# Preview

This is a exercise to ensure i learned network hardening and network security-related hardening practices

The scenario:

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.

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Security risk assessment report

|  |  |
| --- | --- |
| **Part 1: Select up to three hardening tools and methods to implement** | |
| 1. Implement better password policies 2. Set a port filtering through a firewall 3. Set a Multi-Factor Authentication | |

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. All company employers have shared passwords. This can lead to internal threats. It will be hard to find out who leaked a data. Also, password sharing violates compliance best pratices and can lead to fines. Along with that, using a default admin password can lead to a successful brute force or dictionary attack.   The first solution to hardening the security is that a strong password policy should be implemented, with individual password, great password length, uppercase & lowercase, numbers and special characters. A password management system can also ensure protect the company from data breaches.   1. The company don’t have a firewall. This may lead to attacks like a DDoS or DoS. A firewall is a hardware or software that set previously rules to filter authorized IP or PORT coming in or out network traffic. 2. The company don’t have a 2FA or MFA. Even if a password is compromised, 2FA or MFA can ensure that the person accessing is an authorized person, ensuring at least a second authentication |

* Why is the recommended security hardening technique effective?

Its effective because decrease the company vulnerabilties. The attack surface will decrease, making it harder for internal or external threats.

* How often does the hardening technique need to be implemented?

A password policy is implemented once. Firewall maintenance should happen regularly. Network administrators should

ensure that firewall rules are in place that reflect the most up to date standards

for allowed and denied traffic. Traffic from sources that are suspicious should be

placed on a denied traffic list. Firewall rules should be updated whenever a

security event occurs.