7.2.2 Password Attack Facts

Threat agents can use the following methods to discover or crack passwords:

Methods	Description
Password Cracking Tools	Password cracking tools check for unencrypted or weak implementations of encrypted passwords sent through the network. These tools guess passwords by looking for: ▪ Default passwords for new systems ▪ Blank passwords ▪ The word *password* as a password ▪ Rows of letters on the keyboard (such as qwerty) ▪ User's name or login name ▪ Name of significant other, pet, children, etc. ▪ Birthdate ▪ Name of celebrity ▪ Words in the dictionary and adding appendages to dictionary words ▪ Programs, such as SnadBoy's Revelation, which reveal a hidden password in cleartext.
Social Engineering	Social engineers try to get a user to reveal the password. For example, the attacker can pretend to be an administrator that needs the user's password.
Brute Force Attack	A brute force attack consists of an attacker trying to correctly guess many passwords or passphrases. Brute force attacks work by systematically calculating every possible combination that could make up a password and testing it to see if it is the correct password. As the password's length increases, on average, the amount of time it takes to find the correct password increases. In an offline brute force attack, the attacker attacks by herself. In an online brute force attack, the attacker attacks other entities and uses them to attack your system.
Downgrade Attack	A downgrade attack is an attack on a computer system or communications protocol that makes it downgrade the high-quality mode of operation (such as an encrypted connection) in favor of an old, lower-quality mode of operation (such as cleartext) used for backward compatibility with older systems. This is a flaw found in OpenSSL. It allows the attacker to negotiate to a lower version of TLS between the client and server. This is one of the most common types of downgrade attacks. Downgrade attacks are often implemented as part of a man-in-the-middle attack and can be used to enable a cryptographic attack that might not be possible otherwise. Removing backward compatibility is often the only way to prevent downgrade attacks.
Keylogging	Keylogging software can capture a user's screens, clipboard data, and visited websites in addition to logging keystrokes.
Rainbow Table	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, but at the expense of memory. ▪ Rainbow tables or matrices can be extremely large and expansive, consuming up to 30 GB of space.

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 accessed by an attacker who gains read access.
- An account database file is pulled from a backup.

Use the following strategies to protect against password attacks:

- Educate users on how to create and remember strong passwords. Enforcing strict password restrictions might actually weaken network security if you do not educate users about proper procedures to take to protect 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.
  - 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 not to respond to requests for passwords from administrators or other seemingly 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 methods available in the operating system to protect the password file.
- 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.