LESSON NOTES

CYBERSECURITY

Domain 2.0 - General Security Concepts

2.4.14 - Password Attacks

Lesson Overview:

Students will:

- Analyze potential indicators to determine the type of attack.

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

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

2.4 - Given a scenario, analyze indicators of malicious activity

- Password Attacks
    - Spraying
    - Brute force

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
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Password Attacks

A password attack is just as one would think. The main purpose of these types of attacks is to gain a target's password to have their credentials and log in as that target. Passwords are meant to authenticate a user on a system, but this can get compromised if a malicious person can 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 or Store Plaintext Passwords

One of the most obvious ways for a malicious person to log into someone's account is if they have the plaintext or unencrypted password. A plaintext or unencrypted password is simply the user's password. Obviously, this would be bad for the targets 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: an intercepted target email containing a password, a keylogger can capture keystrokes as a target type 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 plain text unless necessary.

Brute Force

What happens if a malicious user does not have the target's plaintext password? Well, there are a few methods they can use to attempt to crack a password. A popular method is through brute force. A ***Brute Force*** attack is done by trying all combinations and permutations (such as a password) until the right guess works. This attack, therefore, is 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 brute force attack that uses commonly used words or passwords from a list. Wordlists of cracked or leaked password files from old cyberattacks are available. 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 combination, only ones in the dictionary or script.

Spraying

In scenarios where a malicious actor has only a limited number of attempts at a password before the account locks or lacks the time for a 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 it lucky. For instance, 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 Attack (Optional)

Rainbow Tables are a 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. Rainbow tables are particularly effective against weaker passwords and hashing algorithms.

Defense

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