BINUS University

Academic Career: ***Undergraduate / ~~Master~~ / ~~Doctoral~~ *)***			**Class Program:** ***~~International~~ / Regular / ~~Smart Program~~ /*** ***~~Global Class~~ / ~~BINUS Online Learning~~ *)***		
☑ **Mid Exam** ☐ **Final Exam**	☐ **Compact Term Exam** ☐ **Others Exam : _____**		**Term : ~~Odd~~ / Even / ~~Compact~~ *)** **Period (Only for BOL) : ~~1~~ / ~~2~~ *)**		
☑ **Kemanggisan** ☐ **Alam Sutera** ☐ **Bekasi**	☐ **Senayan** ☐ **Bandung** ☐ **Malang**	☐ **Semarang**	**Academic Year :** **2022 / 2023**		
Exam Type*	:	~~Onsite~~ / Online	Faculty / Dept.	:	School of Computer Science
Day / Date**	:	Wednesday / May 03rd 2023	Code - Course	:	COMP68440001 – Mobile Penetration Testing
Time**	:	13:00	Code - Lecturer	:	Team
Exam Specification***	:	☐ Open Book ☐ Open Notes ☐ Close Book ☐ Submit Project ☐ Open E-Book ☐ Oral Test	BULC (Only for BOL)	:	-
			Class	:	All Classes
Equipment***	:		Student ID ***	:	
☐ Exam Booklet ☐ Laptop ☐ Drawing Paper – A3 ☐ Calculator ☐ Tablet ☐ Drawing Paper – A2 ☐ Dictionary ☐ Smartphone ☐ Notes			Name ***	:	
			Signature ***	:	
*) *Strikethrough the unnecessary items* **) *For Online Exam, this is the due date* ***) *Only for Onsite Exam*					

Please insert the test paper into the exam booklet and submit both papers after the test.

The penalty for CHEATING is DROP OUT!

Learning Outcomes:

LO 1: Describe Android Application Life Cycle and Fundamental
LO 2: Perform Static Analysis and Dynamic Analysis of Android Application
LO 3: Identify API and Android Application Vulnerabilities
LO 4: Analyze and Recommend Hardening Strategy for Android Application

I. Essay (20 %)

1. **[LO 1, 20 %]**

   Read and **analyze** the most-recent case about J&T APK scam: https://www.kompas.com/tren/read/2022/12/02/120200965/viral-unggahan-soal-dugaan-modus-penipuan-via-pengecekan-resi-format-apk?page=all

Verified by,

Nadia – D5782 and sent to Cyber Security Program on 03 27, 2023

Why do you think the perpetrators choose Android platform to distribute the malicious application? Why do you think these kinds of scams are more seldom occurred in iOS platform? Use **factual** and **data** to support your argument.

II. Case Study (80 %)

2. [LO 2, LO 3, & LO 4, 80 %] Practical Penetration Testing

Read and **understand** the specified OWASP MASTG v1.5.0 requirements below:

- Data Storage and Privacy Requirements (MSTG-STORAGE-*)
- Resilience Requirements (MSTG-RESILIENCE-*)
- Cryptography Requirements (MSTG-CRYPTO-*)
- Network Communication Requirements (MSTG-NETWORK-*)

After that:

a. **Identify** at least **4 (four) issues/vulnerabilities** in the APK that violates any of the OWASP MASTG v1.5.0 requirements stated above.
b. For each of the identified issues/vulnerabilities, create a Penetration Testing report in accordance with the "**Executive Summary – POC – Recommendation**" format. See below for a report example.
c. You are allowed to perform *dynamic analysis* on the APK. However, be sure to **always provide at least 1 evidence** based on ***static analysis*** to support the argument in your report (e.g., snippets of vulnerable code, *proof-of-concept* to mod the APK, etc.).

Read Carefully:

- Use this OWASP MASTG v1.5.0 checklist as a source of reference: https://github.com/OWASP/owasp-mastg/releases/download/v1.5.0/Mobile_App_Security_Checklist_en.xlsx
- You can download the APK here (Use password: **MobPenE23**): https://binusianorg-my.sharepoint.com/personal/chrisando_pardomuan_binus_edu/_layouts/15/guestaccess.aspx?share=Ev-g9OeA-45Bnov4O9wRIwIBdVzXUmJHalwmBnD01iqu7Q&e=cwlQBK
- Find a CTF-style Flag (i.e., MOBPEN{a-zA-Z0-9_}) inside the APK for a **+5 bonus points ☺.**

Report Example

A. Issue:
Weak Root Detection (MSTG-RESILIENCE-1)

B. Executive Summary:
We discovered that implements a rather weak Root Detection mechanism that could easily bypassed by even an inexperienced penetration tester. This issue occurred because the application only checks for the existence of a "Superuser.apk" file inside the Android, with no other layers of checking.

C. POC:
<Insert step-by-step to reproduce the issue here>

Verified by,

Nadia – D5782 and sent to Cyber Security Program on 03 27, 2023

<Include screenshot documentation and evidence>

D. Recommendation:

Implement a more robust Root Detection mechanism, such as integrating SafetyNet API, checking for writable partitions and system directories, etc.

-- Good Luck --

Verified by,

Nadia – D5782 and sent to Cyber Security Program on 03 27, 2023