Security risk assessment report

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

1. Password Management Tools (e.g., LastPass or 1Password): These tools help store, generate, and manage complex and unique passwords for different applications and services, eliminating the need for employees to remember or share them. They provide encryption to secure stored passwords.

2. Network Intrusion Detection and Prevention System (NIDS/NIPS, e.g., Snort or Suricata): These systems monitor and analyze network traffic for malicious activity. They can block or alert about suspicious traffic patterns and are pivotal in adding a protective layer beyond just a firewall.

3. Multifactor Authentication (MFA) System (e.g., Duo Security or Google Authenticator): MFA requires users to provide two or more verification factors to gain access to a resource, such as an application, online account, or a VPN. This significantly reduces the risk of unauthorized access.

Part 2: Explain your recommendations

1. Implement a Strict Password Policy and Use Password Management Tools: Encourage employees to use password management tools to ensure that they have strong, unique passwords for every application and service they use. This eliminates the need to share passwords or write them down, reducing the risk of password-related breaches. Furthermore, enforce mandatory password changes periodically and educate employees about the dangers of sharing passwords. Recommendation: Introduce LastPass or 1Password to the employees. Conduct training sessions on how to utilize these tools and emphasize the importance of unique passwords for each service.

2. Establish Firewall Rules and Implement NIDS/NIPS: Without firewall rules, the organization's network is like an open door for malicious actors. Properly configured firewall rules will filter out unnecessary and potentially harmful traffic. Moreover, using Network Intrusion Detection and Prevention systems will further safeguard the network by detecting and preventing malicious activities in real-time.
   Recommendation: Set up a dedicated team to review and establish robust firewall rules tailored to the organization's needs. Invest in an NIDS/NIPS solution like Snort or Suricata to monitor the network's traffic continuously.

3. Implement Multifactor Authentication (MFA) Across All Critical Systems: Relying solely on passwords is a significant security risk. By adding an additional layer of authentication, the chances of unauthorized access diminish drastically, even if passwords are compromised. MFA is especially crucial for accessing critical systems, such as databases, admin panels, and employee accounts.
   Recommendation: Start by introducing MFA on the most critical systems like the admin panels and databases. Gradually, roll it out to cover all systems, including employee email and work accounts. Use tools like Duo Security or Google Authenticator to facilitate this.