

These are sample MCQs to indicate pattern, may or may not appear in examination

**University of Mumbai**  
**Online Examination 2020**

Program: BE Computer Engineering

Curriculum Scheme: Revised 2016

Examination: Fourth Year Semester VII

Course Code: CSDL07031 and Course Name: Advance System Security & Digital Forensics

Time: 1hour

Max. Marks: 50

**Note to the students:-** All the Questions are compulsory and carry equal marks .

Q1.	Why Private networks can be a richer source of evidence than the Internet?
Option A:	They retain data for longer periods of time
Option B:	Owners of private networks are more cooperative with law enforcement
Option C:	Private networks contain a higher concentration of digital evidence
Option D:	Private networks contain a less concentration of digital evidence

Q2.	When a file is deleted
Option A:	The file remains intact.
Option B:	The FAT entry for the file is zeroed out so it shows that the area is available for use by a new file.
Option C:	The first character of the directory entry file name is changed to a special character.
Option D:	The last character of the directory entry file name is changed to a special character.

Q3.	What can be used to verify the original drive with the forensic copy?
Option A:	a password
Option B:	a hash analysis
Option C:	disk to disk verification
Option D:	Bit-Stream Copy

Q4.	Which of the following is a proper acquisition technique?
Option A:	Disk to Image
Option B:	Disk to Disk
Option C:	Sparse Acquisition
Option D:	Image to Disk

Q5.	Which of the following is not a type of volatile evidence?
Option A:	Routing Tables
Option B:	Main Memory
Option C:	Log files
Option D:	Cached Data

Q6.	What is essential to system for frequently comprising critical patches to security holes?
Option A:	System software
Option B:	Utility Software
Option C:	Software executables
Option D:	Software updates

Q7.	How many types of buffer-overflow attack are there?
-----	---

Option A:	4
Option B:	2
Option C:	5
Option D:	3

Q8.	What is a covert channel?
Option A:	Using a communications channel in a way that was not intended
Option B:	Tunneling software
Option C:	A Trojan removal tool
Option D:	Using a communications channel in the original, intended way

Q9.	What is a major feature of segmentation?
Option A:	Program is divided in data memory and program memory
Option B:	Program is executed in segments
Option C:	Program is divided into pieces having different access rights
Option D:	It has effect of an unbounded architecture

Q10.	In Kerberos, the Ticket Granting Ticket (TGT) is used for which of the following?
Option A:	Identification
Option B:	Authorization
Option C:	Authentication
Option D:	Multifactor authorization

Q11.	Which Bell-LaPadula property keeps lower-level subjects away from accessing objects with higher-level security?
Option A:	* (star) Security Property
Option B:	No write up property
Option C:	No read up property
Option D:	No read down property

Q12.	Which of the following is NOT a valid access control mechanism?
Option A:	DAC (Discretionary Access Control) list.
Option B:	SAC (Subjective Access Control) list.
Option C:	MAC (Mandatory Access Control) list.
Option D:	RBAC (Role Based Access Control) list.

Q13.	Lack of access control policy is _____
Option A:	Bug
Option B:	Threat
Option C:	Vulnerability
Option D:	Attack

Q14.	What is the punishment in India for stealing computer documents, assets or any software's?
Option A:	6 months of imprisonment and a fine of Rs. 50,000
Option B:	1 year of imprisonment and a fine of Rs. 100,000
Option C:	2 years of imprisonment and a fine of Rs. 250,000
Option D:	3 years of imprisonment and a fine of Rs. 500,000

Q15.	What is the full form of ITA-2000?
Option A:	Information Tech Act -2000
Option B:	Indian Technology Act -2000
Option C:	International Technology Act -2000
Option D:	Information Technology Act -2000

Q16.	What is the name of the IT law that India is having in the Indian legislature?
Option A:	India's Technology (IT) Act, 2000
Option B:	India's Digital Information Technology (DIT) Act, 2000
Option C:	India's Information Technology (IT) Act, 2000
Option D:	The Technology Act, 2008

Q17.	What types of protocols are used in VPNs?
Option A:	Application level protocols
Option B:	Tunnelling protocols
Option C:	Network protocols
Option D:	Mailing protocols

Q18.	VPN is abbreviated as _____
Option A:	Visual Private Network
Option B:	Virtual Protocol Network
Option C:	Virtual Private Network
Option D:	Virtual Protocol Networking

Q19.	In which layer frequency band is defined and wireless signals are encoded?
Option A:	Medium Access Layer
Option B:	Physical Layer
Option C:	Logic Link Control Layer
Option D:	Network Layer

Q20.	What was the security algorithm defined for the IEEE 802.11
Option A:	WEP
Option B:	RSN
Option C:	WPA
Option D:	SSL

Q21.	A _____ is a software bug that attackers can take advantage to gain unauthorized access
Option A:	System error
Option B:	Bugged system
Option C:	Security bug
Option D:	System virus

Q22.	How do you prevent Clickjacking
Option A:	Add X-FRAME header
Option B:	Add X-FRAME-OPTIONS header
Option C:	Add HSTS header

Option D:	DD CLICK-FRAME-OPTIONS header
-----------	-------------------------------

Q23.	Which is the latest version of OAuth
Option A:	1.0
Option B:	2.0
Option C:	3.0
Option D:	4.0

Q24.	XSS stands for _____
Option A:	Crack Site Scripting
Option B:	Cross Site Server
Option C:	Cross Site Scripting
Option D:	Crack Server Scripting

Q25.	_____ is an internet scam done by cyber-criminals where the user is convinced d
Option A:	Phishing attack
Option B:	DoS attack
Option C:	Website attack
Option D:	MiTM attack