# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| **This report outlines key network hardening techniques to address identified vulnerabilities and strengthen the organization’s overall security posture**  **Multifactor Authentication (MFA**): Implementing MFA enhances authentication and ensures that only verified users can access sensitive systems, reducing the risk of credential-based attacks.   1. **Firewall Maintenance**: Applying Firewall maintenance would help keep the organization safe from potential attacks by filtering incoming and outgoing traffic and blocking unpermitted traffic. This ensures only the allowed data and packets are entering the network and are also exiting the network, putting the organization and staff at safety. 2. **Password policies** Enforcing a password policy would help the organization understand the proper rulings on how to maintain passwords, this would help keep confidentiality, ensuring that the organization is not doing things like sharing passwords, and also making sure password updates are conducted regularly, minimizing the risk of a potential attack. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| 1. **MFA** should be implemented to require users to verify their Identity in two or more ways to have access to the network. MFA options include password pin number, badge, one-time password (OTP) sent to a cellphone, fingerprint, and more. This can help protect against brute force attacks and similar security events. MFA can be implemented at any time and is mostly a technique that is set up once then maintained. 2. **Firewall Maintenance** should be used for checking and updating security configurations regularly to stay ahead of potential threats. This can happen 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. The National Institute of Standards and Technology (NIST) latest recommendations for **password policies** focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. Password policies can be used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).  * **enforcing unique passwords per employee.** * **Storing passwords using salted hashes.** * **Using minimum length and complexity standards (e.g., 12+ characters, mix of character types).** |