UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION
JANUARY 2016 SEMESTER

COURSE CODE	:	IKB 42003
COURSE NAME	:	INCIDENT HANDLING AND RESPONSE
PROGRAMME NAME	:	BACHELOR OF COMPUTER SYSTEM SECURITY
DATE	:	27 MAY 2016
TIME	:	9.00 am – 11.00 am
DURATION	:	2 HOURS

UniKL MIIT

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 .
5. Please write your answers on the answer booklet provided.
6. Answer all questions in English language ONLY.

THERE ARE 10 PAGES OF QUESTIONS, INCLUDING THIS PAGE.

SECTION A (Total: 75 marks)

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

Question 1

(a) There was a fire at a factory and 60% of the building was destroyed. The damage to the building was $1200. Fire statistics reveal that the Zen factory has had a similar fire due to short circuit at an average of once every 4 years. The vulnerability is high. Senior management decides to spend $2000 installing a fire prevention system in the newly repaired factory. This system requires a $250 per year maintenance contract that extends the warranty of the fire prevention system to 20 years assuming the maintenance is performed annually. The warranty covers the cost of all repairs including parts and labor.

i. Given that the cost of the damages to the building was $1200, what is the total asset value of the Zen Factory?

(3 marks)

ii. Would you advise the management to buy the fire prevention system? Give your evaluation using calculations to prove your answer.

(6 marks)

iii. What is the Annual Rate of Occurrence (ARO) of fires at the Zen factory? Show the calculation.

(2 marks)

iv. What is the Annual Loss Expectancy (ALE) due to the fires at the Zen factory? Show the calculation.

(3 marks)

v. Based on the above scenario, describe the risk assessment that is carried out.

(1 mark)

UniKL MIIT

(b) Risk evaluation is importance to be carried out after the risk analysis process has been completed. Justify **TWO (2)** reasons why risk evaluation is crucial.

(2 marks)

(c) Explain the **FOUR (4)** risk controls strategies.

(8 marks)

UniKL MIIT

Question 2

(a) Emergency action card is deployed when a computer security incident occurs and the staffs are not prepared. Under such condition, briefly explain the **FIVE (5)** steps that can be taken to counter an incident.

(10 marks)

(b) *Over the past several years we have seen a rise in computer intrusions, malicious code, and other security incidents on our network. With approximately 30,000 computers attached to our network, it was no longer feasible for one individual to handle all of the incidents that were occurring. In 2014, we began a focused effort to improve our ability to detect problems, determine their causes, and minimize the damage they cause, preserve related evidence, resolve the problems, and take appropriate disciplinary or legal action. Part of this initiative involved the formation of an incident response team made up of three Department of Information Technology (DoIT) Security staff members and 10 volunteers from various departments at University of Windhill. The Incident Response Team (IRT), which operates as an integral part of the DoIT Security department, was formed as a central collection point for tracking incidents, analyzing information security trends, and working with other incident response teams worldwide. When an incident is detected by or reported to the IRT, DoIT Security begins by logging the incident and assessing its scope and severity. If the incident impacts a critical system or a large number of hosts on our network, DoIT Security mobilizes the IRT volunteers to assist in assessment, awareness, mitigation, and recovery. We involve legal counsel, upper management, human resources, and other departments as needed. The IRT volunteers serve as the primary contacts for their departments when there is an incident involving one or more of their computers as well. IRT volunteers also play a key role by providing advice to other campus IT staff on enhancing security during security incidents and restoring compromised machines.*

i. Discuss **FOUR (4)** benefits that the University Windhill will get from their decision to develop a Computer Security Incident Response Team (CSIRT).

(4 marks)

UniKL MIT

ii. Suggest **THREE (3)** methods best methods that the University could take to evaluate the efficiency and effectiveness of their team.

(3 marks)

iii. An organization that would like to form an incident response team would have to focus on reasons. Identify and explain **FOUR (4)** of these possible reasons.

(8 marks)

UniKL MIIT

Question 3

(a) Explain **TWO (2)** purpose of IP traceback and describe **TWO (2)** proactive tracing methods.

(8 marks)

(b)

0x0000	45c0	005c	c562	0000	1d06	4f81	8003	09f0
0x0010	d2dd	054a	0203	4b44	0000	0000	4500	002c
0x0020	79a4	0000	1c06	4a88	5804	004a	d09b	d9bf
0x0030	7443	0011	6a55	c3d1	0000	0000	6002	00a4
0x0040	44c3	0000	0106	005a	3220	6907	0000	0000
0x0050	0000	0000	0000	0000	0000	0000		

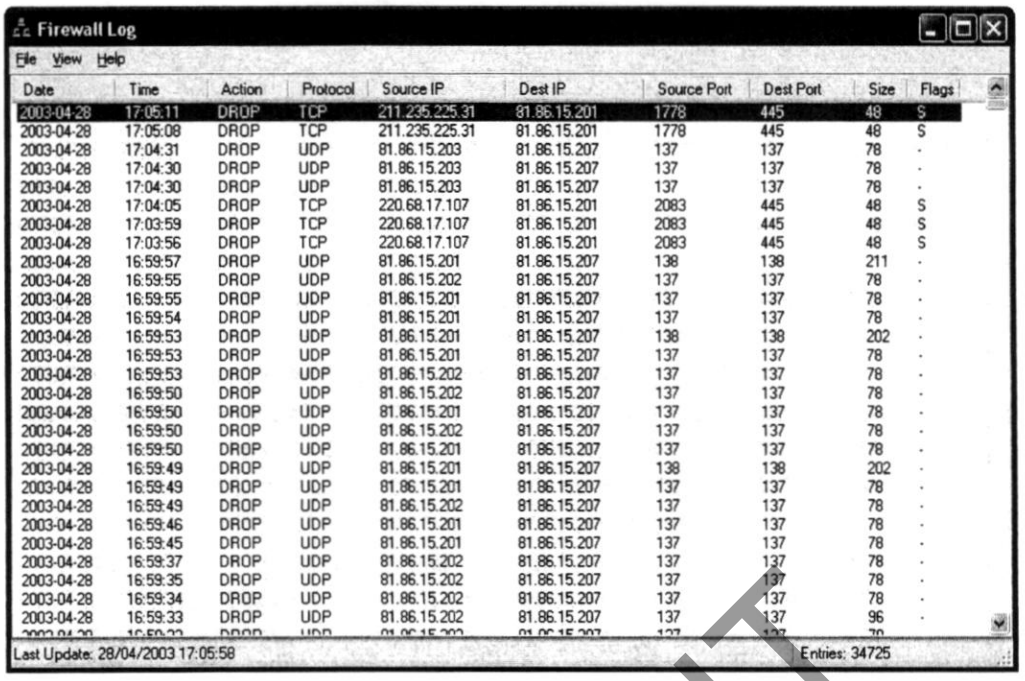
Figure 1 : A Data Dump from an IP Header

Based on Figure 1, interpret the data from the raw packet:

No.	Raw packet data	Meaning
(i)	0x0000 0x0010 0x0020 0x0030 0x0040 0x0050 (1 mark)	
(ii)	45c0 (3 marks)	
(iii)	8003 09f0 (5 marks)	

UniKL MIIT

(c)



Firewall Log

File View Help

Date	Time	Action	Protocol	Source IP	Dest IP	Source Port	Dest Port	Size	Flags
2003-04-28	17:05:11	DROP	TCP	211.235.225.31	81.86.15.201	1778	445	48	S
2003-04-28	17:05:08	DROP	TCP	211.235.225.31	81.86.15.201	1778	445	48	S
2003-04-28	17:04:31	DROP	UDP	81.86.15.203	81.86.15.207	137	137	78	-
2003-04-28	17:04:30	DROP	UDP	81.86.15.203	81.86.15.207	137	137	78	-
2003-04-28	17:04:30	DROP	UDP	81.86.15.203	81.86.15.207	137	137	78	-
2003-04-28	17:04:05	DROP	TCP	220.68.17.107	81.86.15.201	2083	445	48	S
2003-04-28	17:03:59	DROP	TCP	220.68.17.107	81.86.15.201	2083	445	48	S
2003-04-28	17:03:56	DROP	TCP	220.68.17.107	81.86.15.201	2083	445	48	S
2003-04-28	16:59:57	DROP	UDP	81.86.15.201	81.86.15.207	138	138	211	-
2003-04-28	16:59:55	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:55	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:54	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:53	DROP	UDP	81.86.15.201	81.86.15.207	138	138	202	-
2003-04-28	16:59:53	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:53	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:50	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:50	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:50	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:50	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:49	DROP	UDP	81.86.15.201	81.86.15.207	138	138	202	-
2003-04-28	16:59:49	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:49	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:46	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:45	DROP	UDP	81.86.15.201	81.86.15.207	137	137	78	-
2003-04-28	16:59:37	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:35	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:34	DROP	UDP	81.86.15.202	81.86.15.207	137	137	78	-
2003-04-28	16:59:33	DROP	UDP	81.86.15.202	81.86.15.207	137	137	96	-

Last Update: 28/04/2003 17:05:58 Entries: 34725

Figure 2: Firewall log

Based on Figure 2, firewall logs generally provide the best source of information about IP addresses of attacks. Explain why in **FOUR (4)** points.

(8 marks)

UniKL MIIT

SECTION B (Total: 25 marks)

INSTRUCTION: Choose one from questions four or five.
Please use the answer booklet provided.

Question 4

(a) What kind of security concept has/will the following situations violate?

i. Private conversation is being sniffed by a hacker.

(1 mark)

ii. An IIS web server's log file is full and stopped logging any further transaction.

(1 mark)

iii. Distributed Denial of Service (DDOS) is launched to attack ABC corporation and all websites and service are being brought down.

(1 mark)

iv. Hacker hijacked an email sending through servers. The email was modified and then sent to its original receiver. Unfortunately, the receiver did not notice about the changes.

(1 mark)

v. An internet-enabled client-server application which requires user authentication through password is written, the password is encrypted in order to protect the password from sniffing by hackers. However, it was found that a hacker can still easily log in the server.

(1 mark)

vi. The departmental experimental computer is installed with Windows 7 where all students share the same user account.

(1 mark)

vii. A company email server does not have a uninterruptible power supply installed.

(1 mark)

(b) An attack path is a model of the network or possibly the telecommunications route used to launch an attack.

i. Explain under what condition an attack path can be constructed.

(3 marks)

ii. Describe **TWO (2)** methods for constructing an attack path.

(8 marks)

UniKL MIIT

(c) *A school laboratory assistant was fined RM10,000 in default five months jail by the Sessions Court here today for posting comments insulting the Sultan of Perak on a website, the first such case in the country.*

According to the news above, which act under Malaysian Cyber Law will the school laboratory assistant being charged if found guilty?

(2 marks)

(d) *A freelance journalist from Penang was already coping with the pain from a hemorrhoids surgery when she had to endure another hurtful experience – she discovered that her surgeon had taken photographs of her private parts without her consent when she was under.*

When she confronted him, she was told that it was "normal procedure" and a common practice for "medical purposes". Outraged that her privacy had been violated, she sued the doctor.

i. According to the news excerpt above, which act under Malaysian Cyber Law will the assistant being charged if found guilty?

(1 mark)

ii. What is the scope of the Act in (i)?

(4 marks)

UniKL MIIT

Question 5

(a) Read the following scenario and answer the question accordingly.

Today the organization you work for has their network compromised. Consequently, there is a decent amount of valuable information lost. Your IT department has found what has been taken, but does not know what to do next. If you do not have a computer incident response or forensics team, this information might be lost forever and you may never find out who stole it.

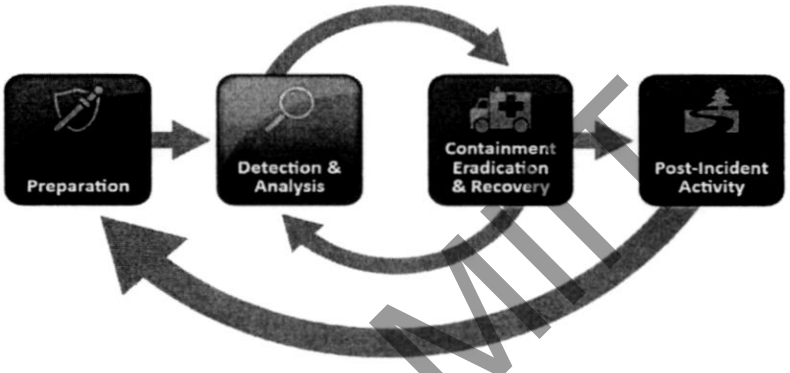


Figure 2: Incident Response Methodology

There are methods an incident response team/forensics team uses to not only track who breached your systems, but stop it from happening again. Based on Figure 2, discuss and elaborate each step taken to counter the said incident.

(14 marks)

(b) Describe **FIVE (5)** possible impacts of social networking sites.

(5 marks)

(c) As a member of the CSIRT, part of the task is to help creating computer security related guidelines for the organisation on usage for social networking sites. Propose **SIX (6)** points or content to be included in the new social media guidelines in your organisation.

(6 marks)

END OF EXAMINATION PAPER

UniKL MIIT