Cybersecurity

Attacks, Threats, and Vulnerabilities

1.2.11 Password Attacks

What are the different types of password attacks and how can a malicious actor use them?

Overview

Given a scenario, the student will analyze potential indicators to determine the type of attack.

Grade Level(s)

10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 1.2

- Given a scenario, analyze potential indicators to determine the type of attack.
  - Password Attacks
    - Spraying
    - Dictionary
    - Brute force
      - Offline
      - Online
    - Rainbow tables
    - Plaintext/unencrypted

Password Attacks

A password attack is just as one would think. The main purpose of these types of attacks is to gain a victim's password in order to have their credentials and log in as that victim. Passwords are meant to authenticate a user on a system, but this can get compromised if a malicious person is able to figure out a person's password. There are many different methods for trying to figure out passwords; this lesson covers the methods in the Security+ objectives.

Never Send/Store Plaintext Passwords

One of the most obvious ways for a malicious person to log into someone's account is if they actually have the plaintext/unencrypted password. A ***plaintext/unencrypted*** password is simply the user's password. Obviously this would be bad for the victims since the malicious user would not even have to guess or crack the password, they would simply be able to use it. However, how do these malicious people gain unencrypted passwords? This can occur in a lot of random ways: a victim can email a password to someone else and it is intercepted, a keylogger can capture keystrokes as a victim types in their password, or even a data breach can compromise passwords if they are stored in plaintext. As simple as this sounds, you should never write down, type out, or store passwords in plaintext unless absolutely necessary.

Brute Force

What happens if a malicious user does not have a victim's plaintext

Teacher Notes:

password? Well, there are a few methods they can attempt to try to crack a password. A popular method is through brute force. A *Brute Force* attack is done by trying all possible combinations and permutations (such as a password) until the right guess works. This attack, therefore, is very slow. Brute force attacks attempted ***online*** will be subject to failed logon restrictions (lock out after X failed attempts). Brute force attacks attempted ***offline*** will not lock you out.

Dictionary Attacks

A much quicker and more efficient version of a brute force attack is by using a dictionary attack. *Dictionary Attacks* are a form of a brute force attack that uses commonly used words/passwords from a list. Wordlists are available of cracked/leaked password files from old cyberattacks. Dictionary attacks are only good against simplistic and weak passwords. To combat dictionary attacks, enforce strong password criteria (complexity, length, re-use, etc.). However, unlike brute force attacks, dictionary attacks will not try every possible combination, only ones in the dictionary or script.

Spraying

What happens if a malicious user only has 5 attempts at a password before the account locks or they do not have the time to run through a dictionary attack? They can try spraying. *Spraying* is trying a few passwords at a time and seeing if they can get lucky. For example, if a malicious person knows that a user loves birds, they might try the following passwords: ***goldfinch***, ***hummingbird***, or ***chickadee*** with the hopes of correctly guessing the password. While this method is not the most effective method, it does not lock the malicious user out of the system, and they are just hoping to get lucky with a guess.

Rainbow Attack

Rainbow Tables are precalculated series of hashes using known hashing algorithms. Rainbow tables are commonly used for cracking passwords. A cracker can simply find the matching hash and look up the input text that gave the result to find the plaintext password. To combat rainbow tables, a user can use a salt. A salt is random data that is used as an additional input to a one-way function that hashes data.

Teacher Notes:

Defense

Defending against password attacks can be done in many different ways depending on the type of attack. To defend against rainbow tables, use a salt with your passwords. Recall from lesson 1.2.10, a salt is random data that is used as an additional input to a one-way hash function. Brute force attacks can be limited by implementing password lockout policies (limiting number of attempts) and by increasing time required between attempts (slowing down time per attempt). To combat dictionary attacks, one should enforce strong password criteria to include password complexity requirements such as inclusion uppercase, lowercase, special characters, and password length.