

Forum: [Hack Forums](#)

Thread: [PASSWORD CRACKING - CREATE THE BEST BRUTE FORCE WORDLIST](#)

OxaByte - May 28, 2020, 8:19 am

This tutorial will show you how to create the BEST wordlist for fast bruteforce password cracking. This should be used if dict attacks have failed.

As with all my tutorials - USE LINUX. There is no reason not to, it takes 30 minutes and its way better for hacking. It also uses way less system resources, which is important for stuff like password cracking as it's resource intensive. If you can't set linux up just post/PM and I'll help.

1) get Crunch - type in terminal: `sudo apt-get install crunch`

2) You use crunch like this: `crunch <min> <max> <charset> -t <pattern> -o <filename.lst>`

min = minimum length of the password

max = maximum length of the password

Charset = Which characters you want to add in your wordlist like abcdefghijklmnopqrstuvwxyz or 1234567890. You will need to do upper and lower case if you want all of them.

-t <pattern> = This is the pattern you want to follow. Lets say you saw them enter the first three letters ('cat' and know the last letter is 'x') and it's an 6 digit password, you could do something like: cat@@@x

This will make all passwords start with cat and change the characters that use @.

-o <output?> is what you want to call the output file.

3) so type: `crunch 6 6 abcdefghijklmnopqrstuvwxyz -t cat@@x -o catfile.lst`

4) type: cat catfile.lst

5) You should see something like:

catusx
catutx
catuux
catuvx
catuwx
catuxx
catuyx
catuzx
catvax
catvbx

6) you can do more complicated things with other options if you need to.

7) be careful of opening a big wordlist in an editor/terminal. It might crash your system if it's too big. There are special tools for editing them.

8) use this with your favourite password cracking program

chatteridiot - May 28, 2020, 10:17 am

Similar tool @ github.com/tp7309/TTPassGen

MightyOne - May 31, 2020, 9:58 am

This seems like a great way of creating some pass lists for brute forcing!
I got a great one im using already but its always good to know ! thanks

drtechy - May 31, 2020, 11:36 am

Where is a good place to get password list

Hex.neo - June 2, 2020, 12:44 am

Thanks, I will check this.

ragedomen - June 8, 2020, 1:16 pm

y wrote the same thats on github

H4x10r - June 8, 2020, 1:29 pm

If you really wanna have some success
use common pw wordlists.

Best source : <https://github.com/berzerk0/Probable-Wordlists>

Use them with RULES !

Best source: <https://github.com/tmsteen/Hob0Rules>

no more to say.

go away with crunch.

crunch is only helpfull if u need to generate pw lists where u at least know a bit about the pw !
then u are able to generate target specific wordlists with crunch with placeholders and stuff.

all other stuff if not needed anymore

hashcat can generate thos pws on the go.

hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a as an example.

grizzslays - June 9, 2020, 10:32 pm

I have a ton of OSINT on a specific target. I have tried Cupp and Crunch using what is available. No luck. I'm thinking they are using the default password that comes with the router does anyone have any ideas/pointers on how to generate a proper wordlist for this situation? I can pay for servers no problem just don't want it to take years via bruteforcing. I have searched for leaked passwords for the router vendor to no avail.

Any help would be greatly appreciated. Will pay for help if need be.

2xTheTap115 - June 9, 2020, 11:04 pm

(Jun 9, 2020 10:32 PM)grizzslays Wrote: [\[CITE\]](#) I have a ton of OSINT on a specific target. I have tried Cupp and Crunch using what is available. No luck. I'm thinking they are using the default

password that comes with the router does anyone have any ideas/pointers on how to generate a proper wordlist for this situation? I can pay for servers no problem just don't want it to take years via bruteforcing. I have searched for leaked passwords for the router vendor to no avail.

Any help would be greatly appreciated. Will pay for help if need be.

At the beginning I would recommend to you what exactly is the manufacturer's rule of creating default passwords (I think that googling router model should bring you relevant knowledge on this topic. If you did not know the manufacturer of this specific hardware, sites such as Macvendor will help you). Then, once you find out, you can easily generate the right dictionary. If your machine you are working on is inefficient, I recommend using GPUhash.me for a small fee in BTC in a relatively short time you can crack such a password (of course not in every case, although my experience with this site shows that its efficiency is some 85%). In addition, I recommend you take a look at my short tutorial on how to generate dictionaries:

[Creating dictionaries based on information from OSINT - Tutorial part 1](#)

[Creating dictionaries based on information from OSINT - Tutorial part 2](#)

I hope it helps you. greetings??

UnreleasedSTL - July 16, 2020, 7:19 am

hopefully this helps, i been really trying to find a good place to find a list for bruteforcing