UNIVERSITI TEKNOLOGI MARA
FINAL EXAMINATION

COURSE	:	INFORMATION AND NETWORK SECURITY
COURSE CODE	:	ITT450
EXAMINATION	:	JANUARY 2012
TIME	:	3 HOURS

INSTRUCTIONS TO CANDIDATES

1. This question paper consists of two (2) parts : PART A (20 Questions)
   PART B (4 Questions)

2. Answer ALL questions from all two (2) parts :

   i) Answer PART A in the Objective Answer Sheet.
   ii) Answer PART B in the Answer Booklet. Start each answer on a new page.

3. Do not bring any material into the examination room unless permission is given by the invigilator.

4. Please check to make sure that this examination pack consists of :

   i) the Question Paper
   ii) a one–page Appendix 1
   iii) an Answer Booklet – provided by the Faculty
   iv) an Objective Answer Sheet – provided by the Faculty

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO

This examination paper consists of 8 printed pages

PART A (20 MARKS)

1. The CEO of your company has just issued a statement that the network must be more secure right away. You have discussed several options with the Chief Security Officer and the Chief Technology Officer. The results of your discussion are to implement IPSec. What are the two prime functions of IPSec that you can let the CEO know will be addressed with the implementation?

   i) Ensure data corruptibility
   ii) Ensure data integrity
   iii) Ensure data availability
   iv) Ensure data security
   v) Ensure data deliverability

   A. i & iii
   B. ii &iv
   C. iv & v
   D. all of the above

2. At a policy meeting you have been given the task of creating the firewall policy. What are the two basic positions you can take when creating the policy?

   i) To deny all traffic and permit only that which is required
   ii) To permit only IP traffic and filter TCP traffic
   iii) To permit only TCP traffic and filter IP traffic
   iv) To permit all traffic and deny that which is required
   v) To include your internal IP address as blocked from incoming to prevent spoofing

   A. iv & v
   B. i, ii & iii
   C. i & iv
   D. all of the above

3. You have recently taken over the security of a mid-sized network. You are reviewing the current configuration of the IPTables firewall, and notice the following rule:

```
ipchains -A input -p TCP -d 0.0.0.0/0 12345 -j DENY
```

   What is the function of this rule?

   A. This rule for the output chain states that all incoming packets from any host to port 12345 are to be denied.
   B. This rule for the input chain states that all incoming packets from any host to port 12345 are to be denied.
   C. This rule for the input chain states that any TCP traffic from any address destined for any IP address and to port 12345 is to be denied.
   D. This rule for the output chain states that any TCP traffic from any address destined for any IP address and to port 12345 is to be denied.

4. Which ones are the two types of ciphers?

   A. Blocking cipher and non-blocking cipher
   B. CBC cipher and EBC cipher
   C. Block cipher and stream cipher
   D. 3DES cipher and AES cipher

5. Which of the following are used to encrypt packet data?

   A. DES
   B. MD5
   C. SHA
   D. AH

6. Which of the following represents a type of exploit that involves introducing programs that install in inconspicuous back door to gain unauthorized access?

   A. File sharing
   B. Trojan horse
   C. Protocol weakness
   D. Session hijack

7. Which of the following is typical of signature-based intrusion detection?

   A. Signature creation is automatically defined
   B. Signature match pattern of malicious activity
   C. Signature are prone to a high number of false positive alarms
   D. Signature focus on TCP connection sequences

8. What does the attacker require to perform a Denial of Service attack?

   A. a means of the network access
   B. prior access to the target
   C. previously installed root kit
   D. username and password

9. What reconnaissance methods are used to discover server running SMTP and SNMP?

   A. TCP scans for port 25 and UDP scans for port 161
   B. TCP scans for port 23 and UDP scans for port 20
   C. TCP scans for port 22 and UDP scans for port 156
   D. TCP scans for port 110 and UDP scans for port 118

10. Which of the following statements represents a false positive alarm situation?

   A. normal traffic or a benign action will not cause a signature to fire
   B. offending traffic will cause a signature to fire
   C. normal traffic or a benign action will result in the signature firing
   D. offending traffic cause a signature to fire

11. The common name for the crime of stealing passwords is

    A. spooling
    B. identity theft
    C. spoofing
    D. hacking

12. Malicious software is known as

    A. badware
    B. malware
    C. maliciousware
    D. illegalware

13. A program that performs a useful task while simultaneously allowing destructive acts is a

    A. worm
    B. Trojan horse
    C. virus
    D. macro virus

14. An intentionally disruptive program that spreads from either from program-to-program or from disk-to-disk is known as a

    A. Trojan horse
    B. virus
    C. time bomb
    D. time-related bomb sequence

15. All of these are suggestions for safe computing **EXCEPT**

    A. Don't borrow disks from other people
    B. Open all e-mail messages but open them slowly
    C. Download shareware and freeware with caution
    D. Disinfect your system

16. Hardware or software designed to guard against unauthorized access to a computer network is known as a(n):

    A. hacker-proof program
    B. firewall
    C. hacker-resistant server
    D. encryption safe wall

17. When customers of a Web site are unable to access it due to a bombardment of fake traffic, it is known as

    A. a virus
    B. a Trojan
    C. cracking
    D. a denial of service attack

18. The scrambling of code is known as

    A. encryption
    B. firewalling
    C. scrambling
    D. password-proofing

19. Collecting personal information and effectively posing as another individual is known as the crime of

    A. spooling
    B. identity theft
    C. spoofing
    D. hacking

20. In 1999, the Melissa virus was a widely publicized

    A. email virus
    B. macro virus
    C. Trojan horse
    D. Time bomb

PART B (80 MARKS)

QUESTION 1

Cryptography is the practice and study of techniques for secure communication which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. One of the cryptography categories is Polyalphabetic Ciphers.

a) Briefly explain how Polyalphabetic Ciphers works.

(4 marks)

b) You are asked to use playfair cipher method. Give the cipher texts that you will get if the secret key and the message that you have to send are as following.

Keyword / Secret key: playbook
Text: life is variable

(10 marks)

c) Use Vigenere Tableau in the Appendix 1. By using the same keyword and message from question (b), give the cipher texts that the sender will get using Vigenere Cipher method.

(10 marks)

QUESTION 2

The Web application layer is the number one target for malicious online attacks. For example, website may possess an attack such as Cross-Site Scripting (XSS).

a) Briefly explain what you know about Cross-Site Scripting.

(3 marks)

b) The vulnerability of the web application let the website prone to cross-site scripting attacks. Briefly explain **THREE (3)** common vulnerabilities that make your Web application expose to cross-site scripting attacks.

(6 marks)

c) Explain **FOUR (4)** potential damages that Cross-Site Scripting can affect to the users and the systems.

(8 marks)

QUESTION 3

You were recently hired as a network specialist at the BARU MULA Company. The company just recently launched a new classified portal for people to buy and sell items online. Unfortunately, as the popularity of this portal grows, it attracts more than just normal clients. The website is also under constant denial-of-service attacks. As the newly recruited network specialist, your first task is to help and solve this problem. When analyzing the attack, you notice that the attack seems to be sending small packets every second. This has cause the following error to be generated:

Maximum number of TCP connection exceeded.

When this happens, the machines will ignore most legitimate connections to the web server and server will stop handling any GET request from clients.

a) Based on the above preliminary analysis, name and describe the type of denial-of-service attack above.

(4 marks)

b) To further confirm your analysis, you have run packet sniffer on the server and monitor a few packets, below is an example of such packet.

```
 45 00 00 3c      fd b140 00
40 06 fd 45      80 02 8c ea
8c d3 a6 04      8f 37 00 50
 b5 3c c0 85      00 000000
a0 02 16 d0      88 c6 00 00
02 04 05 b4      04 02 08 0a
0c 6c
```

The server received hundreds and hundreds of packets such as above. Based on the above packet, fill in the following information:

i) Client IP address

(2 marks)

ii) Client Port number

(2 marks)

iii) Server IP address

(2 marks)

iv) Server Port number

(2 marks)

v) While analyzing the packet, does the packet above show the attack pattern from answer 1(a)? Explain.

(4 marks)

c) You have notice that the attack comes from a single source address. As the Network Specialist, you suggest to setup a firewall rule to drop the packet. List the information that acquires in the firewall rules as shows in the table below.

Source	Destination	Protocol	Source Port Range	Destination Port Range	Action

(3 marks)

d) After the rule is configured, you noticed that the attack has stop for a while. After a few hours, you start to see a new kind of attack. In this new attack, whenever you put in a rule in the firewall to block the source address, the attack will use a new source address immediately. This makes it difficult for you to block the attack using firewall. Give and explain another solution to the above problem.

(6 marks)

QUESTION 4

a) Explain the differences between spoofing and session hijacking.

(4 marks)

b) Give and explain **TWO (2)** examples of session hijacking tools.

(6 marks)

c) Briefly describe what phishing is.

(4 marks)

END OF QUESTION PAPER

	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	
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	26