From: Akshatha K

Security Analyst

TASK 1:

As a security analyst, you have to review the documents published by PCI DSS, NIST, and CIS for password guidelines and determine the recommendations for the following policy. Use **NA** (Not Applicable) if the policy is not explicitly mentioned.

Policy	**NIST Recommendations**	**CIS Recommendation**	**PCI DSS Recommendation**
Minimum password length	5.1.1: At least 8 characters; longer is better	5.1.1: 8 characters for MFA accounts, 14 characters for password-only accounts	8.2.3: At least 7 characters
Password history (number)	5.1.2: Not applicable	5.1.2: Remember last 24 passwords	8.3.1: Remember last 4 passwords
Complexity (Enabled/Disabled)	5.1.1: Disable complexity requirements	5.1.1: Enable, Require a mix of uppercase letters, lowercase letters, digits, and special characters	8.2.3: Enable, Require a mix of uppercase letters, lowercase letters, digits, and special characters
Password expiration (days)	5.1.1: No expiration unless evidence of compromise	5.1.1: At least every 60 days	8.2.4: At least every 90 days
Minimum password age (days)	Not applicable	Not explicitly specified	Not explicitly specified
Session idle time-out (mins)	5.1.3: Not specified	Not explicitly specified	Not explicitly specified
Suspend/remove/disable inactive user accounts (days)	5.1.2: Not specified	5.1.2: Within 30 days for inactive accounts	8.1.3: Within 90 days for inactive accounts

Limit failed login attempts by locking out the user (attempts)	5.1.3: Implement only if evidence of attack	5.1.3: 6 attempts	8.1.6: 6 attempts

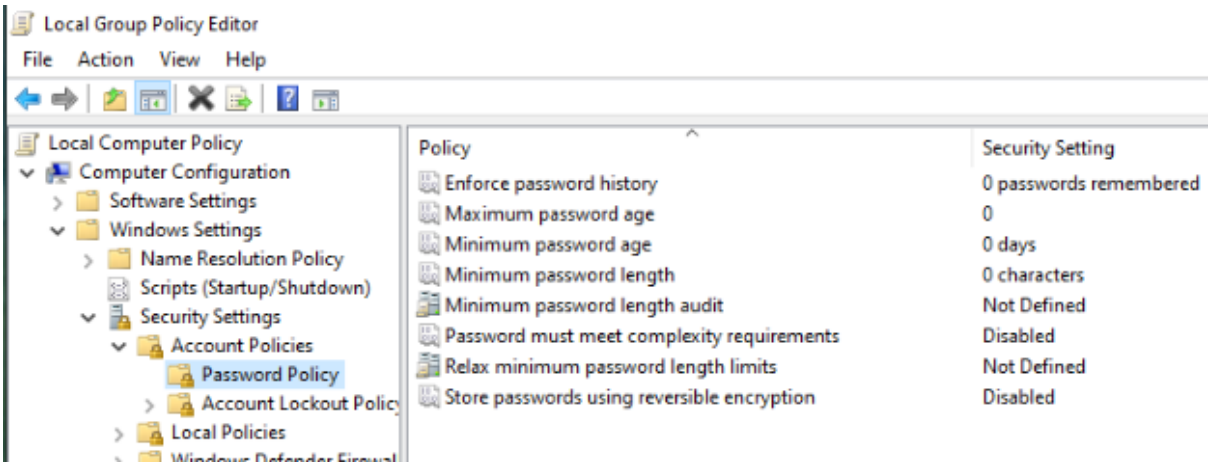
TASK 2:

Review the Password Policy configured in Active Directory and determine if the given default policy is compliant with the NIST, CIS, and PCI DSS recommendations.

Note: To access the Password Policy, launch the **Local Group Policy Editor** by pressing Windows+R, typing **gpedit.msc** into the box, and then pressing the **Enter** key. Next, navigate to **Computer configuration > Windows settings > Security settings > Account policies > Password policy**.

Make relevant changes to ensure the password policy settings are compliant with the given recommendations. Use 0 if the value is NA.

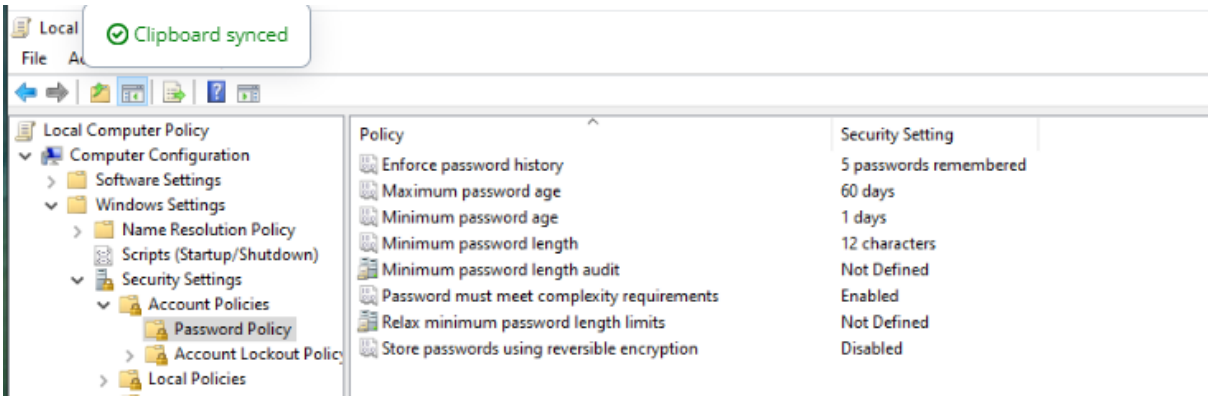
Win22 setting:



Policy Setting	NIST Recommendation	CIS Recommendation	PCI DSS Recommendation	Used Setting
Enforce Password History	0	5 passwords remembered	24 passwords remembered	5
Maximum Password Age	No specific maximum age	60 days or less	90 days or less	60 days

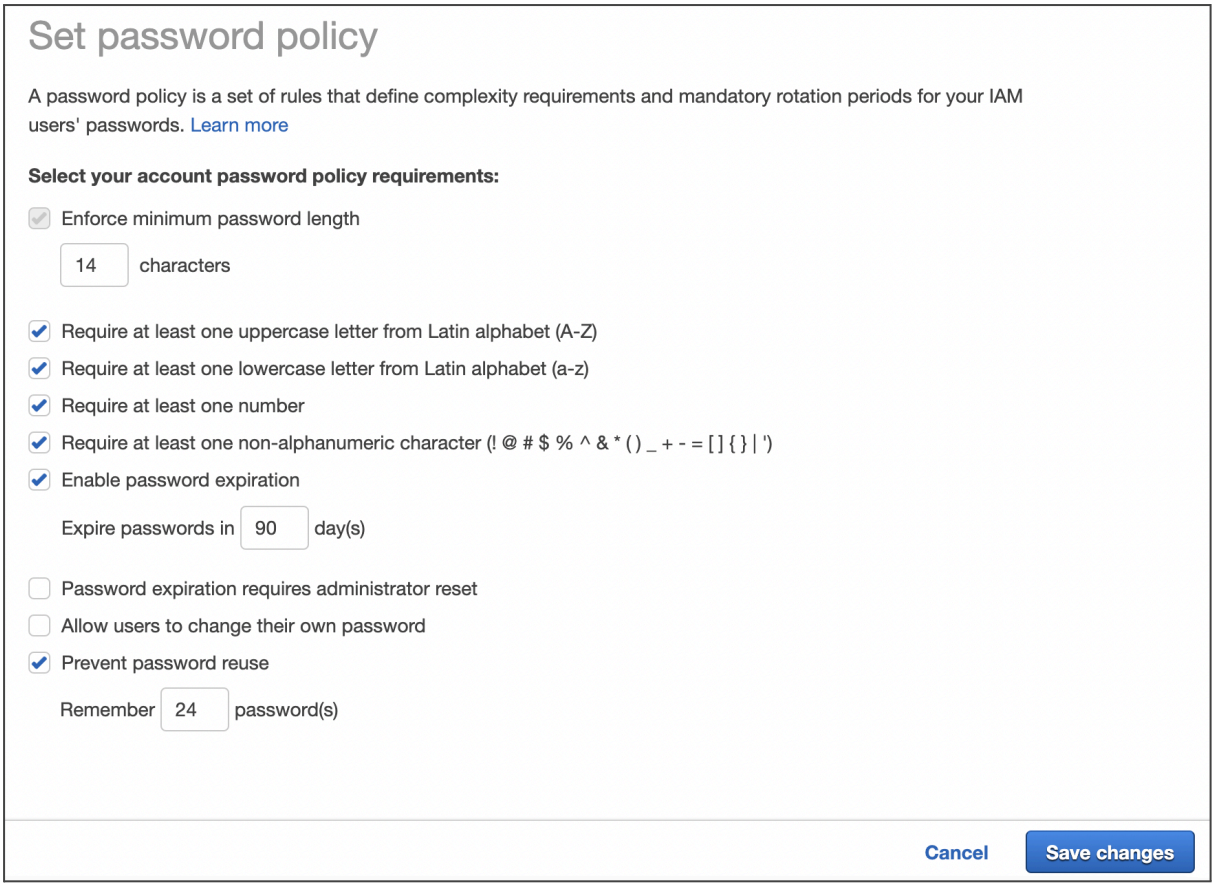
Minimum Password Age	0	1 day	1 day	1 day
Minimum Password Length	At least 8 characters	At least 12 characters	At least 7 characters	12 characters
Password Must Meet Complexity Requirements	Not required (passphrases encouraged)	Enabled	Required	Enabled
Store Passwords Using Reversible Encryption	Not allowed	Disabled	Not allowed	Disabled

Used Setting:



<u>TASK 3:</u>

To ensure that the organization's cloud resources are also compliant with the PCI DSS requirements, review the IAM Password Policy on AWS (as shown in the screenshot) to determine if the account password policy meets the PCI DSS requirements.



Make the relevant changes to ensure that the IAM policy is compliant with PCI DSS requirements.

Parameters	Description	Default Value
Require Uppercase Characters	Requires at least one uppercase letter (A-Z) in the password.	True
Require Lowercase Characters	Requires at least one lowercase letter (a-z) in the password.Requires at least one special character in the password.	True
Requires Symbols	Requires at least one special character in the password.	True
Require Numbers	Requires at least one numeric character (0-9) in the password.	True
Minimum Password Length	Specifies the minimum number of characters required in the password (must be at least 7 characters to meet PCI DSS requirements).	True (14 characters)

Password Reuse Prevention	Prevents users from reusing their previous passwords (PCI DSS requires preventing reuse of the last 4 passwords).	True (Remember last 24 passwords)
Max Password Age	Specifies how long a password can be used before it must be changed (PCI DSS requires passwords to be changed at least every 90 days).	True (90 days)

I

TASK 4:

As a security analyst for the bank, review the **PCI DSS v3.2.1 Quick Reference Guide** to determine the following:

1. Review firewall configuration rules at least every: 6 months.
2. Purge unnecessarily stored data at least: quarterly.
3. Install critical security patches within: 1 month of release.
4. Scan internal and external network vulnerabilities at least: quarterly and after any significant change in the network.
5. Retain visitor logs for at least: 3 months unless otherwise restricted by law.
6. Perform critical log reviews at least: daily.
7. Retain audit trail history for at least: 1 year.
8. Common Vulnerability Scoring System (CVSS) base score for external scans of the components in the cardholder data environment must not be equal to or higher than: 4.0.
9. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every: 6 months and after making changes to these controls.
10. Review security policy at least: annually.
11. Perform a risk assessment process at least: annually and upon significant changes to the environment that identify critical assets, threats, and vulnerabilities and result in a formal assessment.
12. Conduct reviews at least: annually to confirm personnel is following security policies and operational procedures.