

Unit 1

1. The government security model was _____ and _____.
 - a)closed and locked
 - b)closed and open
 - c)open
 - d)none of the above

- 2.The three D's of security are _____,_____ and _____.
 - a)defense
 - b)detection
 - c)deterrence
 - d)demand

- 3.The security program components are _____ in number.
 - a)5
 - b)8
 - c)6
 - d)4

- 4.Policies , Standards , Guidelines are part of _____ security program components.
 - a)Authority
 - b)Framework
 - c) Assessment
 - d)Action

- 5._____ is a plan of action for how to implement the security remediation plans.
 - a) Project plan
 - b)Roadmap
 - c)Maintenance
 - d)Action

6. _____ is used to educate employees ,business partners , and other stakeholders.

- a)Security awareness program
- b) policy enforcement
- c) Project Plan
- d)Gap Analysis

7.An effective security strategy is comprehensive and _____.

- a)static
- b) fixed
- c)not known
- d)dynamic

8. _____ describe how processes are performed by people on an ongoing basis to produce the desired outcomes of the security program in a periodic ,reliable fashion.

- a)Procedure
- b)gap analysis
- c)planning
- d) roadmap

9. _____ controls on the network include audit trail, log files etc.

- a)defense
- b)detective
- c)deterrence
- d)direction

10.Defense controls on the network can include access control devices like firewall, anti-malware, web content filtering.

- a) defense
- b) detective
- c) deterrence
- d)direction

11.Deterrent controls can be implemented by using threat of discipline and termination for violations of policy.

- a) defense
- b)detective
- c) deterrence
- d)direction

12.A Threat is a potential attack or loop hole through which confidentiality is break.

- a)Threat
- b) Threat agent
- c)Threat vector
- d)Remote threat

13.It is a medium through which an exploit or threat is planned or attacked.

- a)Threat
- b)Threat agent
- c)Threat vector
- d)Remote threat

14.Physical damage defines damage due to fire breaks, pollution .

- a)physical damage
- b)deliberate type
- c) c)technical failures
- d)natural events

15. A Threat vector is a medium through which an attacker plants or initiates attack.

- a)Threat
- b) Threat agent
- c)Threat vector
- d)Remote threat

16.The various threat vectors are of the following type

- a)network,user,email,web application
- b) network,user,email, time
- c)date ,user, email, web application
- d)none of the above

17._____ is a computer program or code which is capable of replicating itself by modifying other computer programs.

- a)Virus
- b)Worms
- c)Trojans
- d) RAT

18._____ virus infects the master boot record.

- a)boot sector
- b)file infector
- c)Trojan
- d)worm

19._____ virus attached with program files such as .com,.exe.

- a)boot sector
- b)file infector
- c)Trojan
- d)worm

20.The _____ implants itself in the memory of a computer .

- a)boot sector
- b)file infector
- c)Trojan
- d)Resident Virus

21._____ arrives through email and spread as malicious executable files.

- a)boot sector
- b)file infector
- c)email worm
- d)Trojan

22.To carry out coordinated attacks _____are executed with the task.

- a)boot sector
- b)file infector
- c)bot worm
- d)Trojan

23._____ is a type of malware that is often disguised as legitimate software.

- a)boot sector
- b)file infector
- c)email worm
- d)Trojan

24._____ Trojan are usually downloaded with game or sent as an email attachment.

- a)boot sector
- b)file infector
- c)email worm
- d) Remote access

25._____ attacks flood the intended victim computer with traffic that legitimate connections are denied.

- a)email worms
- b)Trojan
- c)DDOS
- d)none of the above

26.The fullform of MITM IS _____

- a)mission in the man
- b)minutes in the minutes
- c)Man in the middle
- d)Map in the Term Machine

27._____ is used to map IP address to physical machine address.

- a)ARP
- b)RARP
- c)AIP
- d)OSPF

28.The two main approaches to risk analysis are _____.

- a)main and major
- b)qualitative and open
- c)quantitative and close
- d)qualitative and quantitative

29._____ defines how many times in a one-year interval the incident is expected to occur

- a)ARO
- b)AOR
- c)BOR
- d)ARP

30._____ is money expected to be lost if the incident occurs one time.

- a)SEL
- b)SLE
- c)OLE
- d)MLE

31.The fullform of CIA triad is

- a) Confidentiality , Integrity, Availability
- b)Confidentiality, Integrity, Action
- c)Confidentiality , interest, Availability
- d) connection, Integrity, Availability

32. _____ refers to allowing access to those who are authorized to do so.

- a)Confidentiality
- b)integrity
- c)Availability
- d)Access time

33.cryptography, two-factor authentication are used to achieve_____

- a)Confidentiality
- b)integrity
- c)Availability
- d)Access time

34. _____ refers to assurance that data has not been changed.

- a)Confidentiality
- b)integrity
- c)Availability
- d)Access time

35.Hashing algorithm and encryption are used to provide _____

- a)Confidentiality
- b)integrity
- c)Availability
- d)Access time

36._____ assures that the services are available whenever it is needed.

- a)Confidentiality
- b)integrity
- c)Availability
- d)Access time

37.The _____model is most common form of defense known as perimeter security.

- a)lollipop
- b)onion
- c)Potato
- d)Flower

38.the _____ model does not provide different levels of security required for asset.

- a)onion
- b)Potato
- c)Flower
- d) lollipop

39.The _____ provides layered strategy for security.

- a)onion
- b)Potato
- c)Flower
- d)lollipop

40.The _____ model is much harder to predict and penetrate.

- a)onion
- b)Potato
- c)Flower
- d) lollipop

41. _____ involves mapping ,prioritizing planning and resources in a ring of zones based on critical nature of the network resources.

- a)Zone of Trust
- b)Trust of Zone
- c)Zone of customer
- d)Zone of user

42.While designing best practices for network defense, The equipment housing the filling cabinets ,data wiring , laptops etc. must be _____ protected.

- a)physical
- b)logically
- c)no need to protect
- d)ethically

43. _____ booting provides additional security.

- a) Password protected
- b)user protected
- c)manager protected
- d)machine protected

44. _____ booting from USB storage devices stop attackers from bypassing operating system security.

- a) Disabling
- b)enabling
- c)additional
- d)extra

45._____ the operating system involves removing applications and devices that are unnecessary.

- a)softening
- b)hardening
- c)planning
- d)none of the above

46.A _____ is a program or hardware device that filters the information coming through the internet

- a)monitor
- b)printer
- c) firewall
- d)scanner

47.Encryption is method of converting _____into encoded version.

- a)known text
- b)real text
- c)rough text
- d) plain text

48.Sql injections and buffer overflow attacks can only be defeated by programmers using _____ coding practices.

- a)normal
- b)web
- c)Secure
- d)sensitive

49.Implementation of _____ ARP helps in reducing the ARP poisoning.

- a)Static
- b)dynamic
- c)serial
- d)numerical

50.full form of DHCP is _____

- a)dynamic host configuration protocol
- b)Density host configuration protocol
- c)Deep home combine protocol
- d)none of the above

51 .Which of the following is independent malicious program that need not any host program?

- a)Trap Doors
- b)Worm
- c)Trojan Hors
- d)Viruses

52.Which of the following malicious program do not replicate automatically?

- a)Trap Doors
- b)Worm
- c)Trojan Hors
- d)Viruses

53.In computer security, means that computer system assets can be modified only by authorized parties

- a)Confidentiality
- b)Integrity
- c)Availability
- d)Authenticity

54.You are never _____ percent secure.

- a)70
- b)80
- c)100
- d)90

55.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

56. _____ 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

57. _____ condition exists when a program attempts to put more data in a buffer than it can not hold

- a) buffer overflow
- b) buffer fill
- c) buffer overrun
- d) buffer full

58. _____ 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
- d) ARP cracking

59. Authentication is the process by which people prove they are who they say they are

- a) True
- b) false
- c) may be
- d) can't say

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

- a)Kerberos
- b)Railway
- c)SSL
- d)TLS

60. 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
- c)Not sure
- d)Not possible

61. A _____ algorithm simply replaces each character in a message with another character

- a)substitution
- b)transposition.
- c)cipher
- d)decipher

62. 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
- c)such model does not exist
- d)always possible

63. In _____ cryptography the same secret key is used by the sender and the receiver.

- a)symmetric-key
- b)asymmetric-key
- c)digital certificate
- d)digital signature

64. A _____ issues, catalogs, renews, and revokes certificates under the Management of a policy and administrative control.

- a)Certification authority
- b)Registration authority
- c)Revocation Authority
- d)Digital authority

65. _____ defines the protection against denial by one of the parties in a communication
- a) authentication
 - b) non repudiation
 - c) confidentiality
 - d) Integrity

Unit 2

66. _____ checks for user's identity
- a) Authorisation
 - b) Authentication
 - c) awareness
 - d) activeness

67. Authentication based on password is termed as _____
- a). single -factor authentication
 - b) two-factor authentication
 - c) multi-factor authentication
 - d) none of the above

68. When authentication based on user password and biometric factor it is termed as
- a). single -factor authentication
 - b) two-factor authentication
 - c) multi-factor authentication
 - d) none of the above

69. The full form of CHAP is
- a) Character Handshake Authentication Protocol
 - b) Challenge Hands Authentication protocol
 - c) Character Handshake Authentication Protocol
 - d) Challenge Handshake Authentication Protocol

70. One time pin is also termed as _____.

- a) one thread password
- b) one table password
- c) one time payment
- d) one time password

71. _____ use hardware or software-based authentication that generate a random seed based on the current time of the day.

- a) Time Based Keys
- b) Thread Based keys
- c) turn based key
- d) None of this

72. Full form for PKI is _____

- a) public key instance
- b) private key instance
- c) public key infrastructure
- d) permanent key instance

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

- a) CHAP
- b) MS-CHAP
- c) Kerberos
- d) LDAP

74. The full form of LDAP is _____

- a) Lightweight density Access protocol
- b) Lightweight dense Active Protocol
- c) Lightweight Directory Access protocol
- d) Lightweight Directory Active Protocol

75.The Certificates used for authentication are digitally signed by certificate authority called _____

- a)CA
- b)Manager
- c)Officer
- d)Lawyer

76._____ was developed to allow pluggable modules to be incorporated in an overall authentication process.

- a)Extended Authentication Protocol
- b)Extra Authentication Protocol
- c)Extensible Authentication Protocol
- d)Extensible Active Protocol

77._____ system includes use of Facial recognition

- a)Biometric
- b)password
- c)kerberos
- d)Certificate based authentication

78.Consider the following statement

- 1.Authentication establishes who the user is
- 2.Authorization specifies what the user can do

- a)statement 1 is true
- b)statement 2 is true
- c) both statement 1 and 2 are true
- d) both statement 1 and 2 are false

79.Consider the following statement

1.Authorization is a security mechanism used to determine user/client privileges

2.There are variety of authorization like user rights, role based and rule based authorization are available

a)statement 1 is true

b)statement 2 is true

c) both statement 1 and 2 are true

d) both statement 1 and 2 are false

80.User rights management involves

1.creating groups and roles

2.granting right ,privileges to access specific resources

3.Adding,Updating or deleting profiles, groups

All the three statement are true

Statement 1 is true

Statement 2 is true

Statement 3 is true

81.The three primary rules defined for RBAC are

a)Role assignment,Role authorization,permission authorization

b)Role authorization,permission authorization,role level

c)Role authorization,permission authorization,rule level

d)Role assignment,Role authorization,password

82.Consider the following statement

1The windows file system maintains ACL

2.Traditional Unix system do not use ACL

a)statement 1 is true

b)statement 2 is true

c) both statement 1 and 2 are true ----

d) both statement 1 and 2 are false

83. In Unix file permissions are assigned and they consist of three levels of access which are

- a) Owner, Group, and all others
- b) Owner, user, and others
- c) programmer, group, owner
- d) none of the above

84. Consider the following statement

1. Role based authorization is a special type of access control group that links to a set of tasks that a user or set of users can perform

2. Rule based authorization develops the rules that decide what a specific user can do on a system

- a) statement 1 is true
- b) statement 2 is true
- c) both statement 1 and 2 are true ----
- d) both statement 1 and 2 are false

85. The process of converting plain text to cipher text is called _____

- a) encryption
- b) decryption
- c) system
- d) hardware

86. The process of converting cipher text to plain text is

- a) encryption
- b) decryption
- c) system
- d) hardware

87. When the same key is used for encryption and decryption it is called as

- a) Symmetric key cryptography
- b) asymmetric key cryptography
- c) both a and b
- d) neither a nor b

88.when plain text is processed as one bit at a time then it is called

-
- a)block cipher
 - b)stream cipher
 - c)caesar cipher
 - d)modified caesar cipher

89.when plain text is processed in terms of block it is called block cipher

- a)block cipher
- b)stream cipher
- c)caesar cipher
- d)modified caesar cipher

90.Cryptography involves pair of keys is called public key cryptography.

- a)public key cryptography
- b)private key cryptography
- c)known cryptography
- d)unknown cryptography

91.If A and B wants to communicate then

- 1.A must be knowing his own public and private key and B's public key
- 2.A must be knowing his own public key and private key and B' private key

- a)statement 1 and 2 are true
- b)statement 1 is true
- c)statement 2 is true
- d)statement 1 and 2 false

92.consider the following statements

- 1.Root CA is the topmost Certificate Authority
- 2.Root CA have no certificate authority

- a)statement 1 and 2 are true
- b)statement 1 is true
- c)statement 2 is true
- d)statement 1 and 2 false

93. Certificates can be invoked in following situation

1. if employee leaves the organisation
 2. if employee is not happy with certificate
- a) statement 1 and 2 are true
 - b) statement 1 is true
 - c) statement 2 is true
 - d) statement 1 and 2 false

94. Consider the following statement

1. Version field in the digital certificate identifies the version of the certificate
 2. digital Certificate serial number is not unique identifier
- a) statement 1 and 2 are true
 - b) statement 1 is true
 - c) statement 2 is true
 - d) statement 1 and 2 false

95. consider the following statement

1. Electronic code Book is the simplest type where incoming message is divided into block of 64 bits which is encrypted separately
 2. Electronic code Book is the simplest type where incoming message is divided into block of 64 bits which is encrypted together
- a) statement 1 and 2 are true
 - b) statement 1 is true
 - c) statement 2 is true
 - d) statement 1 and 2 false

96. The full form of OLTP is Online transaction processing

- a) Open transaction processing
- b) Online transaction processing
- c) Online trust process
- d) Online transaction print

97.consider the following statement

1.Implement is the first step to create and implement a network security system

2.The other steps are Analyze,test and modify.

a)statement 1 and 2 are true

b)statement 1 is true

c)statement 2 is true

d)statement 1 and 2 false

98.consider the following statement

1.Operating system security is the process of ensuring OS integrity, confidentiality, and availability.

2.in most platforms database and operating system are not at all connected with each other

a)statement 1 and 2 are true

b)statement 1 is true

c)statement 2 is true

d)statement 1 and 2 false

99.Consider the following statements

1.select command never used retrieve information from database.

2.delete command deletes attributes from table

a)statement 1 and 2 are true

b)statement 1 is true

c)statement 2 is true

d)statement 1 and 2 false

100. Consider the following statements

1. Grant commands specify that a particular user or role will have access to perform specific action

2. Grant command removes all permission from specific user.

a) statement 1 and 2 are true

b) statement 1 is true

c) statement 2 is true

d) statement 1 and 2 false

101. Consider the following statements

1. A view is a logical relational database object

2. Simple views can be defined as result of simple select query.

a) statement 1 and 2 are true

b) statement 1 is true

c) statement 2 is true

d) statement 1 and 2 false

102. The types of database backups are

a) full backup, incremental backups, differential backup, transactional backup

b) only full backup

c) only incremental backup

d) only transactional backup

103. In _____ a copy of all data to another set of media is done

a) full backups

b) incremental backups

c) differential backups

d) transactional log backups

104. an _____ operation will result in copying only the data that has changed since the last backup operation.

- a) full backups
- b) incremental backups
- c) differential backups
- d) transactional log backups

105. _____ contain only changes

- a) full backups
- b) incremental backups
- c) differential backups
- d) transactional log backups

106. Consider following statements

- 1. Full backups are done periodically
- 2. Full backups take smaller time to perform as compared to other types.

- a) statement 1 and 2 are true
- b) statement 1 is true
- c) statement 2 is true
- d) statement 1 and 2 false

107. consider the following statement

- 1. regular back up is most important step of server maintenance
- 2. An upgrade and patch will help you to keep your servers safe from malicious attacks.

- a) statement 1 and 2 are true
- b) statement 1 is true
- c) statement 2 is true
- d) statement 1 and 2 false

108. Full form of VPN

- a) Virtual private network
- b) Various Private network
- c) Virtual public network
- d) Virtual Perfect network

109.full form of DMZ

- a)distributed military zone
- b)Demilitarized zone
- c)dedicated many zone
- d)dedicated military zone

110.consider the following statement

1.A firewall is used to separate the inside network from the outside network

2.outside networks are stated as private networks

- a)statement 1 and 2 are true
- b)statement 1 is true
- c)statement 2 is true
- d)statement 1 and 2 false

Unit 3

111.Which among them has the strongest wireless security?

- a)WEP
- b)WPA
- c)WPA2
- d)WPA3

112.A _____ operates in both the physical and the data link layer.

- a)passive hub
- b)repeater
- c)bridge
- d)router

113. Network layer firewall works as a _____

- a)Frame filter
- b)Packet filter
- c)Content filter
- d)Virus filter

114. _____ is the central node of 802.11 wireless operations.

- a)WPA
- b)Access Point
- c)WAP
- d)Access Port

115.Which of the following tasks is not done by data link layer?

- a)framing
- b)error control
- c)flow control
- d)channel coding

116.Which of the following is not the Networking Devices?

- a)Gateways
- b)Linux
- c)Routers
- d)Firewalls

117. Packet-switched networks can also be divided into _____ subcategories: virtual-circuit networks and datagram networks.

- a)five
- b)three
- c)two
- d)four

118 AP is abbreviated as _____

- a)Access Point
- b)Access Port
- c)Access Position
- d)Accessing Port

119. A proxy firewall filters at _____

- a)Physical layer
- b)Data link layer
- c)Network layer or Transport layer
- d)Application layer

120.Which of the following is a valid extended IP access list?

- a)access-list 102 permit ip host 164.42.20.0 any eq 80
- b)access-list 102 permit ip host 164.42.20.0 any eq www
- c)access-list 102 permit tcp host 164.42.20.0 any eq 80
- d)access-list 102 permit icmp host 164.42.20.0 any eq www

121.ACL stands for _____

- a)Access Condition List
- b)Anti-Control List
- c)Access Control Logs
- d)Access Control List

122.Which of the following is not a software firewall?

- a)Windows Firewall
- b)Outpost Firewall Pro
- c)Endian Firewall
- d)Linksys Firewall

123.CRC stands for _____

- a)cyclic redundancy check
- b)code repeat check
- c)code redundancy check
- d)cyclic repeat check

124. Packet filtering firewalls are deployed on _____

- a)routers
- b)switches
- c)hubs
- d)repeaters

125. _____ is actually a multiport repeater. It is normally used to create connections between stations in a physical star topology.

- a) An active hub
- b) passive hub
- c) either (a) or (b)
- d) neither (a) nor (b)

126. There are _____ types of wireless authentication modes.

- a) 2
- b) 3
- c) 4
- d) 5

127. Specifications for a wireless LAN are called

- a) Standard 802.3z
- b) Standard 802.3u
- c) Project 802.3
- d) IEEE 802.11

128. Wireless LANs implement security measures in the

- a) System Layers.
- b) Data Link Layers.
- c) Sub Layers.
- d) Multi Layers.

129. Firewall examines each _____ that are entering or leaving the internal network.

- a) emails users
- b) updates
- c) connections
- d) data packets

130.A _____ forwards every frame; it has no filtering capability.

- a)passive hub
- b)repeater
- c)bridge
- d)router

131.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

132.In _____, resources are allocated on demand.

- a)circuit switching
- b)datagram switching
- c)frame switching
- d)packet switching

133.Internet Control Message Protocol (ICMP) has been designed to compensate _____

- a)Error-reporting
- b)Error-correction
- c)Host and management queries
- d)All of the mentioned

134. Firewall needs to be _____ so that it can grow proportionally with the network that it protects.

- a)Robust
- b)Expansive
- c)Fast
- d)Scalable

135. To use a Simple Network Management System, we need _____

- a)Servers
- b)IP
- c)Protocols
- d)Rules

136.In the _____ layer of OSI model, packet filtering firewalls are implemented.

- a)Application layer
- b)Session layer
- c)Presentation layer
- d)Network layer

137.Firewalls can be of _____ kinds.

- a)1
- b)2
- c)3
- d)4

Unit V

138.Fullform of IaaS is Infrastructure as a service

- a)infrastructure as a service
- b)investment as a service
- c)infrastructure as a system
- d)investment as a system

139.Read the following statement

1.IaaS provides basic storage,computing capabilities

2.It also provides standard services like storage,database management

- a)statement 1 and 2 are true
- b)statement 1 is true
- c)statement 2 is true
- d)statement 1 and 2 false

140.read the statement

1.Paas provides platform to design and develop software application

2.It provides predefined combination of os and application server

a)statement 1 and 2 are true

b)statement 1 is true

c)statement 2 is true

d)statement 1 and 2 false

141.consider the following statement

1.Saas provides software applications on a subscription basic over the internet

2.It is not offered by Sales force

a)statement 1 and 2 are true

b)statement 1 is true

c)statement 2 is true

d)statement 1 and 2 false

142.Consider the following benefits of cloud computing

1.It is possible to monitor central data.

2.A dedicated forensic server can be built in the same cloud

3.The implementation of updates and patches becomes easier.

a)statement 1 , 2 and 3 are true

b)statement 1 is true

c)statement 2 is true

d)statement 3 is true

143.Consider the following Remediation for cloud are

1.Cloud services are restricted by government regulations

2.PCI compliance specifies exactly where and on what physical server the data resides.

a)statement 1 and 2 are true

b)statement 1 is true

c)statement 2 is true

d)statement 1 and 2 false

144. Consider the various security issues in cloud computing

1. The threat against information assets residing in cloud computing environment
 2. The types of attackers and their capability of attacking the computing environments
 3. Emerging cloud security risks
- a) statement 1, 2 and 3 are true
 - b) statement 1, 2 are true
 - c) statement 2, 3 are true
 - d) statement 1 and 2 false and 3 true

145. The different threats that will effect the confidentiality are Insider user threat, External attacker threat and data leakage

- a) entire statement is true
- b) only insider threat is correct
- c) entire statement is false
- d) only data leakage is true

146. The different threats that will affect the integrity of data are data segregation, User Access, Data quality

- a) entire statement is true
- b) only data segregation is correct
- c) entire statement is false
- d) only data quality is true

147. The different threats that will affect the availability of data are change management, Denial of service threat, physical disruption, exploiting weak recovery procedures.

- a) entire statement is true
- b) entire statement is false
- c) only change management is true
- d) only denial of service is true

148. For security Training we can say that

1. It is prerequisite for implementing the SDL.

2. It aims in the development of an individual

- a) statement 1,2 are true
- b) statement 1 is true and 2 is false
- c) statement 2 is true and 1 is false
- d) both statements are false

149. Consider following statement for application security practices

1. Secure design helps in minimizing the schedule disruption risk

2. Threat modelling techniques applied to threat scenarios which helps a team to identify risk

- a) statement 1,2 are true
- b) statement 1 is true and 2 is false
- c) statement 2 is true and 1 is false
- d) both statements are false

150. Consider following statement for application security practices

1. Secure coding uses approved tools to provide scalable security code methods

2. For security code Review, static analysis tools are used for verification of the code against code standards

- a) statement 1,2 are true
- b) statement 1 is true and 2 is false
- c) statement 2 is true and 1 is false
- d) both statements are false

151.Consider following statement for application security practices

1.Security Release Management aims in creating incident response plan,conducting final security review

2.Product security Incident Response includes contacting people for verifying and diagnosing the issue and fixing them

- a)statement 1,2 are true
- b)statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

152.Consider the following statements

1.Web application security is the process of guarding websites.

2.The target for web application attacks are content management system,database administration tools and Saas applications

- a)statement 1,2 are true
- b)statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

153.Consider following statements with respect to web application security

1.SQL injection occurs when an agent uses malicious SQL code to manipulate a backend database

2.An attacker could fool the application into executing unintended commands

- a)statement 1,2 are true
- b)statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

154.Consider following statements with respect to web application security

Cross site scripting is allowing execution of scripts in the victim's browser thus user session can be hijacked

2.It is caused by the improper validation of user supplied data

- a)statement 1,2 are true
- statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

155.Consider following statements with respect to web application security

1.Malicious File Execution can affect PHP, XML ,any framework that accepts filenames or files from user

2.Cross-site Request Forgery results in an unsought transfer of funds, changed passwords or data theft

- a)statement 1,2 are true
- b)statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

156.Consider following statements with respect to Client Application security

1.It is controlled by the developer of the application

2.Developing a secure application with multiple factors requires deep knowledge

- a)statement 1,2 are true
- b)statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

157.Consider following statements with respect to Client application security

1.An administrator can assign the privileges to run the application as low as possible

2.Applications can be administrated by text based files

- a)statement 1,2 are true
- b)statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

158.Consider following statements with respect to Client application security

1.OS security integration with application helps in importing and exporting real time list of users

2.Applications needs to be updated with the latest release and security patches to maintain authenticity

- a)statement 1,2 are true
- b)statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

159.Consider following statements with respect to Remote administration security

1.It allows system administrators to manage collection of machines from central location

2.an attacker can exploit them to issue unauthorised commands

- a)statement 1,2 are true
- b)statement 1 is true and 2 is false
- c)statement 2 is true and 1 is false
- d)both statements are false

160. There is need for remote administration due to reasons like

1. Relocated servers need administration.
 2. Outsourced services during remote access of the services
- a) statement 1, 2 are true
 - b) statement 1 is true and 2 is false
 - c) statement 2 is true and 1 is false
 - d) both statements are false

161. Advantages of remote web administration are as follows

1. A web interface can be accessed from all the major OSs by using browser.
 2. Web interface can be accessed from any location over the internet
- a) statement 1, 2 are true
 - b) statement 1 is true and 2 is false
 - c) statement 2 is true and 1 is false
 - d) both statements are false

162. Disadvantages of remote web administration are

- 1) Accessibility
 - 2) Browser control
 - 3) Support
- a) all three are true
 - b) only accessibility
 - c) only support
 - d) all options are false

163. The various methods for HTTP Authentication are

1. Basic Authentication
 2. Digest Authentication
 3. Captcha
 4. Encrypted basic authentication
- a) all options are correct
 - b) options 1 and 2 are true and 3 and 4 are false
 - c) options 2 and 3 are true and 1 and 4 are false

d)none of the options are true

164.This method is used to verify that the person accessing the system is a human being with the help of distorted image of letters and numbers

- a)captcha
- b)basic authentication
- c)ssl
- d)digest authentication

165.This authentication is required when browser responds with error code 401 while accessing the page

- a)captcha
- b)basic authentication
- c)ssl
- d)digest authentication

166.This authentication uses MD5 to hash the username and password.

- a)captcha
- b)basic authentication
- c)ssl
- d)digest authentication

167.Advantages of Custom Remote Administration are as follows

- 1.It is used to display complex graphics of the console application
- 2.The applications are not easily available for hacking as they may require the installation of third party software for un-authorize access

- a)statement 1and 2 are correct
- b)statement 1 is wrong and 2 is correct
- c)statement 1and 2 are wrong
- d)statement 2 is wrong and 1 is correct

168. Disadvantages of Custom Remote Administration are as follows

1. installation of platform specific operating system is required to control GUI which may include cost

2. The application monitoring can only be performed from computers on which the GUI is installed

- a) statement 1 and 2 are correct
- b) statement 1 is wrong and 2 is correct
- c) statement 1 and 2 are wrong
- d) statement 2 is wrong and 1 is correct

169. Consider the following statements with respect to Session security

1. Unauthorised access can be avoided if session established between client and application is secure

2. if session is insecure then it can be through VPN or SSH

- a) statement 1 and 2 are correct
- b) statement 1 is wrong and 2 is correct
- c) statement 1 and 2 are wrong
- d) statement 2 is wrong and 1 is correct

170. Servers, network attached storage, desktop, laptops are classified as

- a). Computer Equipment
- b). Assets with direct monetary value
- c). Communication equipment
- d) furniture and fixture

171. Routers, switches, firewalls, modems are classified as

- a) Computer Equipment
- b) Assets with direct monetary value
- c) Communication equipment
- d) furniture and fixture

172. Power supplies, UPSs, power conditioners, Generators are classified as

- a) Computer Equipment
- b) Assets with direct monetary value
- c) Communication equipment
- d) Technical equipment

173. old storage devices, memory cards, micro-SD, Memory stick are classified as

- a) Computer Equipment-
- b) Assets with direct monetary value
- c) Storage media
- d) furniture and fixture

174. Racks, chairs, desk, hydraulic system are classified as

- a) Furniture and fixtures
- b) Assets with direct monetary value
- c) Communication equipment
- d) furniture and fixture

175. Cash, jewelry, bonds, cell phones are classified as

- a) Computer Equipment
- b) Assets with direct monetary value
- c) Communication equipment
- d) Assets with direct monetary value

176. Consider following statement with respect to physical vulnerability assessment

1. An asset must be classified and its value to an organisation must be quantified.
 2. A simple walk through must be performed as a starting point to identify potential areas of physical security negligence.
- a) statement 1 and 2 are correct
 - b) statement 1 is wrong and 2 is correct
 - c) statement 1 and 2 are wrong

d)statement 2 is wrong and 1 is correct

177.identify the area which is part of physical vulnerability assessment

- 1.Checking areas for obstruction
 - 2.looking for unlocked windows and doors
- a)buildings
 - b)Computing devices and peripherals
 - c)Documents
 - d)Records and Equipment

178.identify the area which is part of physical vulnerability assessment

- 1.Unattended systems should be logged of or have their screens locked
 - 2.Verify accessibility of systems and peripherals
- a)buildings
 - b)Computing devices and peripherals
 - c)Documents
 - d)Records and Equipment

179.identify the area which is part of physical vulnerability assessment

- 1.checking which confidential documents are not kept properly
 - 2.Documents in the trash or recycle bin must be shredded
- a)buildings
 - b)Computing devices and peripherals
 - c)Documents
 - d)Records and Equipment

180. identify the area which is part of physical vulnerability assessment

1. Make sure that records are locked up when not in use and accessible to authorised person

2. Equipments like faxes, printers, modems have their own security recommendations.

- a) buildings
- b) Computing devices and peripherals
- c) Documents
- d) Records and Equipment

181. Consider which of the following factors decides the significant risk

1. while choosing a location for data center survivability considered to be important than cost

2. site is in flood zone area or high crime area

- a) statement 1 and 2 are correct
- b) statement 1 and 2 are wrong
- c) statement 1 is correct and 2 is wrong
- d) statement 1 and 2 are wrong

182. Identify the security consideration for following

1. Selected office site is at remote location

2. you have to consider potential evacuation

- a) Accessibility
- b) proximity to other buildings
- c) lighting
- d) from the site

183. Identify the security consideration for following

1. poor lights can be avoided

2. lighting should be positioned properly

- a) Accessibility
- b) proximity to other buildings
- c) lighting
- d) from the site

184. identify the security consideration for following

1. distance from other buildings
 2. knowing neighbors
- a) Accessibility
 - b) proximity to other buildings
 - c) lighting
 - d) from the site

185. identify the security consideration for following

1. Test drive need to be conducted in the region with scanners
 2. use of encryption for sensitive traffic is necessary and mandatory
- a) Accessibility
 - b) RF and wireless Transmission Interception
 - c) lighting
 - d) from the site

186. identify the security consideration for following

1. For a data center loss of power supply can have serious impact
 2. UPSs and generators can supply power for some time but systems need to be cooled constantly
- a) Accessibility
 - b) RF and wireless Transmission Interception
 - c) lighting
 - d) Utilities Reliability

187. identify the security consideration for following

1. People in the vicinity must be asked about power/telecom outages
 2. take a look at past construction activities in the area
- a) Accessibility
 - b) RF and wireless Transmission Interception
 - c) Construction and evacuation
 - d) from the site

188. identify the factors user should consider while securing their assets

1. user should lock up the devices or valuables

2. educating asset owner for securing the items

- a) Locks
- b) Doors and file cabinets
- c) Laptops
- d) entry controls

189. Identify the factor to be considered while securing the asset

are 1. file cabinets containing sensitive information must be kept locked

2. the key for this is to be kept out of common reach and

- a) Locks
- b) Doors and file cabinets
- c) Laptops
- d) entry controls

190. Probable areas for placing CCTV are

- 1) High traffic areas
 - 2) Critical function areas
 - 3) Cash handling areas
 - 4) entry and exit point to the enclosure
- a) All four are correct
 - b) Options 1,2 are correct and 3,4 are wrong
 - c) Options 2,3 are correct and 1,4 are wrong
 - d) All options are wrong

191. Consider the following statement with respect to CCTV

1. Lighting in the area also play a critical role in the effectiveness of the camera capturing the footage.

2. For wireless CCTV setup, users should take into account that anything transmitted through airwaves is to be received.

- a) statements 1 and 2 are correct
- b) statement 1 is true and 2 is wrong
- c) statement 2 is true and 1 is wrong
- d) statement 1 and 2 are wrong

192. A _____ is an area designed to allow only one authorized individual entrance at any give time. These are typically used as an anti-tailgating mechanism- to prevent an unauthorised person from following the authorised person

- a) Mantrap
- b) Honey-trap
- c) Cold-trap
- d) hard-trap

193. The important thing any organisation must follow after hiring new employees is to provide them with new _____

- a) ID badges
- b) new uniform
- c) new laptop
- d) new car

194. Any employee without visible ID should never be challenged

- a) true
- b) false
- c) it will decide by security
- d) it is as per employees wish

195.As per the New York State Department Of Labor
Security guard's responsibilities include

- a)to patrol, guard, monitor
- b)to protect, preserve, support
- c)to maintain the security and safety
- d)All of the above

196.For entry control ,the most commonly deployed biometric technologies
are _____ and hand geometry devices

- a)Fingerprint
- b)password
- c)credit card
- d)debit card

197. While securing Laptops we must ensure that_____

- a). It should be physically locked to the desk
- b). must be kept in docking station
- c)cables locks must be used
- d)All the above

198.Switches work at layer _____ of OSI layer model.

- a)one
- b)two
- c)three
- d)four

199.Routers are identified as Layer _____ devices.

- a)one
- b)two
- c)three
- d)four

200. MAC address is _____ bits long.

- a) 32
- b) 128
- c) 64
- d) 48

201 to 205 identify the protocols and match the columns

Part A		Part B	
1	AS	a	Interior Gateway Protocol
2	IGP	b	Exterior Gateway Protocol
3	EGP	c	Autonomous System
4	OSPF	d	Intermediate System to Intermediate System
5	IS-IS	E	Open Shortest path First

- a) 1-c, 2-a, 3-b, 4-e, 5-d
- b) 1-a, 2-b, 3-c, 4-d, 5-e
- c) 1-e, 2-d, 3-c, 4-b, 5-a
- d) 1-b, 2-a, 3-c, 4-e, 5-d

206 to 210 identify the full forms and match the columns

PART A		PART B	
1	MAC	a	International Standard Organisation
2	TCP	b	Internet Protocol
3	UDP	c	User datagram protocol
4	IP	d	Transmission Control protocol
5	ISO	e	Media Access Control

- a)1-a,2-b,3-c,4-d,5-e
- b)1-b,2-c,3-d,4-e,5-a
- c)1-e,2-d,3-c,4-b,5-a
- d)1-e,2-b,3-c,4-d,5-a

211 to 215 Identify the protocol and match

PART A		PART B	
1	RIP	a	Interior Gateway Routing protocol
2	TFTP	b	Routing Information Protocol
3	ICMP	c	Trivial File Transfer protocol
4	SSH	d	Internet Control Message Protocol
5	IGRP	e	Secure Shell Protocol

- a)1-b,2-c,3-d,4-e,5-a
- b)1-e,2-d,3-c,4-b,5-a
- c)1-d,2-c,3-b,4-a,5-e
- d)1-b,2-c,3-d,4-a,5-e

216. _____ is Distance Vector Routing Protocol

- a)Ospf
- b)IS-IS
- c)BGP
- d)IGRP

217. _____ is Link State Routing protocol

- a)Ospf
- b)Rip
- c)BGP
- d)RIP

218.. _____ is Distance Vector Routing Protocol

- a)Ospf
- b)IS-IS
- c)BGP
- d)RIP

219. _____ is Link State Routing protocol

- a)IS-IS
- b)Rip
- c)BGP
- d)RIP

220, Functions of Routers are as follows

- 1.To connect different network segment
- 2.To access DSL services
- 3.To connect two different network architecture

- a)only statement 1 is correct
- b) only statement 3 is correct
- c) only statement 2 is correct
- d) All statements are correct