Nicholas Coleman

Security risk assessment report

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

The client social media organization should immediately implement the following network hardening tools: strict password policies, principle of least privilege, port filtering, and multifactor authentication.

Part 2: Explain your recommendations

Following the NIST’s latest recommendations for password policies should be the default standard at the organization. Passwords should **never** be shared.

Furthermore, the admin password for the database should be unique, complex, and unknown to anyone without administrative privileges. The organization should be following the model of least privilege, which ensures that employees can only access information that is necessary for their job.

Thirdly, the firewalls should be configured to filter traffic coming in and out by disabling access for unused ports, more commonly known as port filtering. This will prevent malicious actors from gaining access to the client network from unused ports.

Lastly, multifactor authentication (MFA) should immediately be implemented as part of the organization’s security protocol. Enabling MFA allows for the organization to have more security, as a malicious actor would have to know more than just a username and password to log in to the target network.