13.4.5 Password Attack Facts

The following are ways that threat agents discover or crack passwords:

- Using tools to check for unencrypted or weakly encrypted passwords sent through the network.
- Guessing passwords by trying:
  - Default passwords for new systems
  - Blank passwords
  - The word *password* as the password
  - Rows of letters on the keyboard (e.g., qwerty)
  - The user's name or login name
  - Names of family members, pets, etc.
  - The user's birth date
  - Names of celebrities
  - Words in the dictionary and adding appendages to dictionary words
- Using *social engineering* to get a user to reveal the password. For example, the attacker can pretend to be an administrator that needs the user's password.
- Using brute force attacks.
- Using tools to crack passwords:
  - Programs that reveal a hidden password in clear text.
  - Keylogging software that can capture a user's screens, clipboard data and visited websites in addition to logging keystrokes.
  - A *rainbow table* applies hashing algorithms to every word in a dictionary (sometimes including hybrids or passwords accumulated in brute force techniques).
    - The results are saved in a table or matrix.
    - An encrypted password is compared to the pre-computed hashed passwords in the matrix until a match is found.
    - This method applies the concept of time-memory trade off, meaning that it can save a considerable amount of time at the expense of memory.
    - Rainbow tables or matrices can be extremely large and expansive, consuming up to 30 GB of space.

Hashed Password Collection

Hashed passwords can be collected in several ways:

- A sniffer captures authentication logon traffic and extracts the hashed password from the network packets.
- An account database file is compromised by an attacker with read access.
- An account database file is pulled from a backup.

Use the following strategies to protect your system from password attacks:

- Educate users on how to create and remember strong passwords. Enforcing strict password requirements might actually weaken network security if you do not educate users about proper procedures for protecting logon credentials. If users do not understand the restrictions that have been implemented, they might try to circumvent these restrictions by writing down passwords. Take the following measures to educate users:
  - Tell users that they should not write down passwords or share logon credentials with other users.
  - Help users avoid common passwords, such as numbers, names, or words an attacker could easily guess.
  - Teach users how to construct and remember complex passwords. For example, for the password **bw2Fs3d**, users might create the following sentence: *bob went 2 the "capital" Florist shop 3 times daily*.
  - Educate users about social engineering tactics. Instruct them never to give their password to anyone—not even administrators or other trusted personnel. Implement policies that prevent administrators from asking for sensitive information.
- Protect access to the password file. Passwords are typically stored in a password database file that uses a one-way encryption algorithm (hashing). Use protection methods available in the operating system to further secure the file.
- Have users change default credentials when accessing applications for the first time or resetting passwords.
- *Salt* the hash to mitigate rainbow table attacks. Salting the hash adds random bits to the password before hashing takes place, thereby producing an entirely different hash value for the password. Because the hacker does not know the extra random bits, the rainbow table will be of no value.
- Implement two-factor authentication.