_____

How to find if your password is vulnerable to a dictionary attack, and how to fix it. (Using Linux!)
By: TechCat-Dev

_____

Introduction:
A dictionary attack is a form of a brute force attack. A dictionary attack works when an attacker has a large list of commonly used passwords, and uses that list to attempt to guess a user's password.
Passwords contained in a dictionary are either generated using a special piece of software, or downloaded and compiled from various data breaches located online.
The most commonly used dictionary used by attackers is called *rockyou.txt*. rockyou.txt contains 14 million unique passwords, and is around 134MB in size. Rockyou.txt was obtained from a data breach from RockYou, a company founded in late 2005 that specialized in developing widgets and applications for MySpace, Facebook, and other social media platforms at the time. The data breach occurred in December of 2009 and effected 32 million user accounts. It's also noted that RockYou did not have the best security, and the attackers used a then 10 year old SQL vulnerability to gain access to the unencrypted database of all RockYou users
Since then, the passwords contained in the RockYou data breach are still being used today due to its easy availability, and generally long length. A copy of rockyou.txt can be found on GitHub with this link: (https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt).

_____

Tutorial:
To find out wether your password is vulnerable to a dictionary attack, you must first download a dictionary online (commonly also referred to as "wordlists").
In this demonstration, I will be using the rockyou.txt wordlist, and a copy of Debian Linux (this will also work on security based distributions like Kali Linux, and any other Linux distributions with grep installed on it).

First, I will open my terminal and use the "cd" command to enter the directory where I have the rockyou.txt dictionary. Then I will run this command (replace "mypassword" with your own password!):

"grep -x "mypassword" rockyou.txt"

after running this command, I will see this output:

```
linux@pc:~/Documents/wordlist$ grep -x "mypassword" rockyou.txt
mypassword
linux@pc:~/Documents/wordlist$
```

Now this shows me that my password, “mypassword” is located inside of the dictionary. This means that an attacker can use the rockyou.txt wordlist to guess the passwords to my various online accounts.
Now, what can I do about this? I wouldn’t want a random attacker logging into my accounts and causing havoc! So this is how I’ll make myself immune to a dictionary attack.
dictionaries usually contain weak, and easy to guess passwords. If I change my password from “mypassword”, to “mYP^$$W0RD!” and then re-run the command, we will see this output:

```
linux@pc:~/Documents/wordlist$ grep -x "mYP^$$W0RD!" rockyou.txt
linux@pc:~/Documents/wordlist$
```

a blank output from grep indicates that it was not able to find the specific string that you requested it to find. Which means that your password is no longer vulnerable to common dictionary attacks!

Written By: TechCat-Dev, on https://blogs.techcat.dev
