UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2011/2012

COURSE NAME	:	NETWORK SECURITY
COURSE CODE	:	BIT 3323 / BIT 33203
PROGRAMME	:	BACHELOR OF INFORMATION TECHNOLOGY
EXAMINATION DATE	:	JANUARY 2012
DURATION	:	3 HOURS
INSTRUCTION	:	ANSWER **ALL** QUESTIONS.

THIS QUESTION PAPER CONSISTS OF SEVEN (7) PAGES

Instruction: Answer **ALL** questions.

Q1 Given the following scenario:

> In computing terms CIA stands for Confidentiality, Integrity and Availability. These three things make up the basic stepping-stones when it comes to securing data stored on a shared resource (of which the Internet is). Without these three things the Internet would be useless. Let's take a look for example at an online banking operation.

Describe how do these three objects relate to its operation.

(a) Confidentiality.

(2 marks)

(b) Integrity.

(2 marks)

(c) Availability.

(2 marks)

Q2 Differentiate between passive and active attacks by filling up the following table.

	Passive Attack	**Active Attack**
Definition		
Method/Technique		
Example Tools		
The Result		
How to Protect		

(10 marks)

Q3 (a) Describe the mean of cryptography.

(2 marks)

(b) Categorize **TWO(2)** classes of key-based encryption algorithms.

(4 marks)

(c) What are **TWO(2)** factors of concern when using brute-force attacks against encryption?

(2 marks)

(d) Encrypt the plaintext "ANONYMOUS ATTACK" with the key "FSKTM" by using the Vigenère table attached (show your works).

(3 marks)

Q4 Draw a flow diagram of Hacking Methodology which would show the step by step of hacking activity.

(10 marks)

Q5 Given the following definitions:

```
A rootkit is a type of program often used to hide utilities on a
compromised system. Rootkits include so-called backdoors to help an
attacker subsequently access the system more easily. A rootkit is
frequently used to allow the programmer of the rootkit to see and access
usernames and log-in information for sites that require them.
```

Propose the actions to countermeasure the above rootkit attack.

(5 marks)

Q6 (a) Given the following scenario:

```
As a new IT Security Officer, you have been assigned to propose new
guidelines to user on how to choose the right password of your
company Human Resource Management System. This new guidelines are
very important as strong defensive measurement from password brute-
force attack.
```

Compose **FOUR(4)** new guidelines.

(4 marks)

(b) Describe how you would compromise a system that relies on cookie-based security.

(2 marks)

(c) Given the following statement:

```
Microsoft Windows is dangerously insecure when unpacked from the
box.
```

Describe the actions to be taken right after you install the Microsoft Windows operating system.

(2 marks)

Q7 (a) Discriminate the good or bad of hiring hackers in your organization (discuss and criticize your answer)

(4 marks)

(b) Evaluate **THREE(3)** different classes of hackers, Black Hats, White Hats and Grey Hats.

(6 marks)

Q8 Given the following scenario:

```
Bob has been hired to perform a penetration test on www.uthm.com. He
begins by looking at IP address ranges owned by the company and details of
domain name registration. He then goes to Staff Directory and Financial
websites to see if they are leaking any sensitive information of have any
technical details online.
```

(a) What phase is Bob involved within the context of penetration testing methodology?

(2 marks)

(b) Given the following scenario:

```
Bob proceed with entering trace routing command which shows the
following output.
```

```
[root@bt5 ~]# traceroute www.uthm.com
traceroute to www.uthm.com (161.139.246.217), 30 hops max, 40 byte
packets
 1  10.65.55.254 (10.65.55.254)  1.239 ms  1.365 ms  1.485 ms
 2  10.59.1.185 (10.59.1.185)  0.381 ms  0.566 ms  0.595 ms
 3  10.59.1.177 (10.59.1.177)  5.700 ms  5.901 ms  6.014 ms
 4  10.59.1.97 (10.59.1.97)  10.536 ms  10.792 ms  10.940 ms
 5  10.59.1.82 (10.59.1.82)  0.599 ms  0.624 ms  0.882 ms
 6  www.uthm.com (161.139.246.217)  0.248 ms !X  0.226 ms !X  0.215 ms !X
[root@bt5 ~]#
```

Identify the destination ip address.

(2 marks)

(c) State the next step of hacking methodology after **Q8(b)**.

(2 marks)

(d) Give **ONE(1)** example of a tool use in **Q8(c).**

(2 marks)

(e) Demonstrate how to use the tool as stated in **Q8(d).**

(2 marks)

(f) Given the following output executed from the tool in **Q8(e)**:

```
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
631/tcp   closed ipp
10000/tcp open   snet-sensor-mgmt
```

Describe about the level of vulnerability of the server.

(2 marks)

(g) Describe how to ensure that the server is running behind a firewall.

(2 marks)

(h) Demonstrate a command to prove the answer in **Q8(g)**

(2 marks)

(i) Describe **TWO(2)** potential attacks can be done from your vulnerability assessment to the server?

(2 marks)

(j) Give **ONE(1)** example of tool from each answer in **Q8(i)**.

(2 marks)

Q9 Given the following article:

Operation Honey Pot

NetSecure, a network security firm, connected six computers - with four operating systems - to the Internet for a week without any virus protection. The results: 4,892 direct attacks by viruses, worms and other types of malicious code, and 46,255 scans by remote computers looking for weaknesses.
Here's what happened:

Windows XP
Service Pack 1
Attacks: 4,857
Results: Attacked successfully within 18 minutes by the Blaster and Sasser worms. Within an hour, the computer was taken over and began attacking other Windows machines.

Windows XP
Service Pack 2
Attacks: 16
Results: Survived all attacks

Apple Mac OS X Jaguar
Attacks: 3
Results: Survived all attacks

Linux, Fedora Core 3
Attacks: 8
Results: Survived all attacks

Source: NetSecure

(a) Given the following statement:

```
From the report of honey pot operation shows that the differences
number of attack of each type of operating systems.
```

Explain why the numbers of attack are different between all operating system.

(5 marks)

(b) Develop a network design based on the Operation Honey Pot report.

(5 marks)

Q10 (a) Write a `Nmap` command that launches a stealth SYN scan against each machine in a class C address space where `target.example.com` resides and tries to determine what operating system is running on each host that is up and running

(3 marks)

(a) Write command that enables Snort to use network intrusion detection (NIDS) mode assuming `snort.conf` is the name of your rules file and the IP address is `192.168.1.0` with Subnet Mask:`255.255.255.0`.

(3 marks)

(b) Given the following definitions:

```
Steganography is the art and science of writing hidden messages in
such a way that no one, apart from the sender and intended
recipient, suspects the existence of the message, a form of security
through obscurity.
```

Compose the steps where you can hide your compressed private message file "`private.txt`" into an image file "`photo.jpg`".

(4 marks)

VIGENERE TABLE

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y