How to crack zip password on Kali Linux

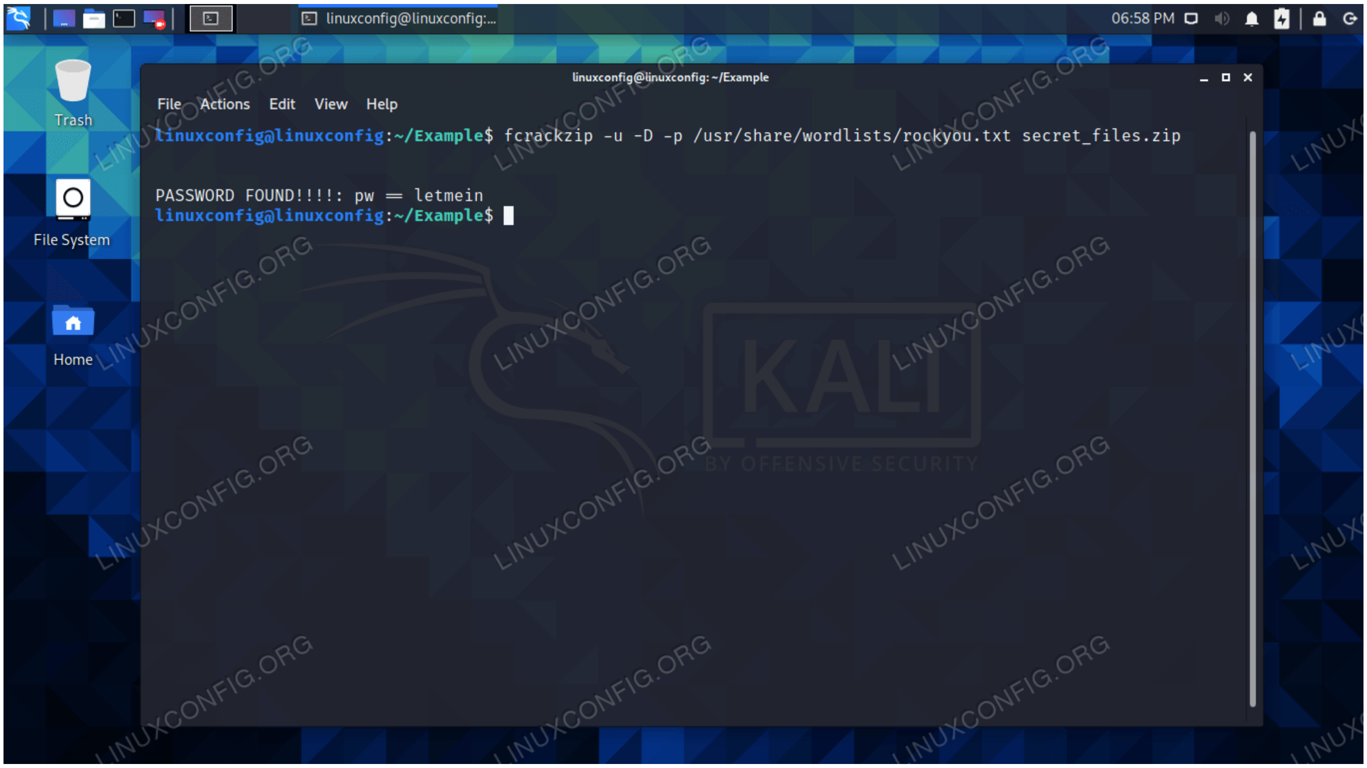
12 January 2021 by Korbin Brown

The objective of this guide is to show how to crack a password for a zip file on Kali Linux.

By default, Kali includes the tools to crack passwords for these compressed archives, namely the fcrackzip utility, John the Ripper and a word list. Follow along with us in the step by step instructions below as we show two different methods for cracking the password of a zip file.

In this tutorial you will learn:

- What tools are used to crack password protected zip files?
- How to crack zip password with John the Ripper
- How to crack zip password with fcrackzip


linuxconfig@linuxconfig:...
06:58 PM
Trash
File System
Home
linuxconfig@linuxconfig: ~/Example
File Actions Edit View Help

```
linuxconfig@linuxconfig:~/Example$ fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt secret_files.zip


PASSWORD FOUND!!!!: pw == letmein
linuxconfig@linuxconfig:~/Example$ 
```

Cracking a password protected zip file on Kali Linux

Software Requirements and Linux Command Line Conventions

Category	**Requirements, Conventions or Software Version Used**
System	Kali Linux
Software	fcrackzip, John the Ripper, wordlist
Other	Privileged access to your Linux system as root or via the `sudo` command.
Conventions	**#** – requires given linux commands to be executed with root privileges either directly as a root user or by use of `sudo` command **$** – requires given linux commands to be executed as a regular non-privileged user

Zip file cracking tools

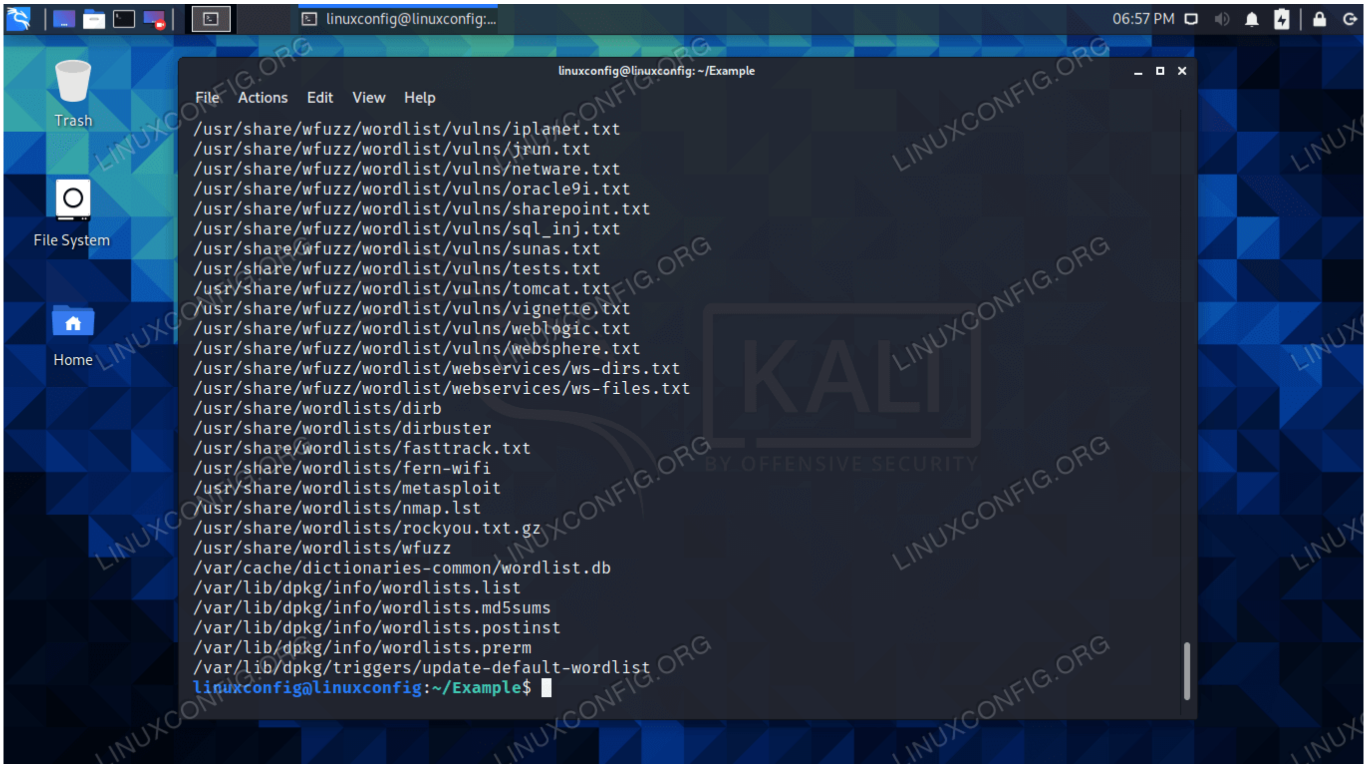
Both the fcrackzip utility and John the Ripper can be used to crack password protected zip files. You can try both of them or just your preferred tool. These utilities can use word lists in order to launch a dictionary attack against the zip file.

Most or all of these utilities should already be on your system, but you can install or update the necessary packages with the following commands.

```
$ sudo apt update
$ sudo apt install john fcrackzip wordlists
```

John the Ripper will automatically use its own wordlist located in `/usr/share/john/password.lst` . You can always use a different wordlist, such as a custom one or a different file on Kali. To quickly locate all the wordlists on your system, use the following command.

```
$ locate wordlist
```

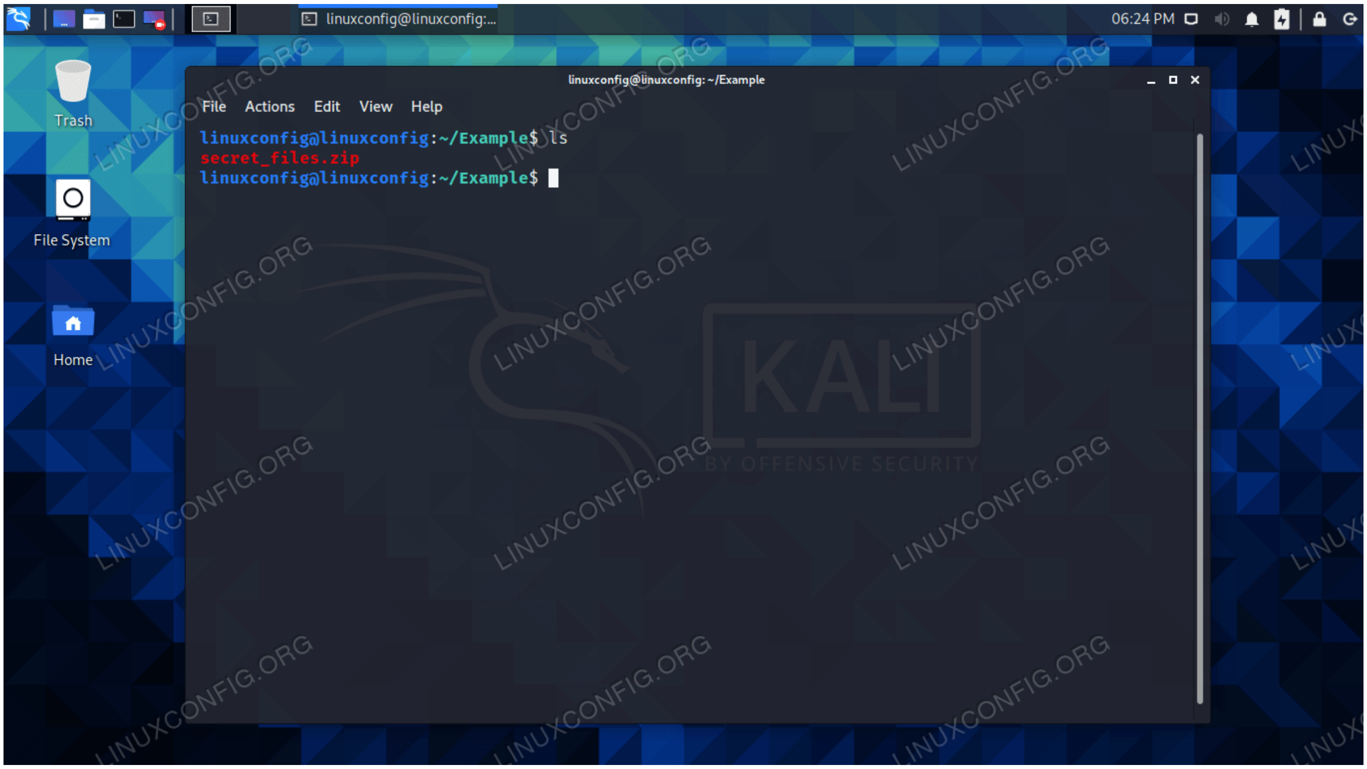


```
/usr/share/wfuzz/wordlist/vulns/iplanet.txt
/usr/share/wfuzz/wordlist/vulns/jrun.txt
/usr/share/wfuzz/wordlist/vulns/netware.txt
/usr/share/wfuzz/wordlist/vulns/oracle9i.txt
/usr/share/wfuzz/wordlist/vulns/sharepoint.txt
/usr/share/wfuzz/wordlist/vulns/sql_inj.txt
/usr/share/wfuzz/wordlist/vulns/sunas.txt
/usr/share/wfuzz/wordlist/vulns/tests.txt
/usr/share/wfuzz/wordlist/vulns/tomcat.txt
/usr/share/wfuzz/wordlist/vulns/vignette.txt
/usr/share/wfuzz/wordlist/vulns/weblogic.txt
/usr/share/wfuzz/wordlist/vulns/websphere.txt
/usr/share/wfuzz/wordlist/webservices/ws-dirs.txt
/usr/share/wfuzz/wordlist/webservices/ws-files.txt
/usr/share/wordlists/dirb
/usr/share/wordlists/dirbuster
/usr/share/wordlists/fasttrack.txt
/usr/share/wordlists/fern-wifi
/usr/share/wordlists/metasploit
/usr/share/wordlists/nmap.lst
/usr/share/wordlists/rockyou.txt.gz
/usr/share/wordlists/wfuzz
/var/cache/dictionaries-common/wordlist.db
/var/lib/dpkg/info/wordlists.list
/var/lib/dpkg/info/wordlists.md5sums
/var/lib/dpkg/info/wordlists.postinst
/var/lib/dpkg/info/wordlists.prerm
/var/lib/dpkg/triggers/update-default-wordlist
linuxconfig@linuxconfig:~/Example$
```

The only other thing you'll need in order to get started is a password protected zip file. If you don't already have one, but would like to follow along, use the following commands to make an example file.

```
$ touch file1.txt file2.txt file3.txt
$ zip -e secret_files.zip file1.txt file2.txt file3.txt
```

You'll be required to enter a password. If you choose something complicated, the password cracking process may take a lot longer. For this example, we'll pick something simple, like "letmein".



```
linuxconfig@linuxconfig:~/Example$ ls
secret_files.zip
linuxconfig@linuxconfig:~/Example$
```

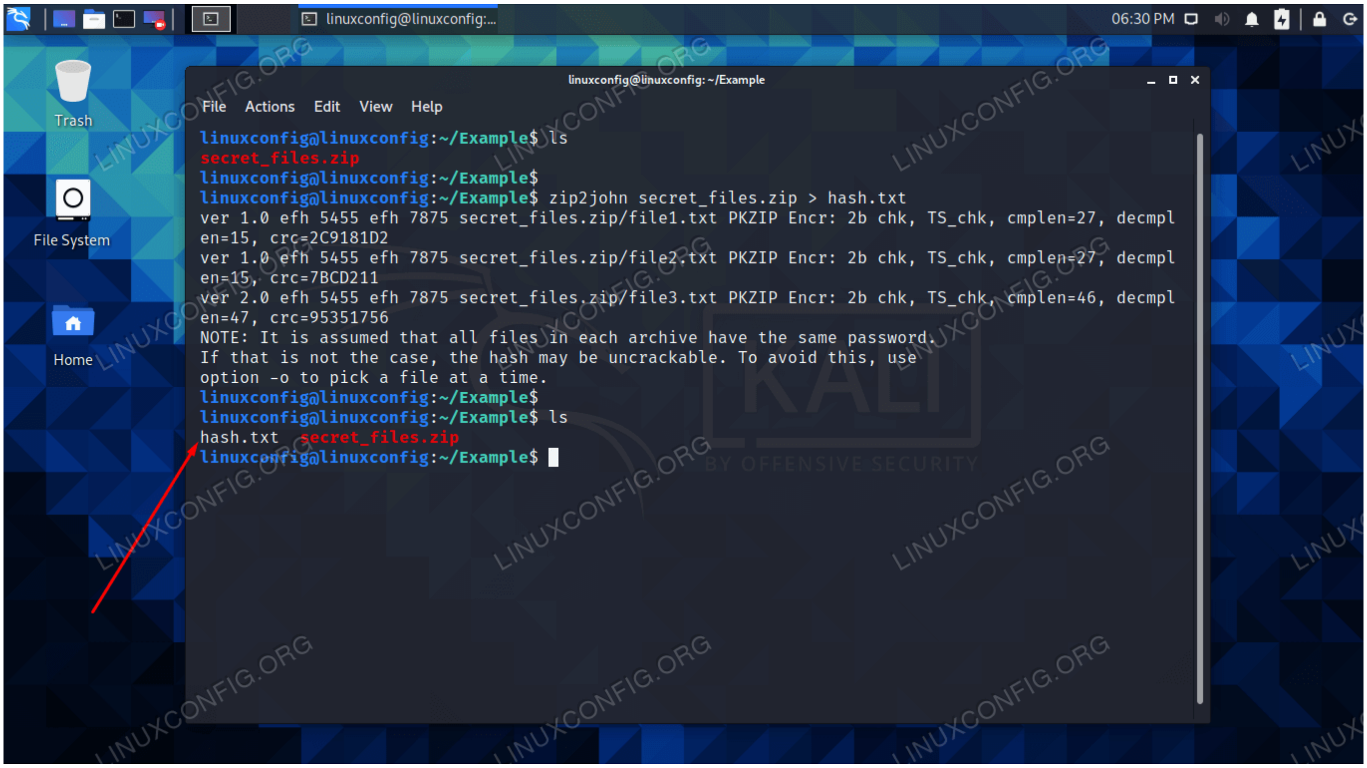
Our password protected zip file that we will try to crack

With the utilities installed and our zip file waiting to be cracked, let's move on to the hacking process below.

Crack zip password with John the Ripper

Step 1 The first step is to create a hash file of our password protected zip file. Use the `zip2john` utility to generate one.

```
$ zip2john secret_files.zip > hash.txt
```


Trash
File System
Home
linuxconfig@linuxconfig:...
06:30 PM
linuxconfig@linuxconfig: ~/Example
File Actions Edit View Help

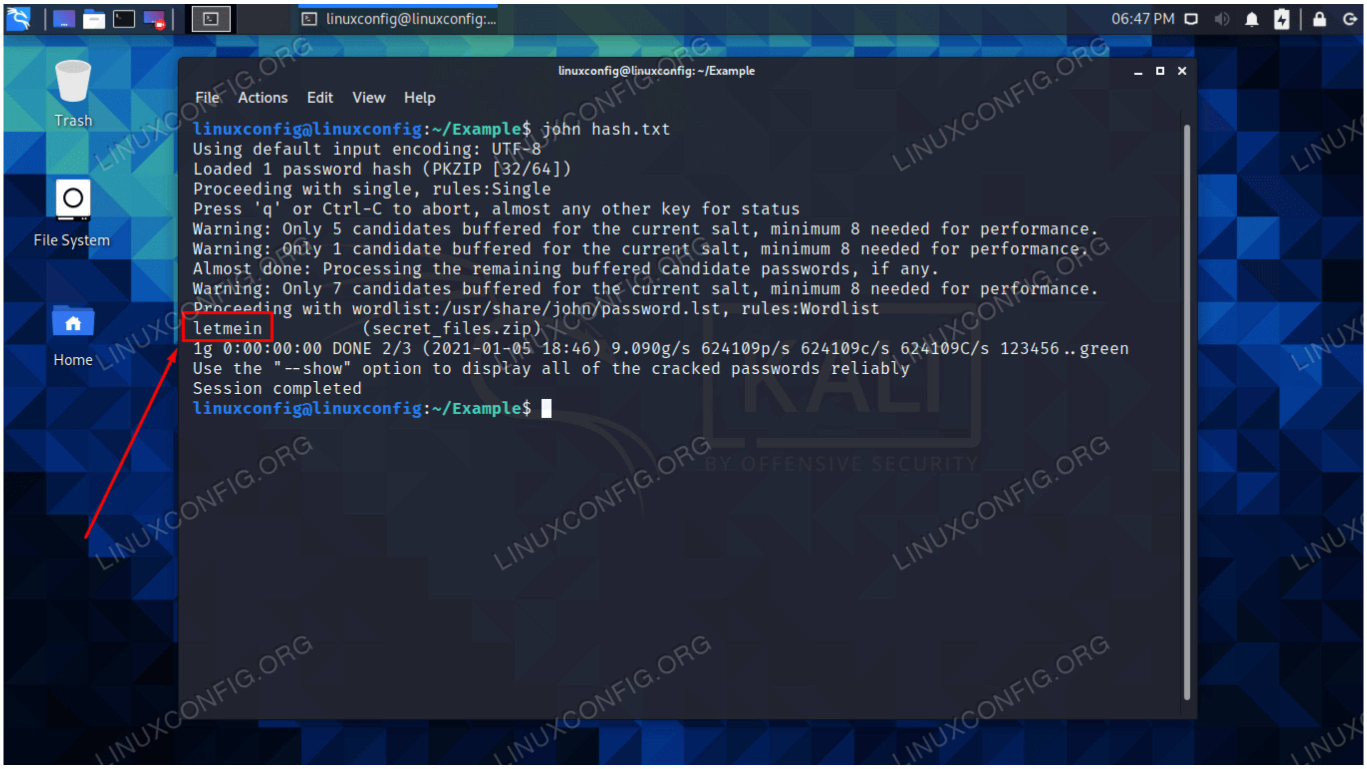
```
linuxconfig@linuxconfig:~/Example$ ls
secret_files.zip
linuxconfig@linuxconfig:~/Example$
linuxconfig@linuxconfig:~/Example$ zip2john secret_files.zip > hash.txt
ver 1.0 efh 5455 efh 7875 secret_files.zip/file1.txt PKZIP Encr: 2b chk, TS_chk, cmplen=27, decmpl
en=15, crc=2C9181D2
ver 1.0 efh 5455 efh 7875 secret_files.zip/file2.txt PKZIP Encr: 2b chk, TS_chk, cmplen=27, decmpl
en=15, crc=7BCD211
ver 2.0 efh 5455 efh 7875 secret_files.zip/file3.txt PKZIP Encr: 2b chk, TS_chk, cmplen=46, decmpl
en=47, crc=95351756
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
linuxconfig@linuxconfig:~/Example$
linuxconfig@linuxconfig:~/Example$ ls
hash.txt  secret_files.zip
linuxconfig@linuxconfig:~/Example$
```

The hash file has been generated

Step 2 The password cracking process will actually be launched against the hash file, not the zip file. Use the following command to begin the process with `john` .

```
$ john hash.txt
```

John was successful in finding the password, and lists the result in its output.


Trash
File System
Home
linuxconfig@linuxconfig:...
06:47 PM
linuxconfig@linuxconfig: ~/Example
File Actions Edit View Help

```
linuxconfig@linuxconfig:~/Example$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
letmein          (secret_files.zip)
1g 0:00:00:00 DONE 2/3 (2021-01-05 18:46) 9.090g/s 624109p/s 624109c/s 624109C/s 123456..green
Use the "--show" option to display all of the cracked passwords reliably
Session completed
linuxconfig@linuxconfig:~/Example$
```

John the Ripper has found the password

If you already have some idea of what the password to your file may be, it can be far more efficient to use a customized wordlist file. Another popular choice is the rockyou.txt file. You can instruct John to use this file with the following command:

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

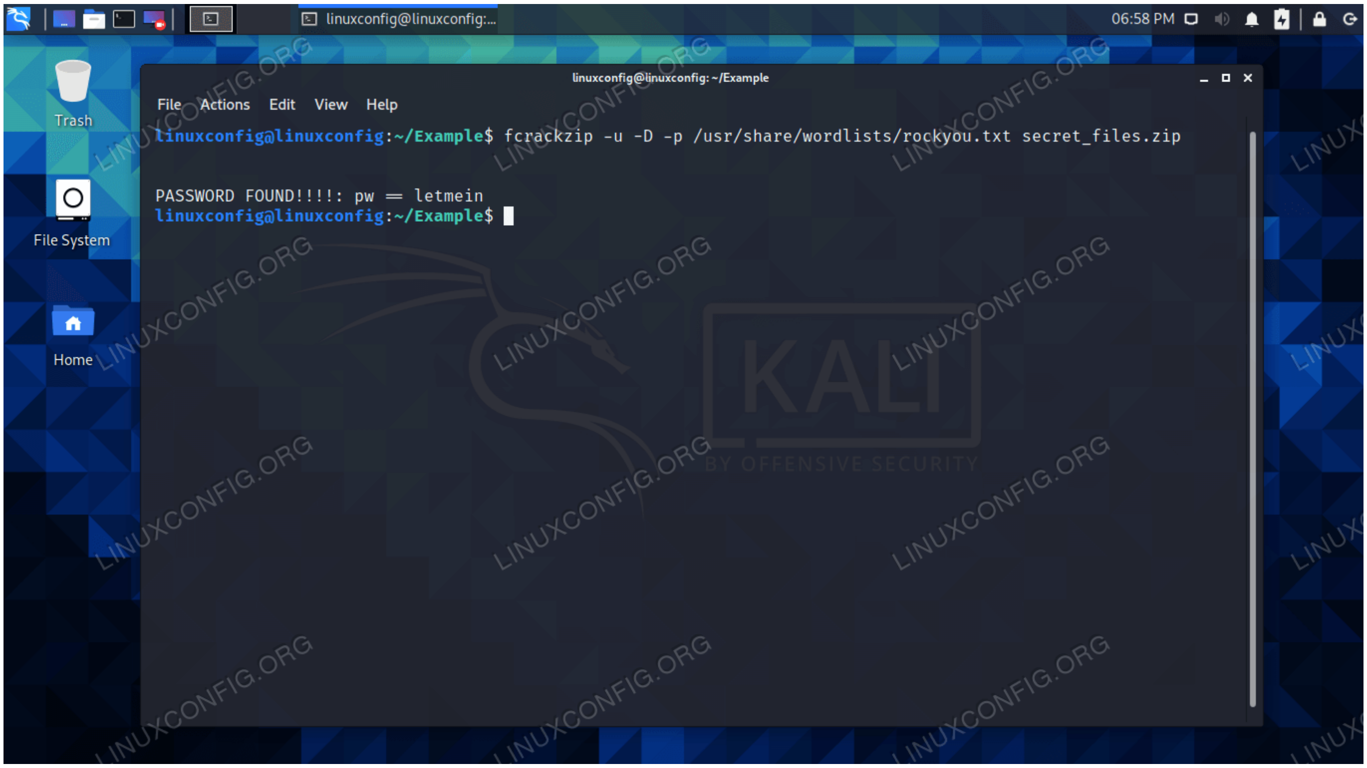
For additional options, check John's help output.

```
$ john --help
```

Crack zip password with fcrackzip

Step 1 To use fcrackzip with the rockyou.txt wordlist, use the following command syntax. There's no need to generate a hash file, as there was with John.

```
$ fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt secret_files.zip
```



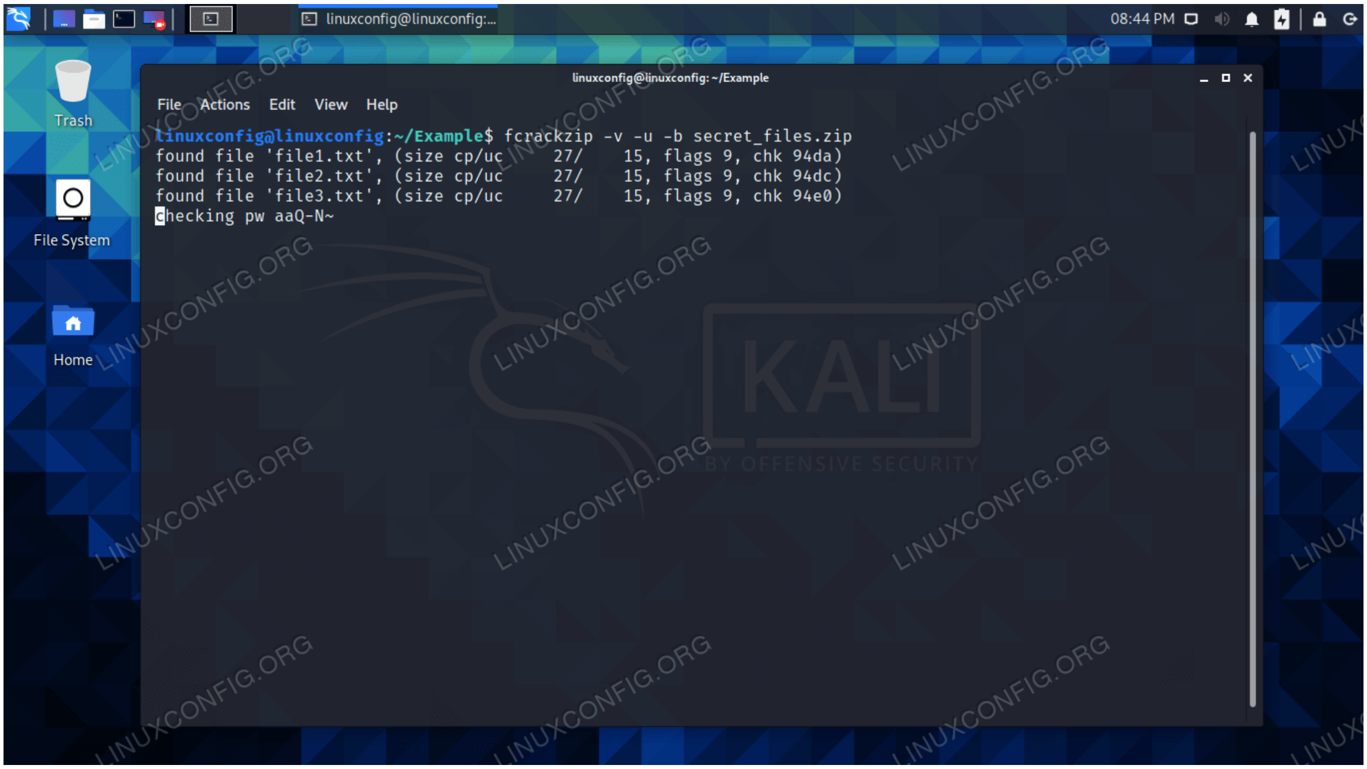
```
linuxconfig@linuxconfig:~/Example$ fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt secret_files.zip


PASSWORD FOUND!!!!: pw == letmein
linuxconfig@linuxconfig:~/Example$ 
```

fcrackzip has found the correct password

Step 2 To use a brute force attack, you can use the `-b` option. It works well with the `-v` (verbose) option, so you can see what password it's currently testing. This method will probably take a very long time, as it just tests for random strings, instead of common passwords.

```
$ fcrackzip -v -u -b secret_files.zip
```



08:44 PM
linuxconfig@linuxconfig:...
linuxconfig@linuxconfig: ~/Example
File
Actions
Edit
View
Help
Trash
File System
Home

```
linuxconfig@linuxconfig:~/Example$ fcrackzip -v -u -b secret_files.zip
found file 'file1.txt', (size cp/uc     27/    15, flags 9, chk 94da)
found file 'file2.txt', (size cp/uc     27/    15, flags 9, chk 94dc)
found file 'file3.txt', (size cp/uc     27/    15, flags 9, chk 94e0)
checking pw aaQ-N~
```

Brute force method with verbose option in fcrackzip

If you don’t have any luck, you can always try a different wordlist. A customized one with suspected passwords is always going to work best. To see more options for fcrackzip, run the following command.

```
$ fcrackzip -help
```

Closing Thoughts

In this guide, we saw two tools on Kali Linux that can be used to crack password protected zip files. We also learned about how to use various wordlists with these tools, which can accelerate the process.

A strong password is still going to be tough to crack, and may take your system a long time to finally come up with the password. Weaker passwords can normally be cracked in a short time by either John the Ripper or fcrackzip.

Related Linux Tutorials:

- List of best Kali Linux tools for penetration...
- How to create compressed encrypted archives with tar and gpg
- How to split zip archive into multiple blocks of a...
- Zip folder in Linux
- How to use zip on Linux
- How to dual boot Kali Linux and Windows 10
- How to install Kali Linux in VMware
- Beginner's guide to compression with xz on Linux
- How to create and manipulate tar archives using Python
- How to search for extra hacking tools on Kali

Kali Linux

commands, filesystem, kali, security

How to install pip on Kali Linux

How to dual boot Kali Linux and Windows 10

NEWSLETTER

Subscribe to Linux Career Newsletter to receive latest news, jobs, career advice and featured configuration tutorials.

SUBSCRIBE

WRITE FOR US

LinuxConfig is looking for a technical writer(s) geared towards GNU/Linux and FLOSS technologies. Your articles will feature various GNU/Linux configuration tutorials and FLOSS technologies used in combination with GNU/Linux operating system.

When writing your articles you will be expected to be able to keep up with a technological advancement regarding the above mentioned technical area of expertise. You will work independently and be able to produce at minimum 2 technical articles a month.

APPLY NOW

CONTACT US

web (at) linuxconfig (dot) org

TAGS

18.04 administration apache applications backup bash beginner browser centos centos8 commands database debian desktop development docker fedora filesystem firewall gaming gnome Hardware installation java kali manjaro multimedia networking nvidia programming python redhat rhel8 scripting security server ssh storage terminal ubuntu ubuntu 20.04 video virtualization webapp webserver

FEATURED TUTORIALS

How to install the NVIDIA drivers on Ubuntu 20.04 Focal Fossa Linux

Bash Scripting Tutorial for Beginners

How to check CentOS version

How to find my IP address on Ubuntu 20.04 Focal Fossa Linux

Ubuntu 20.04 Remote Desktop Access from Windows 10

Howto mount USB drive in Linux

How to install missing ifconfig command on Debian Linux

AMD Radeon Ubuntu 20.04 Driver Installation

Ubuntu Static IP configuration

How to use bash array in a shell script

Linux IP forwarding – How to Disable/Enable

How to install Tweak Tool on Ubuntu 20.04 LTS Focal Fossa Linux

How to enable/disable firewall on Ubuntu 18.04 Bionic Beaver Linux

Netplan static IP on Ubuntu configuration

How to change from default to alternative Python version on Debian Linux

Set Kali root password and enable root login

How to Install Adobe Acrobat Reader on Ubuntu 20.04 Focal Fossa Linux

How to install the NVIDIA drivers on Ubuntu 18.04 Bionic Beaver Linux

How to check NVIDIA driver version on your Linux system

Nvidia RTX 3080 Ethereum Hashrate and Mining Overclock settings on HiveOS Linux

LATEST TUTORIALS

How to build a Tkinter application using an object oriented approach

How to disable SElinux on CentOS 7

Getting started with Tkinter for Python tutorial

Zsh shell installation and configuration on Linux

How to use LUKS with a detached header

How to scrape web pages from the command line using htmlq

How to install and manage fonts on Linux

Kali http server setup

yt-dlp vs youtube-dl

How to manage Bash history

How to install the NVIDIA drivers on Ubuntu 22.04

How to create a flatpak package

How to set, change and delete music tags with Mutagen

Introduction to MySQL storage engines

Introduction to crypttab with examples

How to create temporary files using mktemp on Linux

How to crash Linux

How to build an initramfs using Dracut on Linux

How to uncompress and list an initramfs content on Linux

How to install PipeWire on Ubuntu Linux