

Dictionary-Based Attack User Guide

Eunsaem Lee

December 8th, 2022

Table of Contents

Purpose	3
Installing	3
Obtaining	3
Installing	3
Running	3
Examples	4
python dictionary.py	4
password.log	4
python dictionary.py [exit]	4
Create a user with hashed password on Fedora 36	4

Purpose

A dictionary-based password cracker for Fedora 36 that:

- decrypts passwords in the /etc/shadow
- supports:
 - MD5
 - SHA-256
 - SHA-512
 - yescrypt
- does NOT support:
 - Blowfish
 - DES
- writes results into a log file
- sets path to shadow file
- sets path to dictionary file
- exits the program on prompt

Installing

Obtaining

```
git clone https://github.com/eunsaemy/dictionary-attack
```

Installing

None.

Running


```
To run dictionary.py:  
python dictionary.py
```

Examples

python dictionary.py

```
[root@fedora dictionary]# python dictionary.py
Path to shadow file [default=/current_directory/shadow]:
Path to dictionary file [default=/current_directory/rockyou.txt]:
Looking for a password match for user: md5...
username: md5 | password: united
Looking for a password match for user: sha256...
username: sha256 | password: united
Looking for a password match for user: sha512...
username: sha512 | password: united
Looking for a password match for user: yescrypt...
username: yescrypt | password: united
[root@fedora dictionary]#
```

password.log

 password.log - Notepad

File Edit Format View Help

```
username: md5 | password: united
username: sha256 | password: united
username: sha512 | password: united
username: yescrypt | password: united
```

python dictionary.py [exit]

```
Path to dictionary file [default=/current_directory/rockyou.txt]: exit
Goodbye.
[root@fedora dictionary]#
```

Create a user with hashed password on Fedora 36

```
20:35:14(-)root@localhost:~$ useradd yescrypt
20:35:24(-)root@localhost:~$ echo "yescrypt:united" | chpasswd -c YESCRYPT
```