

Forum:[Hack Forums](#)

Thread: [\[TUT\] Script to generate every possible password up to 8 characters \(for bruteforce\)](#)

Fr0st_Byte - July 13, 2011, 9:00 pm

So I was messing with Hydra, trying to brute force access via SSH the other day. And suddenly, had a thought:

"What if I have every possible password? Yea, it'd take fucking forever, but it would eventually find it..."

So I did some googling, and found this perl script. It will generate every possible password for a password from 1 to 8 characters long (which could be edited for more characters).

Here's the thing. This script makes MASSIVELY HUGE word lists. Think about this:

Every possible four letter password in a text file means literally 78,074,896 "words", which is equal to 372.3 MB. Holly shit. 8 character password lists are WELL over 100 GB. It utilizes every possible password of a set character length with the following possible characters:

a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ` 1 2 3 4 5 6 7 8 9 0 - = [] \ ; ' , . / ~ ! @ # \$ % ^ & * () _ + { } | : " < > ?

I have my Ubuntu partition with 160 GB. I tried making a 8 letter password list with this, and I literally had to stop because I was running out of space (df -h told me I had 2% left, whereas before running I had 3% USED.)

So, here is the script for a great brute-force password list. Yea, brute-force takes forever, but these lists can't be beat.

Save the following code as "whatever.pl". Then (*Nix) run "chmod +x whatever.pl". To use, run this:

```
./whatever.pl X >OUTPUT.txt
```

Where X is the number of characters of each password in the list (8 maximum!!!!) and OUTPUT.txt is the saved file.

The more the number of characters per password, the longer it will take.

Code `#!/usr/bin/perl`

```
if ( ${#ARGV} < 0 ) {  
    print "\nUsage: $0 password_length\n";  
    print "Only 8 characters please. This is\n";  
    print "going to take a long time as it is!\n";  
    exit(1);  
}
```

```
$pass_length = $ARGV[0];
```

@94 = qw(a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ` 1 2 3 4 5 6 7 8 9 0 - = [] \ ; ' , . / ~ ! @ # \$ % ^ & * () _ + { } | : " < > ?);

```
if ( $pass_length < 1 || $pass_length > 8 ) {  
    print "Usage: $0 password_length\n";  
    print "Only 8 characters max please. This is\n";  
    print "going to take a long enough time as it is!\n";  
}
```

```
$a = $b = $c = $d = $e = $f = $g = $h = 94;
```

```
if ( $pass_length == 8 ) {  
    for ($a=0;$a<94;$a++) { for ($b=0;$b<94;$b++) { for ($c=0;$c<94;$c++) { for ($d=0;$d<94;$d++) {  
for ($e=0;$e<94;$e++) { for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {  
    printf("%s%s%s%s%s%s%s%s\n", $94[$a], $94[$b], $94[$c], $94[$d], $94[$e], $94[$f], $94[$g],  
$94[$h]);  
    } } } } } } } }  
} elsif ( $pass_length == 7 ) {  
    for ($b=0;$b<94;$b++) { for ($c=0;$c<94;$c++) { for ($d=0;$d<94;$d++) { for ($e=0;$e<94;$e++) {  
for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {  
    printf("%s%s%s%s%s%s%s\n", $94[$b], $94[$c], $94[$d], $94[$e], $94[$f], $94[$g], $94[$h]);  
    } } } } } } }  
} elsif ( $pass_length == 6 ) {  
    for ($c=0;$c<94;$c++) { for ($d=0;$d<94;$d++) { for ($e=0;$e<94;$e++) { for ($f=0;$f<94;$f++) { for  
($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {  
    printf("%s%s%s%s%s%s\n", $94[$c], $94[$d], $94[$e], $94[$f], $94[$g], $94[$h]);  
    } } } } } }  
} elsif ( $pass_length == 5 ) {  
    for ($d=0;$d<94;$d++) { for ($e=0;$e<94;$e++) { for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) {  
for ($h=0;$h<94;$h++) {  
    printf("%s%s%s%s%s\n", $94[$d], $94[$e], $94[$f], $94[$g], $94[$h]);  
    } } } } }  
} elsif ( $pass_length == 4 ) {  
    for ($e=0;$e<94;$e++) { for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {  
    printf("%s%s%s%s\n", $94[$e], $94[$f], $94[$g], $94[$h]);  
    } } } }  
} elsif ( $pass_length == 3 ) {  
    for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {  
    printf("%s%s%s\n", $94[$f], $94[$g], $94[$h]);  
    } } }  
} elsif ( $pass_length == 2 ) {  
    for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {  
    printf("%s%s\n", $94[$g], $94[$h]);  
    } }  
} elsif ( $pass_length == 1 ) {  
    for ($h=0;$h<94;$h++) {  
    printf("%s\n", $94[$h]);  
    }  
}
```

Pseudonym - July 14, 2011, 3:27 am

(Jul 13, 2011 09:00 PM)Kotto*N[ix]mouth Wrote: [\[CITE\]](#) Spoiler [\(Click to View\)](#)

So I was messing with Hydra, trying to brute force access via SSH the other day. And suddenly, had a thought:

"What if I have every possible password? Yea, it'd take fucking forever, but it would eventually find it..."

So I did some googling, and found this perl script. It will generate every possible password for a password from 1 to 8 characters long (which could be edited for more characters).

Here's the thing. This script makes MASSIVELY HUGE word lists. Think about this:

Every possible four letter password in a text file means literally 78,074,896 "words", which is equal to 372.3 MB. Holly shit. 8 character password lists are WELL over 100 GB. It utilizes every possible password of a set character length with the following possible characters:

a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ` 1 2 3 4 5 6 7 8 9 0 - = [] \ ; ' , . / ~ ! @ # \$ % ^ & * () _ + { } | : " < > ?

I have my Ubuntu partition with 160 GB. I tried making a 8 letter password list with this, and I literally had to stop because I was running out of space (df -h told me I had 2% left, whereas before running I had 3% USED.)

So, here is the script for a great brute-force password list. Yea, brute-force takes forever, but these lists can't be beat.

Save the following code as "whatever.pl". Then (*Nix) run "chmod +x whatever.pl". To use, run this:

```
./whatever.pl X >OUTPUT.txt
```

Where X is the number of characters of each password in the list (8 maximum!!!!) and OUTPUT.txt is the saved file.

The more the number of characters per password, the longer it will take.

Code `#!/usr/bin/perl`

```
if ( ${#ARGV} < 0 ) {  
    print "\nUsage: $0 password_length\n";  
    print "Only 8 characters please. This is\n";  
    print "going to take a long time as it is!\n";  
    exit(1);  
}
```

```
$pass_length = $ARGV[0];
```

```
@94 = qw(a b c d e f g h i j k l m n o p q r s t u v w x y z A B C D E F G H I J K L M N O P Q R S T  
U V W X Y Z ` 1 2 3 4 5 6 7 8 9 0 - = [ ] \ ; ' , . / ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ?);
```

```
if ( $pass_length < 1 || $pass_length > 8 ) {  
    print "Usage: $0 password_length\n";  
    print "Only 8 characters max please. This is\n";  
    print "going to take a long enough time as it is!\n";  
}
```

```
$a = $b = $c = $d = $e = $f = $g = $h = 94;
```

```
if ( $pass_length == 8 ) {
    for ($a=0;$a<94;$a++) { for ($b=0;$b<94;$b++) { for ($c=0;$c<94;$c++) { for ($d=0;$d<94;$d++) {
for ($e=0;$e<94;$e++) { for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {
    printf("%s%s%s%s%s%s%s%s\n", $94[$a], $94[$b], $94[$c], $94[$d], $94[$e], $94[$f], $94[$g],
$94[$h]);
    } }
    } elseif ( $pass_length == 7 ) {
        for ($b=0;$b<94;$b++) { for ($c=0;$c<94;$c++) { for ($d=0;$d<94;$d++) { for ($e=0;$e<94;$e++) {
for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {
            printf("%s%s%s%s%s%s%s\n", $94[$b], $94[$c], $94[$d], $94[$e], $94[$f], $94[$g], $94[$h]);
            } }
        } elseif ( $pass_length == 6 ) {
            for ($c=0;$c<94;$c++) { for ($d=0;$d<94;$d++) { for ($e=0;$e<94;$e++) { for ($f=0;$f<94;$f++) { for
($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {
                printf("%s%s%s%s%s%s\n", $94[$c], $94[$d], $94[$e], $94[$f], $94[$g], $94[$h]);
                } }
            } elseif ( $pass_length == 5 ) {
                for ($d=0;$d<94;$d++) { for ($e=0;$e<94;$e++) { for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) {
for ($h=0;$h<94;$h++) {
                    printf("%s%s%s%s%s\n", $94[$d], $94[$e], $94[$f], $94[$g], $94[$h]);
                    } }
                } elseif ( $pass_length == 4 ) {
                    for ($e=0;$e<94;$e++) { for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {
                        printf("%s%s%s%s\n", $94[$e], $94[$f], $94[$g], $94[$h]);
                        } } }
                    } elseif ( $pass_length == 3 ) {
                        for ($f=0;$f<94;$f++) { for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {
                            printf("%s%s%s\n", $94[$f], $94[$g], $94[$h]);
                            } } }
                    } elseif ( $pass_length == 2 ) {
                        for ($g=0;$g<94;$g++) { for ($h=0;$h<94;$h++) {
                            printf("%s%s\n", $94[$g], $94[$h]);
                            } }
                    } elseif ( $pass_length == 1 ) {
                        for ($h=0;$h<94;$h++) {
                            printf("%s\n", $94[$h]);
                        }
                    }
                }Dam it sended itself before I wrote it, wait for edit
            }
        }
    }
}
```

EDIT: nvm, I had electricity blackout before I was able to send it, not gonna write it all again.
Just maybe instead for (\$h=0;\$h<94;\$h++) you can write foreach \$h (@94) .

creepycreeper - July 14, 2011, 5:37 am

Hi perl noobs:

im gonna show you how python does it:

no assload of nested loops, only recursion:

PHP Code

```
<?php
```

```
def generate(charlist,state,position):
```

```
for i in charlist:
    state[position] = i
    if position == (len(state)-1):
        print "".join(state)
    else:
        generate(charlist,state,position+1)
use as:
PHP Code
<?php
generate("1234567890qwertyuiopasdfghjklzxcvbnm",[None]*8,0)
```

EDIT

rewrite it to the Perl if you please :D... and, sorry for that, but I just have to say it: Pwned N00bs!

EDIT2:

that mybb screwed my indentation

The Elite Noob - July 14, 2011, 6:17 am

hmm, i would love to try a recursive solution, maybe i will,
also OP, nice script mate!

edit ok this is harder then i thought...

well anyways nice job creepycreeper.

Fr0st_Byte - July 14, 2011, 11:05 am

(Jul 14, 2011 05:37 AM)creepycreeper Wrote: [\[CITE\]](#) Hi perl noobs:

im gonna show you how python does it:

no assload of nested loops, only recursion:

PHP Code

```
<?php
def generate(charlist,state,position):
    for i in charlist:
        state[position] = i
        if position == (len(state)-1):
            print "".join(state)
        else:
            generate(charlist,state,position+1)
use as:
PHP Code
<?php
generate("1234567890qwertyuiopasdfghjklzxcvbnm",[None]*8,0)
```

EDIT

rewrite it to the Perl if you please :D... and, sorry for that, but I just have to say it: Pwned N00bs!

EDIT2:

that mybb screwed my indentation

Like I told you, I found this script online. So bite your smart-ass tongue.

creepycreeper - July 14, 2011, 11:17 am

(Jul 14, 2011 11:05 AM)Kotto*N[ix]mouth Wrote: [\[CITE\]](#) Like I told you, I found this script online. So bite your smart-ass tongue.Well, at least I'm smart ass and not dumb-ass like you are, because you weren't even able to write it yourself. It's kinda lame to post other people's code as tutorial too... In

other words - neg rep more, noob

Fr0st_Byte - July 14, 2011, 11:20 am

(Jul 14, 2011 11:17 AM)creepycreeper Wrote: [\[CITE\]](#) Well, at least I'm smart ass and not dumb-ass like you are, because you weren't even able to write it yourself. It's kinda lame to post other people's code as tutorial too... In other words - neg rep more, noob

I'm a dumb-ass? Imfao, because I don't waste my day's learning "Perl", because I have a life and don't waste hours upon hours online, I'm a dumb-ass? You're so clever!

creepycreeper - July 14, 2011, 11:25 am

(Jul 14, 2011 11:20 AM)Kotto*N[ix]mouth Wrote: [\[CITE\]](#) I'm a dumb-ass? Imfao, because I don't waste my day's learning "Perl", because I have a life and don't waste hours upon hours online, I'm a dumb-ass? You're so clever!No, you are dumbass, coz you post tutorials on stuff you know nothing about. And yes, I AM clever

Fr0st_Byte - July 14, 2011, 11:29 am

(Jul 14, 2011 11:25 AM)creepycreeper Wrote: [\[CITE\]](#) No, you are dumbass, coz you post tutorials on stuff you know nothing about. And yes, I AM clever

Oh okay. You have posted NOTHING. NO threads. I have tutorials on shit you know nothing about. So don't flame me for posting a thread, when you haven't contributed to this forum at all! You're just some computer geek who found HF and thought "hey this is cool, I'm gonna learn to hack so I can fuck with my friends facebook!" You don't do shit here so GTFO. For ruining one of my threads, any threads I see you post that are not in the lounge-retard's area I'll do exactly what you've done here.

vive facile - July 14, 2011, 11:30 am

(Jul 14, 2011 05:37 AM)creepycreeper Wrote: [\[CITE\]](#) PHP Code
<?php

```
def generate(charlist,state,position):  
    for i in charlist:  
        state[position] = i  
        if position == (len(state)-1):  
            print "".join(state)  
        else:  
            generate(charlist,state,position+1)
```

Very nice, neat, simple, efficient code creepeycrepper, kudos to you.

creepycreeper - July 14, 2011, 12:27 pm

(Jul 14, 2011 11:29 AM)Kotto*N[ix]mouth Wrote: [\[CITE\]](#) Oh okay. You have posted NOTHING. NO threads. I have tutorials on shit you know nothing about. So don't flame me for posting a thread, when you haven't contributed to this forum at all! You're just some computer geek who found HF and thought "hey this is cool, I'm gonna learn to hack so I can fuck with my friends facebook!" You don't do shit here so GTFO. For ruining one of my threads, any threads I see you post that are not in the lounge-retard's area I'll do exactly what you've done here.let's analyse some parts of your post (I really love doing that):

"You have posted NOTHING."

- except for a code that's better then code, that you posted

"So don't flame me for posting a thread, when you haven't contributed to this forum at all!"

I didn't start flaming, I just posted better way to do it and called you noob(which, as you even later said, you in Perl are). Flaming started when you called me smartass and neg repped me. ad. contribution - what was my code then?

"You're just some computer geek who found HF and thought "hey this is cool, I'm gonna learn to hack so I can fuck with my friends facebook!""
lol, i'm strict white hat and i'm not even using FB

"For ruining one of my threads, any threads I see you post that are not in the lounge-retard's area I'll do exactly what you've done here."

first of all, i didn't ruin it, I imporved it.

ad. you doing to me the same thing I did you: I'm really looking forward for it, I always want to learn from people, who are moe experienced then me. However, I really doubt that this time will ever come, coz apparently, judging from what you've showed here and from your forum threads you are just skiddo with no original ideas.

Fr0st_Byte - July 14, 2011, 12:50 pm

(Jul 14, 2011 12:27 PM)creepycreeper Wrote: [\[CITE\]](#) let's analyse some parts of your post (I really love doing that):

"You have posted NOTHING."

- except for a code that's better then code, that you posted

"So don't flame me for posting a thread, when you haven't contributed to this forum at all!"

I didn't start flaming, I just posted better way to do it and called you noob(which, as you even later said, you in Perl are). Flaming started when you called me smartass and neg repped me. ad. contribution - what was my code then?

"You're just some computer geek who found HF and thought "hey this is cool, I'm gonna learn to hack so I can fuck with my friends facebook!""
lol, i'm strict white hat and i'm not even using FB

"For ruining one of my threads, any threads I see you post that are not in the lounge-retard's area I'll do exactly what you've done here."

first of all, i didn't ruin it, I imporved it.

ad. you doing to me the same thing I did you: I'm really looking forward for it, I always want to learn from people, who are moe experienced then me. However, I really doubt that this time will ever come, coz apparently, judging from what you've showed here and from your forum threads you are just skiddo with no original ideas.

Good show.

I agree with some parts, being honest with you. But, the insults, I don't. Lol, flame me all you want for this post. I like this one quoted above me ?

I just had my nicotine and breakfast, so I'm in a much better mood than I was, and I apologize for my harsh reaction (although I don't appreciate being called a noob in any sense).

The last part of your post, I do take deep offense too.

If you look through my posts, you'll see that for the most part I'm a very passive poster. Non-aggressive. So, no, I'm not backing down from you or anything like that. I still don't agree with you. But I'm not doing this. It's not worth either of our time.

Thank you for posting the refreshment of code. Maybe me saying it was a "tut" was a misleading title, because I didn't teach anything. I have never posted in the Perl section, and know nothing about it.

I believe I'll remove my neg rep, if you can reply without arguing more. This is stupid.

Your post was not my influence to my response. I'm just more awake now, more myself. Trying to be a bigger man than I was earlier, hope you understand.

creepycreeper - July 14, 2011, 1:19 pm

hehe, I wasn't really polite either and overreacted a bit (maybe a lot). I don't really want to have bad blood with anybody I just sometimes like to argue (not really healthy thing to do, but I'm just too good at it). I apologize for calling you dumbass and skiddo too, and maybe I'll really learn something from you, coz I know literary nothing about Metasploit :).

I hope the thing is cleared between us now.

P.S.: don't dare to remove that neg rep from me - with negative I look more badass (i mean it)

+++Ares+++ - July 14, 2011, 7:58 pm

nice mate...keep it up :))

Saustin - July 14, 2011, 10:20 pm

Cool, I might use this code later. Thanks.

PS you two should stop fighting, and creepycreeper I hope you realize he can -3 not just -1 you. Fighting on hackforums is downright retarded, so please stop for everyone's sake.

Fr0st_Byte - July 14, 2011, 10:49 pm

(Jul 14, 2011 10:20 PM)Saustin Wrote: [\[CITE\]](#) Cool, I might use this code later. Thanks.

PS you two should stop fighting, and creepycreeper I hope you realize he can -3 not just -1 you. Fighting on hackforums is downright retarded, so please stop for everyone's sake.

We did. We're cool now lol.

creepycreeper - July 14, 2011, 11:58 pm

(Jul 14, 2011 10:49 PM)Kotto*N[ix]mouth Wrote: [\[CITE\]](#) We did. We're cool now lol.Indeed.

@everyone

By, the way, the code that I posted earlier was in python, and therefore not really fast - I have rewritten it to the C (more than 10 times faster, lol) and made it part of light-hearted introduction to recursion - <https://hackforums.net/showthread.php?tid=1483562> . It focuses on recursion, not password generation, though.