Seat No.: _____ Enrolment No. 2032

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - I - Jan-2023

Subject Code: CTMSCS-S1-P5 **Date: 17/01/2023**

Subject Name: Introduction to Forensic Science and Law

Time: 11:00AM to 02:00PM

Total Marks: 100/90/63

Instructions:

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

			Marks
Q.1	(a)	Explain the terms "MODUS OPERANDI" and "CORPUS DELICTI"	05/2
	(b)	Write short note on: Central Finger Print Bureau (CFPB) Or Government Examiner of Questioned Document (GEQD)	05/4
	(c)	Briefly mention the duties of a Forensic Scientist.	07/5
Q.2	(a)	What is Chain of Custody? Highlight the significance.	05/4
	(b)	What is Narco-Analysis? Explain the procedure of conducting the test and also mention any two hypnotic drugs used for the same. Or Explain the organizational set up of Central Forensic Science Laboratory.	05/2
	(c)	Elaborate about the various tools & techniques applied in the investigation of various physical evidences. Or Explain the collection, packaging techniques and transportation of cyber evidences found on and recovered from a scene of crime.	07/4
Q.3	(a)	Schematically explain the types of courts in India. What kind of criminal/civil cases are being taken up by these courts and been given the conviction? Or What do understand by Cyber Crime? What are the recent fraudulent practices being opted by attackers/hackers/offenders to commit a cyber-frauds?	08/6
	(b)	Write briefly on: i- Section 320 IPC ii- Section 304A IPC iii- Section 45A IEA	08

17/11

17/10

16/6

		iv- Section 138 IEA v- Section 293 CrPC vi- Section 291A CrPC vii- Section 66A IT ACT 2000 viii- Section 67B IT ACT 2000	
Q.4	(a)	Explain the three major Crime Programmes run by the INTERPOL.	05
	(b)	Highlight the main differences between Cognizable and Non-Cognizable offences.	05
	(c)	Explain in detail the principles of Forensic Science.	07
Q.5	(a)	Explain in detail the components of a forensic science report.	05
	(b)	Elaborate Bailable offences and Non-Bailable offences with examples.	05
	(c)	Mention and thoroughly explain the several divisions or branches of Forensic Sciences.	07
Q.6	(a)	Explain the mentioned below: i- CCTNS ii- CDTS iii- NCRB iv- NIA	08
	(b)	In a suspected murder case, the investigating officer recovered a 9-inch sharp knife near the victim's body. Blood stain produced by direct contact of knife blade was observed on the lower part of denim Jeans worn by the victim. Fingerprint expert lifted blood-stained fingerprint from a table lying near the victim. An open running laptop along with a smartphone was also present on the table. On exiting the premises, the I.O observed a CCTV installed just outside the main door of the house. All exhibits were collected, sealed and sent for forensic analysis. Answer the following: i- What information can be furnished by bloodstained fingerprint present on the table? ii- The investigation in this case should be carried out under which sections of IPC? Also, explain the sections. iii- Explain the recovery, preservation and examination the CCTV footage and other smart devices found from the scene of occurrence. iv- How will you establish the presence of attackers at the scene of crime considering the same scenario where CCTV footage and blood prints are not there present at the scene?	08

END OF PAPER

Seat No.: _____ Enrolment No. 2634

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. (Cyber Security) - Semester –I- January 2023

Subject Code: CTMSCS SI P4 **Date: 11/01/2023**

Subject Name: Artificial Intelligence

Time: 11 AM TO 2 PM **Total Marks: 100**

Instructions:

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

Marks

Q.1 **(a)** Define an Intrusion Detection system (IDS). How can Machine learning be applied to IDS? 06/4

OR

Write a note on different types of Python libraries: **I.** NumPy **II.** Pandas **III.** Matplotlib. Give at least **TWO** functions/methods from each library.

(b) Explain underfitting and overfitting. List one method each to avoid underfitting and overfitting. 06/5

(c) Explain in detail the Recurrent Neural Network along with its applications. 08/7

Q.2 **(a)** Explain the following terms using an example: 1) Mean 2) Median 3) Mode 4) Standard deviation and 5) Variance 06/20

OR

Solve the system of linear equation $x - 2y = 1$ and $3x + 2y = 11$. (1, 3)

(b) Explain ways to handle the missing values in data. 06

(c) Consider the following set of points of the form (x, y): {(30, 60), (40, 80), (50, 100)}. Find the least square regression line for the given data points. Using resultant regression line predict the value of y when x = 10. 08

y = 2x + 0 / y = 20

OR

Discuss in detail the various types of Machine learning models.

Q.3 **(a)** Consider the following training data for the **Naive Bayes Classifier**. 10/10

chills	runny nose	headache	fever	flu?
Y	N	Mild	Y	N
Y	Y	No	N	Y
Y	N	Strong	Y	Y
N	Y	Mild	Y	Y
N	N	No	N	N
N	Y	Strong	Y	Y
N	Y	Strong	N	N
Y	Y	Mild	Y	Y

Determine the class of the candidate (Flu =Y/ Flu = N) for the following data. Show step by step execution. 2/15 1/90

Chills	Runny nose	Headache	Fever	flu
Y	N	Mild	Y	? Yes

OR

Define cluster analysis. List and briefly explain types of Clustering. Discuss any ONE clustering algorithm.

(b) Explain in detail the Convolutional Neural Network architecture (CNN). List any two applications of CNN.

Q.4 (a) Explain in brief the different types of layers in an Artificial Neural Network (ANN). Differentiate between single layer neural network and multi-layer neural network

OR

Define activation function and explain its importance. Explain any 4 activation functions in detail.

(b) Write a short note on Face Detection methods and list any two applications of face detection.

(c) Explain Anomaly detection using Machine learning.

OR

Define object tracking. List and discuss types of object tracking. Explain object tracking algorithm with an example.

Q.5 (a) Illustrate with a help of an example the working of a Perceptron model.

(b) Define Image Segmentation. List and discuss various types of Image Segmentation.

OR

Explain in general the end-to-end steps in Natural Language Processing.

(c) Explain the Pattern Recognition process along with its Advantages and Disadvantages

OR

Compute any **8 values** from the following **True Positive**, **True Negative**, **False Positive**, **False Negative**, **Accuracy**, **Error Rate**, **Precision**, **Recall**, **Sensitivity**, **Specificity** and **F1-Score** for the following confusion matrix.

		Predicted	
		Positive	**Negative**
Actual	**Positive**	1884	47
	Negative	36	1007

END OF PAPER

Seat No.: _____ Enrolment No. 2034

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - I JAN 2023

Subject Code: CTMSCS SI P3 **Date: 13/01/2023**

Subject Name: Web Application Security

Time: 11:00 AM to 2:00 PM **Total Marks: 100**

Instructions:

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

		Write any five questions	**Marks**
Q.1	(a)	What is information gathering? Types of information gathering.	04
	(b)	Define CVE and CWE.	04
	(c)	Explain privilege Escalation and its type.	04
	(d)	Write about HTTP vs HTTPS	04
	(e)	Define Cookies and Sessions with example	04
	(f)	Define terms: - -Vulnerability -Threat -Attack -Shellcode.	04
		Write any two questions	
Q.2	(a)	What is VAPT and Importance of vulnerability assessments?	12
	(b)	Explain Broken Authentication and Authorization	12
	(c)	Explain NMAP and Its Scanning Techniques.	12
		Write any four questions	
Q.3	(a)	Explain google hacking and steps for google hacking.	08
	(b)	Explain Encoding and types of Encoding.	08
	(c)	Explain "Using Components with Known Vulnerabilities" with one scenario.	08
	(d)	Explain TCP header.	08
	(e)	Explain File Inclusion Vulnerability.	08
		Write any two questions	
Q.4	(a)	Explain Security Misconfiguration and Sensitive Data Exposure.	12
	(b)	Write a note on Vulnerability assessment Security scanning process.	12
	(c)	What is CMS? And Why CMS Security is important.	12

END OF PAPER

Seat No.: _____ Enrolment No. 2034

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - I - Jan-2023

Subject Code: CTMSCS SI P2 **Date: 09/01/2023**

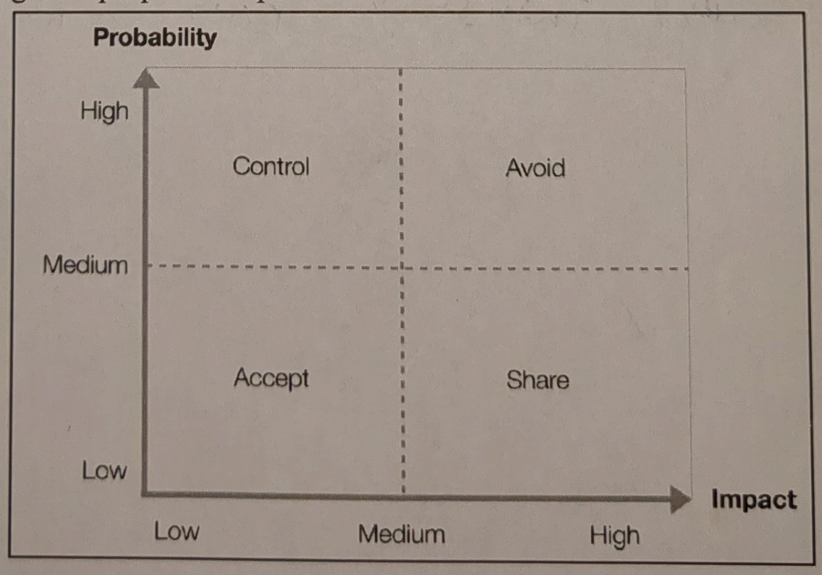
Subject Name: Cyber Security Audit and Compliance

Time: 11:00 – 14:00 **Total Marks: 100**

Instructions:

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

			Marks
Q.1	**(a)**	What is Access Control? Explain the effective solutions to implement this control.	04
	(b)	Define the following term. • Risk Analysis • Governance • Compliances • Risk Mitigation	04
	(c)	Explain the Operations Security control according to ISO 27000 standard in detail.	08
	(d)	Write a detailed note on COBIT5.	09
Q.2	**(a)**	Explain SOC Compliance Reports briefly.	04
	(b)	State the difference between Guideline and Policy.	04
		OR	
	(b)	How to maximize C-I-A of workstation domain.	04
	(c)	Read the figure given below and explain all risk management strategies along with proper examples.	08



(d) Explain any 5 controls of IT Infrastructure with its risk, recommendation and example. 09

Q.3 (a) Write full form of the following: 04
i) HIPAA
ii) NIST
iii) PCI-DSS
iv) BCP

(b) What are the classification of Information? 04

(c) Discuss Disaster Recovery Planning and its various strategies. 08

OR

(c) What Must Your Organization Do to Be in Compliance? 08

(d) Describe the life cycle of BCP. 09

Q.4 (a) What is segregation of duties? 04

OR

(a) How to maximize C-I-A of LAN domain. 04

(b) Explain CAAT with various application control. 04

(c) If you are an auditor, then explain the process of cyber security audit carried out by you. 08

(d) Discuss the process of selecting and implementing effective controls in an organization. 09

OR

(d) Write a note on GDPR and its articles. 09

*****

END OF PAPER

Health Insurance Portability and accountability Act

Payment card industry Data security standard

Seat No.: _____ Enrolment No. 2034

32- Page

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. -CS - Semester -I - Jan-2022

Subject Code: CTMSCS SI P1 **Date: 05/01/2023**

Subject Name: Essentials of Cyber Security and Cyber Warfare

Time: 3 Hours **Total Marks: 100**

92

Instructions:

1. **Write down each question on separate page.**
2. **Attempt all questions.**
3. **Make suitable assumptions wherever necessary.**
4. **Figures to the right indicate full marks.**
5. **Parts of question should be attempted at the same place.**

			Marks
Q.1	(a)	Consider different types of users in the Windows OS and explain the privilege escalation in the Windows OS.	05
	(b)	What is Windows Integrity Control (WIC)? Also compare various levels of WIC with respect to trustworthiness.	05
	(c)	What is Operating System hardening? explain few examples.	07
Q.2	(a)	What are different file permissions in the windows OS?	05
	(b)	With the help of example explain *ipconfig* and *ifconfig*?	05
	(c)	Differentiate the Userspace and Kernal Spaces.	07
Q.3	(a)	Consider the following scenario for the Windows Passwords:	08

S.No.	Username	Password	HASH
01	User1	NFSU_GOA_123	ASDFGHJKL987
02	User2	Nfsu_gandhinagr_456	ZXCVBNMP654
03	User3	Nf$u	QWERTYUI321

(i) With respect to the above table, comment on the password strength and security as per the standard policy and guidelines.

(ii) Also identify the strong password from the above table and explain the possible attacks on the HASH.

(iii) How you will overcome this problem?

Q.3	(b)	With the help of Windows Task Manager, answer the followings: (i) Write step by step process to identify the suspicious process. (ii) Why is chrome process considered as the special case? **OR** Write a shot note on Windows Logs.	08

Q.4	(a)	What is cyber espionage? Also provide the example form recent cases. **OR** Explain any five windows and linux commands use for security incident respond.	05
	(b)	What is the significance of ***iptable*** in the Linux hardening? Also provide the example.	05
	(c)	You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log into your account and fix the problem. What should you do?	07
Q.5	(a)	What is Information assurance (IA)? Also explain its five important pillars. **OR** Explain CHMOD, CHROOT and CHOWN in terms of Linux OS.	05
	(b)	What is Psychological Warfare? Also explain three types of propaganda.	05
	(c)	Define the process of salting. What is the use of salting? **OR** Write a note on **sysinternals** suite.	07
Q.6	(a)	(i) How can an attacker exploit the rootkit attack? What is the use of loadable kernel modules (LKMs) in this attack? (ii) With the help of suitable example, explain the 80/20 rule of functionality?	08
	(b)	Explain any case study on cyber warfare like critical infrastructure information breach incident by state sponsor attack groups.	08

END OF PAPER