How to crack archive password faster

by Milosz Galazka on May 25, 2015 and tagged with Debian, Jessie, Command-line, John the Ripper, Software recommendation

A week ago I wrote about couple of interesting applications to crack archive password, but they were not as fast as I thought. After investigating this topic further I ended up using community-enhanced version of John the Ripper.

Requirements

Install packages required to compile source code.

```
$ sudo apt-get install build-essential libssl-dev
```

Compilation

Create temporary directory which will be used to compile source code.

```
$ mkdir temp
```

Change working directory.

```
$ cd temp
```

Download most recent community-enhanced version.

```
$ wget http://www.openwall.com/john/j/john-1.8.0-jumbo-1.tar.gz
```

Extract downloaded archive.

```
$ tar xfz john-1.8.0-jumbo-1.tar.gz
```

Change working directory.

```
$ cd john-1.8.0-jumbo-1/src/
```

Execute configuration script.

```
$ ./configure
```

Compile source code.

```
$ make -s
```

Compiled software is available in the *run* directory.

```
$ cd ../run
```

You can execute commands directly from that directory.

Simple installation

Create destination directory for application.

```
$ mkdir -p ~/apps/john
```

Copy application to the destination directory.

```
$ cp ~/temp/john-1.8.0-jumbo-1/run/* ~/apps/john/
```

You can execute commands directly from that directory.

```
$ cd ~/apps/john/ && ./john --test
```

Advanced installation

Pass `JOHN_SYSTEMWIDE` parameter in `CFLAGS` during configuration phase.

```
$ ./configure CFLAGS="-DJOHN_SYSTEMWIDE=1"
```

Create destination directory and copy application after compilation process.

```
$ mkdir -p ~/apps/john
```

```
$ cp ~/temp/john-1.8.0-jumbo-1/run/* ~/apps/john/
```

Create configuration directory and move configuration files.

```
$ mkdir ~/.john
```

```
$ mv ~/apps/john/*.conf ~/.john/
$ mv ~/apps/john/password.lst ~/.john/
$ mv ~/apps/john/*.chr ~/.john/
```

Alter configuration files to use shared location.

```
$ sed -i -e "s|\$JOHN|~/.john|" ~/.john/john.conf
```

```
$ sed -i -e "/.include/ s|<\(.*\)>|\"~/.john/\1\"|" ~/.john/*.conf
```

Extend `PATH` variable to include application directory.

```
$ echo "export PATH=\$PATH:~/apps/john" >> ~/.bashrc
```

You can use recently compiled utilities after you login again, alternatively evaluate `~/.bashrc` file to expand `PATH` in current shell.

```
$ source ~/.bashrc
```

Usage

Use `zip2john` utility to get hashed password out of *zip* archive.

```
$ zip2john encrypted.zip > encrypted.hash$
```

Use `john` to crack password.

```
$ john --show encrypted.hash
encrypted.zip:@3ncPa5Sword@::::encrypted.zip

1 password hash cracked, 0 left
```

`rar2john` utility will work in the same way for *rar* archives.

Additional notes

There are other interesting utilities in community-enhanced version which you may like to examine.

```
~/apps/john$ ls -1 *2john
```

```
dmg2john
gpg2john
hccap2john
keepass2john
keychain2john
keyring2john
keystore2john
kwallet2john
```

```
luks2john
pfx2john
putty2john
pwsafe2john
racf2john
rar2john
ssh2john
truecrypt_volume2john
uaf2john
wpapcap2john
zip2john
```

Use `strace` command in case of problems with the location of configuration files.

Post navigation

← How to crack archive password May 18, 2015
How to lock Linux console session June 1, 2015 →

Related Posts

How to strace PHP-FPM processes 14 Oct 2019
How to count TCP connections 07 Aug 2019
How to generate sequence of numbers 05 Aug 2019
How to determine how long specified remote server or device was offline 29 Jul 2019
How to configure sysfs during system boot 22 Jul 2019

Milosz Galazka

milosz (at) sleeplessbeastie (dot) eu

Updated on 2019-11-16