University of Mumbai

Examination 2021 under cluster 7

Examinations Commencing from 1st June 2021

Program: **Information Technology**

Curriculum Scheme: 2016

Examination: TE Semester VI

Course Code: ITDLO6023 and Course Name: Digital Forensic

Time: 2 hour Max. Marks: 80

===

Q1.	**Choose the correct option for following questions. All the Questions are compulsory and carry equal marks**
1.	Most widely used command for listing open ports on unix system is
Option A:	Netstat
Option B:	w-command
Option C:	1s command
Option D:	ps command
2.	__________ is a popular tool used for discovering networks as well as in security auditing.
Option A:	Ettercap
Option B:	Metasploit
Option C:	Nmap
Option D:	Burp Suit
3.	Which of the following deals with network intrusion detection and real-time traffic analysis?
Option A:	John the Ripper
Option B:	LophtCrack
Option C:	Snort
Option D:	Nessus

4.	One of the most common approaches to validating forensic software is to:
Option A:	Examine the source code
Option B:	Ask others if the software is reliable
Option C:	Compare results of multiple tools for discrepancies
Option D:	Computer forensic tool testing projects
5.	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
6.	Which of them is not an appropriate method of router security
Option A:	Unused ports should be blocked
Option B:	Unused interfaces and services should be disabled
Option C:	Routing protocol needs to be programmed by security experts
Option D:	Packet filtering needs to be enabled
7.	____________ is the method for keeping sensitive information in email communication & accounts secure against unofficial access, loss, or compromise.
Option A:	Email security
Option B:	Email hacking
Option C:	Email protection
Option D:	Email safeguarding
8.	The overall I/O rate in RAID level 4 is _____________
Option A:	low
Option B:	very low

Option C:	High
Option D:	MEDIUM
9.	Which of the following will not help in preserving email security?
Option A:	Create a strong password
Option B:	Connect your email to a phone number
Option C:	Use two-factor authentication for password verification and login
Option D:	Click on unknown links and sites
10.	The first tool for making forensic copies of computer storage media was:
Option A:	EnCase
Option B:	Expert Witness
Option C:	dd
Option D:	Safeback
11.	which of the following is not the volatile data for live response
Option A:	System date and time
Option B:	USB
Option C:	Currently running process
Option D:	Currently logged on users
12.	Which command is used to display current running process
Option A:	psloogedon
Option B:	plist
Option C:	ps
Option D:	pslog

13.	Which phase involves data collection and data analysis.
Option A:	Reporting
Option B:	Resolution
Option C:	Investigation
Option D:	Initial response
14.	Which is not the variations of live response
Option A:	Initial live response
Option B:	Pre-initial live response
Option C:	In-depth response
Option D:	Full live response
15.	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
16.	A free tool that is used to enlist listening ports for all the processes.
Option A:	listen
Option B:	listp
Option C:	fport
Option D:	flport
17.	How many major components are there in incident response methodology
Option A:	9
Option B:	3

Option C:	7
Option D:	5
18.	Which is not a step in preparing the response toolkit
Option A:	Searching information
Option B:	Tag a response toolkit media
Option C:	Check the dependencies
Option D:	creating checksum
19.	which of the following is not a part of CSIRT team:
Option A:	Security analysts
Option B:	Lead investigator
Option C:	Information Lead
Option D:	HR/legal representation
20.	Which is the last component/stage of incident response methodoly
Option A:	Resolution
Option B:	Data analysis
Option C:	Reporting
Option D:	Initial response

Q2)	**Solve any Two Questions out of Three 10 marks each**
A	*Explain in detail collecting volatile & non-volatile data in unix-based systems*
B	*Explain volatile data collection procedure in window systems.*
C	*Explain how to use router as a forensic tools.*

Q3)	**Solve any Two Questions out of Three 10 marks each**
A	*Explain RAID techniques in detail.*

B	*State the rule of digital evidence along with its characteristics.*
C	*Explain guidelines for incident report writing.Give one report writing examples..*