Security risk assessment report (My Responses)

Part 1: Select up to three hardening tools and methods to implement
I've investigated and found three potential vulnerabilities and I recommend implementing the following three hardening tools and methods: 1. **Implement Multi-Factor Authentication (MFA):** Firstly, implementing the (MFA) can help strengthen who is logging in and out while securing the account which users to provide more than one type of verification before gaining access to a system like passwords, fingerprint scans, ID cards, or pin numbers. Based on the scenario, it looks it would be best to add another layer of security, MFA makes it more difficult for attackers to gain unauthorized access. 2. **Implement Password Policies**: The second change I noticed is that the scenario and the given documents suggests that the company lacks stronger password policies and measures. I suggest that the organization can implement an improved password policy that sets clear guidelines for what makes a secure password like requiring a minimum password length, using a mix of upper- and lower-case letters, numbers, and special characters, and preventing employees from sharing passwords. This can also include limiting unsuccessful login attempts like locking the account after five failed attempts to secure the account and prevent hacking (social engineering techniques). 3. **Regular Firewall Maintenance:** Thirdly I suggest maintaining and updating firewalls to ensure the network is protected against evolving threats. I noticed that the company lacks this and should implement this as regular firewall maintenance can help review and updating firewall rules to block traffic from suspicious sources. With the documents that are given, it suggests that if doing so these changes, network administrators should make sure the firewalls are configured correctly to allow only trusted traffic while blocking harmful or unauthorized data from entering or leaving the network.

Part 2: Explain your recommendations
With the explanations previously mentioned and based on the scenario that has the vulnerabilities impact the network, it is crucial to implement the three security hardening practices that I have suggested to mitigate future data breaches/attacks. First, implementing Multi-Factor Authentication (MFA) requires users to provide more than one form of verification, such as passwords combined with biometrics or authentication tokens. This adds an extra layer of security, making it significantly harder for attackers to gain unauthorized access. Next, the company should implement stronger password

policies to ensure all passwords are robust and difficult for attackers to guess or crack. The company so far does not have this implemented and invulnerable to bad actors that want to hack into the account. To do this change, the password policy should make a specific password length, upper- and lower-case letters, numbers, and special characters. And also include other polices like not sharing passwords and implementing an account lockout policy after a certain number of failed logins attempts. Lastly, the company lacks implementing a regular firewall maintenance that can protect the network from unauthorized access and malicious traffic. The company should make changes by implementing better firewall rules to be regularly reviewed and updated to ensure only trusted traffic is allowed while unauthorized traffic is blocked. They should also consult with the network administrators to help configure firewalls to adhere to the principle of least privilege, allowing only necessary communication and enforcing strict access control measures.

Additional Information:

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:

1. The organization's employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multifactor 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.

Step 3: Select up to three hardening tools and methods to implement

Think about all of the network hardening tools and methods you have learned about in this course that can protect the organization's network from future attacks. What hardening tasks would be the most effective way to respond to this situation? Write your response in part one of the worksheet.

Step 4: Provide and explain 1-2 recommendations

You recommended one or two security hardening practices to help prevent this from occurring again in the future. Explain why the security hardening tool or method selected is effective for addressing the vulnerability. Here are a couple questions to get you started:

- Why is the recommended security hardening technique effective?
- How often does the hardening technique need to be implemented?

Write your response in part two of the worksheet.

Be sure to address the following criteria in your completed activity:

- One to three network hardening tools and methods.
- The reasons why the tools and methods selected are effective.