MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION

JANUARY 2016 SEMESTER

SUBJECT CODE	:	INB35303
SUBJECT TITLE	:	NETWORK SECURITY
LEVEL	:	BACHELOR
TIME / DURATION	:	(2 ½ HOURS) 9:00AM-11:30AM
DATE	:	25 MAY 2016

INSTRUCTIONS TO CANDIDATES

1. Please read the instructions given in the question paper CAREFULLY.
2. This question paper is printed on both sides of the paper.
3. Answer ALL questions.
4. Please write your answers on the answer booklet provided.

THERE ARE 5 PAGES OF QUESTIONS, INCLUDING THIS PAGE.

INSTRUCTION: Answer ALL questions.
Please use the answer booklet provided.

QUESTION 1: Vulnerability, Threats & Attacks

a) List TWO (2) protocols used to perform REMOTE ADMINISTRATION to servers, routers and switches (configure from remote). Based on the TWO (2) protocols you listed, which protocol is more secure? Justify your answer.

(6 marks)

b) The corporate network of an IT company is believed to be operating with vulnerable network infrastructure (routers, switches, servers or computers). As the Network Engineer there, suggest ways to assess and proof that the corporate network is insecure.

(9 marks)

c) The following question is based on Figure 1:

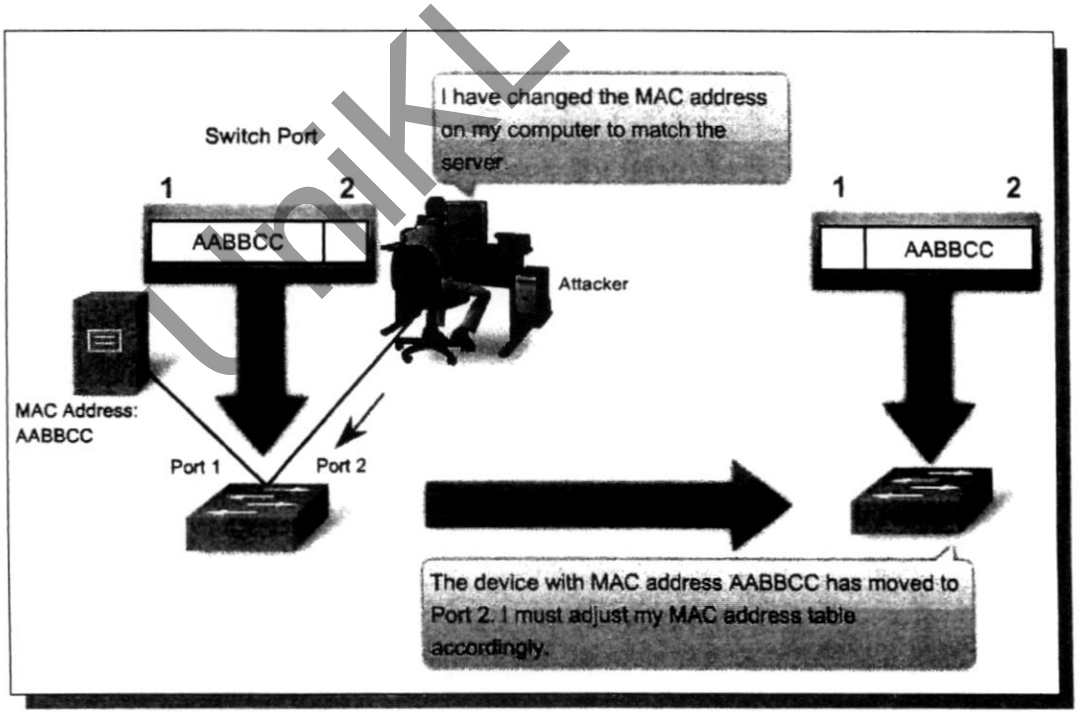

Figure 1: A Type of Network Security Threats & Attack

i. Discuss the network security attack shown in Figure 1. Include the attack NAME, attacker GOALS and the DANGER resulted from this attack to our networking systems to secure good marks.

(6 marks)

ii. List TWO (2) technological solutions available in managed switched systems, to overcome the attack shown in Figure 1.

(4 marks)

[25 MARKS]

QUESTION 2: Virtual Private Networks (VPN)

a) Compare between TRANSPORT MODE and TUNNEL MODE applied to IP PACKETS for ESP implementation. Illustrate a simple tunnel mode link topology diagram to support your answer if necessary.

(10 marks)

b) Discuss the APPLICATION used and CONNECTION COMPLEXITY (user friendliness) of the following remote access VPN solutions for mobile workers:

i. Clientless VPN (SSL)

ii. Client Based VPN (IPSEC)

(8 marks)

c) Based on Figure 2, answer the following questions.

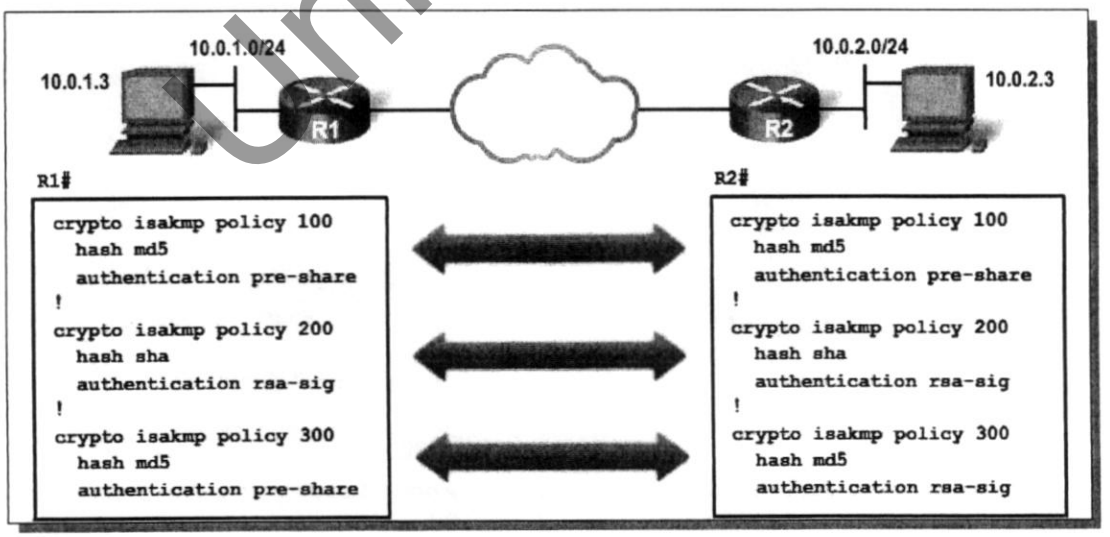

Figure 2: A VPN ISAKMP Phase 1 Configuration

i. Based on the VPN configuration in Figure 2, which ISAKMP policy set number potentially to FAIL? Justify your answer.

(3 marks)

ii. Explain the function of using command HASH for the configuration shown in Figure 2.

(4 marks)

[25 MARKS]

QUESTION 3: Cryptographic Systems

a) State TWO (2) benefits of using ENCRYPTION technology.

(4 marks)

b) Apply TRANSPOSITION methods with KEY=5, then followed by SUBSTITUTION methods with KEY=4 to the below CIPHERTEXT in order to reveal its secret message.

CIPHERTEXT = [PSYKGSOSWH]

(8 marks)

c) A house burglar has stolen your jewelry and hides it under something or somewhere in the house kitchen, during his escape from a police chase. The location of the hidden jewelry is encrypted in secret alphabets using RSA cryptosystem. It is believed that values for p, q are p=3 and q=7 and the public key used is e=17. Decrypt the FOUR (4) secret alphabets [J, R, N, B] to reveal the secret message. (Note: Assume A=1, B=2, C=3 ... Z=26 to convert your finalized answer digits, back into alphabetical plaintext.)

(13 marks)

[25 MARKS]

QUESTION 4: Intrusion Prevention Systems (IPS) & Firewalls

a) Why Intrusion Detection System (IDS) technology is considered outdated nowadays?

(3 marks)

b) Explain the other FOUR (4) SIGNATURE TRIGGERS (ALARMS) available in Cisco IPS.

(8 marks)

c) Describe the following EDGE ROUTER implementation approach listed below, used to secure the perimeter of networks. Use a diagram to support your answer.

i. DEFENSE IN-DEPTH APPROACH

ii. DMZ APPROACH

(6 marks)

d) There are two Adaptive Security Appliance (ASA) firewall modes which are the ROUTED MODE and TRANSPARENT MODE. Discuss the TWO (2) modes.

(8 marks)

[25 MARKS]

END OF EXAMINATION PAPER