5/1/2024

Abby Gopal

Operating Systems

CIS 411

At Artistry Logo Design Co., our priority is to ensure the safe and secure management of passwords by groups on our Linux systems, as outlined in Audit Step 13.

Procedures:

1. Identify Linux Systems:

* Example: Utilize a spreadsheet maintained by the IT department that lists all hardware assets, including hostname, operating system, and location. This spreadsheet can be filtered to identify all Linux machines (e.g., those with Ubuntu or CentOS in the OS column).
* Alternatively, if Artistry employs a network discovery tool like Open-AudIT, it can scan the network and automatically generate a list of active Linux devices.

1. Check for Shadow Password Files:

* Example: Login to a specific Linux system, say the design server named "nyc-design1" with root privileges.
* Use the ls -l /etc/shadow command to view file permissions.
  + - Expected Result: The output should display “-rw-------" permissions, indicating only the root can read and write to the shadow file. This restricts unauthorized access to password hashes.

1. Analyze Shadow Password Files (if accessible):

* Warning: The shadow command exposes password hashes, so use it cautiously and only if necessary.
* Analyze the output for lines beginning with "g:". These represent group entries.
  + - Example: If a line like g: designers:!:10000:0:99999:7::: is found, it indicates the presence of a group named "designers" with a password hash. This is a security risk.
    - Expected Result: Ideally, no group entries with passwords should be present.

1. Review Group Permissions:

* Example: Use the getent group command to list all groups on the system.
* Analyze entries for groups with special privileges, such as the "sudo" group that allows administrative tasks.
* Use the id username command to check group membership for users with elevated privileges. For instance, id logoadmin might reveal membership in the "sudo" group.
  + - Expected Result: Users with elevated privileges should belong to specific groups granting those permissions. Group passwords should not be used for authorization.

Validation:

* The absence of group entries with passwords in the shadow file indicates a secure configuration.
* User privileges should be managed through group memberships and the sudoers file, not group passwords.
* If group passwords are identified, further investigation is necessary to understand their purpose and potential security risks.

Reporting:

* Document the audit findings, including the number of Linux systems reviewed (e.g., 50 design workstations across all offices) and any instances of group passwords encountered (e.g., a group password identified on the "NYC-design1" server).
* Recommend the removal of group passwords and suggest alternative methods for managing user privileges (e.g., sudo groups).

Recommendations**:**

* Disable any existing group passwords identified during the audit.
* Implement role-based access control (RBAC) to assign permissions based on user roles (e.g., designer, project manager, IT admin).
  + Example: Designers might be assigned a group allowing access to design software and project folders, while IT admins would have a separate group with broader system access.
* Utilize the sudoers file to grant specific users elevated privileges for defined commands. For instance, a "logoadmin" user might require sudo access to install design software updates.
* Educate users on secure password practices and avoiding shared group passwords. Conduct security awareness training highlighting the risks of weak passwords and the benefits of multi-factor authentication.

Strong passwords are the cornerstone of any secure system, and at Artistry Logo Design Co., we take this principle seriously. Building upon the foundation laid in Audit Step 9, we're committed to fortifying password security on our Windows servers.

Procedures:

Review Active Directory Password Policy:

* An IT admin logs in to a domain controller in the New York office with local administrator privileges.
* They access the Group Policy Management Console (GPMC) and navigate to the policy applied to the file servers located across all offices.
* Upon reviewing the "Password Policy" settings, they discover the following:
* Minimum password length: 8 characters (not meeting the recommended minimum of 12 characters).
* Require digits, lowercase characters, and uppercase characters: Enabled (positive finding).
* Require special characters: Disabled (increases password guess ability).
* Password history length: 10 passwords (too short, allowing potential password reuse).
* Maximum password age: Not configured (passwords never expire, a security risk).
* Account lockout duration: 10 minutes (reasonable for allowing recovery from accidental lockouts).
* Account lockout threshold: 3 failed login attempts (a low threshold might hinder legitimate users) (Davis et al., 2020).

Validation:

Verify Password Policy Enforcement:

* The IT admin creates a test user account named "design\_test" and attempts to set a weak password like "ArtLogo123!" (8 characters, meeting some but not all complexity requirements).
* The attempt to set the password fails, and an error message pops up, indicating the password doesn't meet the minimum complexity requirements defined in the policy (positive finding).

Review Password Filter (Optional):

In this example, let's assume a password filter is not configured. However, implementing a filter to prevent dictionary words and usernames as passwords would be a recommended security improvement.

Expected Results:

The reviewed Group Policy settings have some positive aspects (complexity requirements enforced) but fall short in other areas (minimum length, password expiration). The password policy enforcement test confirms that weak passwords are rejected.

Reporting:

* The IT admin documents the audit findings, highlighting the need to:
* Increase the minimum password length to 12 characters.
* Enable the requirement for special characters.
* Configure a reasonable maximum password age (e.g., 90 days).
* They recommend implementing a password filter to strengthen password security further.

Recommendations:

* The Artistry Logo Design Co. IT team should adjust the Group Policy settings to enforce the recommended password security practices.
* Implementing multi-factor authentication (MFA) for critical server access would be an additional security measure to consider.
* Regularly reviewing and updating password policies is crucial to stay ahead of evolving cyber threats.
* This example demonstrates how the audit steps can be applied in a practical scenario to identify areas for improvement in password security on Windows servers. By implementing these recommendations, Artistry Logo Design Co. can significantly enhance the security of its IT infrastructure and safeguard sensitive data.

References:

Davis, C., Wheeler, K., & Schiller, M. (Eds.). (2020). *IT Auditing Using Controls to Protect Information Assets, Third Edition*. <https://platform.virdocs.com/read/1290420/206/#/4/4/2>