UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION
JANUARY 2016 SEMESTER

COURSE CODE	:	IKB 41103
COURSE NAME	:	ADVANCE NETWORK SECURITY
PROGRAMME NAME	:	BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN COMPUTER SYSTEM SECURITY BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN NETWORKING SYSTEM
DATE	:	25 MAY 2016
TIME	:	9.00 am – 12.00 noon
DURATION	:	3 HOURS

INSTRUCTIONS TO CANDIDATES

1. Please CAREFULLY read the instructions given in the question paper.
2. This question paper has information printed on both sides of the paper.
3. This question paper consists of ONE (1) section.
4. Answer FOUR (4) questions ONLY.
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English language ONLY.

SECTION A (Total: 100 marks)

INSTRUCTION: Answer FOUR (4) questions ONLY.
Please use the answer booklet provided.

Question 1

Three-tier E-commerce architecture is commonly used by E-commerce projects. In this architecture, clients connect company's databases through web application as shown in Diagram 1.

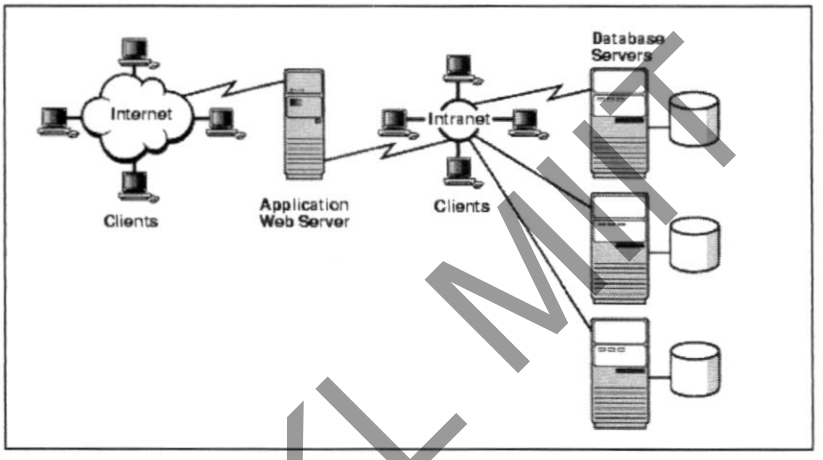

Diagram 1: Three-Tier E-commerce Architecture

By referring to Diagram 1, answer the following questions:

(a) Explain **THREE (3)** methods to implement Three-Tier E-commerce Architecture.

(12 marks)

(b) Dual signature authentication method is used in SET. Based on your information, describe dual signature data flow.

(6 marks)

(c) Describe secure handshake steps of SSL protocol.

(7 marks)

Question 2

A payment gateway is an e-commerce application service provider service that authorizes payments for e-businesses, online retailers, bricks and clicks, or traditional brick and mortar. Secure Electronic Transaction (SET) is a communications protocol standard for securing credit card transactions over insecure networks, specifically, Internet. By referring to above introduction, answer the following questions:

(a) Explain the security methods used in SET protocol.

(10 marks)

(b) List **SEVEN (7)** main functions of payment gateways.

(7 marks)

(c) Describe the sequence events of SET protocol.

(8 marks)

Question 3

Purchase request verification is one of SET functions. In request verification, the merchant verifies customer purchase request as it is shown in Diagram 2.

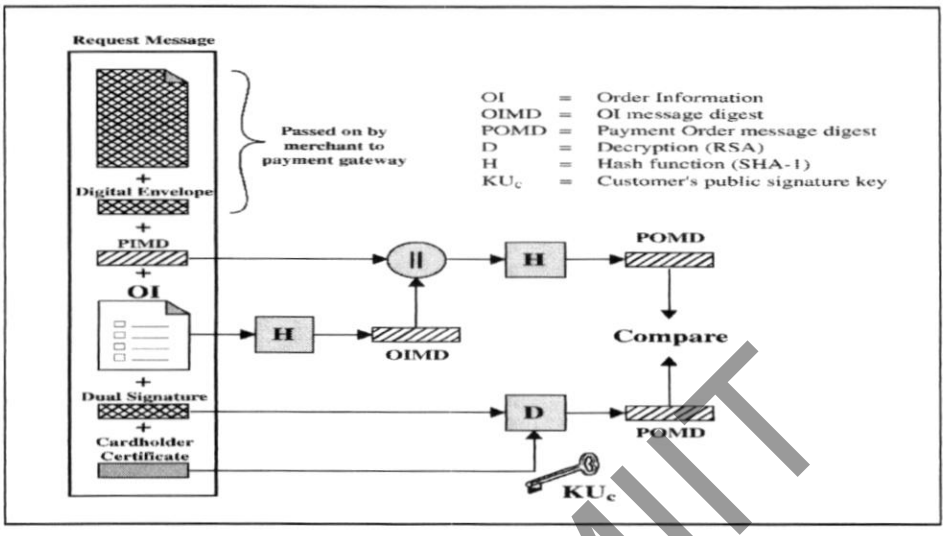

Diagram 2: Merchant purchase request verification

By referring to Diagram 2, answer the following questions:

(a) Describe merchant payment authorization request message.

(11 marks)

(b) Explain the role of digital envelope in SET verification process.

(7 marks)

(c) Discuss the importance of using dual signature in SET verification process.

(7 marks)

Question 4

(a) Write snort rule which fulfill the following description:

i. Drop all request matching criteria

(1.5 marks)

ii. Performs analysis for TCP packets

(1.5 marks)

iii. From any Source IP

(1.5 marks)

iv. From any source Port

(1.5 marks)

v. Destination IP is 10.18.19.

(1.5 marks)

vi. Destination Port is 80 (HTTP)

(1.5 marks)

vii. Content should have value "POST"

(1.5 marks)

viii. Content should have value "Login.aspx" – This is page name.

(1.5 marks)

ix. Word "nocase" specifies matching is not case sensitive

(1.5 marks)

x. Regular expression mentioned as
"pcre:".*username=.*[\'\"\;\:\|\&\$\%\@\\\/<>()+,]" will not be allowed ' "

(1.5 marks)

(b) ICMP flooding attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, it will cause a significant slowdown in the system and might cause the system to be crashed. See Diagram 3.

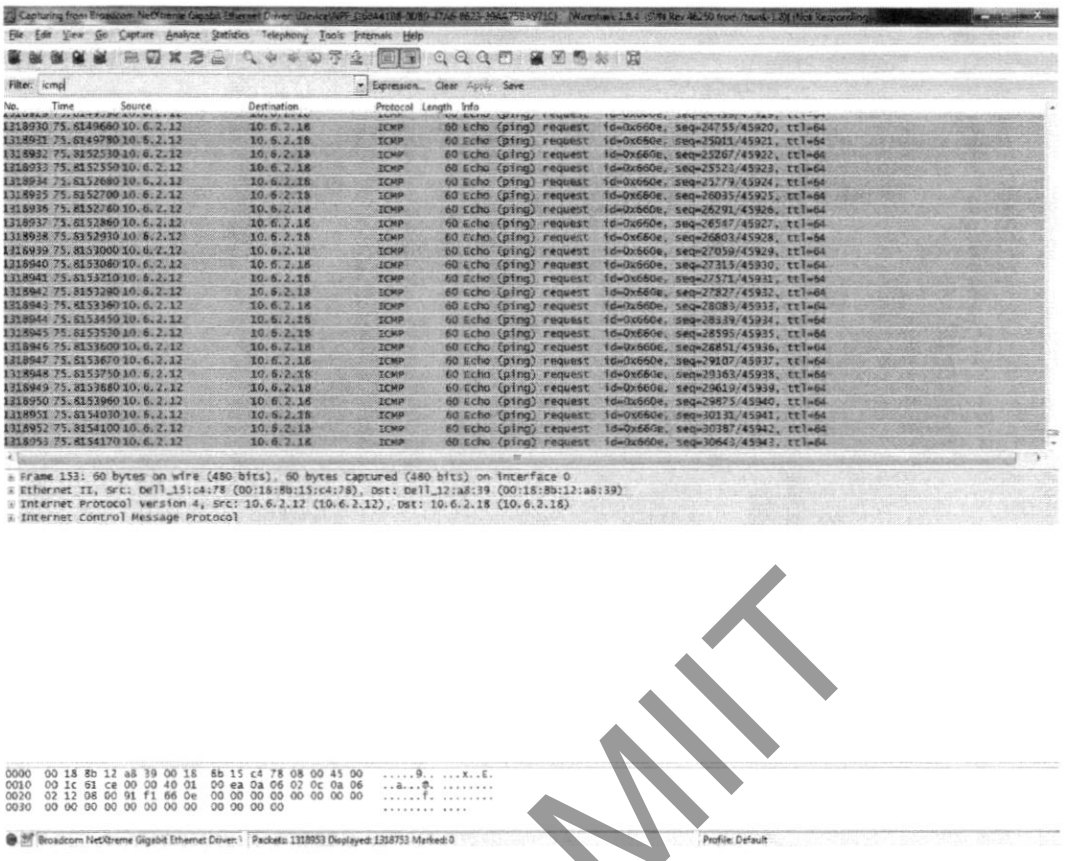

Diagram 3: ICMP flooding attack traffic

By referring to Diagram 3, write a snort rule to detect ICMP attacks. For your information this attack generate 500 ICMP packets in each 2 seconds.

(10 marks)

Question 5

Kavi Corporation E-commerce architecture is shown in Diagram 4. By referring to this diagram answer the following questions:

(a) Describe the SSL protocol architecture.

(7 marks)

(b) Explain SSL protocol record.

(8 marks)

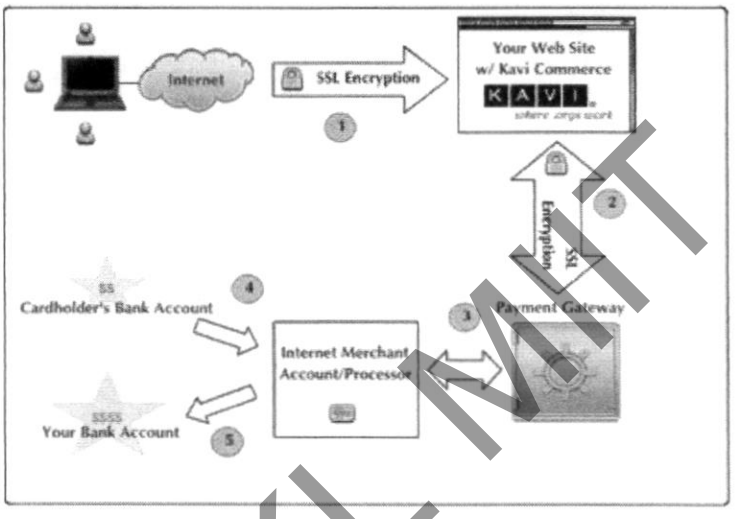

Diagram 4 : Kavi Corporation e-Commerce Architecture

(c) Classifcation methods are used in intrusion detection system (IDS). Explain the main components of classification based IDS architecture as shown in Diagram 5.

(10 marks)

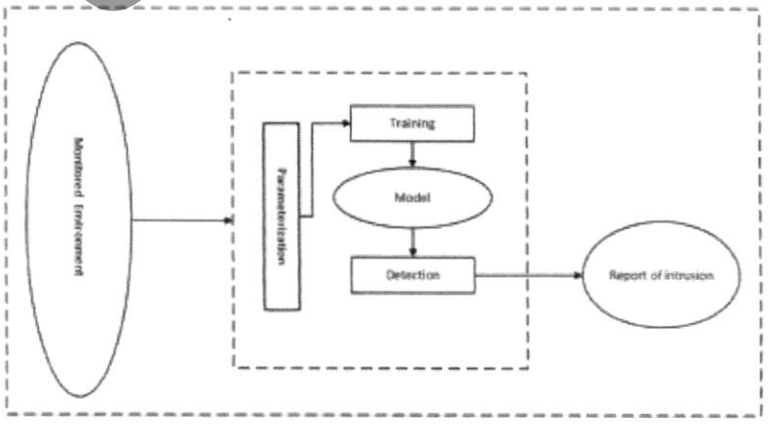

Diagram 5: General classification based IDS architecture

END OF EXAMINATION PAPER