Security risk assessment report

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

The three hardening tools and methods I would implement are as follows:

1. Routine Firewall Maintenance
2. Establishing and Enforcing Strong Password Policies
3. Requiring Multi-Factor Authentication (MFA)

Part 2: Explain your recommendations

Routine firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. This can happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DDoS attacks.

Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack). 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 relying on overly complex passwords.

Multi-Factor Authentication is a security measure which requires a user to verify their identity in two or more ways to access a system or network. Can help protect against brute force attacks and similar security events. MFA can be implemented at any time, and is mostly a technique that is set up once then regularly maintained.