

University of Mumbai

Examination Summer 2022

Program: Electronics and Telecommunication Engineering

Curriculum Scheme: Rev2019

Examination: TE Semester: VI

Course Code: ECCDLO6013 and Course Name: Digital Forensic (DF)

Time: 2 hour 30 minutes

Max. Marks: 80

Q1.	Choose the correct option for the following questions. All the questions are compulsory and carry equal marks
1.	Someone who exploits a security vulnerability in order to spread public awareness that the vulnerability exists, is called?
Option A:	White Hat Hacker
Option B:	Black Hat Hackers.
Option C:	Gray Hat Hackers.
Option D:	Red Hat Hackers.
2.	CSIRT stands for
Option A:	Computer Safety Incident Response Team
Option B:	Computer Security Incident Response Team
Option C:	Computer Security Incident Responsible Team
Option D:	Computer Security Information Response Team
3.	In which phase of Incident Response Methodology, Data Collection and Data Analysis happens
Option A:	Detection of Incident
Option B:	Formulate response strategy
Option C:	Investigate the Incident
Option D:	Reporting
4.	Which statement is not true regarding Evidence Admissibility
Option A:	Evidence should not be competent.
Option B:	Evidence should be relevant.
Option C:	Evidence should be material.
Option D:	Evidence should be obtained legally.
5.	Which of the following is the disk-search utility which is used to perform a search from a physical level?
Option A:	PsLogList
Option B:	Dumpe.exe
Option C:	dtSearch
Option D:	hosts
6.	Which statute protects the privacy of individuals' healthcare data?
Option A:	Privacy Act
Option B:	HIPAA
Option C:	Computer Fraud and Abuse Act
Option D:	DMCA
7.	A computer program that attaches itself to legitimate code and runs with the

	program.
Option A:	Virus
Option B:	Worm
Option C:	Trojan Horse
Option D:	Trapdoor
8.	What will be the response strategy for the DOS attack incidents?
Option A:	Investigate website
Option B:	Reconfigure router to minimize flooding
Option C:	Law enforcement contacted
Option D:	Monitor attackers' activities
9.	System processes and device driver activities are recorded in _____ log
Option A:	System log
Option B:	Application log
Option C:	Security log
Option D:	sysctl
10.	Which tool is used for acquiring and analyzing forensic images?
Option A:	FTK Imager
Option B:	Scalpel
Option C:	Foremost
Option D:	Volatility

Q2(20 Marks)	Solve any Four out of Six (5 marks each)
A	Differentiate passive and active attacks.
B	Differentiate attacks and vulnerabilities.
C	What are the different challenges of evidence handling?
D	Explain the steps of volatile data collection for the Unix system.
E	Differentiate between Virus, Worm, Trojan horse, and trap door.
F	What is packet sniffing? How is it done? What are the threats due to packet sniffing?

Q3 (20 Marks)	Solve any Two Questions out of Three 10 marks each
A	Define cybercrime. Discuss various cybercrime categories in detail.
B	Discuss how network based evidence is collected and analyzed?
C	Write a short note on the Acquisition, Duplication, Analysis, and Recovery of digital evidence

Q4 (20 Marks)	
A	Solve any Two (5 marks each)
i.	Which are possible investigation phases carried out in data collection and analysis?
ii.	Explain Incident Response Methodology (IRM) with a neat diagram.
iii.	Explain various types of law and different levels of law in detail?
B	Solve any One (10 marks each)
i.	What is Intrusion Detection System (IDS)? Discuss different types of IDS and types of intrusion detection systems methods.
ii.	Discuss the necessity of forensic duplication

munotes.in