Dictionary Attack

Mohammed Latif Siddiq (1505069)

June 21, 2020

Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology

Contents

1 Introduction

In crypt-analysis and computer security, a **dictionary attack** is a form of **brute force** attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or password by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

1.1 Definition

A **dictionary attack** is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary (hence the phrase dictionary attack). In contrast to a brute force attack, where a large proportion of the key space is searched systematically, a dictionary attack tries only those possibilities which are deemed most likely to succeed. Dictionary attacks often succeed because many people have a tendency to choose **short passwords** that are **ordinary words** or **common passwords**, or **simple variants** obtained, for example, by appending a digit or punctuation character.

1.2 Types of Dictionary Attack

We can give dictionary attack in two ways : 1) **Offline method** and 2) **Online method**.

1.2.1 Offline Dictionary Attack

In an **offline dictionary attack**, hackers steal the **password storage file** from the target system. This is typically the *Security Account Manager (SAM)* file on Windows and the *./etc/shadow* file on Linux.In most cases, Offline Password Cracking will require that an attacker has already attained administrator / root level privileges on the system to get to the storage mechanism. It is possible, however, that the password hashes could also have been pulled directly from a database using SQL injection, an unprotected flat text file on a web server, or some other poorly protected source.

The common steps in **offline dictionary attack** is :

- Store the possible passwords in a file. This file is known as Dictionary.
- Get the password from the Dictionary as input and encrypt it.
- Capture hash code for password and then compare it with the created hash code from the dictionary
- If it is equal then successfully, password is cracked.

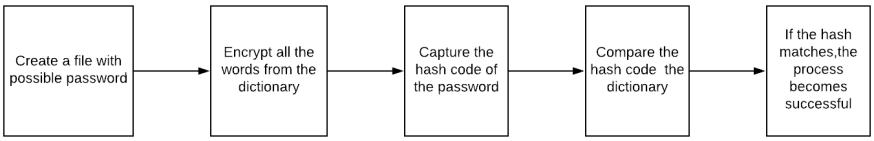

Figure 1: Offline dictionary attack

1.2.2 Online Dictionary Attack

In an **online dictionary attack**, a hacker uses the **same interface** as a regular user to try to gain access to accounts. All the attacker needs is a curated list of likely passwords.

The common steps in **online dictionary attack** is :

- Store the possible passwords in a file. This file is known as **Dictionary**.
- Target any web site, SSH server, FTP server, mail server etc.
- Send request by taking hash code of password from the dictionary
- If the attack is successful,then target will give a positive response

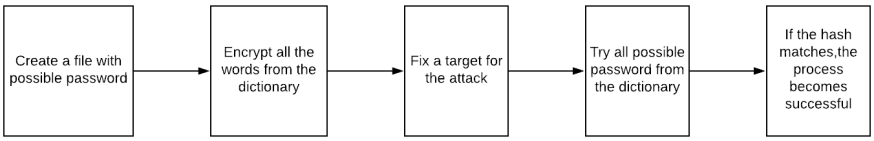

Figure 2: Online dictionary attack