Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. **Multifactor authentication (MFA)** 2. **Password policies** 3. **Firewall maintenance**

Part 2: Explain your recommendations
1. **Multifactor Authentication (MFA)** MFA is a one-time setup that requires ongoing enforcement. It is effective because it adds an additional layer of security beyond just a password. By requiring extra verification factors (e.g., phone app code, security key, fingerprint), it makes stolen, guessed, or shared passwords largely useless on their own. 2. **Password Policies** Password policies are effective because they enforce strong, unique, and non-default credentials. While policies are established once, they need to be updated and reviewed regularly to remain effective. This includes forcing password changes when defaults are detected and conducting periodic policy reviews or updates in line with industry standards. 3. **Firewall Maintenance** Regular firewall maintenance ensures that traffic filtering rules are properly configured to block suspicious or unnecessary inbound and outbound connections. This reduces the attack surface and directly addresses the issue of having no filtering rules in place, which otherwise allows unrestricted access. Maintenance must be performed regularly, including reviewing logs, analyzing rule effectiveness, updating rules for new applications or services, patching firewall firmware or OS, and responding to newly discovered attack methods.