Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
- Multi-Factor Authentication: A security measure that requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, PIN, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. - Password policies: The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focus on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords. - Firewall maintenance: Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats.

Part 2: Explain your recommendations
Since much of the network was insecure through, shared passwords of employees, using the default password, no one used MFA, and the firewall was misconfigured led to a bunch of security flaws from the get-go. Being proactive about this will prevent any future attacks by implementing stronger and unique passwords for each user. Proper authentication and authorization. Make all users implement Multi-Factor authentication when signing in and updating the firewall so that it filters traffic in and out of the network.