UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2017/2018

COURSE NAME	:	WEB SECURITY
COURSE CODE	:	BIS 20303
PROGRAMME CODE	:	BIS / BIW
EXAMINATION DATE	:	DECEMBER 2017 /JANUARY 2018
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS

THIS QUESTION PAPER CONSISTS OF **EIGHT (8)** PAGES

SECTION A

Choose the BEST answer for each of the following questions

Q1 Which of the following can be used for secure exchange of email?

A. Hypertext Transfer Protocol Secure (HTTPS).
B. Secure Electronic Transaction (SET).
C. Pretty Good Privacy (PGP).
D. File Transfer Protocol (FTP).

Q2 Secure Socket Layer (SSL) services at __________ layer.

A. application
B. data link
C. network
D. transport

Q3 Secure Electronic Transaction (SET) is for securing ___________.

A. email transaction
B. file transfer
C. Internet credit card transaction
D. communication

Q4 General Internet Protocol (IP) security mechanism provides **ALL** of the following **EXCEPT** ________.

A. authentication
B. integrity
C. confidentiality
D. key management

Q5 A merchant sends _________ to the payment gateway to obtain payment.

A. capture request
B. transaction request
C. purchase request
D. bill request

Q6 What is the purpose of biometrics in access control?

A. Certification.
B. Authorization.
C. Authentication.
D. Confirmation.

Q7 What is the purpose for using a packet sniffer in Intrusion Prevention System (IPS)?

A. It tracks network connection.
B. It monitors network traffic.
C. It scans network segment for cabling faults.
D. It detects illegal packets on the network.

Q8 A timely review of system access records is an example of _______ security.

A. avoidance
B. deterrence
C. prevention
D. detection

Q9 How does the Intrusion Detection System (IDS) response when it detects Internet Protocol (IP) packets which the sources address is similar with the destination address?

A. Allow the packet to be processed by the network and record the event.
B. Record selected information about the item and delete the packet.
C. Resolve the destination address and process the packet.
D. Translate the source address to destination address.

Q10 What is the purpose of a firewall?

A. To protect networks from incoming and outgoing data traffic.
B. To record data traffic from going out of the network.
C. Block Simple Network Architecture (SNA) traffic.
D. Monitor network traffic.

Q11 Ali leans over to see Siti's password while she login into her computer. What is this security violation known as?

A. Object reuse.
B. Shoulder surfing.
C. Smurf attack.
D. Masquerading.

Q12 Spoofing can be defined as __________.

A. eavesdropping on communications between persons or processes
B. a person or process emulating another person or process
C. a hostile or unexpected entity hidden within another entity
D. the testing of all possibilities to obtain information

Q13 Eavesdropping is considered as what type of attack?

A. Active.
B. Passive.
C. Aggressive.
D. Masquerading.

Q14 Which of the following is an example of hyperlink spoofing?

A. Compromising a web server reference.
B. Connecting the user to a different web server.
C. Executing Hypertext Transport Protocol Secure GET commands.
D. Starting the user's browser on a secured page.

Q15 The information security principle ethics is to prevent __________ activity.

A. illegal
B. harmful
C. untruthful
D. untrusting

Q16 Which of the following shall be used to achieve non-repudiation of delivery?

A. Sender encrypts the message with the recipient's public key and signs it with their own private key.

B. Sender computes a digest of the message and sends it to a Trusted Third Party (TTP) who signs it and stores it for later reference.

C. Sender sends the message to a TTP who signs it together with a time stamp and sends it on to the recipient.

D. Sender gets a digitally signed acknowledgment from the recipient containing a copy or digest of the message.

Q17 Pretty Good Privacy (PGP) provides ___________.

A. confidentiality, integrity, and authenticity

B. integrity, availability, and authentication

C. availability, authentication, and non-repudiation

D. authorization, non-repudiation, and confidentiality

Q18 Which of the following protocol is commonly used to verify dial-up connections between hosts?

A. Unix-to-Unix Communication Protocol (UTJCP).

B. Challenge Handshake Authentication Protocol (CHAP).

C. Point-to-Point Tunneling Protocol (PPTP).

D. Simple Key management for Internet Protocol (SKIP).

Q19 When securing Internet connections, which of the following should be used to protect internal routing and labeling schemes?

A. Virtual Private Networks (VPN).

B. Layer 2 Tunneling Protocol (L2TP).

C. Domain Name Systems (DNS).

D. Network Address Translation (NAT).

Q20 The followings are the network security strategies **EXCEPT** ______.

A. building an iron door for a server room
B. biometric authentication
C. placing a security guard
D. enable antivirus

(40 marks)

SECTION B

State either **TRUE (T)** or **FALSE (F)** for each of the following statement.

Q21 Backdoor allows an unauthorized access to bypass usual security procedures.

Q22 Web defacement is common form of repudiation attack.

Q23 Firewall default setting is to open all incoming and outgoing ports.

Q24 HTTPS refers to the combination of Hypertext Transfer Protocol (HTTP) and Secure Shell (SSH) to implement secure communication between a Web browser and a Web server.

Q25 A zombie is a program that secretly takes over another Internet-attached computer and then uses that computer to launch Denial of Service (DoS) attacks.

Q26 Firewall cannot protect against virus attack.

Q27 The network administrator has to open port number 80 in order to allow email transaction in firewall setting.

Q28 The correct way to display the text script on a Web page is using `<script>` tag.

Q29 Password is the least secure method of authentication.

Q30 Hashing requires public and private keys that are used by the sender and receiver to encode the message.

(10 marks)

SECTION C

Q31 Hotelforyou.com is a provider for room booking service. Amin uses his credit card to book a room through Hotelforyou.com site.

(a) Illustrate procedures for purchase request (customer: Amin).

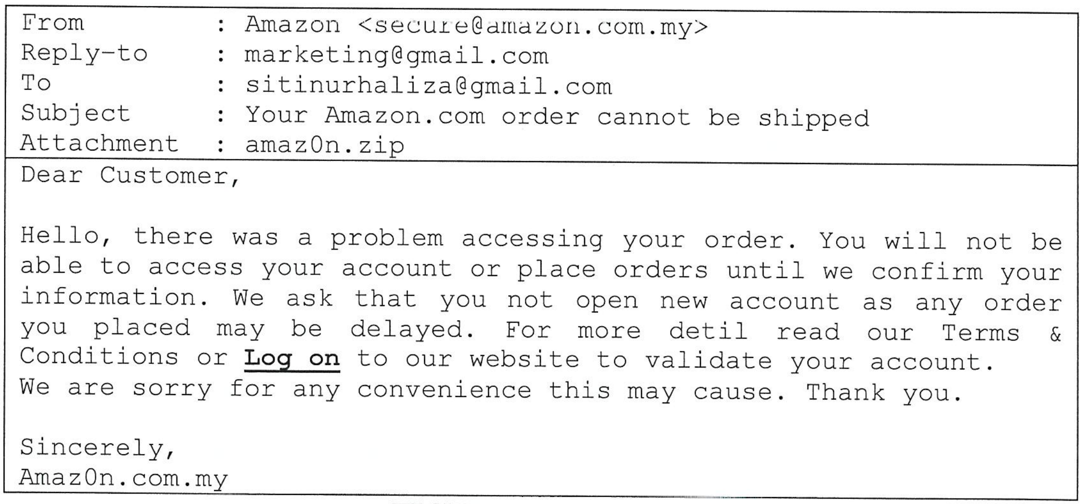
(5 marks)

(b) Explain steps for purchase request (merchant: Hotelforyou.com).

(5 marks)

Q32 Siti Nurhaliza received an email claimed from Amazon as shown in Figure **Q32**. Outline **FIVE (5)** reasons why this email is categorized as a fraud email.

(10 marks)



```
From         : Amazon <secure@amazon.com.my>
Reply-to     : marketing@gmail.com
To           : sitinurhaliza@gmail.com
Subject      : Your Amazon.com order cannot be shipped
Attachment   : amaz0n.zip
```

Dear Customer,

Hello, there was a problem accessing your order. You will not be able to access your account or place orders until we confirm your information. We ask that you not open new account as any order you placed may be delayed. For more detil read our Terms & Conditions or **Log on** to our website to validate your account.
We are sorry for any convenience this may cause. Thank you.

Sincerely,
Amaz0n.com.my

FIGURE Q32

Q33 Using illustration, explain **FIVE (5)** general steps of hacking process.

(10 marks)

Q34 Suppose a hash table of size 7 is used to store integer keys, with the hash function of `h(x) = x mod 7`. Given the inserted elements in the order are 8, 28, 16, 2 and 21. Calculate the initial indexes of each element. Show your working.

(10 marks)

Q35 Recently, Universiti Tun Hussein Onn computer system has been attacked by Anonymous attacker. You have been appointed as the Chief of Security officer.

Suggest **FIVE (5)** network security policies to maintain the confidentiality, integrity and availability of data.

(10 marks)

- END OF QUESTION -