Room No. 4
M.Sc. CS - Sem 2 (12)
Mobile Security

National Forensics Sciences University, Goa Campus
Mid- semester Examination

TA-1 2034

Answer Shift: S17

Branch – Cyber Security
Sem – 3
Date - 28-02-2023
Subject Name - Mobile Security
Subject Code - CTMSCS SII P3
Time- 11:00 A.M. to 11:45 A.M.
Max. Marks- 25
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Multiple Choice Questions (1 mark each)	10 marks
	i. Android was developed by the: a. Open Handset Alliance (OHA) b. Close Handset Alliance c. International Android organization d. None of the above	1 mark
	ii. First commercial version of Android 1.0 (with name Alpha), was released in a. 2007 b. 2008 c. 2009 d. 2006	1 mark
	iii. Google acquired android Incorporation in a. 2004 b. 2005 c. 2006 d. 2007	1 mark
	iv. Activity Manager lies in which layer of android architecture? a. Kernel b. Libraries c. Application Framework d. Applications	1 mark
	v. Which of the following is not the part of application framework? a. Content provider b. View System c. Resource Manager d. Surface Manager	1 mark
	vi. Android's native libraries are written in: a. JAVA b. C or C++ c. Python d. Perl	1 mark

	vii. Which is not an Android Application Components: a. Activity b. Service c. Content d. Assembler	1 mark
	viii. Intent cannot be used for: a. Start Activity b. Broadcast Intent c. Start service d. Start application	1 mark
	ix. Which is not a type of intent a. Explicit b. Implicit c. None	1 mark
	x. Sandboxing is: a. isolate applications from each other b. Connect applications	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
	i. What is Security? What could be possible threats for mobiles?	5 marks
	ii. What is Android Architecture? Explain with diagram.	5 marks
	iii. write about main Application components.	5 marks
	iv. What is Secure Inter Process Communication?	5 marks

National Forensics Sciences University, Goa Campus
Mid- semester Examination

2034

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. (Network, web, wireless, Phone, Social, Physical)	5 marks
	d. What is Secure Inter Process Communication?	5 marks
	e. Discuss about hexdump.	5 marks
Q.2	Attempt all	15 marks
	a. What is Dalvik? How it is different from Smali?	5 marks
	b. What is Android Architecture? Explain with diagram	5 marks
	c. What are different phases of Pen-Testing? (Reconnaissance, Scanning, Gaining Access, Maintaining Access, Clearing Tracks)	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. (Network, web, wireless, Phone, Social, Physical)	7 marks

Seat No.: _____ Enrolment No. 234

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - II - July-2023

Subject Code: CTMSCS SII P3 **Date: 12/07/2023**

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. **Figures to the right indicate full marks.**

Marks

Q.1 Attempt Any 3 Questions (8 Marks each) **24**

(a) Explain Android Architecture in detail.

(b) What is Application Sandboxing? Explain Secure IPC.

(c) What is ADB? Explain ADB Commands with example

(d) What is DVM? Explain execution of DVM with the comparison of JVM

Q.2 Attempt Any 3 Questions (8 Marks each) **24**

(a) Explain Android Boot Process in Detail.

(b) What is the use of Android Manifest? What we can write into Manifest file. Explain it with example of Manifest file.

(c) List OWASP Top-10 vulnerabilities for Mobiles. Explain any three vulnerabilities in details.

(d) What is the use of JADX, JDGUI and DexDump Reverse Engineering

Q.3 Attempt Any 3 Questions (8 Marks each) **24**

(a) What is App Permission? Write a steps to request the permission.

(b) Explain Mobile Application Security Pen-Testing Strategy

(c) What is Reverse Engineering? Explain it using APK Tool

(d) What is Intent? Explain types of Intent with example.

Q.4 Attempt Any 2 Questions (7 Marks each) **14**

(a) Explain MobSF (Mobile Security Framework) in detail?

(b) Explain Security Auditing with Drozer.

(c) Explain QARK with features, advantage, modes, pros and cons.

Q.5 Attempt Any 2 Questions (7 Marks each) **14**

(a) What is Android Traffic Interception. Explain ways to analyze the Android traffic.

(b) Explain Dynamic Instrumentation using Frida with commands.

(c) Explain step by step Active Analysis of Android Traffic using Burp Suite.

END OF PAPER

Date: 28/2/2023

Time: 3:00 to 3.45 pm. TA -1 Examination

MSc – Cyber Security (Sem -II)

CTMSCS S1 P4: Incident Response and Digital Forensics

Room No: 4
MSc CS (IE)
Incident Response

(Max Marks: 25)

Q1 . Answer the following questions (1 x 10 = 10)

1. Cybersecurity is primarily about? A. people B. processes C. technologies D. All of the above
2. What was the name of the first antivirus software? A. ray Tomlinson B. tinkered C. reaper D. repair
3. What describes the immediate action taken to isolate a system in the event of a breach? A. Containment B. Eradication C. Recovery
4. Incidents should be reported to ___? (a) The CERT Coordination Center (b) user (c)client
5. Which type of controls restore the system after a disaster or an event? A. Preventive controls B. Detective Controls C. Corrective controls
6. A..... is a small program embedded inside of a GIF image (a) Web bug (b) Cookie (c) Spyware application.
7. A hacker contacts your phone or E-mails and attempts to acquire your password is called (a) Spoofing (b) Phishing (c) Bugging
8. The main reason to encrypt a file is to (a) Reduce its size (b) Secure it for transmission (c) Prepare it for backup
9. Which one of the following is a key function of a firewall? (a) Monitoring (b) deleting (c)copying
10. A document that contains a description of any event that has happened, which requires further investigation is called _____ A. test Summary report. B. incident report.

Q2: Answer ANY THREE questions (5 x 3 = 15)

a) Define incident. How I/O panel connectors and SATA connectors can be used to minimize computer incidents?

b) Define information security. Explain how the distributed database and centralized database can be secured to avoid incidents.

c) Data integrity is more important than data availability in Chat GPT. Justify your views.

d) What are the steps for incident response, explain using suitable diagram.

2034

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** 19 15

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** 10

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

Seat No.: 2023 Enrolment No. 2023

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester – II, July 2023

Subject Code: CTMSCS SII P4 **Date: 13/07/2023**

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		**Write any five questions**	
	(a)	What are events and incidents?	04
	(b)	What is the difference between imaging and cloning.	04
	(c)	What is and Incident Category and list-out all the categories	04
	(d)	What is Write-Blockers? and Importance of Write Blockers.	04
	(e)	Explain Terms with Example 1.Viruses 2.Spyware 3.Adware 4.Ransomware	04
	(f)	Explain estimating the cost of incidents.	04
Q.2		**Write any two questions**	
	(a)	Elaborate on any 2 computer security incidents. Suggest how to handle such incidents to avoid system failure?	12
	(b)	What are the roles and responsibilities of the incident response team? Elaborate in detail.	12
	(c)	What are the steps required to acquire digital evidence? Explain using a suitable diagram.	12
Q.3		**Write any four questions**	
	(a)	Explain Preparation, Identification, Containment in Details.	08
	(b)	Explain Sign of Incident with Classification.	08
	(c)	What makes you an ideal candidate for a position of incident manager in a network related organization?	08
	(d)	A technology-based company suggested data replication and virtualization as a disaster recovery solution. Justify your answer	08
	(e)	Explain Data Classification with all the categories.	08
Q.4		**Write any two questions**	
	(a)	Explain IRM reports with necessary information with any recent case study with root cause.	12
	(b)	What are the important artifacts related to user activities? How SIEM Tools analyze these artifacts?	12
	(c)	Explain Digital Forensics with proper discussion of "Branches of Digital Forensics"	12

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;
	}
		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

Attempt → 40
Skip → 13 out of 17
Remain → 23
Need → 12

Seat No.: _____ Enrolment No. 7034

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security- Semester End Examination-July-2023

Date: /07/2023

Subject Code: CTMSCS SII P2
Subject Name: Malware Analysis
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.**

			Marks
Q.1	(a)	How to detect the packer? Explain any three methods.	04
	(b)	How to analyzed dynamic linking and run-time linking libraries.	04
	(c)	Explain the Unpacker stub and unpacking methods in detail. **OR** Set-up an ideal lab for dynamic analysis of the malware.	06
	(d)	Illustrate the importance of malware analysis in the industrial aspects.	05
Q.2	(a)	Explain PE Header and its sections. **OR** Discuss pros and cons of Sandbox.	03
	(b)	Discuss Disassembly and their types/algorithms.	07
	(c)	Explain CPU Register their types along with the examples.	08
	(d)	Explain at least 4 types of malwares with their characteristics, behaviour and real life case study in brief.	05
Q.3	(a)	Three functions are commonly found in cases of direct injection: VirtualAllocEx , WriteProcessMemory , and CreateRemoteThread. Explain them briefly.	02
	(b)	Explain the key-logger behavior from Figure 2.0 from page no. 2 **OR** State the difference between Kernal mode and User mode debugging.	02
	(c)	Explain Reverse Engineering process and some important features of IDA Pro.	06
	(d)	Write a detailed note on Breakpoint and its types.	03
Q.4	(a)	What is Hook Injection?	03
	(b)	Explain four major section of main memory.	04
	(c)	Bob is analyzing a malware and he finds an interesting code snippets while doing reverse engineering. Bob needs help from you to understand the code snippet shown at figure 1.0 in page no.2	08

	(d)	Discuss Anti-Reverse Engineering techniques with its types and examples. **OR** Explain any 9 assembly instructions with proper example and description.	09

```
0040286F   push    2                  ; samDesired
00402871   push    eax                ; ulOptions
00402872   push    offset SubKey      ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877   push    HKEY_LOCAL_MACHINE ; hKey
0040287C ❶call     esi ; RegOpenKeyExW
0040287E   test    eax, eax
00402880   jnz     short loc_4028C5
00402882
00402882 loc_402882:
00402882   lea     ecx, [esp+424h+Data]
00402886   push    ecx                ; lpString
00402887   mov     bl, 1
00402889 ❷call     ds:lstrlenW
0040288F   lea     edx, [eax+eax+2]
00402893 ❸push     edx                ; cbData
00402894   mov     edx, [esp+428h+hKey]
00402898 ❹lea      eax, [esp+428h+Data]
0040289C   push    eax                ; lpData
0040289D   push    1                  ; dwType
0040289F   push    0                  ; Reserved
004028A1 ❺lea      ecx, [esp+434h+ValueName]
004028A8   push    ecx                ; lpValueName
004028A9   push    edx                ; hKey
004028AA   call    ds:RegSetValueExW
```

Figure – 1.0

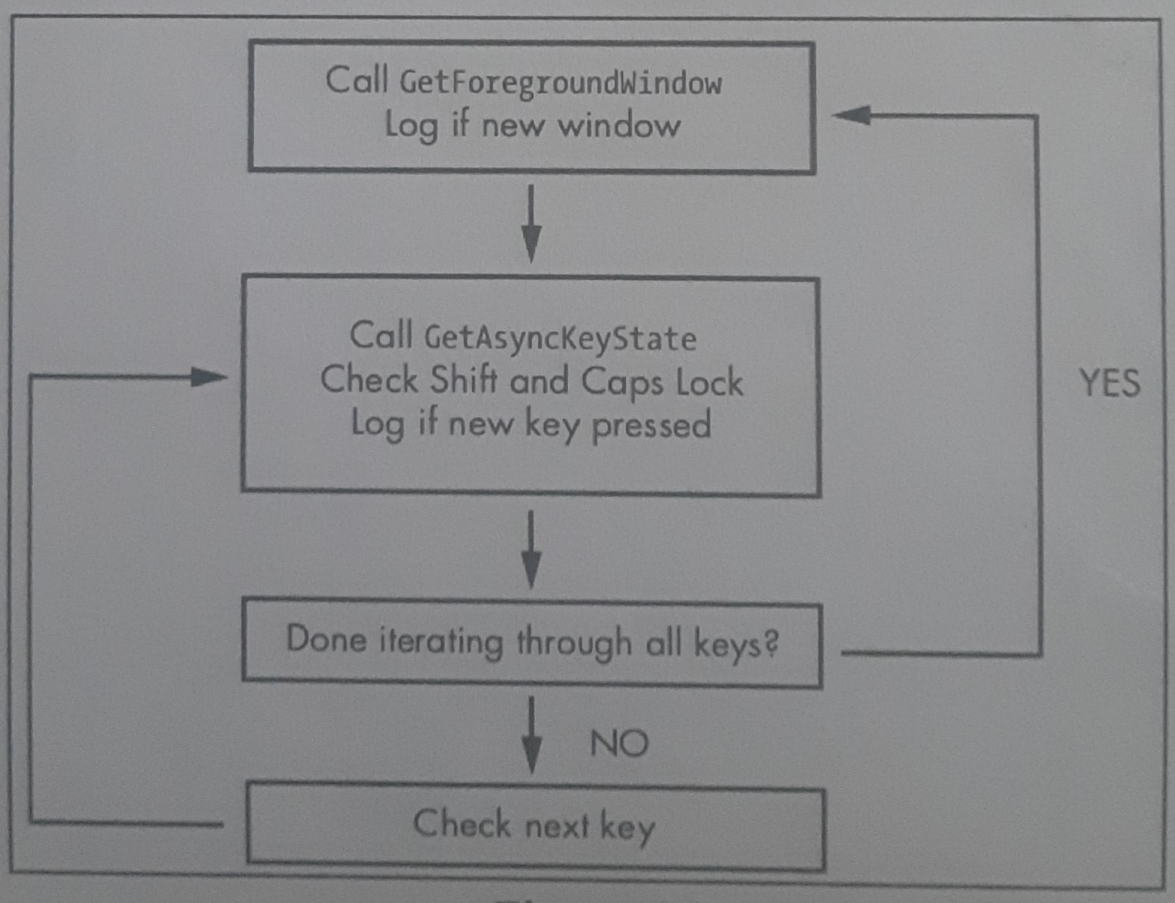

Figure - 2.0