**Activity: Analysis of network hardening**

In this worksheet, you will be presented with a scenario about a social media organization that recently suffered a major data breach caused by undetected vulnerabilities. To address the breach, you'll identify some common network protection tools that can be implemented to protect the overall security of the organization. Next, you'll select a specific vulnerability that the company has and propose different methods of network protection. Finally, you will explain how the methods and tools you choose will be effective in managing the vulnerability and how they will prevent potential breaches in the future.

**Scenario**

You're a security analyst working for a social media organization. The organization recently suffered a major data breach, which compromised the security of its customers' personal information, such as names and addresses. Your organization wants to implement robust network protection practices that can be consistently executed to prevent attacks and breaches in the future.

After inspecting your organization's network, you discover four main vulnerabilities. The four vulnerabilities are as follows:

* Organization employees share passwords.
* The database administrator password is set as the default.
* Firewalls don't have rules to filter traffic 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 worksheet, you will write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

**Step 1: Access the template**

File "*Security risk assessment report*"

**Step 2: Access support materials**

File "*2 SUPPORT Network hardening tools"*

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

Think about all the network protection tools and methods you've learned in this course that can protect your organization's network from future attacks. Which reinforcement tasks would be the most effective way to respond to this situation?

**Step 4: Document the incident**

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

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

Write your answer in the second part of the worksheet.

**What to include in your answer**

Make sure you meet the following criteria in your completed activity:

* One to three network protection tools and methods.
* The reasons why the selected tools and methods are effective

**Example Completed**

File "*Exemplary Security risk assessment report*"

**Example Evaluation**

Compare the copy with your completed activity. Proofread your work using each of the criteria in the issue. What did you do well? Where can you improve? Use your answers to these questions to guide you as you progress through the course.

**Note**: The example represents a possible explanation for the problems facing the social media organization. There are several correct security reinforcement tools and methods to use. What's important is that you've identified the most effective network hardening measures to manage the selected vulnerabilities. In your role as a security analyst, you and your team would explain your decisions and argue why these measures will be effective in securing the network.

The example focuses on the vulnerability of outdated software to a local database. A potential solution to the vulnerability is identified and included in the report to the direct supervisors. The report explains how the company could be compromised in the future if the database is not patched and if employees continue to share passwords.

In the section on the organization's information security policy, the report includes information on the addition of general security enforcement practices, a recommendation on how often enforcement practices should be executed, and an explanation of what the potential consequences are if the policy is not followed. This is an example of how a security risk assessment report can be analyzed and how an information security policy can be written.