Security Risk Assessment Report

Analysis of Network Hardening

Wendy Alayon
16/06/2024 **@syszern**

Table of Contents

Security risk assessment report

Scenario

A security analyst working for a social media organization recently encountered a major data breach that compromised the safety of their customers' personal information, such as names and addresses. The organization is seeking to implement strong network hardening practices that can be performed consistently to prevent future attacks and breaches.

After inspecting the organization's network, the security analyst discovered 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, the security analyst will write a security risk assessment to analyze the incident and explain the methods that can be used to further secure the network.

Three Hardening Tools and Methods for Implementation

Three network hardening tools and methods the organization can implement to address the vulnerabilities found:

1) Password policies
   - Password policies refer to a set of rules and guidelines that dictate how passwords should be created, used, and managed within an organization or system.
   - These policies typically include requirements such as minimum length, complexity (use of uppercase letters, numbers, special characters), expiration

periods (how often passwords must be changed), and prohibitions against reuse of recent passwords.

2) Firewall maintenance
    - Firewall maintenance involves the regular upkeep, monitoring, and management of firewall systems.
    - Maintenance tasks may include updating firewall rules to reflect changes in network architecture, applying software patches and updates to firewall software to protect against vulnerabilities, monitoring firewall logs for suspicious activity, and conducting periodic audits to ensure the firewall configuration remains effective and secure.

3) Multifactor authentication (MFA)
    - Multifactor authentication (MFA) requires more than one method of authentication from independent categories of credentials to verify the user's identity.

Explanation of Recommendations

Enforcing strict password policies discourage password sharing. It requires strong, unique passwords for each user, and regularly rotates passwords to minimize the likelihood passwords being shared or reused. Implementing policies also prohibit the use of default passwords and enforce password complexity requirements (e.g., minimum length, use of special characters). By setting strong password practices and regularly updating policies, the organization can significantly strengthen their defense against malicious actors attempting to exploit password vulnerabilities.

Firewall maintenance should be done regularly to review and update firewall rules and ensure they effectively filter incoming and outgoing traffic based on organizational policies and security requirements. Firewalls act as a barrier between a trusted internal network and untrusted external networks (like the internet). They control incoming and outgoing network traffic based on predefined security rules. Regular maintenance ensures these rules are up to date and effectively enforced, preventing unauthorized access attempts. Properly configured firewalls also defend against various forms of malicious traffic, including malware, viruses, and brute-force attacks. To maintain robust protection, maintenance activities involve updating firewall rules with new threat signatures and patterns. This proactive approach enhances the network's ability to withstand emerging threats.

Implementing multifactor authentication (MFA) adds an additional layer of security beyond passwords. Even if employees share passwords, an attacker would still need the second factor (e.g., a code sent to a mobile device) to gain access, reducing the impact of shared passwords. It significantly reduces the risk of unauthorized access and protects against various forms of malicious activities by requiring multiple forms of verification. Combining MFA with strong password policies and other security measures forms a robust defense against evolving cyber threats.