UNIVERSITI TEKNOLOGI MARA
ONLINE TEST

COURSE	**:**	**INTRODUCTION TO COMPUTER SECURITY**
COURSE CODE	**:**	**ITT320**
DATE	**:**	**JUNE 2022**
TIME	**:**	**2 HOURS**

NAME:	**NOOR RAIHAN BIN ABD RAHIM**
MATRIC NO:	**2020821002**
GROUP:	**JCS1104E**
LECTURER:	**SIR MOHD HAFIZAN BIN MUSA**

PART A (10 MARKS)

1. Which of the following statement regarding the honey pot is FALSE?

   A. A honey pot is a machine setup to simulate valuable server and network.
   B. Honey pot must be attractive enough to the intruder
   C. A honey pot tricks the intruder into believing that he has succeeded in accessing the actual system resources
   D. A honey pot implementation is part of the intrusion deterrence strategy in the organization

2. _____ involves simply trying to make the system less palatable target.

   A. Intrusion deflection
   B. Intrusion deterrence
   C. Anomaly detection
   D. Authentication profiling

3. Which of the following is **NOT** the features that snort can operate?

   A. Banishment vigilance
   B. Network intrusion-detection
   C. Sniffer
   D. Packet loger

4. The anomaly detection of IDS has following mechanisms **EXCEPT**;

   A. Infiltration
   B. Threshold monitoring
   C. Resource profiling
   D. Executable profiling

5. Using asymmetric encryption, Jeff uses _____ to send a message to Ali, and Ali uses _____ to open a message from Jeff.

   A. Jeff's public key, Jeff's private key
   B. Jeff's private key, Jeff's public key
   C. Ali's public key, Ali's private key
   D. Ali's private key, Ali's public key

Question 6 and 7 are related to the input given below.

INPUT 1	1	0	1	1
INPUT 2	1	1	0	1
OUTPUT	?	?	?	?

6. From the input 1 and input 2 above, the expected outcome if we apply **AND** operation is:

A. 1111
B. 1001
C. 0011
D. 0000

7. From the input 1 and input 2 above, the expected outcome if we apply **XOR** operation is:

A. 1000
B. 1111
C. 0110
D. 1001

8. Digital signature CAN NOT provide _____ for the message

A. authentication
B. confidentiality
C. non-repudiation
D. integrity

9. What protocols make up IPsec?

A. AH, PAP, CHAP, IPComp
B. AH, IKE, ESP, IPComp
C. IPComp, MS-CHAP, PAP, AH
D. AH, SPAP, CHAP, IPComp

10. What protects the actual packet data in IPSec?

E. AH
F. ESP
G. SPAP
H. CHAP

PART B (20 MARKS)

QUESTION 1

a) Intrusion Detection System (IDS) is designed to detect sign if there is someone attempted to breach a system and to alert the system administrator that suspicious activity is taking place. List ALL concepts of IDS available.

(5 marks)

- Pre-emptive blocking
- Infiltration
- Intrusion deflection
- Intrusion deterrence
- Anomaly detection

QUESTION 2

a) By using the Caesar Cipher method, encrypt the word **MALAYSIA** by shifting it using **EIGHT (8)** characters. Show your work steps.

(2 marks)

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

M	A	L	A	Y	S	I	A
12	0	11	0	24	18	8	0
8	8	8	8	8	8	8	8
20	**8**	**19**	**8**	**32**	**26**	**16**	**8**
U	I	T	I	G	A	Q	I

=UITIGAQI

b) By using the Caesar Cipher method, the word “CAESAR” with a shift P becomes “RPTHPG”, as shown below:

Plaintext	CAESAR
Key	**shifted P**
Ciphertext	RPTHPG

What is the key (Number of shifting) do we need to make “CAESAR” become “RPTHPG”?

(2 marks)

R = 17
C = 2
17-2 = 15
= key number is shifted 15 characters

c) By using the poli-alphabet substitution, using the keyword **HACK**, encrypt the message **CYBERCRIME**.
Show your work steps.

(3 marks)

H= 7
A = 0
C = 2
K= 10

C	Y	B	E	R	C	R	I	M	E
7	0	2	10	7	0	2	10	7	0
2	24	1	4	17	2	17	8	12	4
9	**24**	**3**	**14**	**24**	**2**	**19**	**18**	**19**	**4**
J	Y	D	O	Y	C	T	S	T	E

=JYDOYCTSTE

d) By using the poli-alphabet substitution, using the keyword **AES**, decrypt the message **REFSSEWEJE** to reveal the original message.
Show your work steps.

(3 marks)

A=0
E=4
S=18

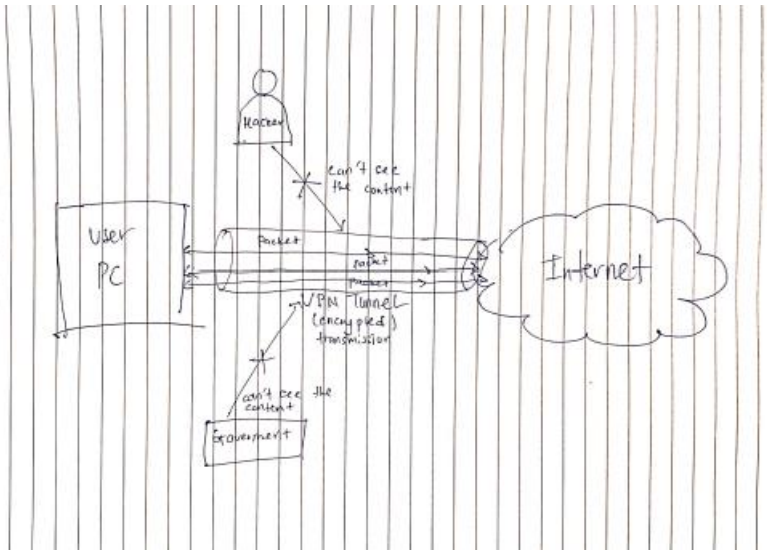
R	E	F	S	S	E	W	E	J	E
0	4	18	0	4	18	0	4	18	0
17	4	5	18	18	4	22	4	9	4
17	**0**	**-13**	**18**	**14**	**-14**	**22**	**0**	**-9**	**4**
R	A	N	S	O	M	W	A	R	E

= RANSOMWARE

QUESTION 3

a) VPN provide an encapsulation data service to guarantee the data we transmit over the internet is safe. By using a diagram illustrate and briefly explain how the VPN is working.

(5 marks)



When connecting to the VPN, the user will be connected to the VPN server that being provided by the VPN provider. This server will be act as a “tunnel” or known aa s VPN tunnel that being in the middle between the user and the internet. All the packets will be transmitted through the tunnel and will be encrypted and nobody can see what is inside the vpn tunnel and the packet content except the user and the vpn provider only. The connection will be slowed little bit since it needs time to encrypt and decrypt all the packets that going through the encrypted vpn tunner.

PART C (10 MARKS)

QUESTION 1

Company XYZ Sdn. Bhd. is planning to implement one of Intrusion Detection System (IDS) technology namely Honey Pot in their untrusted network. You are appointed as network administrator to this company to manage the implementation of their honey pot.

a) Define what is Honey Pot?

(2 marks)

Honeypot is a machine or a server that being set up to disguise as an important server to prevent the hacker getting access to the real server and to analyze the behavior and identity of the hacker such as specter.

b) Describe the benefit of Honey Pot.

(2 marks)

- Security researcher can analyze and do the research on known or unknown threat that try to attack the server without risking the real server
- It will shift the attacker from real server to the honeypot server that look alike the real server to prevent any illegal access.

c) Describe **ONE (1)** example of Honey Pot software that available nowadays.

(1 marks)

- specter

QUESTION 2

Regardless of which protocol you are using for your VPN, each of the protocol they will have their own advantage and disadvantages. For L2TP authentication they are a few authentications available like EAP, CHAP, PAP, SPAP and more.

a) Describe what is SPAP authentication.

(1.5 marks)

SPAP that stands for "Shive Password Authentication Protocol" is one of the L2TP authentication encryption and propriety version of PAP and more secure than PAP that being used in VPN encryption by using HTTP feature protocol to run the authentication.

b) State the differences between PAP and SPAP authentication.

(3.5 marks)

PAP	SPAP
Username and password transmitted through clear text and it will be compared to the database	Username and password are encrypted before send it for authentication.
Easy to be cracked by the Hacker	All the packets are being encrypted in both ways communication
Form basic of authentication	More secure than PAP since the connection is encrypted.

END OF QUESTION PAPER