Sr No	Question	Option 1	Option 2	Option 3	Option 4	Correct Answer
1	What does CIA stand for?	Content,interface,Advancement	Confidentiality, Integrity,Availability	Content, Intervention, Agility	Compatibility, Integration, Ability	Confidentiality, Integrity,Availability
2	What is an important Asset in an organization?	Communication	Synergy	Information	Mobility	Information
3	Who is intended to see or use Information for internal use?	Students	General public, government officials	Teachers, PTA members	employees,contractors,service providers	employees,contractors,service providers
4	VPN stands for?	Virtual private network	Visually paired network	Vital prevention network	Virtual public network	Virtual private network
5	SaaS stands for?	Software as a setup	Software as a service	Softnet as a service	Signal as a service	Software as a service
6	PaaS Stands for?	Platform as a setup	Project as a service	Platform as a service	Projection as a software	Platform as a service
7	IaaS standd for?	Infrastructure as a Service	Infrastructure as a setup	Input as a setup	Infrastructure as a software	Infrastructure as a Service
8	Which attack doesn’t allow a person who is legitimate or authenticated and authorized to use a service?	Virus	BUGS	Trojan horse	Denial of service attack(dos)	Denial of service attack(dos)
9	What is Portability?	platforms or can be transmitted / transferred across.	Cannot be transmitted.	Cannot be used on multiple platofrms	Is at a fixed place and it cannot be transferred.	or can be transmitted / transferred across.
10	Which field is concerned with protecting assests in general?	Software	Security	Service	Platform	Security
11	Which type of Security is concerned with protecting data, hardware and software on a computer network?	Software security	Network Security	Mobile Security	Internet Security	Network Security
12	informationin all its form , whether written,spoken,electronic,graphical or using other methods of	Internal Security	Software security	Mobile Security	Information Security	Information Security
13	What is Deterrence?	event or action by instilling fear or doubt of the consequences.	Having no opinions at all	The action that leads to no consequences.	The action of encouraging everything.	event or action by instilling fear or doubt of the consequences.
14	What is Authority in building a security program?	everyone is denied all the services.	where authorization is not need.	which must include the right level of	level of responsibilty is not required.	include the right level of responsibilty and authorization to
15	What is a framework in building a security program?	Framework is an attack	provide a defensible approach to build a	required to build a security program.	defensible approach to build the security program.	approach to build the security program.
16	What is Assessment in building a security program ?	protected,why and how it leads to a strategy for improving the	Assessing the techniques.	required to build a security program.	Assessment is only for documentational purposes.	protected,why and how it leads to a strategy for improving the
17	What does Planning provide in building a security program?	Planning doesn't provde priorities or timilines.	producing priorities and timelines for security	Planning delays the tasks to be completed.	provide in building a security program	priorities and timelines for security initiatives.
18	What is the role of Action in building a security program?	produce the desired results based on the plans.	team donot produce the desirable results	donot follow the palns laid out.	No actions are taken in building a security program.	produce the desired results based on the plans.

19	What is Maintenance in building a security program?	Miantanance of secuirty program is optional	required by the security program.	that have reached the end stage is now to	maintenance structure laid out for a security program.	reached the end stage is now to maintain them.
20	Which plan defines the actions to be taken when a security event occurs?	Theft plan	Introduction plan	induction plan	Incident Response Plan	Incident Response Plan
21	partners and other stakeholders about the desired behaviour and the actions to be taken in various circumstances to comply	Security awareness program	Deterrence program	Theft program	Decision program	Security awareness program
22	What is threat vector?	No threats exists.	Where a threat can't be found.	and the path it takes to reach a target.	Where a Threat orginates and ends there.	Where a treat originates and the path it takes to reach a target.
23	What are Preventive controls?	Preventive controls donot block the vulnerability.	blocks the security threats before they can	block the security threat after they have	Preventive controls donot block the security threats.	security threats before they can exploit a vulnerability.
24	What are Recovery controls?	Restores the availability of the service	Denies the service.	Cannot use the services it restores.	Doesn't restore anything.	Restores the availability of the service
25	What is the life cycle of Malicious mobile code?	find,lost,repeat	fail, find,repeat	Find, Exploit, Infect, Repeat	lost,failed,exploit,repeat	Find, Exploit, Infect, Repeat
26	The three generally recognised variants of malicious mobile code are....	viruses,worms and trojans	bugs,defect,outage	outage,fail,bugs	main-in-the-middle,bugs,dos	viruses,worms and trojans
27	What are Trojans or Trojan horse pograms?	Self replicating	Depends on another code to infect	program and are activated by an	like man-in-the-middle attack	are activated by an unsuspecting user.
28	What Does APT stand for?	Advanced Performance threats	Adavanced Persistent Threats	Add-ons producing threats	Ad-hoc Performance threats	Adavanced Persistent Threats
29	What does Packet Sniffing do?	It doesn't allow the attacker to look at the transmitted content.	Does not reveal passwords and content.	Denial of service	the transmitted content and may reveal passwords and	transmitted content and may reveal passwords and confidential
30	What are content attcks?	The attacker floods the server with content.	the applications and then sniffs the information	which application is running on a particular	application is running on a particular server and then	application is running on a particular server and then sends
31	What is buffer Overflow?	program expecting input does not do input validation.	when a program expecting an input	when a program expecting an output	Buffer overflows occur when a program is expecting nothing.	program expecting input does not do input validation.
32	ARP Stands for....	Attacker resolution protocol	Address Result protocol	Attacker result protocol	Address Resolution Protocol	Address Resolution Protocol
33	How does ARP Poisoning work?	ARP Poisoining works by responding to the ARP packets.	responding to the ARP requests with Attackers	responding to the ARP requests with Attackers	responding to the ARP requests with systems port	responding to the ARP requests with Attackers MAC address.
34	What is the formal Definition of RISK?	is the probablity of an event that occurs.	the risk is the probablity of an undesired event to	the risk is the probablity of an undesired event to	risk is the probablity of an desired event to cause an	the probablity of an undesired event to cause an undesired result
35	What is the formal Definition of Risk?	of vulnerability) * Cost of the Asset damaged	Profit(Threat+theft) * Cost of the Asset	RISK= Loss(Threat+theft) * Cost of the Asset	Profit(vulnerabilityt+theft) * Asset	vulnerability) * Cost of the Asset damaged
36	What is Confidentiality?	Restriction to access for all the users.	No Restriction of access.	data only to those who are authorised to use it.	those who are not authorised to use it	to those who are authorised to use it.
37	What is Integrity?	been altered in an unauthorized way.	Assurance that the data has been altered.	modified and altered by an unauthorized user.	The data is not in use.	been altered in an unauthorized way.

38	What is Availability?	Assurance that the services are no longer in use.	services will never be needed.	services will be not be available when it's	will be available when it's needed.	Assurance that the services will be available when it's needed.
39	FTP stands for…..	file transmit protocol	File Transfer Protocol	folder transit protocol	Folder transfer protcol	File Transfer Protocol
40	SSH stands for…	Security shell	Secure hardware	Secure Shell or Secure Socket Shell	Secure socket hardware	Secure Shell or Secure Socket Shell
41	What is Port Rate Limiting?	through a port is monitored during a given length of time, if	passing through a port is halted.	passing is stopped and dropped.	through a port is not monitored.	through a port is monitored during a given length of time, if the
42	DHCP stands for..	Dynamic Host Configuration protocol	Domain Host Configuration protocol	Dynamic Host Conflict protocol	Data Host Configuration protocol	Dynamic Host Configuration protocol
43	DNS stand for…	Dynamic network system	Data name system	Dynamic name system	Domain Name System	Domain Name System
44	What is Encryption?	Process of encoding information	Process of analyzing information	Process of decoding information	Caligraphy	Process of encoding information
45	What is Decryption?	Process of encoding information	Process of analyzing information	Process of decoding information	Caligraphy	Process of decoding information
46	BIOS stands for…	Basic input system	Basic output System	Basic input/output system	Basic input Server	Basic input/output system
47	What is an Alternative term for Onion Model?	Defense in depth	Dynamic defense	Defense in Domain	Domain in defense	Defense in depth
48	What is perimeter security?	physical wall around objects of no importance.	or physical wall around no objects	virtual or physical wall around objects of value.	physical wall around objects of no great value	physical wall around objects of value.
49	What are the laws that cover network intrusions that results in theft,fraud or damage are referred as?	Public laws	Hacking laws	Private laws	Key laws	Hacking Laws
50	What is Uptime?	The assurance that the service has expired.	service will be available when it's needed.	service will not be available.	will be available when it's not needed.	The assurance that the service will be available when it's needed.

Sr No	Question	Option 1	Option 2	Option 3	Option 4	Correct Answer
1	_____ mechanism determines the user's identity before revealing the sensitive Information.	Authorization	Authentication	Encryption	Availability	Authentication
2	In _____ process,the user makes a provable claim about individual identity or an entity's identity.	Authentication	Encryption	Availability	Authorization	Authentication
3	In _____ ,The credentials or claim could be a username, password, finger etc.	Encryption	Authorization	Authentication	Encryption	Authentication
4	The inefficient _____ mechanism could significantly affect the availability of the service.	Availability	Authentication	Encryption	Authorization	Authentication

5	An intruder may intercept, modify and replay the document in order trick or steal the information this type of attack is called as _____.	Intergrity	Denial of Service	Man-in-the middle	Fabrication	Fabrication
6	The mechanism to ensures that the sender and receiver are righteous people is known as _____.	Data-origin authentication	Peer entity authentication	Fabrication	Cryptography	Data-origin authentication
7	The mechanism to ensures the security of the established connection between sender and receiver with the help of secret session key is known as _____.	Cryptography	Data-origin authentication	Peer entity authentication	Fabrication	Peer entity authentication
8	Attackers who are able to access to the _____ file for a system can use brute force attacks against the hashed passwords.	Data	Password	Virtual	Authentication	Password

9	Attackers who are able to access to the password file for a system can use _____ attacks against the hashed passwords.	Denial-of-service	Brute force	Man-in-the middle	Non-repudiation	Brute force
10	_____ authentication requires that a user provide a second authentication factor in addition to the password.	Two-factor	Three-factor	Biometric	Mobile	Two-factor
11	Select incorrect type of biometric authentication from the giveen list of options.	Fingerprint scan	Retina scan	Security token	Voice recognition	Security token
12	Select correct type of possession factor from the given list of options.	Fingerprint scan	Security Token	Password	biometric	Security Token

13	Select correct type of knowledge factor from the given list of options.	Security Token	Biometric	password	Security key	Password
14	_____ is an automatically generated numeric or alphanumeric string of characters that authenticates a uset.	Security Token	One-time password	Security key	Pin	One-time password
15	_____ authentication is the process of verifying user via their devices or verifying the devices themselves.	Two-factor	Three-factor	Mobile	Continuous	Mobile
16	In _____ authentication, a company's application continually computes an authentication score.	Two-factor	Mobile	Continuous	Three-factor	Continuous

17	In _____ authentication, the server requests authentication Information i.e. a username and password from the client.	API Key	Mobile	HTTP basic	one-time password	HTTP basic
18	In _____ authentication method, a first-time user is assigned a unique generated value that indicates thet the user is known.	HTTP basic	API key	OAuth	Mobile	API key
19	_____ is an open standard for Token-based authentication and authorization on the internet.	HTTP basic	Open authorization	API key	one-time password	Open authorization
20	The _____ protocol is used for secure remote login from one computer to another	FTP	HTTP	SSH	POP	SSH

21	____ protocol protects the communication security and integrity with strong encryption.	SSH	HTTP	FTP	POP	SSH
22	_____ technique is used to determine the permissions that are granted to an authenticated user.	Authentication	Authorization	Availability	Confidentiality	Authorization
23	The identity of a person is assured by _____.	Encryption	Authentication	Authorization	Face	Authentication
24	_____ checks the access list that the authenticated person has.	Service	Authorization	Authentication	Management	Authorization

25	_____ is the method by which plaintext is converted from a readable form to an encoded version.	Encryption	Decryption	Fabrication	Integrity	Encryption
26	_____ is a method of protecting Information and communications through the use of codes so that only those for whom the information is intended can read and process it.	Cryptography	Confidentiality	Availability	Encoding	Cryptography
27	In _____ encryption, different keys are used for encryption and decryption.	Symmetric key	Digital signature	Public key	Digital certificate	Public key
28	_____ consists of software and hardware elements that a trusted third party can use to establish the integrity and ownership of a public key.	Digital signature	Public key infrastructure	Digital certificate	Encryption	Public key infrastructure

29	____ signs the digital certificate by using its private key.	Cryptographer	Certification Authority	Sender	Receiver	Certification Authority
30	NAS stands for Network-_____ Storage.	Area	Attack	Attached	Administrative	Attached
31	SAN stands for _____ Area Networks.	Secure	Storage	Symmetric	Service	Storage
32	_____ refers to limiting Information access and disclosure to only authorized users as well as preventing access by or disclosure to unauthorised ones.	Confidentiality	Integrity	Availability	Authenticity	Confidentiality

33	_____ is the risk of loss of Information such as confidential data and intellectual property through intentional or unintentional means.	Espionage	Inappropriate administrator access	Data leakage	Fraud	Data leakage
34	_____ refers to the unauthorized interception of network traffic for the purpose of gaining Information intentionally	Exposure	Fraud	Espionage	Hijacking	Espionage
35	An _____ system can help to identify anomalous behaviour on the network that may indicate unauthorized access.	Intrusion Prevention	Intrusion Detection	Password authentication	Data Storage	Intrusion Detection
36	A person who illegally gains access to Information they are not authorized to access commits _____.	Hijacking	Fraud	Damage	Phishing	Fraud

37	_____ refers to the exploitation of a valid computer session to gain unauthorized access to Information or service in a computer system.	Fraud	Data leakage	Hijacking	Phishing	Hijacking
38	_____ is an attempt to trick a victim into disclosing personal information.	Fraud	Data leakage	Phishing	Hijacking	Phishing
39	____ risks affect validity of Information and the assurance that the information is correct.	Authentication	Integrity	Confidentiality	Availability	Integrity
40	___ occurs either when a user intentionally makes changes to data but makes the changes to the wrong dat or when a user inputs data incorrectly.	Data leakage	Fraud	Accidental modification	Denial-of-service	Accidental modification

41	_____ ie a characteristic of a system, which aims to ensure an agreed level of operational performance.	Integrity	Confidentiality	High availability	Authenticity	High availability
42	_____ attack is an attempt to make a computer resource unavailable to its intended users.	Brute force	Man-in-the middle	Denial-of-service	Data leakage	Denial-of-service
43	_____ is any unexpected downtime or unreachability of a computer system or network.	Data leakage	Outage	Fraud	Espionage	Outage
44	____ means when the response time of a computer or network is considered unacceptably slow.	Fraud	Slowness	Espionage	Data leakage	Slowness

45	_____ improves security through control of the connections between hosts and the storage array	Array	Server	Zoning	Offsite data storage	Zoning
46	_____ security allows you to limit the number of database accounts.	Password	Storage	Application	Network	Application
47	_____ backup consists of making a complete copy of all of the data in a database.	Differential	Full	Transaction log	Incremental	Full
48	____ backup consists of copying all of tje data that has changed since the last full backup.	Differential	Full	Transaction log	Incremental	Differential

49	_____ is a protocol for authenticating service requests between trusted hosts across an untrusted network such as the internet.	HTTP	SSH	Kerberos	FTP	Kerberos
50	The infrastructure used to support certificates in an organization is called as _____.	Public Key Infrastructure	Public Key architecture	Public Key Interface	Private Key Encryption	Public Key Infrastructure
51	_____ 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.	Transport Layer Security	Secure Socket Layer	Digital certificate	Kerberos	Secure Socket Layer
52	____ security mechanism used to authenticate and provide access to a facility or system based on the automatic and instant verification of an individual's physical characteristics.	Tansport layer	Password	Biometric	Secure Socket layer	Biometric

53	_____ management is security feature controlling which resources a user can access and what actions a user can perform on those resources.	Role-based Authorization	User rights	Data Storage	Risk	User rights
54	____ is a table that tells a computer operating system which access rights each user has to a particular system object such as a file directory or individual file.	Access Control List	Role based Authorization model	Digital certificate	Kerberos	Access Control List
55	____ authorization requires the development of rules that stipulate what a specific user can do on a system.	Role-based	Password-based	Rule-based	Certificate-based	Rule-based
56	____ is the mechanism an array uses to present its storage to a host operating system.	Serial Number	Packet number	Logical unit number	certificate id	Logical unit number

57	In ____ zoning the accessibility of the host to the LUNs is defined by the switch port.	Port	World Wide Name	Array	Secure Socket layer	Port
58	In network-level security, which is the first step to protect your network from the attack?	Analyze	Implement	Modify	Test	Implement
59	Which is not the layer of Cisco Hierarchical Internetworking model?	Core	Control	Distribution	Access	Control
60	____ networks are stated as the external or public networks.	Inside	Outside	Demilitarized zone	Intranet	Outside

61	____zone is made up of one or more isolated LAN networks that contain shared server resources such as web,DNS and e-mail servers.	Port	World Wide Name	Demilitarized	Intranet	Demilitarized

SR NO	SIC Question Bank Unit 3	OPTION A	OPTION B	OPTION C	OPTION D	CORRECT ANS.
1	PSTN stand for what ?	Private Switched Telephone Network	Public Switched Telephone Network	Private Switched Transmissio n Network	Public Switched Transport Network	B
2	The main layer of The Cisco Hierarchical Internetworking model.	Distribution	Core	Access	Performance	B
	What is VTP ?	Virtual terminal protocol	Virtual transfer protocol	Varient terminal protocol	Virtual tapping protocol	
3	Virtual terminal protocol supports which layer?	Application	Physical	Data link	Presentation	A
4	Controlling access to network by analyzing incoming and outgoing packets is called as	IP Filtering	Data Filtering	Packet Filtering	Firewall Filtering	C
5	TCP/IP previously used by which agency?	DECNET	bISO-NET	DECNET	ARPANET	D
6	As the data packet moves from the upper to the lower layers, what happens to the headers ?	Rearranged	Removed	Added	Modified	C
7	Data Link Layer filters _____ when works as firewall?	Frame filter	Packet filter	Content filter	Virus filter	A
8	What types of protocols are used in VPNs?	Application level protocols	Tunnelling protocols	Network protocols	Mailing protocols	B

9	Intranet is a tool for sharing information throughout what type of organisation ?	single organization	multiple organizations	multilevel organization	connected organizations	A
10	Which Network media type that is used ?	internet	token ring	html	extranet	B
11	Network Topology is which type of layout and connection of network hardware?	logical	physical	dependent	connected	B
12	In networking firewall , which systems are used for controlling traffic movement around the network?	authorized	authentication	autogenerated	automatic	B
14	Who provides an isolated tunnel across a public network for sending and receiving data privately as if the computing devices were directly connected to the private network.	Visual Private Network	Virtual Protocol Network	Virtual Protocol Networking	Virtual Private Network	D
15	Which are the two sub categories of Network layer firewall ?	State full firewall and stateless firewall	Bit oriented firewall and byte oriented firewall	Frame firewall and packet firewall	Network layer firewall and session layer firewall	A
16	Which of the following is / are the types of firewall?	Packet Filtering Firewall	Dual Homed Gateway Firewall	Screen Host Firewall	Dual Host Firewall	A
17	A proxy firewall filters at which layer ?	Physical layer	Data link layer	Network layer	Application layer	D
18	A packet filter firewall filters at which layer ?	Physical layer	Data link layer	Network layer or Transport layer	Application layer	C

19	Firewalls are used to protect:	Home Networks	Corporate Networks	Public networks	Both Home & Corporate	D
20	What is the full form of NAT ?	Network Address Translation	Network Address Transformation	Network Access Translation	Network Access Transformation	A
21	All memory units are expressed as powers of ?	2	5	10	20	A
22	Firewall is a type of ?	Virus	Security	Worm	Trojan Horse	B
23	How many types of Firewalls are there ?	1	2	3	4	C
24	Network layer firewall works as a which type of filter ?	Frame filter	Packet filter	Content filter	Virus filter	B
25	Which server effectively hides the true network addresses ?	proxy	Packet filter	Content filter	Application Gateway	A
26	The first reported type of network firewall , which inspect packets transferred between computers ?	packet filter	Content filter	Connection tracking[edit]	proxy	A
27	Data travels on the internet in small pieces; these are called ?	metadata	packets	Protocols	Virus filter	B
28	Which firewalls do not just look at the metadata; they also look at the actual data transported?	Packet filtering	Application-layer	Stateful packet	Network Layer	B
29	What WLAN device provides communications management services to wireless workstations?	Antenna	Network adapter	Repeater	Access point	D

30	DSSS system spreads the baseband signal by performing what to the baseband pulses with a pseudo noise sequence.	Adding	Subtracting	Multiplying	Dividing	C
31	Frequency hopping involves a periodic change of transmission in which features ?	Signal	Frequency	Phase	Amplitude	B
32	Which family of wireless LAN protocols, collectively known as Wi-Fi and commonly found in many organizations and households?	802.11	803	801	804	A
33	What must be installed and designed in such a way as to encompass your premises' territory and minimize outside signal leakage as much as possible?	LAN	VPN	ETHERNET	WLAN	D
34	As such, Bluetooth is very resistant to which interference unless the interfering signal covers the whole middle ISM band?	microwave	radio	infrared	media	B

35	Full form of WECA is ?	Wireless Ethernet Compatibility Alliance	Wired Ethernet Compatibility Alliance	Wireless Ethernet Collision Allocation	Wired Ethernet Collision Alliance	A
36	Which range of networks uses DSSS?	802.11	802.15	803	both b & c	A
37	Which way is correct to control your wireless signal spread ?	Antenna positioning	Order	sequence	transmitting power	A
38	A radio transceiver can only transmit or receive at a given time on a given frequency, all	full duplex	simplex	half duplex	complex	C
39	To send a packet, the source should know the which of the following addresses ?	MAC Address	IP address	DNS	Both IP address and MAC Address	D
40	The protocol used to find the IP address when Mac address is given is?	RARP	ARP	DNS	IP	B
41	Which connection less protocol used in transport layer in OSI reference model ?	TCP	UDP	IP	RARP	B
42	The dumb device used to provide solution to connectivity in network is which one ?	hub	switch	modem	cables	A
43	The device that operates at layer 3 of the OSI reference model is ?	hubs	switch	modem	Routers	D

44	Which of these is a routing protocol ?	Internet protocol	Hyper text transfer protocol	Border Gateway protocol	User datagram protocol	C
45	Which of these are the updates released by the product vendor which should be applied in a timely manner?	Patches	Updates	Instants	Data	A
46	Web interface accessed by a browser can be monitored by whom ?	Secure Shell Protocol	Diagnostic Services	SNMP	Network Protocol	C
47	What does AAA stands for ?	Accessing, Authorization, Accounting	Accounting Amending, Authorization	Authorization , Accounting, Accessing	Authentication, Authorization, Accounting	D
48	Which of these is the component that determines if an incoming connection is allowed?	Accounting	Accessing	Authenticatio n	Authorization	C
49	Which one is an attempt to slip through the external defenses by masquerading as an internal host ?	Sniffing	Address spoofing	Trojan horse	Worms	B
50	ICMP works in which layer of the OSI reference model	Network layer	Transport layer	Session layer	Data link layer	B

Sr. No	Question	Option 1	Option 2	Option 3	Option 4	Correct Answer
1	_____ are unauthorized activity with malicious intent using specially crafted code or techniques	Attacks	hacking	virus	pipping	1
2	_____ can be classified as attacks or misuse, and they can exploit network protocols or work as malicious content at the application layer	rule break	protocols	Threats	roles	3
3	What is DoS stands for	Defense of Service	Denial of service	Duty of service	delay of service	2
4	_____ is the process of monitoring for and identifying specific malicious traffic	traffic controller	intrusion controller	traffic detection	Intrusion detection (ID)	4
5	(SNMP) means _____	Simple Network Management Protocol	simple net management protocol	sample network management protocol	simple net manage protocol	1
6	(MTU) stands for _____	minimum transmission unit	maximum transmission unit	media transmission unit	maximum transformation unit	2
7	Although _____ protocol attacks abound, most security threats exploit the host's application layer	internet protocol	hyper text	network	transmission control	3
8	A _____ comparison is done between the payload and each potential threat signature in the IDS's database	bit - by - bit	byte - by - bit	bit - by - byte	byte-by-byte	4
9	_____ excel at catching known, definitive malicious attacks	Intrusion detection (ID)	traffic controller	intrusion controller	traffic detection	1
10	There are _____ types of generation Intrusion detection (ID)	2	3	4	5	1
11	_____ IDSs focused almost exclusively on the benefit of early warning resulting from accurate detection.	First-generation	Second-generation	Third-generation	Fourth-generation	1
12	A _____ is installed on the host it is intended to monitor	Home based Ids	host-based IDS (HIDS)	Hetero based Ids	Homo based Ids	2
13	(HIDS) stands for _____	Home based Ids	Hetero based Ids	Host-based IDS	Homo based Ids	3
14	A file-integrity HIDS also sometimes called as _____	protocol	router	firewall	snapshot	4

15	_____- are the most popular IDSs, and they work by capturing and analyzing network packets speeding by on the wire	Network-based IDSs (NIDSs)	Net-based IDSs (NIDSs)	NetProtocol-based IDSs (NIDSs)	Network-by IDSs (NIDSs)	1
16	(NIDSs) stands for _____-	Net-based IDSs (NIDSs)	Network-based IDSs	NetProtocol-based IDSs (NIDSs)	Network-by IDSs (NIDSs)	2
17	For a NIDS to sniff packets, the packets have to be given to the _____-level driver by the network interface card	page	segment	packet	sequence	3
18	A _____segment can be defined as a single logical packet domain	session	data	transport	network	4
19	_____ was proposed in 1985 by noted security laureate Dr. Dorothy E. Denning, and it works by establishing accepted baselines and noting exceptional differences	Module Anomaly detection	Model Anomaly detection	modern anamoly detection	memory anomaly detection	2
20	Model AD stands for_____	Module Anomaly detection	modern anamoly detection	Model Anomaly detection (AD)	memory anomaly detection	3
21	_____ are the most popular type of IDS, and they work by using databases of known bad behaviors and patterns.	Signature-detection or misuse IDSs	login detection	protocol detection	id detection	1
22	_____-generation IDSs are being called intrusion-prevention systems (IPSs).	First	Second	Third	Fourth	2
23	IPSs are proactive, and a false positive means a legitimate service or _____ is being denied	guest	session	host	network	3
24	Central to the ____ field are the definitions of management console and agent	guest	session	host	IDS	4
25	Many _____ systems are server-based and rely on common operating systems (mainly Windows and Linux) to run their hardware interface	pop	VoIP	smtp	snmp	2
26	The _____ element (the “brains” of the operation) of a VoIP system can be either a purposed appliance, a piece of software that runs on a common or specialized server operating system	host control	network control	call control	communication control	3

27	(ACLs) stands for _____	access communication list	application control list	application communication list	access control lists	4
28	(ALG) stands for	session - level gateway	application-level gateway	network - level gateway	transport level gateway	2
29	_____ are configured to use dial peers (defined as “addressable endpoints”) to originate and receive calls.	routers	switches	Gateways	modems	3
30	(MCU) stands for _____	multi-conference unit	multiple communication unit	multiple conference unit	multi-communication unit	1
31	_____ compromises today are frequently targeted at mobile devices, and much of the attention in the industry right now is focused on how to secure the mobile environment.	First point	Endpoint	Middle point	symbol point	2
32	_____ have made a remarkable evolutionary leap, from initially being used as a place to take orders and field complaints, to being a strategic asset that most enterprises cannot survive without	Call centers	service center	hub	company	1
33	_____ on exploits of various systems is so readily available, that taking advantage of open relays is a common recreational and for-profit activity.	data	knowledge	Information	expertism	3
34	_____ system has to create a risk profile for low-tech hacks in an organization .	Assessment Audit	network audit	control audit	pay-off	1
35	A _____ is a computer-based switch that can be thought of as a local phone company.	public branch exchange	protected branch exchange	Private Branch Exchange	People Branch Exchange	3
36	(PBX) stands for _____	Private Branch Exchange	protected branch exchange	public branch exchange	People Branch Exchange	1
37	TEM stands for _____	Traffic expense management	Transport expense management	Tata Expense management	Telecom Expense Management	4
38	TCB stands for _____	trustable computing base	trusted computing base	tranmission computing base	telecom computing base	2

39	Security commences at the _____ level and maps all the way up to the operations of the operating system	internet protocol	hyper text protocol	network protocol	post office protocol	3
40	_____ is the term for establishing a connection with a forged sender address	spoofing	threat	hacking	bluffing	1
41	(DACLs) stands for _____	directory access control lists	defend access control lists	discretionary access control lists	data access contol lists	3
42	_____ is always prohibitive (i.e., all that is not expressly permitted is forbidden) and not permissive.	HTTP	MAC	FTP	SMTP	2
43	_____ requires that access control policy decisions be beyond the control of the individual owners of an objec	Mandatory access control	Memory access control	matadata access control	data access contol lists	1
44	_____ is often known as a reversed version of Bell-LaPadula, as it focuses on integrity labels	TCB	TCSEC	Biba	Sun sparc	3
45	_____- attempts to define a security model based on accepted business practices for transaction processing	Clark-jhonson	Clark-Bohem	Clark-william	Clark-Wilson	4
46	TCSEC makes heavy use of the concept of _____.	caption	label	symbol	protocol	2
47	The Windows _____ is responsible for validating Windows process access permissions against the security descriptor for a given object.	Security Reference Monitor	Referential manager	control panel	task manager	1
48	(SRM) stands for _____	Security Role Manager	Security reference manager	Security Reference Monitor	Security Role monitor	3
49	A _____ defines a standard set of security requirements for a specific type of product (for example, operating systems, databases, or firewalls).	public profile	private profile	people profile	protection profile	4
50	(EALs) stand for _____	Enhanced assurance levels	evaluation assurance levels	enquiry assurance level	expert assurancce level	2

Sr No	Question	Option 1	Option 2	Option 3	Option 4	Correct Answer
1	_____ is a compute resource that uses software instead of a physical computer to run programs and deploy apps.	Virtual Machine	Operating system	commercial softwares	router	**Virtual Machine**
2	_____is computer software, firmware or hardware that creates and runs virtual machines	Vmware	Hypervisor	Hyper V	Microsoft	**Hypervisor**
3	A hypervisor, also known as a _____	VCM	VMM	VMC	VVM	**VMM**
4	What is NAT?	Network Address Transcoder	Net Address Translation	Network Address Translation	Network Addition Translation	**Network Address Translation**
5	When you add a software stack, such as an operating system and applications to the service, the model shifts to _____ model.	Saas	PaaS	IaaS	Saas and PaaS	**Saas**
6	Which of the following is most refined and restrictive service model ?	IaaS	Saas	PaaS	Saas and PaaS	**PaaS**
7	What is SaaS?	Software as a Service	Software as a Security	Security as a Service	Service as a Security	**Software as a Service**
8	Which is not in the Cloud Services?	Saas	PaaS	IaaS	HaaS	**HaaS**

9	Which of these companies is not a leader in Cloud computing?	Google	Catalina	Amazon	Microsoft	**Catalina**
10	Which is not the feature of Cloud Computing?	High Cost	Reliability	Security	Reduced Cost	**High Cost**
11	_____ is the on-demand availability of computer system resources.	Security In Computing	Cloud computing	VMM	Availability	**Cloud computing**
12	There are _____ main service models of cloud computing.	two	three	four	five	**three**
13	_____ offers the fundamental infrastructure of virtual servers.	laaS	PaaS	Saas	HaaS	**laaS**
14	Web applications can be created quickly and easily via _____	Platform as a Service	Infrastructure as Service	Software as a Service	Hardware as a Service	**Platform as a Service**
15	This cloud computing solution involves the deployment of software over the internet to various businesses who pay via	subscription	pay-per-use model	subscription or a pay-per-use model	paytm	**subscription or a pay-per-use model**
16	_____ is done by malicious attackers through the use of free Wi-Fi hotspots set up in public places .	Hotspot hijacking	Trojan Horse	Wi-Fi hijacking	DoS	**Wi-Fi hijacking**

17	A _____ device is classified as any device that uses distinctive personally identifiable characteristics.	Biometric	VMM	Router	Guards	**Biometric**
18	_____ is the process of identifying physical assets and assigning criticality and value to them in order to develop concise controls and procedures	Classification of platforms	Classification of services	Classification	Classification of assets	**Classification of assets**
19	What is a mantrap?	It is trusted security domain	A device for fire suppression	A area designed to allow only one authorized individual	A mechanism for logical accessing control.	**A area designed to allow only one authorized individual**
20	Which of the following is the best choice in choosing security guard for a physical access control mechanism?	When intrusion detection is needed	When discriminating judgment is required	When the allotted security budget is low	When access controls are in place	**When discriminating judgment is required**
21	When choosing a location for a data center or office site what is most important?	survivability	cost	buget	risk	**survivability**
22	_____ of the site is typically the first consideration, and with good reason.	Cost	Accessibility	Location	Buget	**Accessibility**
23	_____ can take your entire network and communications infrastructure down with one fell swoop of a backhoe's bucket.	Construction	excavation	Construction and excavation	construction activities	**Construction and excavation**
24	what is CCTV?	Closed-circuit television	Clear -circuit television	Clean -circuit television	Clone -circuit television	**Closed-circuit television**

25	Which is not characteristic of SaaS?	Multi device support	Web Access	one to many	offline access	**offline access**
26	Locks and Entry Controls are _____	Securing Assets	Securing guards	security devices	security control guard	**Securing Assets**
27	What is the major drawback of anomaly detection IDS?	These are very slow at detection	It generates many false alarms	It doesn't detect novel attacks	it does not generate any alarms	**It generates many false alarms**
28	What are the characteristics of signature based IDS?	Most are based on simple pattern matching	It is programmed to interpret a certain series of packets	It models the normal usage of network as a noise characterizatio	Anything distinct from the noise is assumed to be intrusion	**Most are based on simple pattern matching algorithms**
29	What is the number one concern about cloud computing?	Too expensive	Too many platforms	Security concerns	Accessability	**Security concerns**
30	_____ is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing.	laaS	PaaS	Cloud computing	Saas	**Cloud computing**