Security risk assessment report: Analysis of Network Hardening

Prepared By: Dhyanam
Role: Cyber Security Student (Learning)
Year: 2026

Part 1: Select up to three hardening tools and methods to implement
After inspecting the organization's network, we 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. To address these vulnerabilities organization needs to implement following security hardening tools and methods: 1. Strong Password Policies 2. Firewall Maintenance 3. Multi-Factor Authentication (MFA)

Part 2: Explain your recommendations
This section of the report explains how implementing these Security Hardening Methods will help the organization to address the security vulnerabilities: 1. Strong Password Policies: Organizations use Password Policies to standardize good password practices throughout the business. Policies such as suspending the account after a certain number of logins can

prevent successful Brute Force Attacks. Policies that stop the organization from having default passwords for the admin accounts. Increasing password complexity, requiring more frequent password updates and not allowing passwords from getting reused also helps to stop malicious actors from infiltrating the network. This method is set once and then maintained.

2. Firewall Maintenance: This method ensures checking and updating security configurations regularly to stay ahead of the potential threats. This needs to be done regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.
3. Multi-Factor Authentication (MFA): A security measure which requires a user to verify their identity in two or more ways to access the system or network. MFA options include a password, a pin number, badge, One Time Password (OTP), sent to a cell phone, fingerprint and more. This method is set once and then maintained. This will reduce the organization's employees from sharing their passwords. Now the recipient of the shared password now need to have additional authentication besides a password, MFA makes it less useful to share passwords, therefore making passwords less likely to be shared.