31

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
(ONLINE)
SEMESTER I
SESSION 2020/2021

COURSE NAME	:	MOBILE COMPUTING AND WIRELESS SECURITY
COURSE CODE	:	BIS 30603
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JANUARY/ FEBRUARY 2021
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS 2. PLEASE MAKE SURE TO CLICK "SAVE ANSWER" BUTTON FOR SUBJECTIVE QUESTIONS. OBJECTIVE QUESTIONS ARE SAVED AUTOMATICALLY

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

SECTION A

Choose the BEST answer for each of the following questions.

Q1 Three bank employees are using the corporate network:

- The first employee read an announcement in a company web page using a web browser.
- The second employee perform some financial transactions by accessing the corporate database.
- The third employee joins live audio conference with other corporate managers in branch offices.

If Quality of Service (QoS) is implemented on this network, what will be the priorities from highest to lowest of the different data types?

A. Financial transactions, audio conference, web page.
B. Audio conference, financial transactions, web page.
C. Audio conference, web page, financial transactions.
D. Financial transactions, web page, audio conference.

Q2 is an example of a Trojan horse.

A. Malware that was written to look like a video game
B. Malware that requires manual user intervention to spread between systems
C. Malware that attaches itself to a legitimate program and spreads to other programs when launched
D. Malware that can automatically spread from one system to another by exploiting a vulnerability in the target

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 SSID settings.
D. All of the above.

Q5 Two components that are necessary for a wireless client to be installed on a WLAN are _____ and ________

A. media
B. wireless NIC
C. custom adapter
D. crossover cable
E. wireless bridge
F. wireless client software

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 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.

Q9 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. block access to a WAP
D. prevent wireless clients from accessing the network

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 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

Q12 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

Q13 Two tasks that should be done frequently to ensure the security and integrity of data and applications on mobile devices are and

A. execute a factory reset once a month to remove all unidentified malicious software.
B. back up user data on a regular basis.
C. password protect iTunes or Google Play accounts.
D. use airplane mode if you are accessing the Internet at an open Wi-Fi site.

E. ensure that the operating system software and applications contain the latest updates.
F. unmount all unused disk partitions.

Q14 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. All of the above

Q15 Two potential risks that could result from rooting or jailbreaking a mobile device are ______ and ______ .

A. enabling app access to the root directory.
B. not properly creating or maintaining sandboxing features.
C. allowing the user interface to be extensively customized.
D. improving device performance.
E. Enabling features that are disabled by a cellular carrier.

(30 marks)

SECTION B

Q16 Wifi2u Sdn Bhd has 50 full-time staffs, all of whom have offices or shared workspaces in a two-story building that serves as the company headquarters. Staffs allocation are as follows: 10 staffs in multimedia department, 10 staff in network department, 10 staffs in admin office, 10 staffs in finance department, 5 staff in customer service department and 5 managers located in one room. The customer service and network department are located in first floor while others are placed in second floor. The Wifi2u 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 Wifi2u Sdn Bhd web site servers are in a data center 100 kilometer from Wifi2u Sdn Bhd headquarters.

Each staff has a company-issued laptop, tablet, and smartphone. All staffs are connected to the Wifi2u Sdn Bhd's WLAN. Wifi2u Sdn Bhd has brought your own device (BYOD) policy 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.

(2 marks)

(b) Discuss **TWO (2)** mobile threats.

(4 marks)

(c) Discuss **TWO (2)** WLAN threats.

(4 marks)

(d) Propose **FIVE (5)** Bring Your Own Device (BYOD) security policy to restrict Wifi2u Sdn Bhd. Access from unauthorized user.

(10 marks)

(e) Draw the Wireless Local Area Network (WLAN) design for Wifi2u Sdn Bhd.

(10 marks)

Q17 (a) Write short notes on these technologies.

(i) 5G.

(ii) Wifi 6.

(iii) Captive Portal.

(6 marks)

(b) Describe **TWO (2)** differences between Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2).

(5 marks)

(c) Suggest **FIVE (5)** best practices in designing secure WLAN.

(10 marks)

Q18 Mobile devices have become the central hub for all an individual's personal data. Finances, businesses, pastimes, social lives, private lives, and identities can be accessed through these gadgets. If your phone falls into the wrong hands and does not have the proper protection, the thief can get more than a resell profit. The information that an open smartphone provides is enough for a bad actor to carry out identity theft, especially when the phone line continues to be open.

(a) Discuss **FOUR (4)** best practice to secure mobile devices against disclosure of confidential data?

(4 marks)

(b) Android appear to be most secure operating system in the market compare to iOS operating system.

Discuss this statement. Justify your answer

(6 marks)

Q19 A rogue access point is a wireless access point that has been installed on a secure network without authorization from a local network administrator.

(a) Proposed **THREE (3)** ways to prevent rogue access point installation.

(6 marks)

(b) Recommend **TWO (2)** security management practices to secure the company WLAN.

(4 marks)

-END OF QUESTIONS –