Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools the organization can use to address the security vulnerabilities found include: 1. Password Policies 2. Firewall maintenance 3. Multi factor authentication (MFA) Password policies can be created and refined to include requirements such as a minimum length, required characters and a disclaimer to discourage password sharing. This can also include rules around unsuccessful login attempts, such as locking an account after 5 unsuccessful attempts. Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. MFA requires users to give more than one way to identify themselves to access their account or application. MFA methods include ID cards, pin numbers, fingerprint scanners, one time passcodes (OTP) and more.

Part 2: Explain your recommendations
Having strong password policies can reduce the likelihood of a malicious actor gaining unauthorized access to accounts. The rules around password policies will need to be enforced regularly within the organization to increase user security. Firewall configurations should be implemented to disable any unused ports to prevent possible intrusions. Firewall maintenance should be performed regularly to check and update security configurations to stay ahead of potential threats and increase security posture. Firewall rules should be

updated whenever a security threat occurs, especially an event that allows unusual network traffic into the network. This measure can be used to protect against various DoS & DDoS attacks.

Multi Factor Authorization (MFA) should be implemented to reduce the likelihood that a malicious actor can access a network through brute force attack. It also makes it difficult for people within the organization to share passwords. Having MFA to identify and verify credentials is especially important among users with administrator level privileges. MFA should be enforced regularly