Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

Three hardening tools and methods the organization can use to fix vulnerabilities are the following:

1. Setting up password policies
2. Implementing Multifactor authentication(MFA)
3. Setting up port filtering

Part 2: Explain your recommendations

The first hardening tool/method to implement is creating password policies. This will prevent attackers from easily guessing or brute forcing passwords. This would include changing passwords for default systems and using separate passwords for everything.

After this has been done setting up Multifactor authentication (MFA) would be a good next step in reducing the risk of compromised users. MFA requires users to verify their identity in two or more ways in order to access a system. This includes biometrics, a one-time password (OTP), a pin, a password, etc.. This reduces the risk of unauthorized users from accessing systems because if they gain access to the password the chances of compromising the MFA are slim.

Lastly setting up port filtering rules for the network firewall will provide a first line of defense for unwanted communication from potential attackers. Being able to control network traffic and stop attackers from accessing private networks is an important first step.