Security risk assessment report

Part 1: Identify and list up to three hardening tools and methods to be implemented
Network Hardening Plan The organization recently experienced a major data breach that compromised the security of customers' personal information, including names and addresses. In response, the organization aims to implement robust and consistent network hardening practices to prevent future attacks and breaches. A review of the organization's network revealed four critical vulnerabilities: ● Employees share passwords. ● The database administrator account uses a default password. ● Firewalls lack rules to filter inbound and outbound traffic. ● Multi-factor authentication (MFA) is not implemented. If these vulnerabilities are not addressed, the organization remains at high risk for future data breaches and cyberattacks. To strengthen the network's security posture, the following three hardening tools and practices will be implemented: 1. **Password Policies** – Enforcing strong password policies will help prevent unauthorized access by reducing the risk of password guessing or brute-force attacks. 2. **Firewall Maintenance** – Regularly reviewing and updating firewall configurations will ensure that traffic is appropriately filtered, helping to block malicious access and protect against threats such as DDoS attacks. 3. **Multi-Factor Authentication (MFA)** – Implementing MFA will add an

additional layer of security by requiring users to verify their identity through multiple factors, making it more difficult for attackers to gain unauthorized access.

Part 2: Explanation of selected recommendations

1. **Password Policies**: In this organization, employees share passwords, and the database administrator account uses a default password. To reduce the risk of unauthorized access, password policies should be implemented. These policies will help prevent attackers from easily guessing user passwords—whether through manual attempts or automated scripts that test thousands of stolen credentials (a method commonly known as a brute-force attack).
   Frequency: Tasks should be performed regularly. The policies should be enforced periodically, and the strength of passwords should be reviewed regularly to ensure they meet current security standards.

2. **Firewall Maintenance**: Currently, the firewalls lack defined rules to filter incoming and outgoing network traffic. Proper firewall maintenance involves regularly reviewing and updating security configurations to address emerging threats. In addition to routine checks, firewall rules should be updated in response to specific events—such as incidents involving abnormal traffic patterns. This proactive approach helps protect the network against threats like Distributed Denial of Service (DDoS) attacks.
   Frequency: Tasks should be performed regularly to ensure the firewall remains effective in protecting the network, but should also be updated in response to specific events as needed.

3. **Multi-Factor Authentication (MFA)**: Multi-factor authentication is currently not in use. MFA is a security measure that requires users to verify their identity using two or more methods before accessing a system or network. These methods may include something the user knows (e.g., a password or PIN), something the user has (e.g., a badge or one-time password sent to a mobile device), or something the user has (e.g., a fingerprint). Implementing MFA significantly strengthens access controls and helps defend against brute-force attacks and other unauthorized access attempts. It can be deployed at any time and typically requires minimal ongoing maintenance once configured.
   Frequency: Tasks should be performed once when implementing

MFA, with minimal ongoing maintenance required unless configuration changes are needed.