Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
In order for the social media company to protect itself from another breach, it should implement security hardening tools such as: - Using Port filtering - Implementing stronger password policies - Implementing MFA Port filtering requires the firewall to be set up to block or allow certain port numbers to limit unwanted communications. It can be used to disallow attackers from entering a private network. Implementing stronger password policies such as making sure the administrator doesn't use the default password will make the system less likely to be attacked by brute force. Implementing Multi Factor Authentication is an extra layer of defense that will require users to authenticate with another method on top of a password, this could be using a OTP sent to the user's phone or biometric information.

Part 2: Explain your recommendations
Enforcing multi-factor authentication (MFA) adds an additional layer of security beyond a password. It will reduce the likelihood that a malicious actor can access a network through a brute force. Creating and enforcing a password policy within the company will make it increasingly challenging for malicious actors to access the network. Increasing password complexity, requiring more frequent password updates, and not allowing passwords to be reused also help stall malicious actors from infiltrating the network. Network administrators should ensure that firewall rules are in place for allowed and denied traffic. Traffic from sources that are suspicious should be placed on a denied traffic list. Firewall rules should be updated whenever a security event occurs.