# UNIVERSITI KUALA LUMPUR
## MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

## FINAL EXAMINATION
### JANUARY 2016 SEMESTER

| | | |
|---|---|---|
| COURSE CODE | : | IKB 41403 |
| COURSE NAME | : | SYSTEM AND SOFTWARE VULNERABILITIES |
| PROGRAMME NAME | : | BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN COMPUTER SYSTEM SECURITY |
| DATE | : | 18 MAY 2016 |
| TIME | : | 9.00 am – 11.00 am |
| DURATION | : | 2 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 TWO (2) sections; Section A and Section B.
4. Answer ALL questions in Section A. For Section B, answer ONE (1) question ONLY.
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English language ONLY.

THERE ARE 6 PAGES OF QUESTIONS, INCLUDING THIS PAGE.

**SECTION A (Total: 75 marks)**

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

**Question 1**

(a) The process of ethical hacking can be broken down into five distinct phases. An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain entry into a computer system are similar no matter what the hacker's intentions are. Briefly explain the **FIVE (5)** phases.

(10 marks)

(b) Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks, credit card payment gateways. Briefly explain the goal of launching this attack. List **TWO (2)** ways on how an attacker can do that.

(4 marks)

(c) A password cracker is an application program that is used to identify an unknown or forgotten password to a computer or network resources. It can also be used to help a human cracker obtain unauthorized access to resources. Briefly explain the difference between Brute Force attacks and Dictionary attacks?

(4 marks)

(d) Mohamad Ghazali, is a circuit repairman who fixes electrical and system links. He was brought in for a general investigation at the premises of XInsurance Inc. Mohamad Ghazali was astounded at his discoveries amid a standard check of the AC conduits in the venture. The LAN wires were laid through the pipes. He was enticed to discover the data moving through the LAN wires.

i. What can Mohamad Ghazali do to interrupt the network?

(4 marks)

ii. What are the **THREE (3)** classified data that he can get once he effectively sniffs the system activity?

(3 marks)

**Question 2**

(a) Based on the application and how it processes user-supplied data; SQL Injection can be utilized by an attacker to perform a few types of attacks, for example, compromised availability of data. Clarify the meaning of each attack stated below.

i. Authentication bypass

ii. Information disclosure

iii. Compromised data integrity

(6 marks)

(b) Vile and abusive comments keep on flooding Prime Minister Julia Gillard's Facebook page almost 24 hours after her online question and answer session was hijacked by trolls.

i. Briefly clarify what is session hijacking?

(6 marks)

ii. From your understanding, illustrate the process of session hijacking.

(4 marks)

iii. Before suggesting countermeasures for session hijacking, you need to know session hijacking is successful because of a few factors. List **THREE (3)** factors.

(3 marks)

(c) In social engineering attack, the attacker uses social skills to tricks the victim into disclosing personal information such as credit card number, bank account numbers, or confidential information about their organization or computer system. Social engineering can be broadly divided into three types. Briefly explain ALL types and for each type, give **TWO (2)** examples of social engineering attacks.

(6 marks)

**Question 3**

(a) Wireless networks are inexpensive when compared to wired networks. But, they are more vulnerable to attacks when compared with the wired networks.

i. Discuss the **TWO (2)** basic types of vulnerabilities associated with WLANs.

(2 marks)

ii. The command used to capture packets from the victim AP is:

airodump-ng —bssid 00:13:10:73:FC:C5 –c 6 –w dump mon0

Explain the used of each command:

1. airodump-ng:
2. --bssid:
3. -c:
4. -w:
5. dump:

(10 marks)

(b) Passwords are the most well-known validation method. However, they are also considered the weakest. Give **FOUR (4)** reasons why hackers can easily hack the password that the users use?

(8 marks)

(c) The OWASP Top 10 for 2013 is based on 8 datasets from 7 firms that specialize in application security, including 4 consulting companies and 3 tool/SaaS vendors. This data spans over 500,000 vulnerabilities across hundreds of organizations and thousands of applications. The Top 10 items are selected and prioritized according to this prevalence data, in combination with consensus estimates of exploitability, detectability, and impact estimates. Briefly explain **TWO (2)** web application vulnerabilities from the top 3 listed in OWASP Top 10 2013?

(5 marks)

**SECTION B (Total: 25 marks)**

**INSTRUCTION: Answer only ONE question ONLY.**
**Please use the answer booklet provided.**

**Question 4**

(a) There are many different ways of gaining access to information. A social engineer can use the telephone, intrusion within company property or using the Internet to obtain information. Information can be important whether it comes from the janitor's office or from the CEO's office; each piece of paper, employee spoken to or area visited by the social engineer can add up enough information to attain access to sensitive data and resources of the company. In order to handle this problem discuss **TWO (2)** appropriate countermeasures.

(5 marks)

(b) The primary components that make up your network infrastructure are routers, firewalls, and switches. They act as the gatekeepers guarding your servers and applications from attacks and intrusions. An attacker may exploit poorly configured network devices. Common vulnerabilities include weak default installation setting, wide open access controls, and devices lacking the latest security patches. Discuss **TWO (2)** countermeasures that can help in preventing each network threats listed below:

i. Information gathering
ii. Sniffing
iii. Spoofing
iv. Session hijacking
v. Denial of service

(20 marks)

**Question 5**

(a) Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services. The majority of web application attacks occur through cross-site scripting (XSS) and SQL injection attacks which typically result from flawed coding, and failure to sanitize input to and output from the web application.

i. Suggest **FOUR (4)** common remedies to help prevent SQL injection attacks.

(4 marks)

ii. Provide **THREE (3)** measures that are able to prevent cross-site scripting attack?

(3 marks)

(b) When a PC has been assaulted with a malware, after the cleaning procedure, list and discuss **FIVE (5)** common countermeasures can be executed for further counteractive action.

(10 marks)

(c) Phishing attacks use email or malicious websites to request individual data by acting as a trustworthy organization. Discuss **FOUR (4)** approaches to avoid being a phishing attacks victim.

(8 marks)



**END OF EXAMINATION PAPER**