Course Name: network and system administration

Time: 3 Hours

Instructions:

1. **Answer all questions.**
2. **Open book Exam (include the internet access)**

Fundamental of Cyber Security (20 Marks)

- **Scenario:** A company's employee accidentally clicked on a suspicious link in an email and suspects their computer may be infected. What immediate steps should the company take to mitigate the potential threat?

Question: List and explain at least three immediate actions the company should take to address this situation.

- **Scenario:** A small business is considering migrating its customer data to a cloud storage solution. They want to ensure the security of the data during and after the migration process.

Question: What security measures should the business implement to protect customer data before, during, and after the migration to a cloud storage solution?

- **Scenario:** A company's network has recently experienced several incidents of unauthorized access to sensitive data. They suspect an insider threat. How should the company investigate and mitigate this situation?

Question: Describe the steps the company should take to investigate and address the potential insider threat, considering both technical and non-technical measures.

- **Scenario:** A social engineering attack targeted an organization's employees through a phishing email campaign. Some employees fell for the scam, resulting in compromised accounts.

Outline a comprehensive security awareness training program to educate employees about the risks of phishing attacks and how to recognize and respond to them.

- **Scenario:** A company wants to implement a bring-your-own-device (BYOD) policy to allow employees to use their personal devices for work. They are concerned about the security implications.

Question: What security considerations and best practices should the company implement when creating a BYOD policy to minimize potential security risks?

fundamental networking (60 Marks)

1. **Scenario:** A small business is experiencing network connectivity issues. Some employees can't access the internet or internal resources, while others have no problems. What troubleshooting steps would you take to identify and resolve the issue?

   Question: Outline a step-by-step process for troubleshooting this network connectivity issue, starting from the initial assessment and diagnosis to resolution.

2. **Scenario:** A company wants to set up a secure wireless network for its employees. They are concerned about unauthorized access and want to implement proper security measures.

   Question: Describe the security features and best practices the company should implement to secure its wireless network and protect it from unauthorized access.

3. **Scenario:** An organization is planning to expand its network by connecting multiple branch offices. They want to ensure efficient communication between these offices.

Question: Explain the advantages and disadvantages of different network topologies for connecting branch offices and recommend the most suitable topology for this organization.

4. **Scenario:** A large university is experiencing network congestion during peak hours, causing slow internet access for students and faculty. They want to improve network performance.

   Question: Suggest strategies and network optimization techniques the university can implement to alleviate network congestion and provide faster internet access during peak hours.

5. **Scenario:** A company needs to implement a disaster recovery plan for its network infrastructure. They want to ensure data redundancy and minimal downtime in case of network failures.

   Question: Describe the key components and steps involved in creating a network disaster recovery plan, including backup and failover solutions.

6. **Scenario:** A small business operates a file server that stores sensitive client data. They want to protect the confidentiality and integrity of this data.

   Question: Provide recommendations on how the business can secure the file server and data, including encryption and access control measures.

7. **Scenario:** An organization is planning to migrate its on-premises servers to a cloud-based infrastructure. They need to ensure a smooth transition while maintaining data availability and security.

   Question: Explain the key considerations and steps involved in migrating servers to the cloud, emphasizing data security and availability during the process.

8. **Scenario:** A company's remote employees need secure access to the corporate network and resources. They are concerned about potential security threats.

Question: Describe the methods and technologies the company can use to provide secure remote access for employees while mitigating security risks.

9. **Scenario:** A manufacturing plant wants to implement an Industrial Internet of Things (IoT) network to monitor and control machinery. They are concerned about network reliability and security.

   Question: Outline the network architecture and security measures the manufacturing plant should employ for a reliable and secure IoT network.

10. **Scenario:** An organization needs to segment its network to improve security and reduce the risk of lateral movement by attackers. They want to implement network segmentation best practices.

Linux Scenario-based Questions: (20)

1. **Scenario:** You are the system administrator for a company that uses a Linux server. The server has become unresponsive, and you suspect a high load on the system. What commands and procedures would you use to diagnose and resolve this issue?

   Question: Outline the steps and commands you would use to identify and mitigate the high load issue on the Linux server.

2. **Scenario:** A user accidentally deleted a critical file, and there is no backup available. How can you attempt to recover the deleted file on a Linux system?

   Question: Describe the techniques and commands you can use to attempt file recovery on a Linux system in this scenario.

Question: Detail the troubleshooting steps you would take to identify and resolve the SSH connectivity problem reported by the user.

Batch Scripting Scenario-based Questions:

Scenario: You are responsible for automating a repetitive task on a Windows system using batch scripting. The task involves copying files from one folder to another. How would you create a batch script for this purpose?

Question: Write a sample batch script that copies files from one folder to another, specifying the necessary commands and explanations.

Scenario: A company wants to run a batch script at startup to launch multiple applications on their Windows workstations. How can you create a batch script for this purpose?

Question: Provide a batch script that launches several applications at startup and explains how to configure it to run on Windows workstations.