To pass this course item, you must receive 100%, or 1 out of 1 point, by completing the following activity. You can learn more about graded and practice items in the course overview.

Activity Overview

In this activity, you will be presented with a scenario about a social media organization that recently experienced a major data breach caused by undetected vulnerabilities. To address the breach, you will identify some common network hardening tools that can be implemented to protect the organization’s overall security. Then, you will select a specific vulnerability that the company has and propose different network hardening methods. Finally, you will explain how the methods and tools you chose will be effective for managing the vulnerability and how they will prevent potential breaches in the future.

In the course, you learned network hardening and network security-related hardening practices, such as port filtering, network access privileges, and encryption over networks. Network hardening practices help organizations monitor potential threats and attacks on their network and prevent some attacks from occurring. Some hardening practices are implemented every day, while others are executed every once in a while, such as every other week or once a month. Understanding how to use network hardening tools and methods will help you better monitor network activity and protect your organization’s network against various attacks.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

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:

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-By-Step Instructions

Follow the instructions and answer the following question to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

To use the template for this course item, click the following link and select *Use Template*.

Link to template: Security risk assessment report

OR

If you don’t have a Google account, you can download the template directly from the attachment below.

Security risk assessment report
DOCX File

Step 2: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

To use the supporting materials for this course item, click the following link and select *Use Template*.

Link to supporting materials: Network hardening tools

OR

If you don’t have a Google account, you can download the supporting materials directly from the following attachment.

Network hardening tools
XLSX File

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.

Pro Tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

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.