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.

Part 1: Select up to three hardening tools and methods to implement

1. Enforcing Strong Password Policies and Multi_factor Authentication(MFA)
   a. Require employees to use strong and unique passawords.
   b. Implement multi-factor authentication (MFA) for all sensitive accounts to add an extra layer of security
2. Implementing Firewall Rules and Traffic Filtering
   a. Configure firewalls with strict rules to filter inbound and outbound network traffic
   b. Utilize Intrusion Detection and Prevention Sysrems (IDPS) to monitor for suspicious activity.
3. Changing Default Credentials and Implementing Role-based Acess Control (RBAC)
   a. Ensure all deafult passwords, especially for admin accounts and databases, are changed immediately.
   b. Implement RBAC to restrict acess based on user roles, ensuring emplyees only have acess to the resouces necessary for their job.

Part 2: Explanation of Recommendations

1. *Enforcing Strong Password Policies and Multi factor Authentication(MFA)*
    a. Emplyees sharing passwors is a major security risk. By enforcing unique, complex passwords and requiring periodic updates, we can reduce the likelihood of unauthorized acess.
    b. MFA ensures that even if a password is compromised, attackers woulds still need an additional authentication factor to gain acess.
2. *Implementing Firewall Rules and Traffic Filtering*
    a. The absence of firewall rules makes the organization vulnerable to unauthorized access and data exfiltration.
    b. Firewalls will be configures to allow only necessary traffic while blocking known malicious Ip adresses.
    c. IDPS will be used to detect and responde to potential threats in real time, further strengthening network sexurity.
3. *Changing Default Credentials and Implementing Role-based Acess Control (RBAC)*
    a. Default credentials are easy targets for attacker. Changing these immediatelly will eliminate this vulnerabilities.
    b. RBAC ensures that users have the minimum level of acces necessary, reducing the potential damage if an account is compromised.