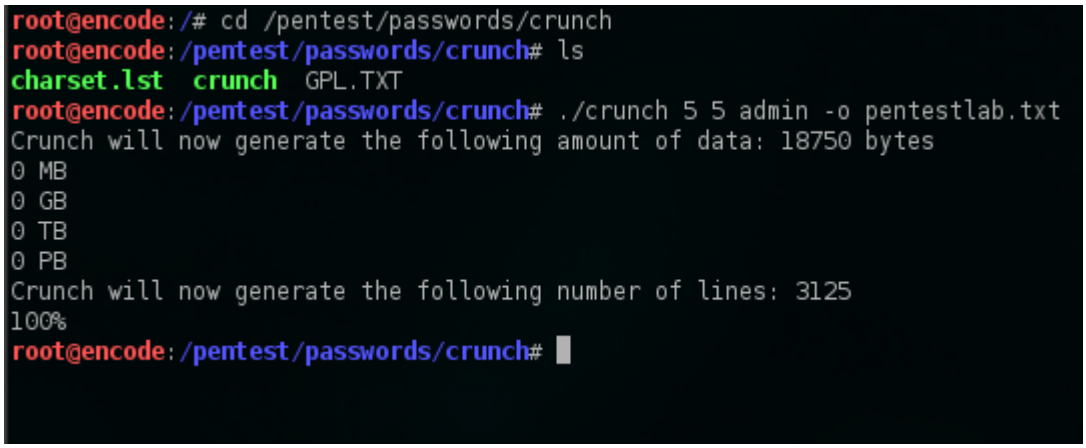
Creating Wordlists With Crunch

pentestlab.blog/category/tools/page/7

July 12, 2012



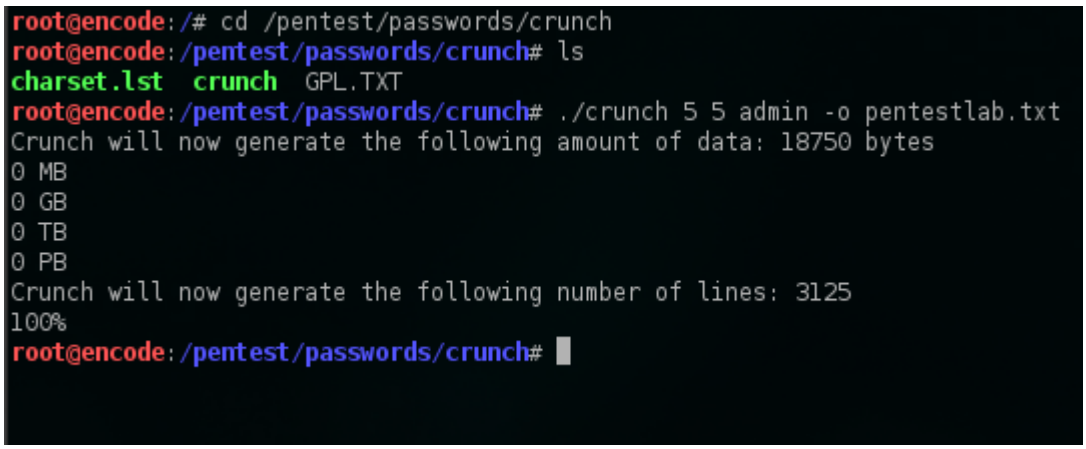
Many times in penetration testing engagements you will discover authentication forms that you will need to bypass in order to gain access to an application or to a remote system.Having a big and a good wordlists always help but as a penetration tester you must be able to create your own custom wordlists depending on the situation.There are a variety of tools that can assist you on this but here we will focus on Crunch.

Create a Sample Wordlist

The first thing that you need to do is to open terminal and write **cd /pentest/passwords/crunch**

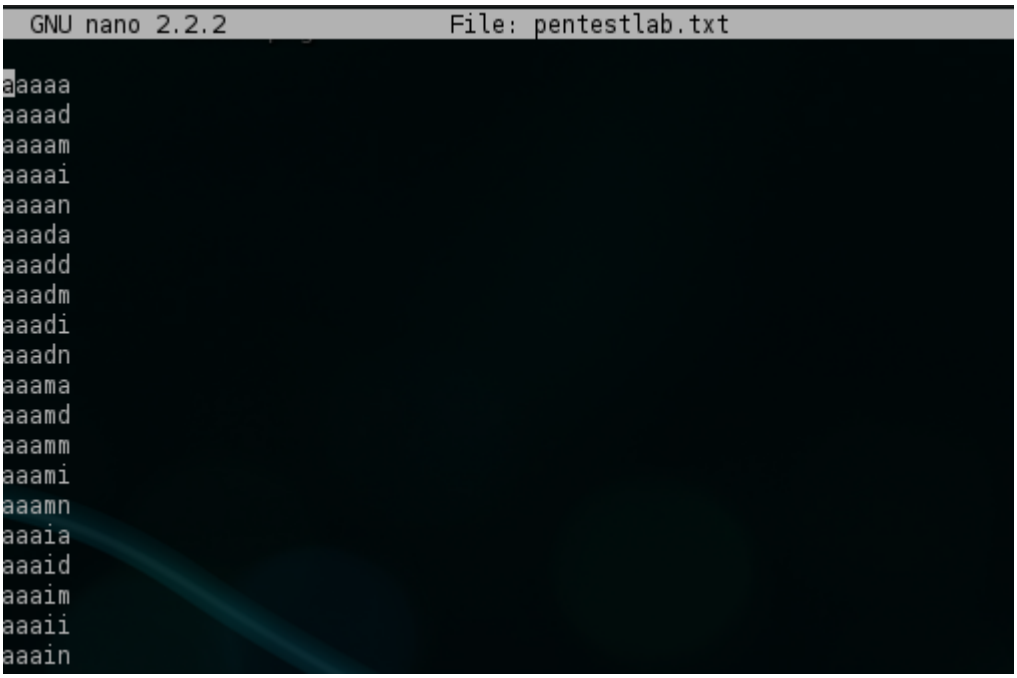
Next we execute the following command

./crunch 5 5 admin -o pentestlab.txt



Create a sample wordlist

This will instruct crunch to create a wordlist that will have minimum length of characters 5,maximum length of characters 5 with the characters of admin and it will save it on a .txt file called pentestlab as you can see it and in the image below.



Output of a sample wordlist

Of course instead of just letters we can create a wordlist that will include only numbers with the command:

./crunch 5 5 12345 -o numbers.txt

The same method applies and if we want to create a wordlist mixed with letters and numbers.

./crunch 5 5 pentestlab123 -o numbersletters.txt

Special Characters

For special characters like !$% you will need to execute something like the following:

./crunch 5 5 pentestlab\%\@\!

This is because some special characters need escaping and the **** is used before the character.

```
root@encode:/pentest/passwords/crunch# ./crunch 5 5 pentestlab\%\@\!
Crunch will now generate the following amount of data: 966306 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 161051
ppppp
ppppe
ppppn
ppppt
pppps
ppppl
ppppa
ppppb
pppp%
pppp@
pppp!
pppep
```

Special Characters

String Permutations

Here there are two options.First options is when we will want to generate something based on the characters of a word.For example **./crunch 1 1 -p abc** will produce the following list:

```
root@encode:/pentest/passwords/crunch# ./crunch 1 1 -p abc
Crunch will now generate approximately the following amount of data: 24 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 6
abc
acb
bac
bca
cab
cba
```

String Permutation – Characters

The second option is when we will want to create a list based on different words.For example the words blue and red can be bluered or redblue.We can achieve this with the command **./crunch 1 1 -p pen test lab**

```
root@encode:/pentest/passwords/crunch# ./crunch 1 1 -p pen test lab
Crunch will now generate approximately the following amount of data: 66 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 6
labpentest
labtestpen
penlabtest
pentestlab
testlabpen
testpenlab
```

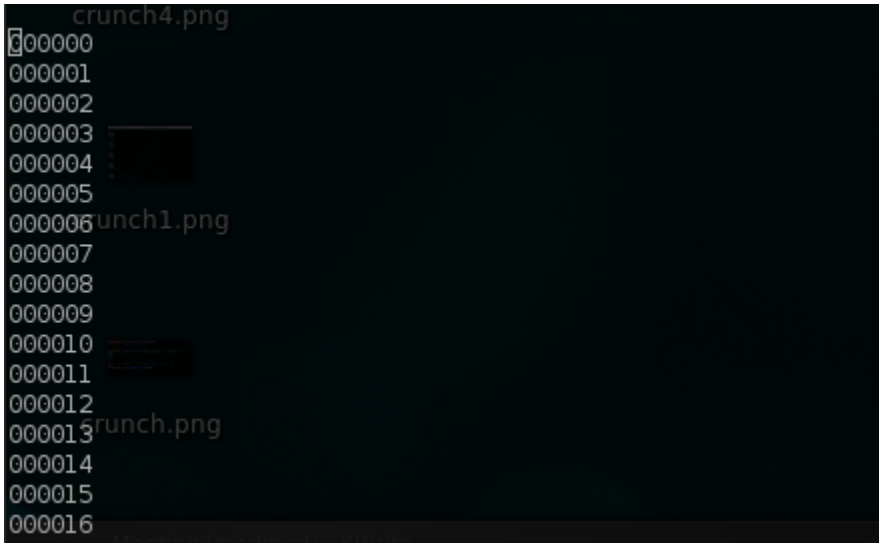
String Permutation – Words

Splitting Wordlists

If we use the -b option we will instruct crunch to create a wordlist which will be divided into multiple files.Another option that we can combine with that command is to choose the size of our wordlist.For example:

./crunch 6 6 0123456789 -b 1mb -o START

This will generate wordlists which will be 1Mb each and with 6 characters size and it will include the characters 0123456789.



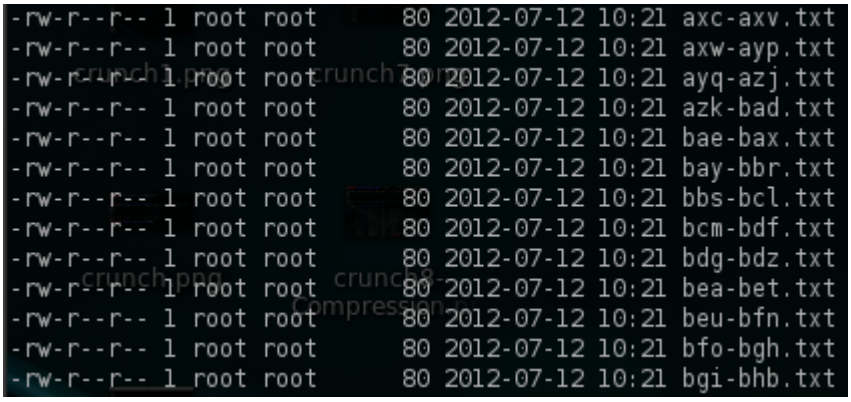
Splitting Wordlists

Specify the number of words

Crunch allows us to specify the number of words in each wordlist.This will create a wordlists that it will contain 20 words maximum by taken a specific charset of lalpha which is [abcdefghijklmnopqrstuvwxyz].

./crunch 3 3 -f charset.lst lalpha -o START -c 20

Alternatively you can use any other charset from the list that comes with crunch if you don’t want to use a custom charset.



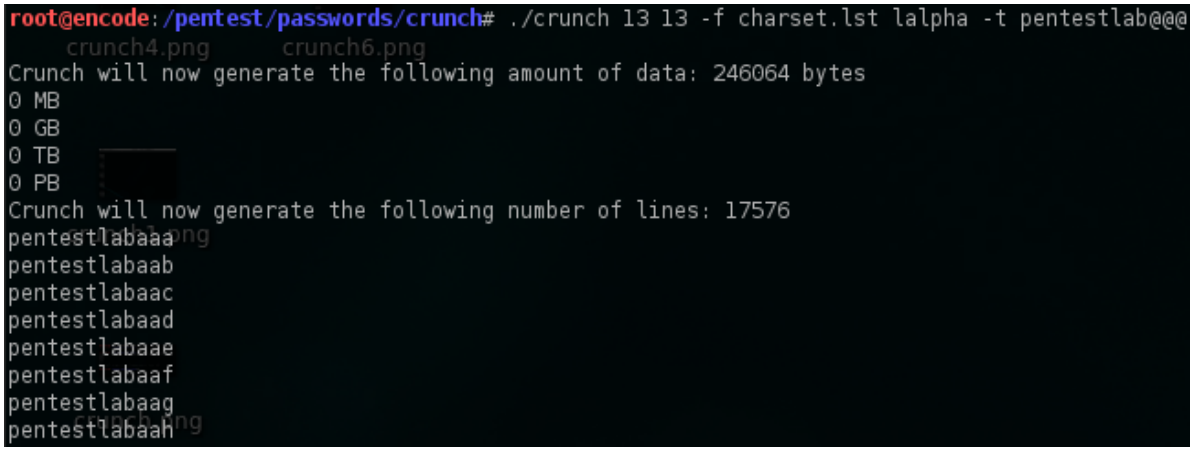
Number of words

Prefix Wordlists

Now lets say that we want to create a wordlist that will contains the word pentestlab followed by 3 random characters.The command for that will be:

./crunch 13 13 -f charset.lst lalpha -t pentestlab@@@

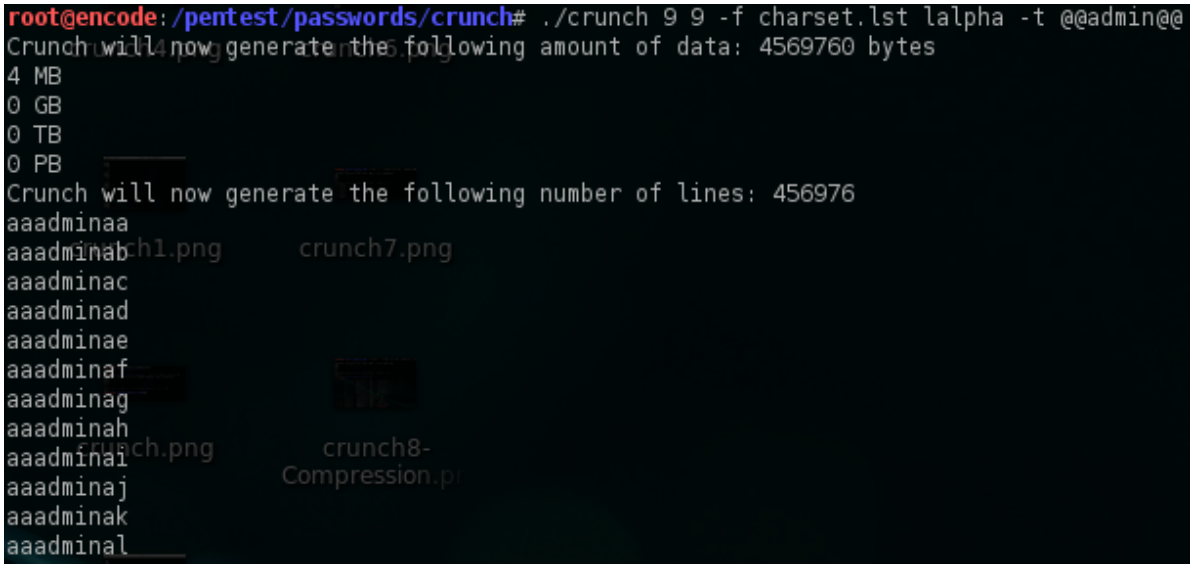
which will produce the following output:



Prefix wordlists – Characters

Alternatively if we want the word admin to be in the middle we can modify the command like this:

./crunch 9 9 -f charset.lst -t @@admin@@

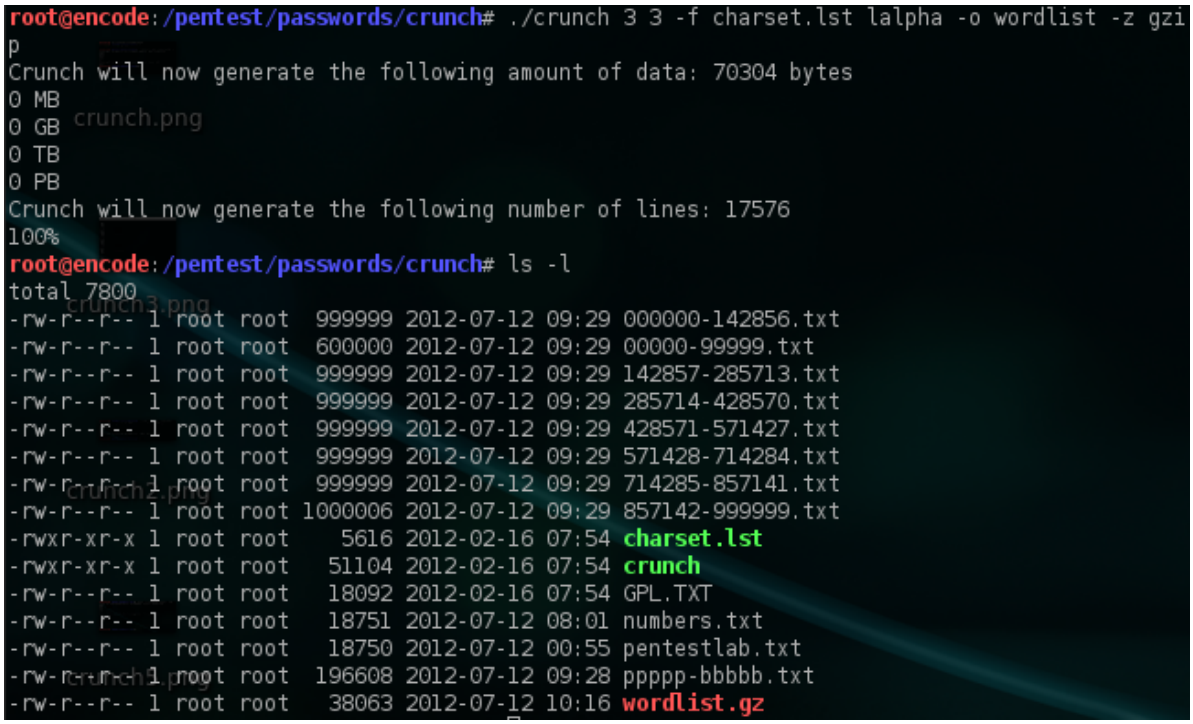


Prefix Wordlists based on words

Compression

You can compress your wordlist with the -z option using either bzip,gzip or lzma.

Example: **./crunch 4 4 -f charset.lst lalpha -o wordlist -z gzip**



Compress the wordlist

Conclusion

Creating wordlists can facilitate your needs when performing a penetration test.Crunch of course offers a variety of options and combinations that a user can play with.Trying to brute force of course an application or a system with a wordlist can of course lock you out depending on the account lockout policy but it always helps if you can have your own custom wordlists that may be help you to obtain access.