Seat No.: 2581 Enrolment No. 016

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

END OF PAPER

Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security (W.E.F. 2021) Examination – August-2022

Subject Code: CTMSCS SII P2 **Date: 02/08/2022**

Subject Name: Malware Analysis

Time: 11:00AM-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 Process Injection.	05
	(b)	Write a short note on reverse engineering tool and its effectiveness in malware analysis.	05
	(c)	What is Cyber-Warfare? Explain with the help of a case study with respect to Malwares OR Explain common executable DLLs of windows with function services.	07
Q.2	(a)	What is anti-virtual machine in malware analysis?	05
	(b)	What is a rootkit?	05
	(c)	Explain malware sandboxing. How various parameters can be identified from sandbox based malware analysis?	07
Q.3		**Write any Two Answer**	
	(a)	What is debugging with stages?	08
	(b)	What are malwares? Explain any 3 types of malwares with examples.	08
	(c)	Explain PE File Headers and Sections	08
Q.4	(a)	Explain some of the advantages of using Assembly Language.	05
	(b)	Explain difference between process explorer and process monitor sysinternal tools.	05
	(c)	What are the goals of malware analysis?	07
Q.5	(a)	How Deep Packet Inspection of network packets can be used in malware forensics? Or What is volatile data in digital forensics?	05
	(b)	Elaborate Malware Process Injection	05
	(c)	Explain simple C code in assembly language. Or Explain malware lab setup stages with example.	07
Q.6		**Write any Two Answer**	
	(a)	Explain any four instruction set of X86 in terms of malware analysis.	**08**
	(b)	Explain APT and its life cycle in detail.	**08**
	(c)	Explain different malware analysis techniques with example.	**08**

Seat No.: _____ Enrolment No. _____

NATIONAL FORENSIC SCIENCES UNIVERSITY

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

Subject Code: CTMSCS SII P3
Subject Name: Mobile Security
Time: 11:00 AM to 2:00 PM **Date: 03/08/2022**

Instructions: **Total Marks: 100**

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)**		
	(a)	Explain the android application architecture?	14
	(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)**		
	(a)	Explain Android Boot Process in Detail?	21
	(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)**		
	(a)	Explain OWASP Top-10 vulnerabilities for Mobiles?	16
	(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)**		
	(a)	Explain Jadax, Jdgui, and Dexdump reverse engineering process?	24
	(b)	Explain Android Partitions and File Systems?	
	(c)	Explain inter-process communication of android applications?	
	(d)	Explain android traffic passive analysis and active analysis?	

END OF PAPER

Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

MSc Cyber Security – Semester II – August 2022

Subject Code: CTMSCS SII P4

Subject Name: Incident Response & Digital Forensics **Date: 04/08/2022**

Time: 11.00AM to 2.00PM

Instructions: **Total Marks: 100**

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

IR & Digital Forensics
Lab Practical Work

GROUP B:

Q1) Oh Damn!!! I am not able to understand a single damn thing. Hey You, please help me identify the following things from the attached logs (Apache) and Prepare a Report Stating the same. [30]

1. Total No. of Unique IP Addresses.
2. List of All Unique IP Addresses.
3. Total No. of Countries Involved
4. Countries with Maximum Request.

(Hint 1: Use SAWMILL or any other log analysis tool to have a look at logs)

The file name is apache_logs (URL: shorturl.at/fgrwM)

Q2) Perform a user defined activity and identify the event logs using sysmon & create a custom view filter in Event Viewer showing the event with Individual's Name. [30]

Q3) Installation of WAZUH and identifying attacks based on any user defined scenario. [40]