CONFIDENTIAL

MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION

JANUARY 2016 SEMESTER

SUBJECT CODE	:	IKB42303
SUBJECT TITLE	:	OPERATING SYSTEM SECURITY
LEVEL	:	BACHELOR
TIME / DURATION	:	9.00 am – 11.30 am (2 ½ HOURS)
DATE	:	22 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. This question paper consists of ONE (1) SECTION – SECTION A.
4. Answer ONLY FOUR (4) of the FIVE (5) questions.
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English.

THERE ARE 4 PAGES OF QUESTIONS, EXCLUDING THIS PAGE.

SECTION A (Total: 100 marks)

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

Question 1

a. Differentiate between */etc/password* and */etc/shadow* files. Give reason for keeping user account information in these two different files.

(6 marks)

b. The *chmod* utility is used to setup Linux's first line of defense. Explain the symbolic and absolute (octal) modes of operation for the *chmod* utility?

(6 marks)

c. Describe the *Bell-LaPadula* and *Biba* security models and explain the difference between the two models based on their security policies?

(8 marks)

d. Convert the following permission strings into their respective **octal values** and write down their description.

Permissions (Symbolic)	Permissions (Octal)	Description
rwxr-xr-x		
rwxrw-r-x		
rw-rw-r--		
rw-rw----		
rw-r-xr-x		

(5 marks)

[Total: 25 Marks]

Question 2

a. The Intrusion Detection Systems (IDS) are not a *preventive* measure. Do you agree with this statement? Provide justification with your answer in case you agree or disagree.

(5 marks)

b. The following scenario of public-key encryption (asymmetric-key cryptosystems) is given. Analyze it and answer the questions given below:

Scenario: Alice and Bob want to share their public keys with each other. Alice sends her public key to Bob. An intruder Eve intercepts Alice's public key and sends her own public key to Bob. When Bob transmits his public key to Alice, Eve again substitutes it with her own and sends it to Alice. This way, Eve receives public keys of both Alice and Bob. Alice and Bob are unaware that the public keys they received are of Eve. Eve simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party.

i. What type of attack is mentioned in the above scenario?

(2 marks)

ii. Explain how Eve is able to decrypt, read and possibly modify messages exchanged by Alice and Bob.

(6 marks)

iii. Provide a solution for this problem of public-key cryptosystems.

(6 marks)

c. The output of the command ls –l /tmp is:

```
drwxrwxrwt 30 root root 20480 Mar 11 14:17 /tmp
```

The /tmp (mentioned above) is used to create temporary files related to different users in the system. How to avoid deletion of files and sub-directories from /tmp as well as keeping its permission rwxrwxrwx (777)?

(6 marks)

[Total: 25 Marks]

Question 3

a. The Trusted Platform Module (TPM) is used to build a chain of trust starting from BIOS up till the applications running on the OS. How this chain of trust is built? Explain your answer with a diagram.

(7 marks)

b. Explain how Trusted Platform Module (TPM) keys are more secure than other software-protected keys? Explain your answer with a key hierarchy diagram.

(7 marks)

c. The PCRs inside a TPM can only be modified through PCR extend operation. Explain the PCR extend operation with the help of the given formula?

$$\mathrm{PCR}_i^{\tau+1} = \text{SHA-1}(\mathrm{PCR}_i^{\tau} \,||\, \mathrm{m})$$

(7 marks)

d. Operating system works as a *control program* and as a *resource allocator*. Explain these two features of an Operating System?

(4 marks)

[Total: 25 Marks]

Question 4

a. In Linux firewall (iptables) two *targets* are used to deny packets, *DROP* and *REJECT*. Describe the impactful difference in these two targets.

(6 marks)

b. There are **THREE (3)** different types of Linux firewall configurations. Explain these configurations in detail.

(6 marks)

c. Describe **FOUR (4)** most important Linux System Monitoring Tools that every system admin should know.

(8 marks)

d. Differentiate between *anomaly detection* and *misuse detection* based intrusion detection systems.

(5 marks)

[Total: 25 Marks]

Question 5

a. Differentiate between an Intrusion Detection System (IDS) and a Firewall.

(5 marks)

b. IDSs are classified into two broad categories based on their *deployment in the system*. Explain these **TWO (2)** categories in detail and provide examples for each category.

(10 marks)

c. As a system administrator, your task is to harden security of the Linux-based servers in your newly joined company. Describe any **FIVE (5)** most important methods to harden security of the servers?

(10 marks)

[Total: 25 Marks]

END OF EXAMINATION PAPER