Identifying Common Password Attacks

Those who can't do, ~~teach~~ steal. As illustrated throughout the module, a password is a private and confidential piece of data. It has the ability to protect sensitive personal and business information. A simple set of characters can be the sole gatekeeper to all of your financial and private information. Because of this, attackers continuously target passwords in hopes of gaining access to data. Below, you will find several techniques most commonly used among attackers.

BRUTE FORCE

Brute force involves using an automated program that can guess passwords very quickly. This program may use several different techniques, including:

- Using a list of the most common passwords
- Using a dictionary of common words
- Failing other techniques' attempt combinations of letters and numbers

This technique needs to make many guesses in a short amount of time, so a simple account lockout or delay can slow this down.

GUESSING GAME

Since account lockouts are generally tracked for each account separately, a variation of this technique is to guess the most common passwords against a list of accounts to avoid triggering the account lockout safety mechanism.

Research has shown that the top 5 passwords most commonly used on the Internet are:

- 123456
- 12345
- 12345678
- password
- iloveyou

Passwords comprised of simple words, names, places, numbers, and even combinations (such as 'abc123') are trivial to guess. The best way to prevent these attacks is to follow best practices for creating strong passwords.

BEING SNEAKY

One of the oldest and simplest methods for someone to get your password is to simply steal it. This can be done in many ways, such as:

- Watching over your shoulder as you type it
- Finding a sticky note hidden under the keyboard (or worse, right on the monitor!)
- Viewing it in a text file on the computer when you step away for a coffee break

Believe it or not, attackers will even pose as IT staff or personnel in hopes of obtaining your personal information.

COMPROMISE

Another method for an attacker to get your password is through the compromise of a third party system, such as an online forum or retailer.

It is highly unlikely that a malicious user is looking to change the settings of your social networking profiles- what they really want is access to your shared passwords in order to access other accounts holding sensitive information.

Think of a compromise as having a “domino effect” on your stored information. If an attacker gains access to one secure system, such as LinkedIn account, he or she now as the login credentials to attempt to infiltrate other secure systems, such as your personal banking site.

Be warned, if an attacker accomplishes this feat, the chances of reversing the process and protecting your information are minimal. However, by following password best practices such as not reusing passwords for multiple systems, you can minimize the damage that can be done.

Remember, a password is private and confidential personal data, and should be treated and protected as such.