National Forensics Sciences University, Goa Campus
Mid-semester Examination

Programme – M.Sc. DFIS Sem – I Date- 10.10.2024

Subject Name- Incident Response Management Subject Code- CTMSDFIS SI P3

Time- 1.5 Hours Max.Marks- 50

Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Solve any four	20 marks
	a. List out the benefits of Incident management.	5 marks
	b. How do you identify the occurrence of an incident?	5 marks
	c. Discuss the different functions/activities of the incident reporting organization such as CERT-IN.	5 marks
	d. Discuss the role of CVE Numbering Authority (CNA). Does CERT-IN fall in this category?	5 marks
	e. Explain the procedure to handle an incident faced by a manufacturing plant.	5 marks
Q.2	Attempt all	15 marks
	a. List out the different categories of the incident.	5 marks
	b. List out the different tools used in IRM.	5 marks
	c. How do you estimate the cost of an incident?	5 marks
Q. 3	Attempt a and b	15 marks
Q.3 a	Attempt any one	
Q.3 a	I. How do you prioritize the incidents, explain by considering a security breach in a Fintech company.	8 marks
	OR	
	II. Discuss the role of virtualization in incident handling.	8 marks
Q.3 b	Attempt any one	7 marks
Q3 b	I. How does the IRM team handle phishing attacks and employee password compromise? Explain the procedure in detail.	7 marks
	OR	
	II. How does the IRM team handle infrastructure monitoring and weak passwords? Explain the procedure in detail.	7 marks

CERT-In Incident Reporting Form

Contact Information of the Reporter

- Name & Role / Title:- Yash Rana, Security Analyst
- Organisation: XYZ Corporation
- Contact No.: +91 1234567890
- Email: yashrana@xyz.com
- Address: XYZ Tech Park, Sector 12, New Delhi, India

Basic Incident Details

- Affected entity: XYZ Corporation (internal report)
- Incident Type:
  - ✓ Unauthorised access of IT systems/data
  - ✓ Compromise of critical systems/information
  - ✓ Attack on servers such as Database, Mail, and DNS
  - ✓ Data Breach
  - ✓ Malicious code attacks

- Is the affected system/network critical to the organization's mission?
  - Yes - This attack impacted critical databases, web servers, and employee email systems.

Basic Information of Affected System

- Domain/URL: xyzcorp.com
- IP Address: 192.168.1.100 (internal)
- Operating System: Windows Server 2019
- Make/Model/Cloud details :- Hosted on AWS EC2 instances
- Affected Application details: SAP, ERP, ~~internal~~ internal emailservers, and client databases
- Location of affected system: New Delhi, India
- Network and ISP: XYZ Corp Network on Aitrel Business

Brief description of the Incident
The incident involved unauthorized access to the XY2 Corporation's primary databases server on 10/11/2024 at 23:00 hrs. A sophisticated malicious code was deployed, resulting in unauthorized data extraction and a breach of sensitive client information. Initial detection occurred on 11/11/2024 at 08:30 hrs when the internal monitoring systems flagged unusual data flow.

- Occurrence date & time : 10/11/2024 23:00 hrs
- Detection date & time : 11/11/2024 08:30 hrs

National Forensics Sciences University, Goa Campus
Mid - Semester Examination

Programme - MSc Digital Forensics and Information Security Sem – I

Date- 09/10/2024

Subject Name: Introduction to Forensic Science and cyber laws Subject Code – CTMSDFIS SI P5

Time- 1.5 Hours Max. Marks - 50

Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	**Solve any four**	**20 marks**
	a. Write a note on volatile vs non-volatile memory and their significant differences.	5 marks
	b. Give an insight on the importance of the code of conduct of a forensic scientist in Forensic science. Justice, non malif, autonomy, Beneficence.	5 marks
	c. Discuss the establishment of BPR&D and briefly mention its function.	5 marks
	d. What do you understand by Data Depiction? Why it is important in Forensic Science.	5 marks
	e. Write a note on the establishment of Central finger Print Bureau (CFPB).	5 marks
Q.2	**Attempt all**	**15 marks**
	a. Prepare a comprehensive report on the digital evidence given to you.	5 marks
	b. What are duties of Forensic Scientists? Identification, Evidence collection, Analysis, Document & report, conclusion	5 marks.
	c. What is the difference between RAM and ROM.	5 marks
Q. 3	**Attempt a and b**	**15 marks**
Q.3 a	Attempt any one	
Q.3 a	I. Discuss Section 66 of IT act, 2000 with an appropriate case study.	8 marks
	OR	
	~~II.~~ Write a note on any four Tools and Techniques used in Forensic Science.	8 marks
Q.3 a	**Attempt any one**	**7 marks**
Q3 b	I. Elaborate on the term "Cyber ethics" and its importance in cyber security.	7 marks
	OR	
	~~II.~~ Elaborate on the purpose and functioning of the National Investigation Agency.	7 marks

*** All the best***

Balistics

National Forensics Sciences University, Goa Campus
TA-1 Examination

Program Name – ~~BSC-MSc Forensic science~~ (5-year integrated) Sem – I

Date- 11/09/2024

Subject Name- Introduction to Forensic Science and Cyber Law

Subject Code- CTMS_CS/DFIS/AIDS SI P5

Time- 45 minutes Max. Marks- 25

Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1		Multiple Choice Questions (1 mark each)	10 marks
	I.	Find the correct order of forensic science laboratories set up in India- a. CFSL>SFSL>RFSL>MFSL b. MFSL>RFSL>SFSL>CFSL c. SFSL>CFSL>MFSL>RFSL d. RFSL>SFSL>CFSL>MFSL	1 mark
	II.	The first fingerprint bureau was established in a. Delhi b. Chennai c. Kolkata d. Shimla	1 mark
	III.	The first central forensic Science laboratory (CFSL) in India was established in a. Kolkata b. Delhi c. Hyderabad d. Chandigarh	1 mark
	IV.	"When two objects come in contact there is always an exchange of materials". This statement was given by Ed ________.	1 mark
	V.	Law of comparison, compares between a. People with dissimilar likes b. People from extended family c. Identical twins d. People with similar likes	1 mark
	VI.	The role of the Forensic Document Examiner is to- a. Verify the documents involved in forgery case b. Verify the handwriting c. Verify the Ink used d. All of the above	1 mark
	VII.	Study of human skeletal structure comes under a. Forensic Chemistry b. Forensic Anthropology c. Forensic Pathology a. Forensic Entomology	1 mark

	VIII.	Identification of volatile and non-volatile poisons of organic and Inorganic compounds carried out in_______________ a. Biology division b. Chemistry division [✓ c.] Toxicology division d. Physics division	1 mark
	IX.	Choose the correct role of DFSS a. Promote research and development in forensic field b. Guide, regulates and controls the working of FSLs c. It provides scientific aid and criminal justice systems [✓ d.] All	1 mark
	X.	**"The prompt action is necessary** in all aspects of criminal investigation". This sentence is best suited for which principle- a. Law of analysis [✓ b.] Law of Progressive change c. Law of circumstantial fact d. Law of Probability	1 mark
Q.2	Answer any 3 questions (3x5 marks each)		15 Marks
	i.	Explain, "There is an urgent need for Forensic experts in India".	5 marks
	ii.	Discuss the various laws of Forensic Science.	5 marks
	iii.	Why Forensic science is a multi-disciplinary field? And what is its significance?	5 marks
	iv.	State the organization order of various forensic science laboratories in India and their function.	5 marks

Seat No.: ________ Enrolment No.___________

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (December – 2024)
M.Sc. Digital Forensics and Information Security
Semester - I

Subject Code: CTMSDFIS SI P5 **Date: 10/12/2024**
Subject Name: Introduction to Forensic Science and Cyber Law
Time: 2:30 PM- 5:30 PM **Total Marks: 100**

Instructions:

1. **Write down each question on a separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**

			Marks
Q.1		**Attempt any three.**	
	(a)	Explain the basic principles of Forensic Sciences with suitable examples.	**08**
	(b)	What is Interpol? Describe its role in combating crimes at the international level.	**08**
	(c)	Discuss the different theories of punishment and the kinds of punishments prescribed under the Bhartiya Nyaya Sanhita, 2023, including their objectives and implications.	**08**
	(d)	What are the different types of computer storage media and list out 5 differences between RAM and ROM.	**08**
Q.2		**Attempt any three.**	
	(a)	What are the various contemporary disciplines in Forensic science and their applications in the current scenario?	**08**
	(b)	Write a note on the National Investigation Agency (NIA).	**08**
	(c)	Write short notes on the following: i. CCTNS ii. CFPB	**08**
	(d)	Explain the organizational setup of Forensic Science laboratories in India.	**08**
Q.3		**Attempt any three.**	
	(a)	What is an Expert witness? Write a brief procedure involved in the examination of witnesses.	**08**
	(b)	Present a format of Report writing and state the importance of data depiction.	**08**
	(c)	Write a note on the establishment of BPR&D.	**08**
	(d)	Write a short note on the IT Act 2000 with an appropriate Case study.	**08**

Q.4		**Attempt any two.**	
	(a)	What are bailable and non-bailable offences, and how are they determined under the Criminal Procedure Code?	**07**
	(b)	What are the elements of the Criminal Justice system? Elaborate on the significance of 'mens rea' and 'actus reus'.	**07**
	(c)	Write a note on the code of conduct as a Forensic Scientists.	**07**
Q.5		**Attempt any two.**	
	(a)	What is the difference between murder and culpable homicide? What sections differentiate that and how is the punishment different?	**07**
	(b)	Elaborate on the term Cyber ethics and its current importance in cyber security.	**07**
	(c)	What is FIR and its types? What is the significance of FIR in the Criminal Justice system?	**07**

--- End of Paper---