Security risk assessment report

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

To address the identified vulnerabilities, the following hardening tools and methods are recommended:

1. **Enforce Multi-Factor Authentication (MFA)**
   MFA requires users to verify their identity through at least two different methods, such as a password and a biometric scan, or a password and a one-time code sent to their phone.
2. **Adopt a Centralized Password Management System and Policy**
   Centralized tools can enforce password complexity, rotation schedules, and prevent password reuse. They also provide employees with secure ways to store and retrieve credentials.
3. **Configure and Monitor Firewalls with Traffic Filtering Rules**
   Setting up strong inbound and outbound filtering rules ensures that only authorized traffic can traverse the network. Regular monitoring and updating these rules are vital to addressing emerging threats.

Part 2: Explain your recommendation(s)

1. **Multi-Factor Authentication (MFA)**
   MFA significantly improves security by adding layers to the authentication process. Even if a password is compromised, attackers still need access to the second factor, such as a mobile device or biometric data. This practice directly addresses the issue of employees sharing passwords because a second factor ensures individual accountability.
2. **Password Management System**
   Centralized password management not only helps enforce strong policies but also reduces human error, like reusing or sharing weak passwords. For instance, employees will no longer need to remember complex passwords, as the system will securely manage them. By implementing this, the risk of credential-based attacks, such as brute force or credential stuffing, is minimized.

3. **Firewall Configuration and Monitoring**
   A properly configured firewall acts as the first line of defense against malicious traffic. By implementing rules that restrict unauthorized access and by monitoring traffic patterns regularly, the organization can identify and block suspicious activity early. These measures are crucial to preventing network-level attacks, such as malware infiltration and data exfiltration.