## Incident Analysis:

The organization has recently suffered a major data breach, resulting in the compromise of customers' personal information, including names and addresses. To prevent future attacks and breaches, it is essential to identify and address four major vulnerabilities within the organization's network infrastructure.

| Part 1: Select up to three hardening tools and methods to implement |
| --- |
| Three hardening tools the organization can use to address the vulnerabilities found include:<br>1. Password Sharing Among Employees<br>2. Absence of Multifactor Authentication (MFA)<br>3. Lack of Firewall Rules<br><br>Employees within the organization share passwords, which poses a significant security risk. Password sharing weakens the confidentiality of accounts and increases the likelihood of unauthorized access. Also, the organization's database admin password remains set to the default. This exposes the database to potential exploitation, as default passwords are widely known and easily exploited by attackers.<br><br>Multifactor authentication (MFA) is not utilized within the organization. Without MFA, accounts are more susceptible to unauthorized access, particularly in the event of compromised credentials.<br><br>The firewalls in place lack defined rules to filter incoming and outgoing traffic. This lack of filtering allows potentially malicious traffic to enter and exit the network undetected, increasing the risk of intrusion. |

| Part 2: Explain your recommendation(s) |
| --- |
| Implement strict password policies that discourage sharing and require strong, unique passwords for each user. Immediately change the default admin password to a strong, unique one. Regularly update and strengthen all database credentials. Educate employees about the importance of password security.<br><br>Implement MFA for all user accounts, especially those with access to sensitive data. MFA provides an additional layer of security by requiring users to provide two or more forms of authentication.<br><br>Develop and enforce firewall rulesets that restrict traffic to only necessary ports and services. Implement Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor and block suspicious traffic. |