## **Scenario**

# 

# Review the following scenario. Then complete the step-by-step instructions.

# You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers’ personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.

# After inspecting the organization’s network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

# The organization’s employees' share passwords.

# The admin password for the database is set to the default.

# The firewalls do not have rules in place to filter traffic coming in and out of the network.

# Multi Factor authentication (MFA) is not used.

# If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.

# In this activity, you will write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

# 

# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| 1. Set strong password policies.  2. MFA (Multi Factor Authentication)  3.Configure firewall settings regularly | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Strong password policies need to be set to avoid employees sharing passwords with each other. Setting password policies will help to avoid threat actors from accessing the users’ and employees’ accounts.  Using MFA users and employees both need to verify their identity at two levels which will help in reducing the chances of a threat actor getting access to organization’s softwares and personal data of users.  Configuring the firewall regularly helps the organization to prevent any latest attacks  Setting proper firewall rules makes it filter more accurately. |