National Forensics Sciences University, Goa Campus

Mid-semester Examination

Branch – MSc Cyber Security
Subject Name- Incident Response & Digital Forensics
Max. Marks- 50

Sem-II **Date** - 20-4-2023
Subject Code – CTMSCS SII P4
Time- 1.5 Hours

Instructions:

1. Answer all questions as per the sequence of question number
2. Assume suitable data, wherever applicable

Q.1 Solve ANY FOUR **20 marks**

a. Define incident. Draw a suitable diagram and explain the incident handling process in detail. 5 marks

b. A computer having IP address 192.168.0.10 is connected to the LAN. How to confirm that the computer is not infected by a botnet? 5 marks

c. Write in brief how Splunk can help in real-time log analysis. 5 marks

d. What is timeline analysis? How vertical timeline is different from the Gantt chart timeline? 5 marks

e. An IOT device is placed in the paddy field for regular field assessment. It is sending data to the cloud server along with the other sensors. What are the preventive measures required to safeguard these sensors from malware? 5 marks

Q.2 Attempt all **15 marks**

a. “information warfare is a battle fought in cyberspace, online, and over computer networks.” Considering this situation, justify how the CIA plays an important role in the Indian defense system. 5 marks

b. How password attack is different from a DDOS attack? How to prevent a system from these attacks? 5 marks

c. Using a suitable diagram suggest steps for incident response. 5 marks

Q. 3 Attempt a and b **15 marks**

Q.3 a Attempt any one

Q.3 a Give four key reasons why incident prioritization is important. 8 marks

OR

Q.3 a What is the need for data management in a data warehouse? What are the data recovery technologies used by these organizations? 8 marks

Q.3 b Attempt any one 7 marks

Q3 b Define virtualization. How to create a virtualization environment for resource management?

OR

Q3 b Write in detail about the following incident-reporting organizations: 7 marks

a) National Institute of Standards and Technology (NIST)

b) Open Web Application Security Project (OWASP)

END OF PAPER

National Forensics Sciences University, Goa Campus

Mid- semester Examination

Branch – Cyber Security	**Sem –** II	**Date-** 19/04/2023
Subject Name - Mobile Security		**Subject Code** - CTMSCS SII P3
Time- 1.5 Hours		**Max.Marks- 50**

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

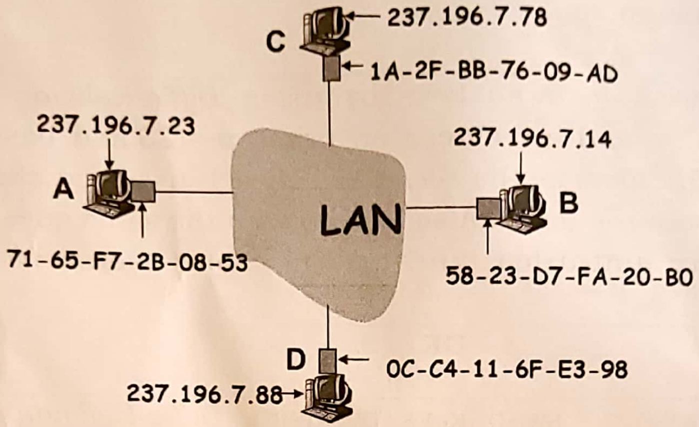
Q.1	Solve any four	20 marks
	a. What are ADB commands. Explain any five of them.	5 marks
	b. Explain important features of Santoku. Why it is important for mobile forensics?	5 marks
	c. What is Pen-testing? Explain different strategies for Pen-Testing.	5 marks
	d. What is Secure Inter Process Communication? android [illegible] stub	5 marks
	e. Discuss about hexdump.	5 marks
Q.2	Attempt all	15 marks
	a. What is Dalvik? How it is different from Smali? human readable bytecode	5 marks
	b. What is Android Architecture? Explain with diagram	5 marks
	c. What are different phases of Pen-Testing?	5 marks
Q. 3	Attempt a and b	15 marks
Q.3 a	Attempt any one	
Q.3 a	I) Explain the OWASP top 10 vulnerabilities for Mobiles?	8 marks
	OR	
	II) What is security audit? What are the challenges in conducting the security audit? Discuss different phases of security audit?	
Q.3 a	Attempt any one	7 marks
Q3 b	I) What is reverse Engineering? What is APK tools? Discuss its important features.	
	OR	
	ii) Discuss the vulnerability assessment. Explain different types of vulnerability testing.	7 marks

National Forensics Sciences University, Goa Campus

M.Sc. CS - Semester -II

Mid- Semester Examination

Subject Code: CTMSCS SII P1 **Date: 17/04/2023**
Subject Name: Network Security
Time: 90 Minutes **Total Marks: 50**
Instructions - 1) Answer all questions. 2) Assume suitable data. 3) Scientific Calculator is allowed. 4) Parts of the question should attend the same place.

Q.1	Attempt all.	**20 marks**
(a)	 C 237.196.7.78 1A-2F-BB-76-09-AD 237.196.7.23 A 71-65-F7-2B-08-53 LAN 237.196.7.14 B 58-23-D7-FA-20-B0 D 0C-C4-11-6F-E3-98 237.196.7.88 Consider the above network topology, **User A** wants to communicate with **User B**. Explain the explain ARP protocol with respect to this scenario. Further consider **User C** as the attacker and explain the ARP spoofing in the same topology. Also highlight the all-possible attack vectors and attack surfaces.	5 Marks
(b)	Illustrate ***ElGamal ECC Encryption*** algorithm with the example.	5 Marks
(c)	Encrypt the following message using **Playfair cipher**. Message: **jacuzzi** Key: **jail**	5 Marks
(d)	(i) Calculate the power modulo, $191^{930} \bmod 103$. (ii) Find the value of **Φ(65)** and **Φ (99)**.	5 Marks
Q.2	Attempt all.	**15 Marks**
(a)	Write note on DOS and distributed denial-of-service (DDoS) attacks.	5 marks
(b)	What is the zero point of an elliptic curve?	5 marks
(c)	Explain the differences between error control and flow control.	5 marks
(d)	Define Following terms: (i) Primitive Root (ii) Masquerading (iii) Diffusion (iv) Relatively Prime (v) Avalanche Effect	5 marks

Q.3	Attempt any one.	**15 Marks**
(a)	Use two global prime number ***17*** and ***31***, the value of ***e*** is ***7*** and message ***M*= 3**, calculate the public key, private key, and the corresponding cipher text. Also prove that *RSA* decryption is the inverse of *RSA* encryption.	08 Marks
	OR	
	Use two global prime number ***37*** and ***43***, the value of ***e*** is ***71*** and message ***M*= 2**, calculate the *public key*, *private key*, and the corresponding cipher text. Also prove that *RSA* decryption is the inverse of *RSA* encryption.	
(b)	*Alice* and *Bob* wish to swap keys by using *Diffie-Hellman* key exchange algorithm and are agreed on prime ***p*** = ***23*** and base or generator is ***g*= 5.** Calculate the *secret key* of each user and *shared session key* for both the users. Also explain with the same question that how can *Eve* (untrusted third person) exploit *Man-in-Middle attack.*	07 Marks
	OR	
	Alice and *Bob* wish to swap keys by using *Diffie-Hellman* key exchange algorithm and are agreed on prime ***p*** = ***31*** and base or generator is ***g*= 3**. Calculate the secret key of each user and shared session key for both the users. Also explain with the same question that how can *Eve* (untrusted third person) exploit Man-in-Middle attack.	

**~~~~END OF PAPER~~~~**

National Forensics Sciences University, Goa Campus

Mid- semester Examination

Branch – M.Sc. Cyber Security & M.Sc. DFIS **Sem – II** **Date - 18/04/2023**

Subject Name – Malware Analysis & Malware Analysis & Forensic

Subject Code - CTMSCS SII P3 & CTMSDFIS SII 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. What is hashing, and how is it useful in digital forensics?	5 marks
	b. What information can you obtain from the headers and sections of a PE file, and how is this useful in malware analysis?	5 marks
	c. What is the difference between a function call and a jump in.	5 marks
	d. What is Assembly language, and how is it different from high-level programming languages?	5 marks
	e. What is Dynamic Analysis, and how is it different from Static Analysis?	5 marks
Q.2	**Attempt all**	**15 marks**
	a. List data transfer instruction types and explain anyone with suitable example.	5 marks

	b. Convert this C Program to Assembly Language.
	If (x == 0)
	{
	X = 5;
	}
	Else
	{
	X =1;
	}
	pus abx
		5 marks

	c. As given below output write assembly language program on it. (2501 H) = 99H (2502 H) = 39H Result (2503 H) = 99H + 39H = D2H	5 marks

	Since, 1 0 0 1 1 0 0 1 (99H) + 0 0 1 1 1 0 0 1 (39H) 1 1 0 1 0 0 1 0 (D2H)	
Q. 3	**Attempt a and b**	**15 marks**
Q.3 a	i. What are the different types of CPU registers in x86 and explain common x86 Assembly Language instructions?	8 marks
Q3 b	~~ii.~~ What are some of the techniques used in Dynamic Analysis, and when is each technique most effective?	7 marks