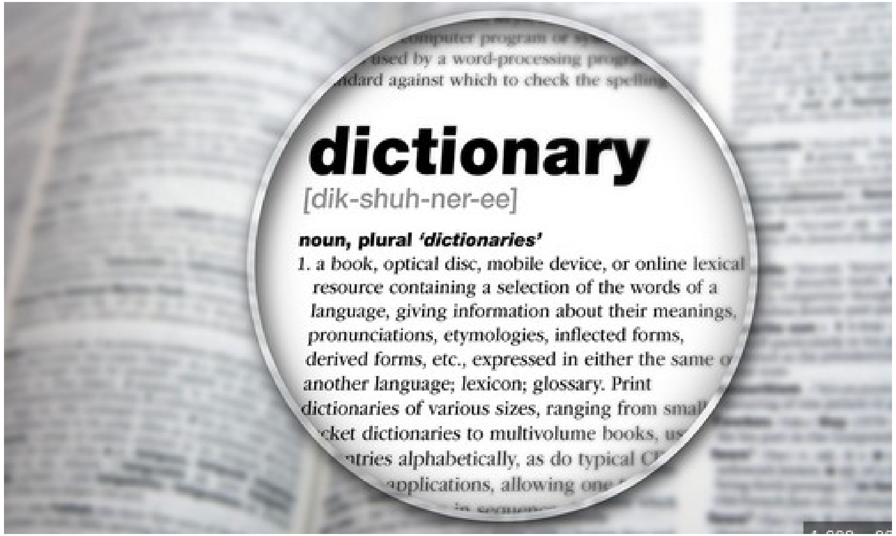
Password Cracking

The Basics

Types of Attacks

1. Brute Force
2. Dictionary
3. Credential Stuffing
4. Rainbow Table



computer program or sy
used by a word-processing progr
ndard against which to check the spelling

dictionary

[dik-shuh-ner-ee]

noun, plural *'dictionaries'*

1. a book, optical disc, mobile device, or online lexical resource containing a selection of the words of a language, giving information about their meanings, pronunciations, etymologies, inflected forms, derived forms, etc., expressed in either the same or another language; lexicon; glossary. Print dictionaries of various sizes, ranging from small ·cket dictionaries to multivolume books, us ·ntries alphabetically, as do typical C applications, allowing one

Brute Force Attacks

1. Often becomes a game of guessing
2. Works the best on weak passwords
3. Mostly an automatic process with established tools
    a. Hydra tool
    b. John the Ripper
    c. Hashcat
4. Many solutions available
    a. Lock out policy
    b. Multi-factor authentication
    c. Good password practices

Dictionary Attacks

1. A form of brute force
    a. Refined methodology using common passwords and users
2. Specifically targets a list of common passwords
3. Normal methods to prevent Brute force still apply
4. One Time passwords do well to prevent password cracking but especially dictionary attacks

Credential Stuffing Attacks

1. When an already compromised accounts user and password are used on another account
2. Extends Brute force attacks by using existing user and passwords
3. This is why getting compromised in one account necessitates changing other passwords as well
4. Using different passwords mitigates the damage of this type of attack

Rainbow Table Attacks

1. Takes advantage of the hashed nature of modern passwords
2. Limited number of Hashing algorithms
3. Using a list of passwords run through a hashing algorithm attackers attempt to guess the password
4. Mitigated through salting or hashing the passwords twice

Good Practices

1. Most password cracking methods require some form of brute force
    a. Use good complexity rules
        i. Capital letters
        ii. Lower case letters
        iii. numbers
        iv. symbols
    b. Length trumps almost everything
2. Avoid words in common dictionary attacks
    a. Password
    b. Letmein
    c. qwerty

HashCat

1. Prides itself in being a fast tool
2. Runs on Linux, Windows and Mac
3. Can preform on GPU or CPU
4. Includes OS specific “password recovery” options
   a. RedHat 389-DS LDAP
   b. macOS v10.7
   c. Windows Hello PIN/Password

Sources

Dictionary Image: https://peterjamesthomas.com/data-and-analytics-dictionary/suggested-definitions-for-the-data-analytics-dictionary/

Rainbow Table Image:

https://loveziaar.life/product_subset/397152575_.html

Brute force slide:

https://www.imperva.com/learn/application-security/brute-force-attack/

HashCat:

https://hashcat.net/hashcat/

Sources 2

Dictionary Slide:

https://web.mit.edu/kerberos/krb5-latest/doc/admin/dictionary.html

Credential stuffing Slide:

https://www.imperva.com/learn/application-security/credential-stuffing/

Rainbow table Slide:

https://www.beyondidentity.com/glossary/rainbow-table-attack

Good practices

https://www.it.ucsb.edu/general-security-resources/password-best-practices