

Forum: [Hack Forums](#)

Thread: [\[Help\] Piping Crunch with Hashcat](#)

LulSecurity - July 31, 2015, 12:25 pm

Hey guys I've been trying to Pipe Crunch to Hashcat for a while now, and nothing has worked I've used "crunch 1 3 ABC | Hashcat -m 0 -a 0 [file name]" I have also tried doing it in reverse, I've searched Google and haven't found anything useful. Any help would be appreciated :)

Hydra - August 1, 2015, 2:58 am

Hashcat got an implement function called mask attack. Take a look at it here:

http://hashcat.net/wiki/doku.php?id=mask_attack

I think it will help you.

LulSecurity - August 1, 2015, 9:14 am

So if I was to insert:

```
Code hashcat -m 500 -a 3 -1 a? /root/hashes/hash.txt --increment ?a?a?a?a?a?a? -o /root/Desktop/happy.txt
```

Would this basically go through every combination (alpha-numeric)

Hydra - August 1, 2015, 9:31 am

```
Code hashcat -m 500 -a 3 /root/hashes/hash.txt -i ?a?a?a?a?a?a -o /root/Desktop/happy.txt
```

Mix-Alpha-Numeric-Symbol from 1 to 6 digits.

You can specify the charset:

```
?l = abcdefghijklmnopqrstuvwxyz  
?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ  
?d = 0123456789  
?s = !"#$%&'()*+,-./:;<=>?@[\\]^_`{|}~  
?a = ?l?u?d?s
```

LulSecurity - August 1, 2015, 9:39 am

Alright, But would using Code -1 ?a be the same as using Code --custom-charset1=?l?u?d?s

Hydra - August 1, 2015, 10:09 am

(Aug 1, 2015 09:39 AM)LulSecurity Wrote: [\[CITE\]](#) Alright, But would using Code -1 ?a be the same as using Code --custom-charset1=?l?u?d?s

yes. You can use custom charsets if you want to bruteforce upper, lower and numbers (?u?l?d) without the symbols. Then you use the custom charset "-1 ?u?l?d" and use the mask ?1?1?1?1?1?1

You can read everything about maskattack and charsets here:

http://hashcat.net/wiki/doku.php?id=mask_attack

LulSecurity - August 1, 2015, 10:33 am

Thank you for all the help you've offered ??

I have one last question. What would be the fast way to crack a hash?

Since I don't want to wait 12 hours to crack a hash :P but if there isn't any other way I have no problem waiting.

LSDoom - August 1, 2015, 11:20 am

(Aug 1, 2015 10:33 AM)LulSecurity Wrote: [\[CITE\]](#) Thank you for all the help you've offered ??

I have one last question. What would be the fast way to crack a hash?

Since I don't want to wait 12 hours to crack a hash :P but if there isn't any other way I have no problem waiting.

Fastest way is a straight dictionary attack, unless you know the exact layout. If you know the password layout you can use a mask to get it.

After that dictionary attacks with rules, then just use more advanced rules as the simple ones fail.

Then mask attacks with common masks and finally a straight brute-force attack. A straight brute-force attack will most likely take a very long time depending on your rig and password length, but you will be able to crack any password that ever existed (In theory). It might take 1 billion years, but it is going to crack at some point.