Sr.No	Questions	Correct Answer
1.	According to the CIA Triad, which of the below-mentioned element is not considered in the triad? a) Confidentiality b) Integrity c) Authenticity d) Availability	C
2.	CIA triad is also known as _____ a) NIC (Non-repudiation, Integrity, Confidentiality) b) AIC (Availability, Integrity, Confidentiality) c) AIN (Availability, Integrity, Non-repudiation) d) AIC (Authenticity, Integrity, Confidentiality)	B
3.	_____ of information means, only authorised users are capable of accessing the information. a) Confidentiality b) Integrity c) Non-repudiation d) Availability	A
4.	_____ means the protection of data from modification by unknown users. a) Confidentiality b) Integrity c) Authentication d) Non-repudiation	B
5.	When you use the word _____ it means you are protecting your data from getting disclosed. a) Confidentiality b) Integrity c) Authentication d) Availability	A
6.	When integrity is lacking in a security system, _____ occurs. a) Database hacking b) Data deletion c) Data tampering d) Data leakage	C
7.	Why these 4 elements (confidentiality, integrity, authenticity & availability) are considered fundamental? a) They help understanding hacking better b) They are key elements to a security breach c) They help understands security and its components better d) They help to understand the cyber-crime better	C

8.	This helps in identifying the origin of information and authentic user. This referred to here as _____ a) Confidentiality b) Integrity c) Authenticity d) Availability	C
9.	Data _____ is used to ensure confidentiality. a) Encryption b) Locking c) Deleting d) Backup	A
10.	Data integrity gets compromised when _____ and _____ are taken control off. a) Access control, file deletion b) Network, file permission c) Access control, file permission d) Network, system	C
11.	_____ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction. a) Network Security b) Database Security c) Information Security d) Physical Security	C
12.	From the options below, which of them is not a threat to information security? a) Disaster b) Eavesdropping c) Information leakage d) Unchanged default password	D
13.	Compromising confidential information comes under _____ a) Bug b) Threat c) Vulnerability d) Attack	B
14.	Which of the following are not security policies? a)Regulatory b)Advisory c)Availability d)User Policies	C

15.	Examples of User Policies is/are: a)Password Policies b)Internet Usage c)System Use d)All of the above	D
16.	_____ Policy ensures that the organization is maintaining standards set by specific industry regulation. a)Regulatory b)Advisory c)Availability d)User Policies	A
17.	_____ Policy is like standards rules and regulations set by the management to advise their employees on their activity or behavior a)Regulatory b)Advisory c)Availability d)User Policies	B
18.	What defines the restrictions on employees such as usage? a)Regulatory b)Advisory c)Availability d)User Policies	D
19.	The full form of OSI is OSI model is _____ a) Open Systems Interconnection b) Open Software Interconnection c) Open Systems Internet d) Open Software Internet	A
20.	In _____ layer, vulnerabilities are directly associated with physical access to networks and hardware. a) physical b) data-link c) network d) application	A
21.	Loss of power and unauthorized change in the functional unit of hardware comes under problems and issues of the physical layer. a) True b) False	A

22.	Which of the following attack can actively modify communications or data? a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	C
23.	OSI architechture mainly focuses on: 1) Security Attack 2) Security Techniques/Mechanisms 3) Categories of Security Service a)1 b)1 &3 c) 2& 3 d)1,2,3	D
24.	IT security department must periodically check for security logs and entries made during office hours. a) True b) False	A
25.	Release of Message Content and Traffic analysis are type of : a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	D
26.	If communication between 2 people is overheard by a third person without manipulation of any data, it is called as: a) Release of Message Content-Passive Attack b) Traffic analysis -Passive Attacks c) Release of Message Content- Active Attacks d) Traffic analysis -Active Attacks	A
27.	If communication between 2 people is overheard by a third person without extraction of any data, it is called as: a) Release of Message Content-Passive Attack b) Traffic analysis -Passive Attacks c) Release of Message Content- Active Attacks d) Traffic analysis -Active Attacks	D
28.	No modification of data is a characteristic of a)Active Attack b)Passive Attack	A
29.	Which of the following are Active attack types	D

	a)Masquerade b)Replay c)Modification d)All of the above	
30.	_____ means when an attacker pretends to be authentic user a)Masquerade b)Replay c)Modification d)Traffic analysis	A
31.	_____ attack is when original data is modified and malicious data is inserted a)Masquerade b)Replay(Rewrite) c)Modification d)Traffic analysis	B
32.	When original data is changed to make it non-meaningful by attacker it is known as a)Masquerade b)Replay c)Modification of Messages d)Traffic analysis	C
33.	Which is the type of attack when Network is made unavailable for user a)Masquerade b)Replay c)Modification d)Denial of Service	D
34.	Modification of Data is done in: a)Both Active and Passive Attacks b)Neither Active and Passive Attacks c) Active Attacks d)Passive Attacks	A
35.	The information that gets transformed in encryption is _____ a) Plain text b) Parallel text c) Encrypted text d) Decrypted text	A
36.	1. The process of transforming plain text into unreadable text.	B

	a) Decryption b) Encryption c) Network Security d) Information Hiding	
37.	A process of making the encrypted text readable again. a) Decryption b) Encryption c) Network Security d) Information Hiding	A
38.	A unique piece of information that is used in encryption. a) Cipher b) Plain Text c) Key d) Cipher	C
39.	Assurance that authentic user is taking part in communication is: a)Authentication b)Authorization c)Access Control d)Auditing	A
40.	ATM pin while withdrawing money is an example of using: a)Authentication b)Authorization c)Access Control d)Auditing	B
41.	Study of creating a d using encryption and decryption techniques. a) Cipher b) Cryptography c) Encryption d) Decryption	B
42.	An attack in which the user receives unwanted amount of e-mails. a) Smurfing b) Denial of service c) E-mail bombing d) Ping storm	C
43.	The process of disguising plaintext in such a way that its substance gets hidden (into what is known as cipher-text) is called _____	D

	a) cryptanalysis b) decryption c) reverse engineering d) encryption	
44.	In _____ same keys are implemented for encrypting as well as decrypting the information. a) Symmetric Key Encryption b) Asymmetric Key Encryption c) Asymmetric Key Decryption d) Hash-based Key Encryption	A
45.	The procedure to add bits to the last block is termed as _____ a) decryption b) hashing c) tuning d) padding	D
46.	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	B
47.	Cryptanalysis is used _____ a) to find some insecurity in a cryptographic scheme b) to increase the speed c) to encrypt the data d) to make new ciphers	A
48.	Conventional cryptography is also known as _____ or symmetric-key encryption. a) secret-key b) public key c) protected key d) primary key	A
49.	_____ is the art & science of cracking the cipher-text without knowing the key. a) Cracking b) Cryptanalysis c) Cryptography d) Crypto-hacking	B
50.	In _____ a sequence of actions is carried out on this block after a block of plain-text bits is chosen for generating a block of cipher-text bits.	A

	a) Block Cipher b) One-time pad c) Hash functions d) Vigenere Cipher	