



TUTORIAL

Create Wordlists with Crunch

BY TRT 11/2/15 1:11 PM 1/16/16 8:55 AM

Greetings all. Before I get into the tutorial, I would like to mention that I am fairly new to Null Byte (been lurking for some time though), and what really appeals to me about this place is its tight, family-like community where everyone is always willing to help each other and the constant search for knowledge that inhabits this subdomain is a driving motivator for me to join in. I'm glad I arrived at the right time. Anyway, **wipes tears** (not really)...

This is a tutorial for newbies and anyone who hasn't yet used Crunch before. Crunch is a utility that is used to create wordlists using letters, numbers, and symbols for every possible combination or according to specific rules. I will be covering this command-line tool in great depth, dissecting each option and demonstrating its purpose. So to start off, in this demonstration I will not assume that you have a particular OS, other than to mention that I will only be covering those based on UNIX.

To begin with, [download Crunch](#) and navigate to the downloaded tgz file in Terminal. Then unzip the tgz file and install crunch.

```
> cd /path/to/folder/containing/crunch-3.6.tgz
```

```
> tar -xf crunch-3.6.tgz
> cd crunch-3.6 && make && make install
```

So now you can call the *crunch* command from anywhere in the Terminal app. Great, so now that it's out of the way, let's get straight into the usage. The syntax for Crunch is:

```
> crunch min max charset options
```

The *min* and *max* are the minimum and maximum lengths (respectively) for your desired wordlist. By default *charset* is not required, but you can use it to limit the characters of your wordlist to the ones you specify. If you choose to use *charset* then you must maintain the correct order, which is lowUP123@%# (lowercase letters, then uppercase letters, then numbers and finally symbols). You can skip any of them, but the order must always remain the same. Example:

```
> crunch 2 6 qrs347
```

The command above will produce a wordlist for every possible combination of the characters qrs347 from 2 to 6 characters in length.

Now let's look at the options.

- b : the maximum size of the wordlist (requires -o START)
- c : numbers of lines to write to the wordlist (requires -o START)
- d : limit the number of duplicate characters
- e : stop generating words at a certain string
- f : specify a list of character sets from the charset.lst file
- i : invert the order of characters in the wordlist
- l : allows the literal interpretation of @,%^ when using -t
- o : the output wordlist file
- p : print permutations without repeating characters (cannot be used with -s)
- q : Like the -p option except it reads the strings from a specified file
- r : resume a previous session (cannot be used with -s)
- s : specify a particular string to begin the wordlist with
- t : set a specific pattern of @,%^
- z : compress the output wordlist file, accompanied by -o

Reference:

@ represents lowercase letters

, represents uppercase letters
% represents numbers
^ represents special characters

Examples:

1) > crunch 5 5 abcde14 -t @@@14 -d 2@ -o syskey.txt -z

A zipped syskey.txt wordlist starting with "aab14" and ending in "eed14" will be produced from the above. The reason why the start is not "aaa14" is because -d 2@ allows for only 2 duplicate lowercase letters. Adding -i would invert the results, and adding -e dde14 would stop after the line "dde14" (or "41edd" in the case of an inverted output) is produced.

2) > crunch 5 5 bcopuw2468 -s cow28 -c 33 -b 20mb -o START

The above will result in a 20mb text file and containing combinations for bcopuw2468 starting with "cow28" and ending on the 33rd line of the theoretical outcome.

3) > crunch 2 4 -p kite sky car -o owl.txt

In this example the words 'kite' 'sky' and 'car' will be printed in all orders possible (wholly, not by letter) and outputted into output owl.txt without taking into account the min and max numbers. None of the words will be repeated. If only one word is included, it will be used as a character set. You could use -q instead of -p to extract words from a specific file.

4) > crunch 6 6 -t @^42%3 -l a^aaaa -o art.txt

In this case Crunch will treat the ^ symbol as itself, rather than a representative of a special character. The sequence will commence with "a^4213" and end in "z^4293" and the output art.txt will be produced.

5) > crunch 4 6 -f /path/to/charset.lst -o words.txt

Assume the situation where you enter the above command and then decide to pause the process midway. When you come back later, you may restore the session by adding -r option to the syntax, while keeping the rest exactly the same.

If you still feel the need to mud your feet by reading paragraphs of illustrations and explanations for eons, you may type...

> man crunch

...to view the Crunch manual, but there's no need since we've just examined it from head to toe.

Now that we have it all covered, you have access to limitless ways in which you could use Crunch during a penetration test. One could obviously point out that it acts great as a password generator, so in turn being useful for password cracking using let's say Hydra or John. I will divulge all of the uses of wordlists in a future tutorial, and other utilities that you could use to perfect the relevance of the contents of said wordlists, thereby enabling a more thorough approach to password cracking or other similar scenarios.

Before concluding this how-to, I would like to mention that I will be prolonging this series to cover many different tools used in the sphere of hacking, and possibly a future series relating to privacy and how it can be achieved in an effective way. Please feel free to add suggestions to anything. I'm more than happy to receive feedback.

That's it for today, I hope you all learned the ins and outs of the tool Crunch, and expect many similar tutorials in the coming days/weeks.

TRT

Just updated your iPhone? You'll find new features for Podcasts, News, Books, and TV, as well as important security improvements and fresh wallpapers. [Find out what's new and changed on your iPhone with the iOS 17.5 update.](#)

[WonderHowTo.com](#) [About Us](#) [Terms of Use](#) [Privacy Policy](#)

Don't Miss:

All the New iOS 16.5 Features for iPhone You Need to Know About
Your iPhone Has a Secret Button That Can Run Hundreds of Actions
7 Hidden iPhone Apps You Didn't Know Existed

You're Taking Screenshots Wrong — Here Are Better Ways to Capture Your iPhone's Screen
Keep Your Night Vision Sharp with the iPhone's Hidden Red Screen
Your iPhone Finally Has a Feature That Macs Have Had for Almost 40 Years
If You Wear Headphones with Your iPhone, You Need to Know About This

By using this site you acknowledge and agree to our terms of use & privacy policy.

We do not sell personal information to 3rd parties.