13.7.4 Password Facts

Passwords are probably the most common authentication credential used on computer systems. However, passwords have the following weaknesses:

- Most users choose passwords that are easy for themselves to remember, but also easy for others to guess. Using social media, an attacker might be able to guess a user's password (using information such birthdays, names of family members, favorite sport teams, or pet names).
- Automated attacks can be employed which try all likely or possible combinations in order to discover (or crack) a password. The following table lists common automated password attacks (which are also sometimes referred to as password cracks):

Attack	Description
Dictionary	A dictionary attack tries to guess a user's password using a list of words from a dictionary. Often symbols and upper and lower case characters are substituted inside the dictionary word. The dictionary attack frequently works because users tend to choose easy-to-guess passwords. A strong password policy is the best defense against dictionary attacks.
Hybrid	A hybrid attack adds appendages to known dictionary words. For example, 1password, password07, p@ssword1.
Brute force	A brute force attack tries to identify a user's password by exhaustively working through all possibilities of all letter, number, and symbol combinations until the correct password is identified. Brute force attacks will always be successful if given enough time, yet they are frequently the most time consuming method of attack.

Countermeasures for password attacks include the following:

- Require that user passwords:
  - Contain multiple character types, including uppercase, lowercase, numbers, and symbols.
  - Are a minimum length of eight characters (longer is even better).
  - Do not contain any part of a username or email address.
  - Do not contain words found in the dictionary.
- Require that user passwords be changed frequently (such as every 30 days). This is called password aging.

  Be aware that requiring overly complex passwords or changing them too frequently can cause users to circumvent security policies by writing down their passwords.

- Retain password history to prevent re-use.
- Implement multifactor authentication.
- Audit computer systems for excessive failed logon attempts.
- Implement account lockout to lock accounts when multiple incorrect passwords are used.
- Monitor the network or system for sniffing and password theft tools

In Windows, edit the Local Security Policy to modify password settings for a local computer, or the Default Domain Policy to control passwords for all computers in an Active Directory domain. The following table lists various policy settings that you should know.

Setting Group	Description
Password Policy	The password policy defines characteristics that valid passwords must have. Settings that you can configure in the password policy include: - **Minimum password length** requires passwords to have a minimum length. In general, longer passwords are more secure than shorter ones (although they can be harder to remember). - **Password complexity** prevents using passwords that are easy to guess or easy to crack. It forces passwords to include letters, symbols, a combination of lower case and caps, and numbers. - **Maximum password age** forces users to change the password after the specified time interval. - **Minimum password age** prevents users from changing the password too quickly.

	▪ **Enforce password history** requires users to input a unique (previously unused) password when changing the password. This prevents users from reusing previous passwords.
Account Lockout Policy	Use account lockout settings to protect user accounts from being guessed and to also prevent accounts from being used when hacking attempts are detected. Lockout policy settings are: ▪ **Account lockout threshold** specifies the maximum number of incorrect logon attempts. Once the number has been reached, the account will be locked and logon disabled. A common setting is to lock the user account when three consecutive incorrect passwords have been entered. ▪ **Account lockout duration** determines the length of time the account will be disabled (in minutes). When the time period expires, the account will be unlocked automatically. Setting this to 0 means that the account remains locked until manually unlocked by an administrator. ▪ **Reset account lockout counter after** determines the amount of time (in minutes) that passes before the number of invalid attempt counter is reset. For example, if a user enters two incorrect passwords, the incorrect counter will be cleared to 0 after the timer has expired.