Security risk assessment report

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

Three hardening tools that can be used to increase network security posture

- **Multi-Factor Authentication (MFA)**
- **Password Policies**
- **Port filtering**

Part 2: Explain your recommendations

Password Policies will require employees to create complex and unique passwords. By doing so, the likelihood of a brute force attack succeeding will be significantly reduced. Passwords that are both complex and unique provide a strong defense against unauthorized access attempts.

MFA serves as an extra layer of protection, ensuring that even if a malicious attacker acquires an employee's password, they would still need to provide additional verification. This additional layer works in conjunction with Password Policies to fortify the security of passwords, making it extremely difficult for an attacker to compromise critical employee accounts.

Port filtering helps address potential vulnerabilities in the company's firewall. It involves the blocking of ports that are not actively in use. This serves to limit unwanted communication, preventing potential attackers from gaining access to the company's private network. By controlling the ports that are open and accessible, the organization strengthens its defense against external threats and unauthorized intrusions.