Cybersecurity

2.4.14 – Password Attacks

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Password Attacks

- Attacks designed to gain a target's password to have their credentials to log in as that target.
- The most obvious way for a malicious person to get someone's password is if they have the plaintext or unencrypted password.
- Other methods of gaining unencrypted passwords:
  - Intercepting an email meant for someone else that has a password in it
  - A keylogger can capture keystrokes as a target types in a password
  - Data breaches of passwords stored in plaintext
- As a precaution, you should NEVER write down, type out, or store plaintext passwords unless absolutely necessary!

Attacks For This Lesson

- There are many different methods for trying to figure out passwords; this lesson covers the methods in the Security+ objectives.
  - Brute Force
  - Dictionary Attacks
  - Spraying
  - Rainbow Attack (optional)

Brute Force

- No plaintext, no problem – tries every combination and permutation (such as a password) until the right guess works.
- Attack is very slow
- Can be subject to failed logon restrictions (lock out after X failed attempts) when online
- Brute force attacks attempted offline will not lock you out.

Dictionary Attacks

- Need speed? Look it up!
- Dictionary attacks are a faster form of brute force that use commonly used words or passwords from a list.
- Wordlists of cracked or leaked password files from old cyber attacks are available.
- Dictionary attacks are only good on simplistic or weak passwords.
- Unlike brute force, dictionary attacks don’t try every combination, only what’s on the list!
- Combat this by enforcing strong password criteria (complexity, length, reuse, etc.)

Spraying

- When a malicious user has only a limited number of attempts at a password before the account locks or lacks the time for a comprehensive dictionary attack, they may resort to password spraying.
- This technique involves trying a small set of commonly used passwords across numerous accounts, hoping to strike lucky.
- For example, if the attacker knows a user's fondness for birds, they might try passwords like 'goldfinch,' 'hummingbird,' or 'chickadee.'
- While not the most efficient method, password spraying avoids account lockouts and relies on the chance of guessing a password correctly.

Rainbow Tables

- A precalculated series of hashes using known algorithms commonly used for cracking passwords
- An attacker can simply find the matching hash and look up the input text that produced that result to find the plaintext password.
- Particularly effective against weaker passwords and hashing algorithms

Defense

- Brute Force
  - Implement password lockout policies, increase wait time between attempts
- Dictionary Attacks
  - Enforce strong password criteria to include uppercase letters, lowercase letters, numbers, special characters, and password length.
- Rainbow Tables
  - Use a salt with your passwords.
  - Lesson 1.4.5 defines a salt as random data that is used as an additional input to a one-way hash function.