Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The three hardening tools that the organization can use to address these vulnerabilities are: 1. Setting and enforcing strict password policies 2. Implementing multi-factor authentication 3. Performing regular firewall maintenance Password policies can be drawn up to include a length limit, acceptable list of characters and disclaimer to discourage password sharing. A control should also be placed in case of brute force attacks such as logging the number of password attempts, or the user losing access after a number of unsuccessful attempts. Multi-Factor Authentication (MFA) include the use of special identifying features such as biometrics, OTPs (One-Time Passwords), another code etc. This involves additional steps for a user logging in after entering their username and passwords. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. This can be done regularly or in response to a particular event that occurred due to firewall failures.

Part 2: Explain your recommendations
Since one of the major issues was the sharing of passwords by the organization's employees and the use of weak passwords—in this case, a default password for the administrator account—enforcing stricter password policies can make it significantly harder for malicious actors to gain access to the network. The use of stronger passwords and ensuring that the same password is not reused, as per the policies, reduces susceptibility to brute force attacks. Additionally, logging the number of login attempts and restricting access after a specific number of unsuccessful attempts provides an effective control measure in such scenarios. Multi-Factor Authentication (MFA) enhances network security by requiring additional authentication steps beyond just a password. Even if a malicious actor identifies a user's password through brute force attacks or other

methods, they will still be unable to access the network remotely due to the secondary authentication factors in place.

Firewall Maintenance should be conducted regularly. Network analysts must ensure that the firewall meets the highest standards for filtering and managing incoming traffic according to regulations. Traffic from suspected malicious sources should be blocked immediately and added to a denied traffic list. Firewall rules should also be updated in response to events that allow abnormal network traffic into the system. This measure can help protect the network from various DDoS attacks.