

Seat No.: _____

Enrolment No. _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - II - August - 2022

Subject Code: CTMSCS SII P1

Date: 01/08/2022

Subject Name: Network Security

Total Marks: 100

Time: 11:00 to 2:00 PM

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 Protocol and its type	05
(b) Explain Three-way handshake	05
(c) Explain OSCAR Methodology	07
OR	
Explain any seven Wireshark filters with syntax	
Q.2 (a) Explain Flow analysis techniques	05
(b) Explain DNS in Detail	05
(c) Explain Encryption and its Type with Example.	07
Q.3 (a) Explain TCP Header and UDP Header	08
(b) Explain TCP Segment Header	08
OR	
Explain GRE Protocol and use of GRE	
Q.4 (a) Explain Web Proxy and its types.	05
(b) Explain Reconnaissance and enumeration	05
OR	
(c) Explain CAM Overflow in details	
(c) Explain SMTP in Detail with diagram	07
Q.5 (a) Explain Authentication Server	05
(b) Explain CIA Triage	05
(c) NIDS VS NIPS	07
Q.6 (a) Explain Authentication and its type in detail	08
(b) Explain OSI Model in Detail	08

Generic Routing
Encapsulation

END OF PAPER

NATIONAL FORENSIC SCIENCES UNIVERSITY**M.Sc. Cyber Security - Semester - II - Aug-2022****Subject Code: CTMSCS SII P3****Date: 03/08/2022****Subject Name: Mobile Security****Time: 11:00 AM to 2:00 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	
(a) Write the ADB commands?	05
(b) Write short notes on android content provider?	05
(c) Explain insecure logging and hardcoding issues?	05
Q.2	
(a) Explain Android Manifest file with example?	05
(b) Write short notes on reverse engineering in android applications?	05
Q.3 Attempt Any 2 Questions (7 Marks each)	14
(a) Explain the android application architecture?	
(b) Explain MobSF (Mobile Security Framework) in detail?	
(c) Explain the Android application security vulnerability assessment using QARK?	
Q.4 Attempt Any 3 Questions (7 Marks each)	21
(a) Explain Android Boot Process in Detail?	
(b) Differentiate Static Analysis Vs Dynamic Analysis?	
(c) Explain Security Auditing with Drozer?	
(d) Explain Mobile Application Security Pen-Testing Strategy?	
Q.5 Attempt Any 2 Questions (8 Marks each)	16
(a) Explain OWASP Top-10 vulnerabilities for Mobiles?	
(b) What is application permission? List types of permission. Write a step to request permission.	
(c) Explain the Frida and Objection framework for android dynamic instrumentation?	
Q.6 Attempt Any 3 Questions (8 Marks each)	24
(a) Explain Jadx, Jdgui, and Dexdump reverse engineering process?	
(b) Explain Android Partitions and File Systems?	
(c) Explain inter-process communication of android applications?	
(d) Explain android traffic passive analysis and active analysis?	

NATIONAL FORENSIC SCIENCES UNIVERSITY**MSc Cyber Security – Semester II – August 2022****Subject Code: CTMSCS SII P4****Date: 04/08/2022****Subject Name: Incident Response & Digital Forensics****Time: 11.00AM to 2.00PM****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)	Explain CIA.	05
	(b)	Write a note on DAC, MAC, RBAC, MLS. [OR] Write a note on Authentication, Authorization, Accountability	05
	(c)	Write a brief note on Post Incident Activity.	07
Q.2	(a)	Write a note on Incident Prioritization.	05
	(b)	Write a short note on signs of Incidents.	05
	(c)	What is computer security incident? Discuss any 5 types of Incidents. [OR] Discuss any 7 types of malware with the best mitigation possible for each one of them.	07
Q.3	(a)	Discuss Preparation and Identification phase of incident handling.	08
	(b)	Discuss Containment and Eradication phase of incident handling	08
Q.4	(a)	What is Slack Space?	05
	(b)	Explain packaging, labeling and transportation aspect of Digital Forensic Investigation. [OR] Write a note on Incident Response Team Roles.	05
	(c)	Explain the digital forensic process	07
Q.5	(a)	What is Chain of Custody	05
	(b)	Write a note on estimating the cost of handling the incident.	05
	(c)	Explain the cybercrime investigation SOP.	07
Q.6	(a)	Explain Acquisition Techniques and types of acquisition types for mobile devices and computers.	08
	(b)	What is Digital Forensics, Discuss it's importance and Discuss the challenges in digital forensics. [OR] Write a case-study explaining the importance of Digital Forensic Investigation.	08