Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2019/2020

COURSE NAME	:	MOBILE COMPUTING AND WIRELESS SECURITY
COURSE CODE	:	BIS 30603
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	DECEMBER 2019 / JANUARY 2020
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.

Q1 A basic service set for Wireless Local Area Network (WLAN) is comprised of _____.

A. several access point operating as a single network
B. an access point and several wireless clients
C. several clients connected together
D. back-end wired Local Area Network (LAN)

Q2 Hackers do the following after compromising your phone **EXCEPT** _____.

A. shoulder surfing
B. access your voice mail
C. steal your information
D. use your application credential

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 _____ is the central node of 802.11 wireless operations.

A. Wi-Fi Protected Access (WPA)
B. Access Point
C. Wireless Application Protocol (WPA)
D. Access Port

Q6 Which of the following is **NOT** an appropriate way of targeting a mobile phone for hacking?

A. Target mobile hardware vulnerabilities.
B. Target application vulnerabilities.
C. Setup Keyloggers and spyware in smart-phones.
D. Steal the phone.

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 Activate _____ when you want to use it, otherwise turn it off for security purpose.

A. flash Light
B. application updates
C. bluetooth
D. screen rotation

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 Service Set Identifier (SSID) broadcast _____.

A. is one of the measures used in securing wireless networks
B. makes a WLAN harder to discover
C. blocks access to a Wireless Application Protocol (WAP)
D. prevents wireless clients from accessing the network

Q12 Scanning wireless networks is used to _____.

A. see which website employees are using
B. prevent data leakage
C. frequency-jam unauthorized access points
D. verify that security measures are in place on unauthorized access points

Q13 Do not keep _____ passwords, especially fingerprint for your smartphone because it can lead to physical hacking if you are not aware or asleep.

A. biometric
B. PIN-based
C. alphanumeric
D. short

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 Mobile malware tends to focus on which of the following?

i. Gaining control of phones to launch Distributed Denial of Service (DDoS).
ii. Gaining access to the ports that control Global Positioning System (GPS) and other location information.
iii. Gaining control of phone file systems to steal data and photos.
iv. Locking out the user phone for ransom.

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

(30 marks)

SECTION B

Q16 You are a network security officer at NetPower Sdn Bhd. NetPower Sdn Bhd has 30 full-time staffs, all of whom have offices or shared work spaces in a two-story building that serves as the company headquarters. Staffs allocation are as follows: 5 staffs in multimedia department, 10 staff in network department, 3 staffs in admin office, 3 staffs in finance department, 5 staff in customer service department and 4 managers located in separate room. The customer service and network department are located in first floor while others are placed in second floor. The NetPower Sdn Bhd WLAN has a switch, a multiservice wireless LAN controller, and six wireless access points strategically located to provide coverage to all staffs. The network is protected by a firewall. The NetPower Sdn Bhd web site servers are located in a data center 100 kilometer from NetPower Sdn Bhd headquarters.

Each staff has a company-issued laptop, tablet, and smartphone. All staffs are connected to the NetPower Sdn Bhd's WLAN. NetPower Sdn Bhd has brought your own device (BYOD) policy in order to control operation costs.

Based on the given scenario, answer the following questions:

(a) Suggest **TWO (2)** tools that can be use to analyse vulnerabilities in WLAN.

(1 mark)

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

(3 marks)

(c) Propose **THREE (3)** BYOD security policy to restrict NetPower Sdn. Bhd. access from unauthorized user.

(6 marks)

(d) Draw the WLAN design for NetPower Sdn. Bhd.

(10 marks)

Q17 (a) Compare **THREE (3)** features of 3G, 4G and 5G technologies.

(6 marks)

(b) Describe **TWO (2)** differences between WPA and WPA2.

(4 marks)

(c) 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.

List **THREE (3)** steps to mitigate the risk against disclosure of confidential data.

(3 marks)

(b) Compare **THREE (3)** differences of Android and Apple iOS features.

(6 marks)

(c) You are conducting an Android malware static analysis on a malware named crushmyheart.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(c)(i).**

Table Q18(c)(i)

Permission	Possible Threat
READ_PHONE_STATE	
WRITE_EXTERNAL_STORAGE	
INTERNET	
ACCESS_WIFI_STATE	
READ_CONTACTS	

(5 marks)

(ii) List **TWO (2)** basic files or folders when Android application is unzipped using APKTool.

(1 mark)

Q19 (a) Recommend **THREE (3)** security management practices to secure the company WLAN.

(6 marks)

(b) 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.

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

(5 marks)

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

(4 marks)

-END OF QUESTIONS-