UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2017/2018

COURSE NAME	:	MOBILE COMPUTING AND WIRELESS SECURITY
COURSE CODE	:	BIS 30603
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	DECEMBER 2017 / JANUARY 2018
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **THREE (3)** PAGES

Q1 You are conducting an Android malware static analysis on a malware named thisismalware.apk using APKTool software. From the analysis, you are able to extract file which contains declared permissions of the malware.

(a) Explain **ONE (1)** possible threat for each of permissions below.

(i) READ_PHONE_STATE

(ii) WRITE EXTERNAL STORAGE

(iii) CAMERA

(iv) ACCESS_FINE_LOCATION

(v) READ_CONTACTS

(10 marks)

(b) Write command for APKTool to analyze thisismalware.apk.

(2 marks)

(c) List **FOUR (4)** basic files or folders when Android application is reverse-engineered using APKTool.

(8 marks)

Q2 (a) Describe **FOUR (4)** mobile malware delivery methods commonly used to infect smartphone users.

(8 marks)

(b) Explain why smartphone user should not download applications from third party application market.

(4 marks)

(c) The Open Web Application Security Project (OWASP) is an international foundation and open community dedicated to enabling organization to develop secure applications. Recognizing mobile threats as current security issues, the OWASP had list Unsecure Data Storage as one of the top 10 mobile device vulnerability. This vulnerability occur when sensitive data is stored in location with no or inadequate security. If the smartphone or mobile device is breached or compromised, the result could be data loss, fraud or even stolen credentials. Attacker commonly exploit this vulnerability through mobile malware and the impact can be severe.

Discuss **TWO (2)** remediation approaches for this vulnerabilities.

(8 marks)

Q3 A rogue access point is a wireless access point that has been installed on a secure network without explicit authorization from a local network administrator, whether added by a well-meaning employee or by a malicious attacker.

(a) List **FIVE (5)** possible vulnerabilities of rogue access point installation.

(10 marks)

(b) Discuss **TWO (2)** actions to prevent the installation of rogue access point.

(10 marks)

Q4 DEF Company had hired you as a Network Security Administrator to manage the company Wireless Local Area Network (WLAN).

(a) Identify **FOUR (4)** ongoing security management practises to secure Wireless Local Area Network (WLAN) company security.

(12 marks)

(b) State **FOUR (4)** authentication and access restriction that can be implemented to secure Wireless Local Area Network (WLAN) company security.

(8 marks)

- END OF QUESTION -