Security risk assessment report

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

1. Firewall maintenance: The organization does not have the firewall rules to filter out traffic so the rules should be updated to prevent attacks such ip spoofing or DDoS attack.

2. MFA authentication should be used.

3. The NIST standard for passwords must be followed

Part 2: Explain your recommendations

Firewall maintenance is used to prevent the attacks by not allowing suspicious packets thereby protect the network from the threat actors.

MFA authentication means using two or more ways to authenticate the users. This is very useful because it prevents the loss of customer accounts even after the threat actor comprises the user‘s password by dictionary or brute force attack.

From the study of major vulnerabilities found the organization's employees are using default passwords and sharing their passwords. This should be prevented and employees must not share passwords nor have the default ones. The NIST recommends using salting and hashing the passwords of the users and the organization's employees. Hashing refers to the process of converting the plain text of the password into hash values, it is strong because the hashing is a time function and salting refers to adding random text into the hash values.