6.6.9 Hardening Authentication Facts

This lesson covers the following topics:

- Hardening authentication methods
- Hardening authentication best practices

Hardening Authentication Methods

Hardening means to strengthen. You want to make sure your authentication methods are strong so that you can be confident that users accessing your network are who they say they are.

The following table provides various methods for strengthening your authentication.

Method	Description

Password Policies	Account policies help you control the composition and use of passwords. Password policies include:
	- Enforce password history - This determines the number of unique new passwords that have to be used before an old password can be reused. This helps to prevent users from reusing any recent passwords.
	- Maximum password age - This requires users to change their password after a given number of days.
	- Minimum password age - This determines the number of days that a password must be used before the user can change it. This prevents users from reverting back to their original password immediately after they have changed it.
	- Minimum password length - This identifies the minimum number of characters in a password.
	- Password must meet complexity requirements - A complex password prevents using passwords that are easy to guess or crack. Complex passwords must meet the following minimum requirements:
	  - Cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters
	  - Must be at least six characters in length
	  - Must contain characters from three of the following four categories:
	  - English uppercase characters (A through Z)
	  - English lowercase characters (a through z)
	  - Base-10 digits (0 through 9)
	  - Non-alphabetic characters (for example, !, $, #, or %)
	Complexity requirements are enforced when passwords are changed or created.

Multifactor Authentication	When possible, multifactor authentication should be used. This means using more than one method to authenticate your users. End users can be authenticated using three types of factors: - Something you know - Something you have - Something you are Robust authentication processes use two or more of these factors.

Account Restrictions	Account restrictions place restrictions on the use of a user account for login. For example, you can: ▪ Prohibit multiple concurrent logins ▪ Allow logins only during certain days and hours ▪ Allow logins only from specific computers ▪ Create expiration dates for user accounts for temporary users to prevent them from being used past a certain date
Account Monitoring	Account monitoring can help you detect unusual or risky behavior. You should monitor for the following: ▪ Login activity. ▪ Suspicious logins for the user (spikes, logins at unusual time of day, and/or frequent or failed logins). ▪ Remote-access traffic.
Account Maintenance	The following list provides best practices for account maintenance: ▪ Delete an employee#39;s account when the employee leaves the organization. ▪ Disable inactive accounts. ▪ Use automatic account expiration when applicable. ▪ Restrict remote access only to authorized clients (filtering by IP address).
Limit Remote Access	The following precautions should be taken when administering remote access: ▪ Allow remote access to the network only for those users who need it to perform their duties (not standard for all users). ▪ Do not allow remote access clients to connect directly to the internal network. Allow remote access clients to connect to a DMZ and then monitor the traffic. ▪ Restrict remote access only to authorized clients . You can filter by IP address.
Account Lockout Policies	Account lockout disables a user account after a specified number of incorrect login attempts. Account lockout policies include: ▪ Account lockout duration - Specifies the number of minutes a locked-out account remains locked out before automatically becoming unlocked. When set to 0, an administrator must unlock the account. ▪ Account lockout threshold - Specifies the number of failed logon attempts that causes a user account to be locked out. ▪ Reset account lockout counter after - Specifies the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. For example, if this value is set to 60 minutes and the account lockout threshold is set to 5, the user can enter up to four incorrect passwords within one hour without the account being locked. Account lockout can be used to prevent attackers from guessing passwords, but it can also be used maliciously to lock an account and prevent a valid user from logging in.

Hardening Authentication Best Practices

When controlling user account and password security, be aware of the following:

- For large environments, implement a password management system with a self-service password reset management system. This allows a user to change his or her own password and ensures that only he or she knows it. In a system where administrators hand out passwords that users cannot change, passwords lack security. In this type of arrangement, no matter how complex the password is, more than one person knows what it is. This can affect the security of the system.
- Implement account auditing to track incorrect login attempts. Small numbers of incorrect logon attempts occur naturally as users mistype or forget passwords. Large numbers of incorrect login attempts could identify a potential hacker trying to guess passwords.
- Scan systems to identify unused user accounts or accounts with blank passwords.
- When implementing account lockout and account policies on Microsoft systems:
  - The Local Security Policy controls policies for user accounts that are defined on a local system.
  - Policy settings in Group Policy are linked to the domain control settings for all user accounts in the domain. Settings defined at other levels in Group Policy do not affect password or account lockout settings.
- Disable and/or remove unnecessary accounts installed on the operating system by default, or disable specific user accounts that are no longer needed.
- Prohibit the use of generic user accounts. Generic accounts, such as guest or administrator accounts in Windows, should be disabled.
- Prohibit the use of shared user accounts.
  Shared accounts:
  - Increase the likelihood of the account being compromised. Because the account is shared, users tend to take security for the account less seriously. For example, one organization found that the passwords for shared user accounts proliferated to the point where hundreds of current and former employees knew them.
  - Make password management more difficult. Because password changes must be communicated to multiple users, many system administrators avoid making any password changes at all. If the password is well known, employees (including former employees that no longer need access to the account) may still know the password.
  - Reduce responsibility for the account. Because users view the account as communal, users may do things with the account that they would not do with their personal account.
  - Destroy audit trails for the account. Because multiple users are associated with the account, it can be difficult to identify who is actually responsible for actions performed with the account.
  - Make it difficult to monitor the account for unusual activity. Because multiple users are associated with the account, it is much more difficult to define behaviors that are normal and behaviors that are abnormal. This is problematic because identifying abnormal account activity is key to detecting attacks on your systems.