UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
SEMESTER I
SESSION 2022/2023

COURSE NAME	:	COMMUNICATION AND NETWORK SECURITY
COURSE CODE	:	BIS 30903
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	FEBRUARY 2023
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS. 2. THIS FINAL EXAMINATION IS CONDUCTED VIA **CLOSED BOOK**. 3. STUDENTS ARE **PROHIBITED** TO CONSULT THEIR OWN MATERIAL OR ANY EXTERNAL RESOURCES DURING THE EXAMINATION CONDUCTED CLOSED BOOK.

THIS QUESTION PAPER CONSISTS OF **EIGHT (8)** PAGES

SECTION A

Choose the BEST answer for each of the following questions.

Q1 What name is given to an amateur hacker?

A. Red Hat.
B. Black Hat.
C. Blue Team.
D. Script Kiddie.

(2 marks)

Q2 What command can be used to encrypt all plaintext passwords?

A. `password secret`
B. `enable secret security`
C. `enable password secret`
D. `service password-encryption`

(2 marks)

Q3 __________ provides a secure remote login through a virtual interface.

A. Secure Shell (SSH)
B. Spanning Tree Protocol (STP)
C. Trivial File Transfer Protocol (TFTP)
D. Simple Network Management Protocol (SNMP)

(2 marks)

Q4 What is the main purpose of the command below?

```
Router(config)# enable secret level 5 bis30903
```

A. To enable secret password using SHA.
B. To enable secret password using MD5.
C. To enable secret password grants access to privileged EXEC level 5.
D. To enable secret password can only be set by individuals with privileges for EXEC level 5.

(2 marks)

Q5 __________ requires users to prove who they are.

A. Accounting
B. Auditing
C. Authorization
D. Authentication

(2 marks)

Q6 A network administrator wants to create a new view so that a user only has access to certain configuration commands.

In role-based Command Line Interface (CLI), which view should the administrator use to create the new view?

A. Superview.
B. CLI view.
C. Root view.
D. Admin view.

(2 marks)

Q7 A(n) __________ provides filtering at the network layer, but also analyzes traffic at Open System Interconnection (OSI) Layer 4 and Layer 5.

A. Stateful Firewall
B. Next Generation Firewall
C. Packet Filtering (Stateless) Firewall
D. Application Gateway (Proxy) Firewall

(2 marks)

Q8 Which of the following is a benefit of using a firewall in a network?

A. It is susceptible to IP spoofing.
B. It is do not reliably filter fragmented packets.
C. It is use complex ACLs, which can be difficult to implement and maintain.
D. It sanitizes protocol flow, which prevents the exploitation of protocol flaws.

(2 marks)

Q9 Network Access Control (NAC) systems can have the following capabilities, **EXCEPT** __________.

A. route filtering
B. incident response
C. profiling and visibility
D. security posture checking

(2 marks)

Q10 A student wants to create or modify a role based CLI access view and enter view configuration mode and provide security to access network resources.

What command should the student use?

A. `R2(config)#aaa new-model`
B. `R2(config)#parser view abc`
C. `R2(config)#aaa authorization exec default local`
D. `R2(config-view)#commands exec include all show`

(2 marks)

Q11 Which of the following is **NOT** types of VPN connection?

A. Site-to-site.
B. Leased line.
C. Remote access.
D. Secure Sockets Layer (SSL).

(2 marks)

Q12 What is a feature of an Intrusion Prevention System (IPS)?

A. It has no impact on latency.
B. It is deployed in offline mode.
C. It can stop malicious packets.
D. It is primarily focused on identifying possible incidents.

(2 marks)

Q13 __________ is a network security tool that performs real-time traffic analysis and generates alerts when threats are detected on IP networks.

A. Snort
B. Nmap
C. Nessus Vulnerability Scanner
D. Switch Port Analyzer (SPAN)

(2 marks)

Q14 A __________ occurs when an IPS generates an alarm after processing normal user network traffic.

A. false negative
B. false positive
C. true positive
D. true negative

(2 marks)

Q15 Keyword __________ is used to document and interpret the purpose of the Access Control List (ACL) statement on a Cisco device.

A. `eq`
B. `established`
C. `remark`
D. `description`

(2 marks)

SECTION B

Q16 As an information security student, you need an Intrusion Prevention System (IPS) to detect and stop a network attack.

(a) Describe **FOUR (4)** steps of how an IPS works.

(8 marks)

(b) Determine the alert/alarm category generated by an IPS such as Snort based on the description below.

(i) No security incident has occurred.

(1 mark)

(ii) The alert does not indicate an actual security incident.

(1 mark)

(iii) The alert has been verified to be an actual security incident.

(1 mark)

(iv) An undetected incident has occurred.

(1 mark)

(c) Write the `show` commands that can be used to verify the Snort IPS configuration and operation based on the following description.

(i) To display the status of the Unified Threat Defense (UTD) engine.

(2 marks)

(ii) To display an overview of resources that are utilized by the applications.

(2 marks)

(iii) To display the Unified Threat Defense (UTD) configuration.

(2 marks)

(iv) To display a list of resources that are committed to a specified application including attached devices.

(2 marks)

Q17 You are working at a company, Azanius Sdn Bhd as a network security specialist. You were asked by the company to design the company's network, where it involved three branches located in Perlis, Perak, and Pahang.

You are required to write the correct Internetwork Operating System (IOS) commands to perform the following tasks. Use the addressing table information as shown in **Table Q17**.

Table Q17

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
Perlis	Se0/3/0 - DCE	202.10.10.201	255.255.255.252	-
	Fa0/0	192.168.10.1	255.255.255.0	-
Perak	Se0/2/0	202.10.10.202	255.255.255.252	-
	Se0/2/1 - DCE	202.10.10.205	255.255.255.252	-
	Fa0/0	192.168.20.2	255.255.255.0	-
Pahang	Se0/1/0	202.10.10.206	255.255.255.252	-
	Fa0/0	192.168.30.3	255.255.255.0	
PC-X	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC-Y	NIC	192.168.20.10	255.255.255.0	192.168.20.2
PC-Z	NIC	192.168.30.10	255.255.255.0	192.168.30.3

(a) Configure **ALL** routers in Perlis, Perak, and Pahang.

(6 marks)

(b) Configure **ALL** switches in Perlis, Perak, and Pahang.

(6 marks)

(c) Configure a username as `admin` and `AzaniusNet@81` as the password using the type 8 hashing algorithm on the router in Perlis.

(2 marks)

(d) Configure dynamic routing `RIPv2` for router in Perak and Pahang.

(3 marks)

(e) Configure static routing for router in Perak and Pahang.

(3 marks)

Q18 You have been asked by a senior network administrator to implement an Access Control List (ACL) to filter traffic and mitigate network attacks on a network.

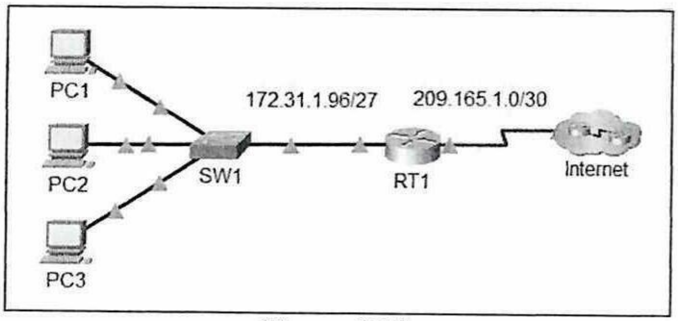

Figure Q18

Table Q18

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	172.31.1.126	255.255.255.224	N/A
	S0/0/0	209.165.1.2	255.255.255.252	
PC-A	NIC	172.31.1.101	255.255.255.224	172.31.1.126
PC-B	NIC	172.31.1.102	255.255.255.224	172.31.1.126
PC-C	NIC	172.31.1.103	255.255.255.224	172.31.1.126
Server-X	NIC	64.101.255.254	-	-
Server-Y	NIC	64.103.255.254	-	-

Based on information in **Figure Q18** and **Table Q18**, answer the following questions.

(a) Calculate the wildcard mask for PC-A LAN.

(1 mark)

(b) Calculate the wildcard mask for PC-B LAN.

(1 mark)

(c) Write suitable Internetwork Operating System (IOS) commands to perform the following tasks using Extended ACL configuration.

(i) Deny access from PC-A to Server-X only for HTTP (port number 80).

(2 marks)

(ii) Deny access from PC-A to Server-X, only for HTTPS (port number 443).

(2 marks)

(iii) Deny access from PC-B to Server-X, only for FTP (port number 21).

(2 marks)

(iv) Deny ICMP access from PC-Z to Server-X.

(2 marks)

-END OF QUESTIONS-