(Mock) Network Security Risk Assessment

A computer network with a shield and icons

Description automatically generated

Material & instructions developed by: Google Cybersecurity Professional Certificate Course

Completed by: Alexander Herman on 01/17/24

**Table of Contents:**

Activity Overview (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Scenario (Provided): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**2**

Security Risk Assessment (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3**

Hardening Recommendations (My Work): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**3**

**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.

**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**

After a recent security review of the organization’s network security posture, several major vulnerabilities were discovered that could have been the exploit(s) used in the recent data breach. The first one being that employees are sharing passwords. Not only does this show that the confidentiality of the company’s data faces major risk, but so does the integrity as employees could potentially have accessed each other’s online accounts. Continuing with password vulnerabilities, the admin password for the company database is set to the default. These are two major vulnerabilities that should not have existed in the first place and can be hardened with little to no cost. Thirdly, the weak password policy is not protected by any sort of MFA or 2FA to verify the identity of end users trying to access the company’s digital assets. Finally, although firewalls are being utilized, they are essentially useless as they have not been properly configured to filter specific inbound and outbound traffic. Overall, there is a high level of risk from threat actors, inside threats, and regulatory agencies that could impose fines for non-compliance.

**Hardening Recommendations**

**Administrative Recommendations:**

* Fire the security leader at the company as there has been a complete lack of duty to protect the company’s assets and stakeholders
* Implement a strong password policy, UAP policy, & BYOD policy (if applicable)
* Implement company-wide security awareness training
* Implement regular security audits to identify new vulnerabilities and promote continuous security posture improvement
* Review industry specific compliance regulations and ensure compliance

**Technical Recommendations**

* Properly configure firewall filtering rules to limit access only to strictly necessary ports
* Deploy network monitoring tools/processes to proactively scan for suspicious or unusual activity
* Deploy MFA or 2FA method for at least admin accounts but should deploy for all employees
* Ensure data is encrypted in transit & at rest
* Establish user access controls for applications, network access, and databases using law of least privilege
* Ensure applications, operating systems, & security devices are up to date and regularly checked