UNIVERSITI KUALA LUMPUR
MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY

FINAL EXAMINATION

JANUARY 2016 SEMESTER

SUBJECT CODE	: IFD 30203
SUBJECT TITLE	: NETWORK SECURITY
LEVEL	: DIPLOMA
DATE	: 22 MAY 2016
TIME	: 2.00PM- 5.00PM
DURATION	: 3 HOURS

INSTRUCTIONS TO CANDIDATES

1. Please read the instructions given in the question paper CAREFULLY.
2. This question paper is printed on both sides of the paper.
3. This question paper consists of TWO SECTIONS: SECTION A and SECTION B.
4. Answer ALL questions in SECTION A. Use the answer booklet.
5. For SECTION B, answer ALL questions.
6. Please write your answers for SECTION B on the answer booklet given.
7. Answer all questions in English.

THERE ARE 10 PAGES OF QUESTIONS, INCLUDING THIS PAGE.

SECTION A (TOTAL 25 marks)

INSTRUCTION: Answer ALL questions

Please use the answer booklet provided

1. "Individual uses email or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords". This statement describes
   A. Phisher
   B. Spammer
   C. Phreaker
   D. Wardialing

2. A _____ executes arbitrary code and installs copies of itself in the infected computer's memory, which infects other hosts.
   A. Virus
   B. Worm
   C. Spyware
   D. Trojan

3. A _____ is a software application that uses a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.
   A. Port redirection
   B. IP Spoofing
   C. Packet sniffer
   D. Dictionary cracking

4. "An individual taking advantage of a trust relationship within a network". This statement describes
   A. Smurf attack
   B. Ping of Death
   C. TCP flood attack
   D. Trust exploitation

5. To increase the security of passwords, the following Cisco IOS commands should be utilized, **EXCEPT**:
   A. Enforce minimum password length
   B. Specify the banner MOTD
   C. Disable unattended connections
   D. Encrypt config file passwords

6. To improve security for virtual login connections, the login process should be configured with specific parameters, **EXCEPT**:
   A. Implement delays between successive login attempts
   B. Enable login shutdown if DoS attacks are suspected
   C. Generate system logging messages for login detection.
   D. Make passwords lengthy

7. When Alice sends a message to Bob, Bob uses _____ to VERIFY her message
   A. Bob's private key
   B. Bob's public key
   C. Alice's private key
   D. Alice's public key

8. _____ is needed when the router is compromised or needs to be recovered from a misconfigured password.
   A. Telnet
   B. SSH
   C. Password recovery
   D. Line vty

9. Below are the benefits of AAA, **EXCEPT**:
   A. Encrypt password
   B. Increased flexibility and control of access configuration
   C. Scalability
   D. Multiple backup systems

10. _____ provides the method of identifying users.
    A. Authorization
    B. Accounting
    C. Authentication
    D. Accessible

11. Which command enables the AAA by using the global configuration command?
    A. aaa new-model
    B. aaa authentication
    C. aaa authorization
    D. aaa accounting

12. Which command uses to deny multicast address?
    A. R1(config)# access-list 150 deny ip 0.0.0.0 0.255.255.255 any
    B. R1(config)# access-list 150 deny ip 172.16.0.0 0.15.255.255 any
    C. R1(config)# access-list 150 deny ip 224.0.0.0 15.255.255.255 any
    D. R1(config)# access-list 150 deny ip 127.0.0.0 0.255.255.255 any

13. Below are the technologies used in firewall, **EXCEPT**:
    A. Demilitarize Zone
    B. ACL
    C. Advance ACL
    D. Zone Based Policy (ZPF)

14. A _____ is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DoS attacks.
    A. Command
    B. Alarm
    C. Trigger
    D. Signature

15. "The administrator defines behaviors that are suspicious based on historical analysis." The statement briefly describes _____ based detection.

A. Policy
B. Pattern
C. Anomaly
D. Trigger

16. _____ occurs when an intrusion system generates an alarm after processing normal user traffic that should not have resulted in the alarm.

A. False positive
B. False negative
C. True positive
D. False negative

17. The following are the non-endpoint LAN devices, **EXCEPT**:

A. Switches
B. Network Appliances Control
C. IP Telephony devices
D. Storage area networking (SAN) devices

18. The task of breaking encrypted message or codes into readable message is known as _____

A. Decapsulation
B. Cryptanalysis
C. Signal hack
D. Cryptonic

19. A network LAN can be secured through the following methods below, **EXCEPT**:

A. Device hardening
B. AAA access control
C. Rail Fence
D. IPS implementations

20. _____is a practice and study of determining the meaning of encrypted information.

A. Cryptanalysis
B. Cryptology
C. Steganography
D. Cipher text

21. _____ transforms ciphertext back into clear text making it readable by authorized users.

A. Decryption
B. Encryption
C. Cryptanalysis
D. Hashing

22. _____ is a system to accomplish the encryption/decryption, user authentication, hashing, and key-exchange processes

A. Hashing
B. Cryptosystem
C. Steganography
D. Bibliography

23. Below are the services provided by VPN, **EXCEPT**:

A. Accountability
B. Authentication
C. Confidentiality
D. Integrity

24. _____ securely connect remote users, such as mobile users and telecommuters, to the enterprise.

A. Site- to- site VPN
B. Extranet VPN
C. Intranet VPN
D. Remote Access VPN

25. _____ are two main protocols used by IPSec to create a security framework.

A. AES and DES
B. AH and Diffie Hilman
C. ESP and SHA-1
D. AH and ESP

SECTION B (TOTAL 75 marks)

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

Question 1

a. "AAA is one of the core concepts to know when implementing security on Cisco devices. Each of these items has its own part of the security picture and each should be configured to secure a device". Based on the statement, briefly explain the characteristics of AAA concept

(6 marks)

b. List **THREE (3)** areas of router security

(3 marks)

c. List **THREE (3)** characteristics of a good password

(3 marks)

d. Describe **TWO (2)** characteristics of Secure Shell (SSH)

(4 marks)

e. "Two of the most used AAA protocols are Terminal Access Controller Access-Control System (TACACS+) and Remote Authentication Dial In User Service (RADIUS)".
Based on the statement, differentiate the characteristic of TACACS+ and RADIUS

(6 marks)

f. "Cisco IOS routers can implement AAA using either local username or Cisco Secure Access Control Server".
Illustrate the process of implementing AAA using Cisco Secure Access Control Server

(3 marks)

[25 marks]

Question 2

a. Answer the following questions:

i. Give **TWO (2)** examples of Intrusion Detection System (IDS)

(2 marks)

ii. Briefly explain **TWO (2)** disadvantages of IDS over IPS

(4 marks)

iii. Explain the differences between IDS and IPS

(4 marks)

b i. Based on Figure 1, briefly explain the characteristics of Zone Base Policy filtering firewall

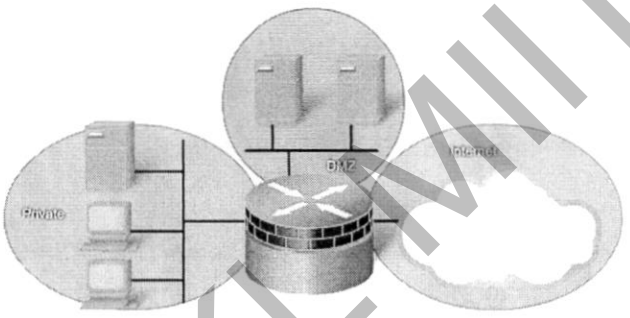

Figure 1: Zone Based Policy Firewall

(4 marks)

c. Give **TWO (2)** examples of action that can be taken by Port Security if a MAC address differs from the list of secure addresses.

(4 marks)

d. Give **ONE (1)** example of hashing methods.

(1 mark)

e. Answer the following questions

i. Describe the characteristic of Virtual Private Network (VPN)

(2 marks)

ii. Differentiate between Intranet VPN Extranet VPN

(4 marks)

[25 marks]

Question 3

a. Answer the following questions

i. Apply the Vernam Cipher algorithm to a plain- text message N A T I O N A L T R E A S U R E using one time- pad to produce cipher- text. Given the one time- pad is:

X Y Z A B C O P Q R S T E F G H

(6 marks)

ii. By using THREE shift key from Ceaser Cipher, decrypt the following sentence

S D V V Z L W K I O B L Q J F R O R U

(4 marks)

b. Describe **THREE (3)** characteristics of Symmetric Encryption

(6 marks)

c. Briefly explain **TWO (2)** function of Hashing

(4 marks)

d. Give example for each of the following hashes, protocol and algorithm

	Integrity	Authentication	Confidentiality
Common cryptographic hashes, protocols, and algorithms	i. _____ ii. _____	HMAC-MD5 iii._____	iv._____ v. _____

(5 marks)

[25 marks]

END OF EXAMINATION PAPER