Security Risk Assessment Report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Based on the identified vulnerabilities, the following three hardening tools and methods are recommended for the organization:  **Multifactor authentication (MFA)**  MFA is a recommended tool for securing the network and preventing unauthorized access. A user must verify their identity using two or more methods, such as a password and a fingerprint, before accessing the system or network. This will prevent attackers from gaining access to the network even if they have obtained the user's password. MFA can be implemented once and then maintained to ensure continued security.  **Firewall maintenance and rules configuration**  Firewalls are the first line of defense for networks and are used to block unauthorized network traffic. Firewall maintenance involves checking and updating security configurations regularly to stay ahead of potential threats. The firewall rules can be updated in response to an event that allows abnormal network traffic into the network. In addition, the firewalls should have regulations to filter traffic coming in and out of the network, which is currently a vulnerability in the organization. Port filtering can be implemented as part of this measure to block or allow certain port numbers and limit unwanted communication.  **Password policies**  The organization should implement password policies recommended by the National Institute of Standards and Technology (NIST) to prevent attackers from easily guessing user passwords. The latest NIST recommendations focus on using methods to salt and hash passwords rather than requiring overly complex passwords or enforcing frequent changes to passwords. Password policies are used to prevent brute-force attacks and can be implemented and maintained consistently to ensure continued security.  Overall, these three hardening tools and methods will significantly improve the security of the organization's network by preventing unauthorized access and reducing the risk of network attacks and data breaches. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Multifactor authentication (MFA) is a security measure that requires users to verify their identity in two or more ways to access a system or network. It can help protect against brute force attacks and other similar security events. In this case, I recommended implementing MFA as a way to address the vulnerability of employees sharing passwords. Requiring multiple factors for authentication makes it much more difficult for an attacker to gain access to the network even if they do obtain a password. MFA can be set up once and then maintained.  Firewall maintenance and rules configuration involves regularly checking and updating security configurations to avoid potential threats. This can be done regularly, but rules can also be updated in response to an event that allows abnormal network traffic into the network. In this case, I recommended implementing firewall rules to filter traffic coming in and out of the network as a way to address the vulnerability of the firewalls not having any rules in place. Setting up rules limiting traffic passing through the network can help prevent potential attacks.  Lastly, regarding password policies, I recommended implementing the latest recommendations from the National Institute of Standards and Technology (NIST) for password policies. The latest recommendations focus on using methods to hash passwords rather than requiring overly complex passwords or enforcing frequent changes to passwords. Password policies are used to prevent attackers from quickly guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack). Implementing strong password policies makes it much more difficult for an attacker to gain access to the network using compromised passwords.  The recommended security hardening techniques are effective in enhancing the security of the system in several ways:  Multifactor authentication (MFA) requires multiple pieces of evidence to authenticate a user, such as a password and a code sent to a mobile device. This makes it much more difficult for attackers to gain access to sensitive information, even if they manage to obtain the user's password.  Firewall maintenance and rules configuration help ensure that only authorized network traffic can enter or leave the system. This can prevent attackers from exploiting vulnerabilities in the network to gain access to the system or to exfiltrate data.  Password policies can help to ensure that users choose strong passwords and change them frequently, reducing the risk of password-based attacks.  How often these techniques need to be implemented depends on the system's specific circumstances and the organization that owns it. Generally, MFA and firewall rules should be reviewed and updated regularly to ensure they are still effective against new threats and vulnerabilities. Password policies should also be reviewed periodically to ensure that they remain effective and relevant. It is also important to promptly implement security patches and updates to address any newly discovered vulnerabilities. |