Justin Goncalves

7/23/24

Project: Apply OS Hardening Techniques

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.

Network Hardening Tools: Network hardening tools

Follow the instructions and answer the questions below to complete the activity.

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

Given the vulnerabilities identified in the scenario and the goal of preventing future attacks, the following three hardening tools and methods would be most effective:

1. **Multifactor Authentication (MFA):**
   - **Description:** MFA requires users to verify their identity using two or more methods, such as a password and a one-time code sent to a phone or an authentication app.
   - **Effectiveness:** Implementing MFA significantly enhances security by adding an additional layer of verification. Even if an attacker obtains the password, they would still need the second factor to gain access, which is often more challenging to

compromise. This would directly address the vulnerability related to the lack of MFA and protect against unauthorized access.

2. **Strong Password Policies:**
   - **Description:** Enforce the use of complex, unique passwords and prohibit password sharing. Implement policies requiring regular password changes and the use of password managers.
   - **Effectiveness:** Strong password policies reduce the risk of password-related vulnerabilities, such as default passwords and password sharing among employees. By ensuring that all passwords are unique and complex, it becomes much harder for attackers to guess or crack them through brute force methods.
3. **Firewall Maintenance and Configuration:**
   - **Description:** Regularly update and configure firewall rules to filter traffic entering and leaving the network. Implement intrusion detection and prevention systems (IDPS) to monitor and block malicious traffic.
   - **Effectiveness:** Properly maintained and configured firewalls can prevent unauthorized access and block malicious traffic before it reaches the network. This addresses the vulnerability of having no traffic filtering rules in place, thereby significantly reducing the risk of data breaches and other network attacks.

These three methods collectively enhance the organization's security posture by addressing critical vulnerabilities related to authentication, password management, and network traffic filtering. Implementing these measures will help prevent unauthorized access, reduce the risk of brute force attacks, and ensure that only legitimate traffic can enter and exit the network.

Part 2: Explain your recommendations

1. Multifactor Authentication (MFA)
Effectiveness: Multifactor Authentication (MFA) is highly effective in mitigating the risk of unauthorized access because it requires multiple forms of verification. Even if an attacker successfully guesses or steals a password, they would still need the additional authentication factor (e.g., a one-time code sent to the user's phone or biometric verification) to gain access. This layered approach significantly reduces the likelihood of successful breaches due to compromised credentials.

Implementation Frequency: MFA is generally implemented as a one-time setup for each user, followed by regular maintenance and monitoring. Users might need to re-authenticate periodically or when accessing the network from new devices. Continuous monitoring and periodic reviews are essential to ensure the effectiveness of MFA.

2. Strong Password Policies
Effectiveness: Implementing strong password policies is crucial for ensuring that passwords are not easily guessable or crackable. Enforcing the use of complex passwords, regular password changes, and the prohibition of password sharing ensures that each user's credentials are unique and secure. This method effectively addresses the vulnerabilities related to default passwords and shared passwords among employees.

Implementation Frequency: Password policies should be enforced continuously, with users required to update their passwords at regular intervals (e.g., every 60-90 days). Regular audits and compliance checks are necessary to ensure adherence to the policies and to educate users on best practices for password security.

3. Firewall Maintenance and Configuration
Effectiveness: Firewalls serve as the first line of defense against external threats by filtering incoming and outgoing traffic based on predefined security rules. Regular maintenance and updating of firewall rules help protect the network from unauthorized access and malicious traffic. Implementing Intrusion Detection and Prevention Systems (IDPS) alongside firewalls enhances security by monitoring traffic for suspicious activities and blocking potential threats in real-time.

Implementation Frequency: Firewall rules and configurations should be reviewed and updated regularly, at least monthly, or immediately in response to specific security events. Continuous monitoring is essential, with periodic audits to ensure that the firewall settings align with the latest security best practices and the evolving threat landscape.

Summary: By implementing MFA, strong password policies, and regular firewall maintenance, the organization can significantly enhance its security posture. These measures address critical vulnerabilities, making it harder for attackers to gain unauthorized access and ensuring that network traffic is tightly controlled and monitored. Regular implementation and maintenance of these hardening techniques are vital for sustained network security and resilience against potential breaches.