Activity Analysis Network Hardening: Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers' personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.

After inspecting the organization's network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

1. The organization's employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multifactor authentication (MFA) is not used.

If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.

In this activity, you will write a security risk assessment to analyze the incident and explain what methods can be used to further secure the network.

Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Multifactor Authentication (MFA): Effectiveness: MFA is a highly effective security measure to implement in mitigating security threats because it adds an additional layer of authentication beyond the traditional username and password. It requires users to provide two or more forms of verification before granting access, making it significantly more challenging for unauthorized individuals to gain entry. **Mitigation Mechanisms:** Mitigating Password-Based Attacks: MFA mitigates the risk of password-based attacks, including brute force, credential stuffing, and phishing. Even if an attacker obtains or guesses a user's password, they would still need the second factor (e.g., a time-based code from a mobile app) to gain access. Protection for Privileged Accounts: For accounts with elevated privileges, such as administrators, MFA ensures that only authorized individuals can access sensitive systems or data. Remote Access Security: MFA is crucial for securing remote access to the network or sensitive resources, providing an additional layer of security for users connecting from external locations. **2. Firewall Maintenance:** Effectiveness: Firewalls are a fundamental security tool for controlling network traffic and preventing unauthorized access. Regular maintenance and proper configuration are essential for their effectiveness. **Mitigation Mechanisms:** **Traffic Filtering:** Firewalls filter incoming and outgoing network traffic based on predefined rules. Properly configured firewalls can block malicious traffic, such as known attack patterns, malware, and suspicious IP addresses. **Rule Updates:** Regularly updating firewall rules ensures that they reflect current network requirements and emerging threats. This adaptability helps in

staying ahead of new attack methods.

Intrusion Detection and Prevention: Advanced firewalls may include intrusion detection and prevention capabilities to identify and block unusual or malicious traffic patterns.

Segmentation: Firewalls enable network segmentation, separating sensitive resources from less secure areas. This containment strategy limits the impact of a breach.

3. Network Access Privileges:

Effectiveness: Controlling network access privileges is crucial for reducing the attack surface and ensuring that users and devices only have access to resources necessary for their roles.

Mitigation Mechanisms:

Least Privilege Principle: Implement the principle of least privilege, where users and devices are granted only the minimum access rights needed to perform their tasks. This reduces the risk of unauthorized access to sensitive data or systems.

Role-Based Access Control (RBAC): RBAC assigns permissions based on job roles, ensuring that individuals have access to resources aligned with their responsibilities.

Regular Access Reviews: Conduct regular access reviews to revoke unnecessary permissions and privileges, especially for accounts that are no longer in use or for employees who have changed roles.

Account Monitoring: Continuously monitor user and device activities to detect and respond to suspicious behavior or unauthorized access attempts.

By implementing these hardening tools, an organization can significantly enhance its security posture and reduce the likelihood of data breaches and security incidents. These measures collectively create multiple barriers and layers of defense, making it more challenging for attackers to exploit vulnerabilities and gain unauthorized access to critical resources.

Part 2: Explain your recommendations

To bolster cybersecurity for a social media company, three critical strategies are recommended. First, implementing Multifactor Authentication (MFA) is essential to protect user and customer accounts. MFA requires users to provide two or more forms of verification, adding a robust layer of security. It should be enforced for all users, especially privileged accounts and API access. Additionally, secure account recovery procedures and real-time monitoring of MFA events are vital components of this strategy.

Second, Firewall Maintenance is crucial for controlling network traffic and shielding internal systems from external threats. This involves configuring firewalls to filter both incoming and outgoing traffic, regularly updating rules to adapt to emerging threats, and considering intrusion detection/prevention and web application firewalls. Network segmentation should also be implemented to isolate sensitive data and systems.

Lastly, controlling Network Access Privileges plays a pivotal role in limiting exposure and potential attacks. The principle of least privilege should be applied rigorously, granting users and employees only the access required for their roles. Role-Based Access Control (RBAC), regular access reviews, continuous account monitoring, and Privileged Access Management (PAM) are key elements of this strategy. Together, these recommendations create a multi-layered defense to safeguard user data, internal systems, and critical assets from unauthorized access and cyber threats, reinforcing the cybersecurity posture of the social media company.