Natanauan, Lucky D.
4IT-B

1. Read the case-study scenario (see attached doc file).
2. Answer the following questions:

a. What are your roles and responsibilities as a junior system administrator in this situation? What steps would you take to solve each of these problems?

- As a junior system administrator, my job would be to fix the network, security, software, and backup issues. So, to handle these issues. For the Network Problems, I would check the network hardware and look for issues in the network logs. And then I'd update the firmware, replace faulty equipment, and improve bandwidth management if needed. As for the Unauthorized Access, I'll investigate the suspicious login attempts, secure the affected accounts by resetting passwords, and implement multi-factor authentication (MFA) to strengthen security. Next is for the Outdated Software issues, I'll audit all devices for outdated software and schedule updates. Automated tools would be used to ensure systems stay up to date. Lastly to fix the Backup Issues, I'll fixed it by identifying why they are failing, repairing damaged backups, and setting up alerts to prevent future failures. A cloud-based backup solution could also be introduced for added reliability.

b. Which of these issues do you think should be dealt with first? Explain why and how you would handle the most urgent issues.

- I think the **Unauthorized Access** because it poses an immediate security risk. I'd secure the compromised accounts, implement MFA, and notify management and employees to protect the company's data and systems.

c. How would you create a plan to prevent these problems from happening in the future? Think about network reliability, security, keeping software updated, and ensuring data backups work properly. What tools or methods would you use?

- **Network Reliability:** I would regularly update the network hardware and I'll use a monitoring tools to detect issues early. I'll consider having a backup network paths in case of failure.
- **Security:** I'll strengthen the security by enforcing MFA, updating antivirus software, and performing regular security audits.
- **Software Updates:** I'll use a automated patch management tools to keep all the systems up to date.
- **Data Backups:** I'll implement a regular testing of backups, monitor backup failures, and use both local and cloud backups to ensure data safety.

d. How would you communicate with other departments about the actions you are taking to fix these problems, and what steps would you take to make sure their work isn't disrupted?

- I'll provide regular updates to department heads about the fixes and explain the next steps. Schedule major updates during non-working hours to reduce downtime. Ensure users are informed about actions they need to take, like changing passwords, with clear and simple instructions.