UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2018/2019

COURSE NAME	:	MOBILE COMPUTING AND WIRELESS SECURITY
COURSE CODE	:	BIS 30603
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	DECEMBER 2018 / JANUARY 2019
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **SEVEN (7)** PAGES

SECTION A

Choose the BEST answer for each of the following questions. Write ALL answer in the answer script.

Q1 You are sitting in a library and would like to share files with a coworker sitting across the table. To accomplish this, the coworker connects to a wireless Service Set Identifier (SSID) managed by your laptop. What type of network topology is this?

A. Unsecure.
B. Ad hoc.
C. Basic Service Set.
D. Extended Service Set.

Q2 Rogue access point is _____________.

A. an unauthorized access point that has been placed on your Local Area Network (LAN)
B. an access point configured to broadcast the corporate Service Set Identifier (SSID)
C. an access point using Wired Equivalent Privacy (WEP) or WEP2 security
D. an access point that has been compromised by an intruder

Q3 Consider the following scenario for a Global System for Mobile communication (GSM) system:

After a first handoff from Mobile Switching Center (MSC)-A to MSC-B. Then, the mobile moves into the coverage area of a base station connected to MSC-C.

Which of the following is **TRUE**?

i. The connection is extended from MSC-B to MSC-C
ii. The segment from MSC-A to MSC-B is dropped
iii. A new segment is set up from MSC-A to MSC-C
iv. The end-to-end connection is rerouted

A. i and ii.
B. ii and iii.
C. i, ii and iii.
D. i, ii, iii and iv.

Q4 Wardriving looks for which of the following vulnerabilities?

A. The use of default administrative usernames and passwords.
B. No or weak encryption.
C. The use of default Service Set Identifier (SSID) settings.
D. All of the above.

Q5 An evil twin is a ________________.

A. version of rogue Access Point (AP) in which the device masquerades as a legitimate AP
B. social engineering scam
C. Bluetooth hack that takes over another device
D. peer-to-peer hack

Q6 Which of the following is an example of a malware-delivery technique?

A. Captive portals.
B. USB exploits that jailbreak phones when they are connected to PCs.
C. Likejacking.
D. All of the above.

Q7 The best way to increase the range of wireless signal is by ___________.

A. adding another access point (AP) on the same frequency and channel
B. telling employees to move closer
C. using a wireless extender
D. turning on the AP power

Q8 In _____, multiple access is achieved by allocation different time slots for the different user.

A. CDMA
B. FDMA
C. TDMA
D. FPGA

Q9 Antenna which attempts to direct all its energy in a particular direction is called a _______.

A. directional antenna
B. single direction antenna
C. one to one antenna
D. propagation antenna.

Q10 What is the main difference between Mobile Device Management (MDM) and Mobile Application Management (MAM)?

A. MDM is used on Apple phones and MAM is used on Android phone.
B. MDM handles the device activation, enrollment and provisioning, whereas MAM assist in the delivery of software.
C. MAM handles the device activation, enrollment and provisioning, whereas MDM assist in the delivery of software.
D. MDM can perform integrity checks on applications.

Q11 Disabling SSID broadcast ____________.

A. is one of the measures used in securing wireless networks
B. makes a WLAN harder to discover
C. block access to a WAP
D. prevent wireless clients from accessing the network

Q12 What should user do to protect their mobile devices against theft or lost?

A. Use pass codes / PINs to lock the screen.
B. Enable phone finding.
C. Enable remote wiping capabilities.
D. All of the above.

Q13 The simplest way to avoid mobile device fingerprinting is __________.

A. disable Javascript
B. delete the cookie file after used
C. regularly reset the phone to its factory setting
D. lie about your preferences on e-commerce sites

Q14 Drive-by browser exploits which target?

A. Access point with no encryption.
B. Mobile device on highways.
C. Near field communication-based applications.
D. Web browser plug-ins for Java, Adobe Reader, and Flash on mobile devices.

Q15 Which of the following is the key difference between the Android and Apple iOS security approaches?

A. Open source models are more secure.
B. Apple uses walled garden approach requiring all applications to go through its system.
C. Google Play lacks security checks.
D. Google uses walled garden approach requiring all applications to go through its system

(30 marks)

SECTION B
Answer ALL questions

Q16 You are a network professional that is part of the IT team at SuperDuper Media. One year ago, SuperDuper Media launched a social media Web site aimed at young urban professionals. The company also released a mobile app for accessing the site from Google Android, Apple iOS, and Windows Phone devices.

SuperDuper Media has 35 full-time employees, all of whom have offices or shared work spaces in a two-story building that serves as the company headquarters approximately 10,000 square feet. The SuperDuper Media WLAN has a Gigabit managed switch, a multiservice wireless LAN controller, and seven wireless access points strategically located to provide coverage to office staff. The network is protected by a firewall. The SuperDuper Media Web site servers are located in a data center 100 miles from SuperDuper Media headquarters.

Five employees are account representatives who are on the road at least 80 percent of the time, and each representative has a company-issued laptop, tablet, and smartphone. They use a large, shared office in the headquarters building when they are not traveling. The full-time employees use company-owned computers that connect to the WLAN. In an effort to control costs during the launch, SuperDuper Media has Bring Your Own Device (BYOD) policy.

Based on the given scenario, answer the following questions:

(a) Suggest **TWO (2)** tools that can be used to analyse vulnerabilities in Wireless Local Area Network (WLAN).

(2 marks)

(b) Identify **THREE (3)** mobile threats.

(6 marks)

(c) Propose **THREE (3)** Bring Your Own Device (BYOD) security policy to restrict SuperDuper Media access from unauthorized user.

(6 marks)

(d) Recommend **FOUR (4)** ongoing security management practices to secure the company Wireless Local Area Network (WLAN).

(6 marks)

(e) Draw the Wireless Local Area Network (WLAN) design for SuperDuper Media.

(10 marks)

Q17 (a) Describe **THREE (3)** differences between WEP, WPA, and WPA2.

(9 marks)

(b) Discuss **FIVE (5)** best practices in designing secure WLAN.

(10 marks)

Q18 (a) Your mobile device has been stolen. Your employer is concerned about a scenario where confidential data leak to unauthorized user.

Suggest **THREE (3)** steps to mitigate the risk against disclosure of confidential data?

(6 marks)

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

(i) Explain **ONE (1)** possible threat for each of permissions in **Table Q18(b)(i).**

(10 marks)

Table Q18(b)(i)

Permission	Possible Threat
READ_PHONE_STATE	
WRITE_EXTERNAL_STORAGE	
CAMERA	
ACCESS_FINE_LOCATION	
READ_CONTACTS	

(ii) Write command for APKTool to analyze malwarehere.apk.

(1 mark)

(iii) List **FOUR (4)** basic files or folders when Android application is unzipped using APKTool.

(4 marks)

-END OF QUESTION –