**JOSEPH MULOKI-KISIRA S23B13/034 B24322**

**Section A**

1. B
2. C
3. C
4. D
5. B
6. A
7. C
8. C
9. B
10. A

**Section B**

11.

SymmetricEncryption: Same key used for the encryption and decryption. It is faster but relies on secure key distribution. For instance: AES (Advanced Encryption Standard).

Asymmetric Encryption: Uses one key publicly and one for private. The public key is used to encrypt data, and the private key to decrypt it. It is more secure but slower. Example: Rivest-Shamir-Adleman (RSA).

12.

Improved Productivity – Reduces human error by automating repetitive tasks such as device setups and patching updates.

Better Protection – Maintains security compliances, adopts policies promptly, and effectively deals with any threats in real time.

Growth Potential – Lets firms create and oversee extensive systems with a minimum of manual effort.

13.

| RADIUS | TACACS+ |
| --- | --- |
| Encrypts only passwords | Encrypts the entire packet |
| Employs UDP (speedier yet less dependable) | Utilizes TCP (dependable and more secure) |
| Integrates authentication and authorization | Divides authentication, authorization, and accounting (AAA) |
| Network access purposes (e.g., Wi-Fi, VPN) | Device administration purposes (e.g., routers, switches) |

14.

Centralized Control:

SDN separates control plane from data plane so you can manage and see the network.

Dynamic Security Policies:

Enforce security policies in real-time across the network, adapting to threats.

Security Response Automation:

Automate response to security incidents (e.g., isolate compromised hosts, reroute traffic).

Micro-Segmentation:

Segment the network to limit threat movement.

Integrates with Security Tools:

Integrates with firewalls, IPS and other security solutions for defense in depth.

### 15.

Isolate Sensitive Data:

Segments separate critical systems (e.g., finance, HR) from general network traffic, reducing exposure to threats.

Contain Breaches:

Prevent attackers from moving laterally in the network, contain breaches to a single

Segment.

Improved Monitoring and Control:

More focused monitoring and enforcement of security policies per segment.

Compliance:

Helps you meet regulatory requirements by isolating sensitive data and systems.

16.

Simplified Device Management:

APIs allow programmatic interaction with Cisco devices, enabling automation of configurations, updates, and monitoring.

Integration with Tools:

APIs enable integration with third-party tools (e.g., Ansible, Python scripts) for orchestration and automation.

Real-Time Data Access:

Provides real-time access to device telemetry and status, improving visibility and decision-making.

Scalability:

Facilitates management of large-scale networks by automating repetitive tasks across multiple devices.

Enhanced Security:

Enables automated enforcement of security policies and rapid response to threats.

17.

**General key**

enable

conf t

hostname Router1

ip domain-name ucu.ac.ug

crypto key generate rsa modulus 2048

exit

**Enable ssh**

conf t

line vty 0 4

transport input ssh

login local

exit

**Local user**

conf t

username admin secret joseph123

exit

18.

conf t

vlan 10

name Finance

exit

interface FastEthernet0/1

switchport mode access

switchport access vlan 10

exit

conf t

interface FastEthernet0/1

switchport mode access

switchport access vlan 10

exit

19.

conf t

ip dhcp snooping

ip dhcp snooping vlan 10

interface FastEthernet0/1

ip dhcp snooping trust

Exit

conf t

ip arp inspection vlan 10

interface FastEthernet0/1

ip arp inspection trust

exit

20.

1. Limit SSH Access by IP Address

Use Access Control Lists (ACLs) to allow only trusted IPs to connect via SSH:

1. Enable Login Delay and Failures Restriction

Introduce a delay between login attempts to slow down brute-force attempts:

b).

Control Plane Policing (CoPP)

Control Plane Policing (CoPP) is a Cisco IOS feature that protects a network device’s control plane (CPU and memory) from excessive or malicious traffic, including DDoS attacks, brute-force attempts, and flooding attacks.

It helps ensure that the router/switch can continue handling essential network functions by rate-limiting unnecessary or malicious traffic directed to the device itself.

This feature helps protect the router’s control plane from excessive SSH connection attempts by limiting traffic: