Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| * Password policies * Multifactor authentication (MFA) * Disabling unused ports   The National Institute of Standards and Technology's (NIST) latest recommendations for password policies focuses on using methods to salt and hash passwords, rather than requiring overly complex passwords or enforcing frequent changes to passwords.  A security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.  Ports can be blocked on firewalls, routers, servers, and more to prevent potentially dangerous network traffic from passing through.  A firewall function that blocks or allows certain port numbers to limit unwanted communication. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| It will become increasingly difficult for malicious actors to gain access to the network if the company establishes and enforces a password policy. To help improve user security, the password policy's rules will need to be regularly enforced within the organization.  By requiring multi-factor authentication (MFA), malicious actors will be less likely to use brute force or similar attacks to gain access to a network.Additionally, password sharing within the organization will be more difficult with MFA. Recognizing and confirming certifications is particularly basic among workers with director level honors on the organization. MFA ought to be  implemented consistently.  By disabling unused ports, we ensure that attackers' options are significantly reduced. |