علیرضا رضایی

تحقیق جلسه هفتم

Resources

https://www.onelogin.com/learn/6-types-password-attacks

https://crashtest-security.com/password-attack/

**Types of Password Attacks**

## 1. Phishing

Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily.

examples of phishing:

- **Regular phishing.** You get an email from what looks like goodwebsite.com asking you to reset your password, but you didn't read closely and it's actually goodwobsite.com. You "reset your password" and the hacker steals your credentials.
- **Spear phishing.** A hacker targets you specifically with an email that appears to be from a friend, colleague, or associate. It has a brief, generic blurb ("Check out the invoice I attached and let me know if it makes sense.") and hopes you click on the malicious attachment.
- **Smishing and vishing.** You receive a text message (SMS phishing, or smishing) or phone call (voice phishing, or vishing) from a hacker who informs you that your account has been frozen or that fraud has been detected. You enter your account information and the hacker steals it.
- **Whaling.** You or your organization receive an email purportedly from a senior figure in your company. You don't do your homework on the email's veracity and send sensitive information to a hacker.

## 2. Man-in-the-Middle Attack

Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other

## 3. Brute Force Attack

If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.

types of brute force attacks:

**1. Simple brute force attacks –** A hacker uses logic and data about a user to guess the most likely password. This technique is used for simple passwords, such as those containing a combination of pet name-year and birth.

**2. Credential stuffing –** This involves using previously exposed login combinations that were maliciously obtained across vulnerable websites. In such attacks, hackers typically take advantage of the fact that entities tend to re-use their username-password combinations across multiple services.

**3. Hybrid brute force attacks –** An attacker combines **simple weak password-guessing** with automated software that performs **credential stuffing** to uncover complex passwords. In most production systems, entities use slight variations of passwords across different websites. Attackers also rely on user data patterns across services to improve the accuracy of credential stuffing tools.

**4. Reverse brute force attacks –** In this attack, a hacker starts with a known password and then searches for usernames that match it. As threat actors often have access to multiple databases of leaked credentials, it is easy to identify common passwords within a particular group of users.

## 4. Dictionary Attack

A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries."

## 5. Credential Stuffing

Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in.

## 6. Keyloggers

Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker.