Sample Questions - Semester III Information Security

Sr. No.	Question	Module No.	Option a	Option b	Option c	Option d
1	An _____attack attempts to alter system resources or effect their operations.	1	PASSIVE	ACTIVE	MAN -IN-MIDDLE	MEET-IN-MIDDLE
2	Which of the following principle is violated if the computer suystem is not accessible	1	confidentiality	availability	access control	authenticati on
3	The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key	2	12	8	18	16
4	How many keys does the Triple DES algorithm use?	2	2	3	2 OR 3	3 OR 4
5	Which of the following statements are true i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption ii) The CTR mode does not require an Initialization Vector iii) The last block in the CBC mode uses an Initialization Vector iv) In CBC mode repetitions in plaintext do not show up in ciphertext	2	iii)	ii) and iv)	i), ii), iii) and iv)	i), ii), and iv)
6	_____ is a popular session key creator protocol that requires an authenticatio nserver and a ticket-granting server.	2	KDC	Kerberos	CA	KDD
7	Mututal Authentication requires the ___ involved in communication to authenticate each other	3	3	1	2	4
8	Which of the following does authentication aim to accomplish?	3	Restrict what operations/data the user can access	Determine if the user is an attacker	Flag the user if he/she misbehaves	Determine who the user is

9	Number of phases in the handshaking protocol?	4	2	3	4	5
10	The client_key_exchange message uses a pre master key of size –	4	48 bytes	56 bytes	64 bytes	32 bytes
11	) Which of the following can be used to authenticate and encrypt IP (Internet Protocol) traffic?	4	ESP (Encapsulating Security Payload)	S/MIME (Secure Multipurpose Internet Mail Extensions)	IPSec (Internet Protocol Security)	IPv2 (Internet Protocol version 2)
12	SAML supports ___ and _____	4	confidentiality and integrity	authorization and confidentiality	authentication and confidentiality	authentication and authorization
13	_____ analyses network traffic to look for evidence of attack	5	intrusion prevention systems	intrusion detection systems	Firewalls	DMZ
14	Patterns that you look for inside a data packet used to detect one or more types of attacks are called _____	5	Logs	False alarms	Alerts	Signatures
15	Network Intrusion Detection System run on a system that connect to the _____	5	Application software	hub, switch, or router	only to the router	only to the switch
16	the _____ prilivige allowsthe user to make changes to the database	6	INSERT, DELETE AND UPDATE	INSERT AND SELECT	UPDATEAND SELECT	INSERT SELECT AND DELETE
17	privileges ARE managed using _____ operations	6	GRANT , UPDATE	REVOKE , UPDATE	GRANT AND REVOKE	REVOKE
18	In a _____ database, information retrieved by means of aggregate queries on an attribute	6	RELATIONAL DATABASES	HIERARCHICAL DATABASE	STATISTICAL DATABASES	DATABASE MANAGEMENT SYSTEMS
19	An _____is a technique performed by analyzing data in order to illegitimately gain knowledge about a subject or database.	6	Active attack	passive attack	inference attack	man in the middle attack
20	Network layer firewall works as a _____	7	Frame filter	Packet filter	Content filter	Virus filter

21	Which of the following is / are the types of firewall?	7	Packet Filtering Firewall	Dual Homed Gateway Firewall	Screen Host Firewall	Dual Host Firewall
22	_____ is a set of rules that governs whatis and what is not allowed through the firewall.	7	DMZ	Rule Base	dynamic packet filter	Proxy server
23	A firewall needs to be ____ so that it can grow with the network it protects.	7	Robust	fast	expensive	scalable
24	WPS stands for _____	8	WiFi Protected System	WiFi Protected Setup	WiFi Protocol Setup	Wireless Protected Setup
26	What is the size of the Temporal Key for the case of TKIP?	8	64 bits	128 bits	256 bits	512 bits