# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Multifactor Authentication (MFA):  Implement MFA for all critical systems and user accounts.  Require users to provide multiple forms of verification before accessing sensitive data or systems.  MFA can prevent unauthorized access even if passwords are compromised.  Firewall Maintenance and Rule Configuration:  Regularly review and update firewall rules and configurations.  Configure firewalls to block unnecessary ports and traffic.  Implement intrusion detection and prevention systems (IDS/IPS) to monitor and respond to suspicious activities.  Password Policies:  Enforce strong password policies based on the latest recommendations.  Require unique, complex passwords with a combination of characters.  Implement methods to hash and salt passwords to enhance security.  These methods collectively address the vulnerabilities related to weak authentication, lack of firewall rules, and inadequate password practices. By implementing these measures, the organization can significantly enhance its network security and reduce the risk of future attacks and breaches. | |
|

| **Part 2: Explain your recommendations** |
| --- |
| Multifactor Authentication (MFA):  Implementing multifactor authentication (MFA) is a critical step to enhance the organization's network security. MFA requires users to provide multiple forms of verification before accessing sensitive systems or data. By combining something the user knows (like a password) with something they have (like a smartphone or hardware token), MFA adds an additional layer of security. This approach safeguards against attacks that rely solely on compromised passwords, such as brute force attacks. Even if an attacker obtains a user's password, they would still need the second factor to gain access, making unauthorized access significantly more challenging.  Firewall Maintenance and Rule Configuration:  Regularly reviewing and updating firewall rules and configurations is essential to prevent unauthorized access and protect the network from various threats. By configuring firewalls to block unnecessary ports and traffic, the organization can minimize the attack surface and reduce the risk of external threats. Intrusion detection and prevention systems (IDS/IPS) can actively monitor network traffic for suspicious activities and respond in real-time to potential threats, further strengthening the network's security posture.  Password Policies:  Enforcing strong password policies is crucial to safeguarding user accounts and preventing unauthorized access. By requiring users to create unique, complex passwords that incorporate a mix of characters, including uppercase, lowercase, numbers, and special symbols, the organization can significantly reduce the risk of brute force attacks. Hashing and salting passwords provide an added layer of protection, making it much more difficult for attackers to reverse-engineer passwords even if they gain access to the stored password hashes.  These recommendations directly address the vulnerabilities identified in the organization's network. The implementation of MFA ensures that compromised passwords alone cannot lead to unauthorized access. Regular firewall maintenance and configuration reduce the exposure of the network to potential threats by controlling incoming and outgoing traffic. Enforcing strong password policies, along with advanced hashing techniques, makes it significantly harder for attackers to gain unauthorized access through password-based attacks. Collectively, these measures will enhance the network's security posture, minimize vulnerabilities, and greatly reduce the risk of future data breaches and attacks. |