signature-based and event-based
c. Active and reactive
d. Intelligent and passive

Q74. Preventative intrusion detection systems
a. Are cheaper
b. Are designed to stop malicious activity from occurring
c. Can only monitor activity
d. Were the first types of IDS

Q75.Which of the following is not a capability of a network-based IDS?
a. Can detect denial of service attacks
b. Can decrypt and read encrypted traffic
c. Can decode UDP and TCP packets
d. Can be tuned to a particular network environment

Q76. Which of the following are not assets?
a. Hardware
b. Inventory
c. Equipment or software failure
d. Cash

Q77. The first commercial IDS product was
a. Stalker
b. NetRanger
c. IDES
d. RealSecure

Q78. A good backup plan will include which of the following?
a. The critical data needed for the organization to operate
b. Any software that is required to process the organization's data
c. Specific hardware to run the software or to process the data
d. All of the above

Q79. In which backup strategy are only the files and software that have changed since the last full backup saved?
a. Full
b. Differential
c. Incremental
d. Delta

Q80. _____ provides all the necessary components and mechanisms to transmit data between two computers over a network.
a. IP
b. TCP/IP

c. ARP
d. None of above

Q81. Which of the following is independent malicious program that need not any host program?
a. Trap Doors
b. Worm
c. Trojan Horse
d. Viruses

Q82. Which of the following malicious program do not replicate automatically?
a. Trap Doors
b. Worm
c. Trojan Horse
d. Viruses

Q83. In computer security, ……. means that computer system assets can be modified only by authorized parities
a. Confidentiality
b. Integrity
c. Availability
d. Authenticity

Q84. The three D's of security
a. Defense, Detection ,Divide
b. Defend ,Detect ,Dig
c. Defense ,Deterrence ,Detection
d. Divide ,Disguise ,Detect

Q85. You are never _____ percent secure.
a. 70
b. 80
c. 100
d. 90

Q86. What is the function of a firewall?
a. protects the computer in case of fire
b. Block or screen out spam
c. Prevents the CPU from being overheated
d. Helps to prevent outsiders from obtaining unauthorized access

Q87. _____ is the act of capturing packets of data flowing across a computer network.
a. packet catching
b. packet snipping
c. Packet sniffing
d. packet pulling

Q88. _____condition exists when a program attempts to put more data in a buffer than it can hold
a. buffer overflow
b. buffer fill
c. buffer overrun
d. buffer full

Q89. _____is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet
a. ARP Protocol
b. ARP sniffing
c. ARP poisoning(ARP Spoofing)
d. ARP cracking

Q90. Authentication is the process by which people prove they are who they say they are
a. true
b. false

Q91. _____ is a network authentication system based on the use of tickets.

a. Kerberos
b. Railway
c. SSL
d. TLS

Q92. Secure Sockets Layer (SSL) is a certificate-based system that is used to provide authentication of secure web servers and clients and to share encryption keys between servers and clients
a. True
b. False

Q93. A _____algorithm simply replaces each character in a message with another character
a. substitution algo
b. transposition algo
c. cipher text (Encrypted message)
d. decipher(Decrypted message)

Q94. CIA triad focuses on three aspects of information protection.
a. Confidentiality, Interest, and Availability
b. Confidentiality, Integrity, and Availability
c. Confidence, Integrity, and Availability
d. Confidentiality, Integrity, and Authentication

Q95. A better approach is the lollipop model of security. It is a layered strategy, often referred to as defense in depth
a. True
b. False

Q96. In _____cryptography the same secret key is used by the sender and the receiver.
a. symmetric-key -1 -secret key
b. asymmetric-key -2
c. digital certificate
d. digital signature

Q97. A _____issues, catalogs, renews, and revokes certificates under the Management of a policy and administrative control.
a. Certification authority
b. Registration authorithy
c. Revocation Authority
d. Digital authority

Q98. _____defines the protection against denial by one of the parties in a communication
a. authentication
b. non repudiation
c. confidentiality
d. Integrity

Q99. With one predefined command, the attacker can cause all the zombies tobegin to attack another remote system with a distributed denial of service (DDoS) attack
a. True
b. False

Q100. If the virus executes, does its damage, and terminates until the next time it is executed, it is known as a _____
a. nonresident virus
b. stealth virus
c. overwriting virus
d. prepending virus

101) A _____ program must be conducted for development teams which includes technical security awareness training and role-specific training.
a. Security training
b. Security coding
c. Security Testing
d. Documentation

102) Security _____ is performed to find security issues by running application code.
a. Documentation
b. Monitoring
c. Testing
d. Modeling

103) _____ is a technique for reviewing the security properties of a design and identifying potential issues and fixes.
a. Threat Modeling
b. Code Review
c. Cookies
d. SQL injection attack

104) _____ Scripts are used for performing validations like limiting the size of the input fields, disallow certain characters.
a. Server side
b. Client side
c. SQL query

d. Application

105) Limiting the number of connections per second per IP address and use of strong passwords can prevent _____ attack.
a. Brute-force
b. SQL injection
c. Buffer overflow
d. Cookies

106) Application security is mainly controlled by the _____ of the application, as he/she requires extensive knowledge about various areas like GUI, network connectivity, OS interaction and sensitive data management for writing secure programs.
a. Server
b. Developer
c. Client
d. Company

107) _____ is common method of verifying that the person on the other end is a human being by showing a distorted image of letters and numbers and requiring the user to type them in correctly.
a. OTP
b. password
c. CAPTCHA
d. graphics

108) Web interface has _____ quick development time than GUI.
a. slow
b. fast
c. medium
d. regular

109) A web interface can be accessed from any _____ location through internet.
a. Remote
b. low
c. high
d. source

110) Customized client GUIs can be used to display _____ that cannot be shown using a regular web administration interface.
a. Complex graphics
b. header
c. footer
d. image

111) One of the following is a disadvantage of custom web administration.
a. Availability
b. encryption
c. specific OS
d. complex graphics

112) Keeping applications up to date with the latest security _____ is one of the most important security measures.

a. patches
b. forms
c. OS
d. Release

113) _____ is a technique to find security issues by inspecting application code, using static analysis tools or manual code review or a combination.
a. Security code review
. secure design
c. Testing
d. Documentation

114) _____ is a technique to inject crafted SQL into user input fields that are the part of the web forms.
a. SQL injection
b. brute-force
c. buffer overflow
d. cookies

115) _____ Attacks are those that do not come under any specific category but still they are considered as risk to website security.
a. General
b. cookies
c. forms
d. scripts

116) Databases can be used in various capacities, except:
a. Application support
b. Secure storage of sensitive information
c. Online transaction processing (OLTP)
d. VPN

117) Microsoft SQL Server database platform uses a default TCP port of
a. 1527
b. 1433
c. 3306
d. None of the above

118) Encryption in databases can be done
a. by storing encrypted data in the DB.
b. Through VPN
c. Providing passwords
d. Restricting Access

119) The various Database Security Layers are:
a. Server Security Layer
b. Network Level Security
c. Transport Level Layer
d. Encryption Level

120) The ANSI Standard SQL language provides for the ability to use three commands for administering permissions to tables and other database objects, the fourth wrong command being

a. Grant
b. Revoke
c. Deny
d. Commit

121) Perhaps the most commonly used method of controlling data access is
a. cursors
b. views
c. trigger
d. sequence

122) Instead of layers DBAs provide access to objects, some objects are given except
a. view
b. Stored procedure
c. trigger
d. application

123) To what granular level can security be provided
a. Application
b. Table
c. Column
d. Schema

124) Triggers are used as security objects except
a. to fire creation of a row in another table
b. to perform detailed auditing
c. to create views
d. enforce complex data-base related rules

125) Web based developers would handle security at the level of
a. Application
b. User
c. Operating System
d. Column

126) Data validation in multiple places prevents the following except
a. errors
b. malware
c. data corruption
d. System crashes

127) The most important data validation feature using hidden fields is called
a. hacking
b. SQL injection
c. spoofing
d. masquerading

128) If you back up 13GB of data to tape media and then the database becomes corrupted, the recovery time might be
a. two hours.
b. three hours

c. four hours
d. five hours

129) Backups can be of these types except
a. Full
b. Differential
c. Transaction log
d. user-defined

130) Backup taken while system is up and running is called:
a. Cold backup
b. Hot backup
c. Severe Backup
d. mild Backup

131) 1 .Intrusion is action or process that compromises Authentication, integrity, availability of system
a. force fully
b. With Permission
c. Without Permission
d. Both A and C

132) What are the different types of intruder detection Model?
a. Host Based.
b. Network Based.
c.User Based.
d. Both B and C

133) In which approach references a baseline pattern of normal system activity to identify active intrusion?
a. Anomaly detection.
b. Penetration identification.
c. Profile based
d. Machine based.

134) In which approach references a baseline pattern of normal system activity to identify active intrusion?
a. Anomaly detection.
b. Penetration identification.
c. Profile based
d. Machine based.

135) What are the different ways to classify IDS?
a. Statistical anomaly detection
b. Rule based detection
c. Both A and B
d. Stack based.

136) In which approach use Network traffic for particular network segment analyses and detection of threats?
a. Host based IDS.
b. Network based IDS.

c. Profile based IDS.
d. Rule based detection.

137) What are the characteristics of signature based IDS?
a. Most are based on simple pattern matching algorithms
b. It is programmed to interpret a certain series of packets
c. It models the normal usage of network as a noise characterization
d. Anything distinct from the noise is assumed to be intrusion activity?

138) For which IDS system is difficult to analyse the intrusion on multiple computers?
a. Host based IDS.
b. Network based IDS.
c. Profile based IDS.
d. Rule based detection.

139) Which Protocol used in fragmentation Attacks?
a. FTP.
b. IP.
c. HTTP.
d.UDP.

140) Which file IDS use to record all detected events and these record use for analyzing and reporting purposes?
a. Exe File.
b. Log Files.
c. System File.
d. UB File.

141) Full Form of SIEM?
a. Security Information and Event Management.
b. Secure Internet and Environment Management.
c. System Interface and Event Management.
d. Serial interface and Event log Managements.

142) IDS stand for?
a. Information Detection System
b. Intrusion Detection System
c. Institute Detection System
d. Image Detection System

143) _____ is the term for establishing a connection with a forged sender address.
a. Sequence Guessing.
b. spam
c. Spoofing
d. Session hijacking

144) _____ that identifies the users and groups who are allowed or denied access.
a. DACL
b. SACL
c. ACE
d. ISP

145) Bell-Lapadula model was revolutionary when it was published in .....
a. 1969
b. 1976
c. 1987
d. 1990

146) Biba is often know as a _____ version of Bell-Lapadula.
a. reserved
b. reversed
c. revolutionary
d. pure

147) Trusted Network Interpretation of the TCSEC also know as the _____ book.
a. Orange
b. Red
c. Yellow
d. Pink

148) Mandatory access control (MAC) is implemented in _____
a. Solaries
b. Windows
c. Network
d. Trusted BSD and Trusted Solaries

149) Which if the following is not the functionality of a Discretionary access control.
a. Individual user may not determine the access control.
b. Work well in commercial and academic sector.
c. Not suited for the military
d. effective for private web site. etc

150) _____ is a model that help is determining the protection right for example, read or write in computers system.
a. Chinese wall
b. Take Grant
c. Clark Wilson
d. Biba

151) Which of the following is not the main element of an effective reference monitor.
a. Always
b. not subject to preemption
c. Tamper proof
d. Heavy weight

152) _____ maintain access control policy.
a. Bell-Lapadula
b. Labels
c. Reference Monitor.
d. Windows

153) Which of the following is not the goal of the trust worthy computing initiative.
a. Security
b. Privacy

c. Reliability
d. Authentication

154) _____ defines a standard set of security requirement for a specific type of a product (e.g OS,database or firewall)
a. Protection
b. Security
c. EAL
d. TOE

155) Common criteria part _____ details the specific security functional requirements and details a criterion for expressing the security functional requirements for target of evaluation
a. 1
b. 2
c. 3
d. 4

156) According to classifications of operating system security 'D' determines
a. Minimal protection
b. Discretionary protection
c. Structured Protection
d. Security Domains

157) _____ are security-related information that has been associated with object such as files, process devices.
a. Reference monitor.
b. MAC
c. Labels
d. DAC

158) Which is not a part of Building a Security Program
a. Authority
b. Framework
c. Planning
d. Défense

159) Switches and Firewall come under the category of _____ assets
a. Technical equipment
b. Computer equipment
c. Communication equipment
d. Security equipment

160) Racks and NEMA-rated enclosures come under the category of _____ assets
a. Technical equipment
b. Furniture and Fixtures
c. Communication equipment
d. Storage equipment

161) One of the following comes under the category of Technical equipment
a. Air-conditioners
b. Servers
c. Fax machine

d. Credit-cards

162) The main areas of Physical Vulnerability assessment are
a. Buildings
b. Computing devices and peripherals
c. Documents and Records
d. All of the Above

163) Threats to Employee safety and break-inns are due to
a. Poor lighting
b. No security guard
c. Remotely located offices
d. High crime areas

164) Power outages can cause irreparable damages to
a. Remote offices running PCs
b. Servers
c. Data centers
d. None of above

165) _____ is an area designed to allow only one authorized person to enter in
a. Mantrap
b. Human trap
c. One pass
d. Secure Pass

166) Antitailgating mechanism is used to prevent _____ person from closely following an authorized person through an open door
a. All Authorized
b. Unauthorized
c. Both Authorized and Unauthorized
d. Few Authorized

167) _____ is used to confirm the identification of an individual through fingerprint, voice, face, retina, iris etc
a. Passwords
b. Signature verification
c. PCMC Card
d. Biometric device

168) Forcible entry or intrusion into the premises of an organization can be prevented by using
a. Security Guards
b. CCTV Cameras
c. Infra-red sensors
d. RF devices

169) For Intrusion detection _____ is/are used
a. CCTV cameras
b. Alarms
c. Both a and b
d. Radio Frequency Sensor

170) _____ standard is concerned with the Physical Security of Computer resources
a. ISO 45002
b. ISO 37002

c. ISO 1700
d. ISO 27002

171) The COBIT is an Acronym for
a. Control Operation for Information and Related Terminologies
b. Computer Organization and Information Related Technologies
c. Computer Operation for Information and Related Terminologies
d. Control Objectives for Information and Related Technologies

172) One of the following is not a criteria for selecting site location for Security
a. Construction and excavation
b. RF and wireless transmission interception
c. Lighting
d. Markets and Malls

173) One of the following does not comes under the duty of Security Guards
a. Prevention of forcible intrusion
b. Prevention of Theft
c. Repairing of faulty CCTV
d. Prevention of Abuse and Arson

174) Database security measures include authenticated users access to
a. data
b. Network
c. database
d. all of the above

175) -------- is the most secured method of centrally storing important and sensitive data
a. Relational databases
b. OLTP
C. server side databases
d. object level databases

176) central repositories are
a. data warehouse
b. does the data analysis and reporting
c. both a and b
d. only a

177) OLTP stands for
a. Online transaction processing
b. Online termination processing
c. online transaction precedence
d. online termination program

178) ----- Command specifies that a particular user or role will have access to perform specific action on database objects
a. REVOKE
b. GRANT
c.UPDATE
d. DENY

179) ------- command removes any current permission settings for the specified users or roles

a. REVOKE
b. GRANT
c.UPDATE
d. DENY

180) A ----- is a logical relational database object that actually refers to one or more underlying database tables
a. REVOKE
b. VIEW
c. SELECT
d. DENY

181) A trigger is a _____
a. stored procedure in a database
b. automatically invoked if a sepicific action takes place within a database
c. does not automatically invoked if a sepicific action takes place within a database
d. both a and b

182) "Database system requires Granular permissions"
The above statement is
a. True
b. False

183) ------ is the process of replicating stored data of database
a. database backup
b. database recovery
c.both a and b
d. none

184) In Transactional Log backups _____
a. data modified are written in log file and then copied to actual database
b.data modified are directly written into the actual database

185) If an unauthorized database transaction was performed at 4.00 p.m on Monday ,then the databse can be restored through which backup
A. differential backups
b. full backups
c. point- in time backups
d. transactional log backups

186) Database auditing means _____
a. keeping a log of data
b. data modification
c. usage of permissions
d. all of the above

187) When an employee record changes, corresponding changes can be easily made by calling
a. SQL commands
b. stored procedures
c. view query
d. nested query

188) The process of determining permission that are granted to a particular login is called as
a. authentication
b. validation
c. authorization
d. verification

189) Which is not a Fundamental storage infrastructure?
a. Storage networks
b. Arrays
c. Servers
d. Vectors

190) What is full form of LUNs?
a. logical unit numbers
b. linear unit numbers
c. linear uniary numbers
d. linear uniion numbers

191) _____ refers to the unauthorized interception of network traffic for the purpose of gaining information intentionally.
a. Packet Sniffing
b. Espionage
c. Packet Replay
d. Packet Spoofing

192) The alternative to port zoning, in which the zones are created relative to the ports the servers are connected to on the switch, is _____.
a. Arrays
b. Servers
c. WWN zoning,
d. Administration Channel

193) _____ is the risk of loss of information, such as confidential data and intellectual property, through intentional or unintentional means.
a. Data leakage
b. Theft
c. Exposure
d. Forwarding

194) Computer and storage failures that corrupt data , damage the integrity of that data is called _____.
a. Data Deletion
b. Data Loss
c. Data Corruption
d. Malfunctions

195) The most common cause of data integrity loss is _____.
a. Accidental Modification
b. Data Corruption
c. Data Deletion
d. Malfunctions

196) _____ is any unexpected downtime or unreachability of a computer system or network.
a. DOS
b. An Outage
c. DDos
d. Slowness

197) What is full form of NAS?
a. New-attached storage
b. New-available storage
c. Network-attached storage
d. Neutral attached storage

198) What is full form of SANs?
a. Service area networks
b. Storage area networks
c. Selected area networks
d. Single area networks

199) _____storage is composed of a storage device such as a NAS appliance or a storage array.
a. Permanent
b. Temporary
c. Secondary
d. Primary

200) Administration of the storage environment should be done through a network that is separate from the main _____network.
a. Corporate
b. Personal
c. Public
d. Protected

201) Using tools to capture network packets is called ,
a. Packet spoofing
b. Packet sniffing
c. Packet relay
d. Packet replay

202) _____ have the authority to bypass all security controls, and this can be used to intentionally or mistakenly compromise private data.
a. Users
b. Management
c. Administrators
d. Manger

203) _____may be perpetrated by outsiders but is usually committed by trusted employees.
a. Fraud
b. Crime
c. Misuse
d. Inception

204) _____ in the context of computing refers to the exploitation of a valid computer session.

a. Inception
b. Fraud
c. Crime
d. Hijacking

205) _____ is an attempt to trick a victim into disclosing personal information.
a. Spam
b. Phishing
c. Fraud
d. Hijacking

206) _____risks affect both the validity of information and the assurance that the information is correct.
a. Integrity
b. Availability
c. Confidentiality
d. Authority

207) Using tools to reproduce traffic and data that was previously sent on a network is called _____.
a. Packet spoofing
b. Packet sniffing
c. Packet replay
d. Packet relay

208) A denial of service (DoS) attack or distributed DoS (DDoS) attack is an attempt to make a computer resource _____to its intended users.
a. Unavailable
b. Available
c. Private
d. Public

209) The process of transforming plain text into unreadable text.
a. Decryption
b. Encryption
c. Network Security
d. Information Security

210) A process of making the encrypted text readable again.
a. Decryption
b. Encryption
c. Network Security
d. Information Security

211) A system for encryption and decrytion is called as_____
a. Cryptosystem
b. Decryption
c. Encryption
d. Security System

212) What is the minimum number of cryptographic keys required for secure two-way communications in symmetric key cryptography?

a. 1
b. 2
c. 3
d. 4

213) In _____Claude E. Shannon publishes an article called"A mathematical theory"
a. 1935
b. 1945
c. 1955
d. 1965

214) In _____ U.S adopted a block cipher design as national standard- Data Encryption Standard.
a. 1963
b. 1973
c. 1983
d. 1993

215) In _____, DES is replaced by the AES.
a. 1997
b. 1998
c. 1999
d. 2000

216) Symmtric key cryptography uses the _____ key for encryption and decryption.
a. same
b. different
c. fixed
d. variable

217) Which one of the following is a cryptographic goal that cannot be achieved by a secret key cryptosystem?
a. Nonrepudiation
b. Confidentiality
c. Availability
d. Integrity

219) Which one of the following cipher types operates on large pieces of a message rather than individual characters or bits of a message?
a. Stream cipher
b. Caesar cipher
c. Block cipher
d. ROT3 cipher

220) In which year Giovan Bellaso envisions the first cipher to use a proper encryption key ?
a. 1834
b. 1553
c. 1854
d. 1556

221) Who invented the Play fair Cipher, which encrypts pairs of letters instead of single ones?
a. Edward Hebern

b. Poland
c. Charles Wheatstone
d. IBM

222) What is the name of the group that IBM have formed in 1970's to design a block cipher to protect customer data?
a. Crypto Group
b. Stream Cipher Group
c. Block Cipher Group
d. Cipher Suites Group

223) Scrambling the data according to a secret key is known as?
a. Caesar Cipher
b. Decryption
c. Code cracking
d. Encryption

224) In encryption, the order of the letters in a message is rearranged by _____
a. substitution ciphers
b. quadratic ciphers
c. transpositional ciphers
d. both transpositional ciphers and substitution ciphers

225) What is the minimum number of keys required for secure two-way communications in symmetric key cryptography?
a. 1
b. 2
c. 3
d. 4

226) In asymmetric key cryptography, the private key is kept by _____
a. sender
b. receiver
c. sender and receiver
d. all the connected devices to the network

227) What is cipher?
a. both algorithm for performing encryption and decryption and encrypted message
b. encrypted message
c. decrypted message
d. algorithm for performing encryption and decryption

228) Which one of the following cipher types operates on large pieces of a message rather than individual characters or bits of a message?
a. Stream cipher
b. Caesar cipher
c. Block cipher
d. ROT3 cipher

229) The _____ is the original message before transformation.
a. ciphertext
b. plaintext

c. secrettext
d. simpletext

230) How many types of firewalls are there?
a)1
b)2
c)3
d)4

231) Which is that software installed using an internet connection as they come by-default with operating systems?
a) Hardware
b)Software
c) stateful Inspection firewall
d) Microsoft firewall

232) While entering or leaving the internal network,firewalls examine which of the following?
a) emails users
b) updates
c) connections
d) data packets

233) Which of the below defines the packet filtering firewall rules.
a) Access Control List
b) Protocols
c) Policies
d) Ports

234) Which port number is used to effectively manage the firewall?
a) 70
b) 71
c) 80
d) 72

235) Which address results in same address translation?
a) NAT
b) Static NAT
c) Dynamic NAT
d) PAT

236) Which of the following is used to filter, analyse and perform heuristic behavior detection to help the network security administrators?
a) UDP
b) ICMP
c) SIEM
d) DNS

237) Using which filtering methods, firewalls can subtract the spam from your email messages?
a) URL filtering
b) Web content filtering
c) application filtering
d) Email spam filtering

238) What actually generates the traffic on servers and workstations?
a) firewalls
b) Web content
c) applications
d) spam

239) Which layer of OSI model, packet filtering firewalls are implemented?
a) Application layer
b) Session layer
c) Presentation layer
d) Network layer

240) which is the following process does converting one IP address to another, and logging of traffic?
a)NAT
b)Static NAT
c)Dynamic NAT
d)PAT

241) A proxy firewall works at which layer?
a) Network Layer
b) Session layer
c) Presentation layer
d) Application layer

242) Which of the following involves submitting as many requests as possible to a single internet service, overloading it and preventing it servicing legitimate requests?
a) DOS attack
b)Masquareaing
c)phishing
d)Backdoor

243) What does IP mean?
a)Instance protocol
b)Internet protocol
c)Instant Protocol
d)Intellectual property

244) which of the following are types of firewall?
a)Packet filtering firewall
b)Dual homed network firewall

c)Screenhost firewall
d)Application filtering firewall

245) Network layer firewall has two sub-categories as _____
a. State full firewall and stateless firewall
b. Bit oriented firewall and byte oriented firewall
c. Frame firewall and packet firewall
d. Network layer firewall and session layer firewall

246) A proxy firewall filters at _____
a. Physical layer
b. Data link layer
c. Network layer
d. Application layer

247) If you have more than one computer connected in the home, it is important to protect every computer. You should have a ____firewall (such as a router) to protect your network:
a. Hardware
b. Software
c. HTML
d. None of these

248) A firewall needs to be _____ so that it can grow proportionally with the network that it protects.
a. Robust
b. Expensive
c. Fast
d. Scalable

249) The first reported type of network firewall is called a _____, which inspect packets transferred between computers.
a. packet filter
b. Content filter
c. Connection tracking
d. proxy

250) _____ firewalls do not just look at the metadata; they also look at the actual data transported.
a. Packet filtering
b. Application-layer
c. Stateful packet
d. Network Layer

251. 1 .Intrusion is action or process that compromises Authentication, integrity, availability of system

A. force fully

B. With Permission

C. Without Permission

D. Both A and C

252. What are the different types of intruder detection Model?

A. Host Based.

B. Network Based.

C.User Based.

D. Both B and A

253. In which approach use Network traffic for particular network segment analyses and detection of threats?

A. Host based IDS.

B. Network based IDS.

C. Profile based IDS.

D. Rule based detection.

254. For which IDS system is difficult to analyse the intrusion on multiple computers?

A**.** Host based IDS.

B. Network based IDS.

C. Profile based IDS.

D. Rule based detection.

255. IDS stand for?

A. Information Detection System

B. Intrusion Detection System

C. Institute Detection System

D. Image Detection System

256. Which file IDS use to record all detected events and these record use for analyzing and reporting purposes?

A. Exe File.

B. Log Files.

C. System File.

D. UB File.

257. Full Form of SIEM?

A. Security Information and Event Management.

B. Secure Internet and Environment Management.

C. System Interface and Event Management.

D. Serial interface and Event log Managements.

258.For Intrusion detection _____ is/are used

A. CCTV cameras

B. Alarms

C. Both a and b

D. Radio Frequency Sensor

259. The COBIT is an Acronym for

A. Control Operation for Information and Related Terminologies

B. Computer Organization and Information Related Technologies

C. Computer Operation for Information and Related Terminologies

D. Control Objectives for Information and Related Technologies

260. One of the following does not comes under the duty of Security Guards

A. Prevention of forcible intrusion

B. Prevention of Theft

C. Repairing of faulty CCTV

D. Prevention of Abuse and Arson

261. Security _____ is performed to find security issues by running application code.

A. Documentation

B. Monitoring

C. Testing

D. Modeling

262. Limiting the number of connections per second per IP address and use of strong passwords can prevent _____ attack.

A. Brute-force

B. SQL injection

C. Buffer overflow

D. Cookies

263. _____ is a technique to inject crafted SQL into user input fields that are the part of the web forms.

A. SQL injection

B. brute-force
C. buffer overflow
D. cookies

264. Bell-Lapadula model was revolutionary when it was published in

A. 1969
B. 1976
C. 1987
D. 1990

265. Biba is often know as a _____ version of Bell-Lapadula.4
A. reserved
B. reversed
C. revolutionary
D. pure