Activity Exemplar: Apply OS hardening techniques

Section 1: Identify the network vulnerabilities involved in the incident

The vulnerabilities involved in the incident are:

1. **Employees share passwords** – This increases the risk of unauthorized access and makes it difficult to track accountability.

2. **The admin password for the database is set to the default** – Default passwords are easy to guess or widely available, making it simple for attackers to gain access.

3. **Firewalls do not have rules in place to filter traffic** – Without firewall rules, malicious traffic can freely enter and leave the network.

4. **Multifactor authentication (MFA) is not used** – Without MFA, a compromised password can grant full access to sensitive systems.

Section 2: Document the incident

The organization recently experienced a major data breach, exposing customers' personal information, such as names and addresses. After investigating, it was found that weak security measures contributed to the breach.

- Employees frequently shared passwords, making unauthorized access easier.

- The database admin password was left as the default, allowing attackers to gain access easily.

- No firewall rules were in place to monitor incoming and outgoing network traffic, increasing the likelihood of external attacks.

- Multifactor authentication (MFA) was not implemented, meaning a compromised password could provide full system access.

The security analyst conducted a thorough audit and identified these vulnerabilities as the root causes of the breach.

Section 3: Recommend one or more remediations for the vulnerabilities

To prevent similar incidents, the following network hardening techniques should be implemented:

1. **Enforce Strong Password Policies:**
    - Require unique, complex passwords for each employee.
    - Prevent password sharing by enforcing individual user authentication.
    - Implement a password manager to help employees generate and store secure passwords.
2. **Change Default Credentials and Secure Administrative Accounts:**
    - Immediately change the admin password to a strong, randomly generated one.
    - Enforce role-based access control (RBAC) to restrict administrative privileges.
    - Regularly audit and update credentials to minimize risks.
3. **Implement and Configure Firewalls:**
    - Set up strict firewall rules to filter traffic entering and leaving the network.
    - Deploy intrusion detection and prevention systems (IDS/IPS) to monitor suspicious activity.
    - Regularly review and update firewall configurations to address new threats.
4. **Require Multifactor Authentication (MFA):**
    - Enable MFA for all user accounts, especially administrative ones.
    - Use one-time passcodes (OTPs) or security tokens as additional authentication factors.
    - Conduct regular employee training on MFA benefits and proper usage.

By implementing these security hardening techniques, the organization will significantly improve its cybersecurity posture and reduce the likelihood of future breaches.