University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: BE Information Technology
Curriculum Scheme: Rev2016
Examination: Third Year Semester VI
Course Code: **ITDLO6023** and Course Name: **Digital Forensics**

Time: 1 hour Max. Marks: 50

==========

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

Q1.	The legal risks of ethical hacking include lawsuits due to _____ of personal data.
Option A:	stealing
Option B:	disclosure
Option C:	deleting
Option D:	hacking
Q2.	Before performing any penetration test, through legal procedure, which key point listed below is not mandatory?
Option A:	Know the nature of the organization
Option B:	Characteristics of work done in the firm
Option C:	System and network
Option D:	Type of broadband company used by the firm
Q3.	The chain of Custody means_____
Option A:	Maintaining chain of all investigations and investigators
Option B:	Taking all evidences in personal custody to show our findings
Option C:	Recording all evidences in chain and then ask for custody of the same to attorney
Option D:	evidence collected should not be accessed by any other unauthenticated person.
Q4.	Locard's Exchange Principle states that_____
Option A:	It is impossible for a criminal to act, especially considering the intensity of a crime, without leaving traces of this presence.
Option B:	There is always a way for criminals to escape from all the evidence. Just it is needed to find the way.
Option C:	There are always some or the other tool exist which can be used by investigators to extract evidences from any system without disturbing data
Option D:	It is possible for investigators to alter the data on a suspect machine which is vulnerable to cyber attack.
Q5.	Network-based evidence information can not be obtained from
Option A:	IDS logs
Option B:	Verbal Communication
Option C:	Router logs

Option D:	Firewall logs
Q6.	…..includes reviewing all the data collected during investigation
Option A:	Forensic analysis
Option B:	Forensic checking
Option C:	Error Finding
Option D:	Review
Q7.	Which is the last component/stage of incident response methodology
Option A:	Resolution
Option B:	Data analysis
Option C:	Reporting
Option D:	Initial response
Q8.	What should be the response strategy for DoS attack?
Option A:	Interview with people
Option B:	Reconfigure router to minimize effect of the flooding.
Option C:	Seal the organization
Option D:	Keep track of time
Q9.	Which of the following is not the requirement for evidence admissibility
Option A:	Evidence should be competent
Option B:	Evidence should be relevant
Option C:	Evidence should be obtained legally
Option D:	Evidence should look real
Q10.	During data collection, what is the standard way of obtaining remote logs from a centralized host
Option A:	chklog
Option B:	ChkLog
Option C:	logs
Option D:	SYSLOG
Q11.	The overall I/O rate in RAID level 4 is _____
Option A:	low
Option B:	very low
Option C:	high
Option D:	medium
Q12.	RAID stands for _____

Option A:	Redundant Allocation of Inexpensive Disks
Option B:	Redundant Array of Important Disks
Option C:	Redundant Allocation of Independent Disks
Option D:	Redundant Array of Independent Disks
Q13.	Deleted or missing partitions can identified by using the -------- tool
Option A:	sigfind
Option B:	encase
Option C:	safeback
Option D:	odd
Q14.	The intent of a _____ is to overkill the targeted server's bandwidth and other resources of the target website.
Option A:	Phishing attack
Option B:	DoS attack
Option C:	Website attack
Option D:	MiTM attack
Q15.	Which of the following is not a sniffing tool?
Option A:	Wireshark
Option B:	Dude Sniffer
Option C:	Maltego
Option D:	Look@LAN
Q16.	Following is an example of network based evidence
Option A:	Obtain the system time
Option B:	Obtain Back up
Option C:	Obtain IDS logs
Option D:	Obtain Oral testimony from witness
Q17.	The number of columns in a routing table required for classless addressing is
Option A:	One column
Option B:	Two column
Option C:	Three column
Option D:	Four column
Q18.	When does a criminal investigation usually begin?
Option A:	when someone finds evidence of or witnesses a crime
Option B:	when witness or victim makes an allegation to the police
Option C:	When criminal informs to organisation about crime

Option D:	When all proofs are collected against criminal
Q19.	The initial stage in a cyberstalking investigation is to:
Option A:	Search for additional digital evidence
Option B:	Analyze crime scene characteristics
Option C:	Conduct victimology and risk assessments
Option D:	Interview the victim
Q20.	A common technique that is highly useful and can be applied in a computer intrusion investigation is to simply focus on file system activities around the time of known events. This embodies a principle known as:
Option A:	Temporal proximity
Option B:	Timeline analysis
Option C:	File system analysis
Option D:	Temporal aggregation
Q21.	Why is it important to hide your identity when conducting an online investigation?
Option A:	To reduce the risk of alerting the offender
Option B:	To get yourself in the mindset of covert web investigating
Option C:	To make it easier for you to determine the offender's location
Option D:	To Search the Web using distinctive aspects
Q22.	Encase tool is used for
Option A:	Create the image of hard disk drive
Option B:	To generate technical report
Option C:	To see which are the system are still alive in network
Option D:	To create report in PDF file
Q23.	Making a copy of original drive by using computer forensic tool is called as
Option A:	Acquisition
Option B:	Validation
Option C:	Reporting
Option D:	Autopsy
Q24.	Which is one of the purpose of validation and discrimination
Option A:	Physical data copy
Option B:	Hashing
Option C:	Logical data copy
Option D:	Command line acquisition

Q25.	_____ is a digital forensics platform that with efficiency analyses smartphones and harddisks
Option A:	NSRL
Option B:	Autopsy
Option C:	SANS SIFT
Option D:	Keystroke logger

University of Mumbai

Examination 2020 under cluster 4 (PCE)

Program: BE Information Technology
Curriculum Scheme: Rev2016
Examination: Third Year Semester VI
Course Code: **ITDLO6023** and Course Name: **Digital Forensics**
Time: 1 hour Max. Marks: 50

==========

Question	Correct Option (Enter either 'A' or 'B' or 'C' or 'D')
Q1.	**B**
Q2.	**D**
Q3.	**D**
Q4.	**A**
Q5.	**B**
Q6.	**A**
Q7.	**C**
Q8.	**B**
Q9.	**D**
Q10.	**D**
Q11.	**C**
Q12.	**D**
Q13.	**A**
Q14.	**B**
Q15.	**C**
Q16.	**D**
Q17.	**D**

Q18.	**B**
Q19.	**D**
Q20.	**A**
Q21.	**A**
Q22.	**A**
Q23.	**A**
Q24.	**B**
Q25.	**B**