Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Firewall Maintenance 2. Password Policies 3. Penetration Test (Pen Test)

Part 2: Explain your recommendations
1. Firewall Maintenance: Based on the information provided, it was noted that the firewalls lack rules to filter traffic, rendering them essentially useless. This represents a fundamental flaw, and the implementation of proper rules is crucial as the first and most basic step in firewall management. 2. Password Policies: Not only are employees sharing passwords, but passwords are also not being changed from the default settings. It is evident that the establishment of robust password policies is necessary for the security of both employees and users. 3. Penetration Test (Pen Test): It is apparent that the company lacks knowledge of basic cybersecurity fundamentals. To address this, regular penetration testing is recommended to identify and address vulnerabilities. While specific recommendations for rules and methods can be provided, it is essential for the company to develop the capability to conduct pen tests independently, as external advice may not be continuously available.