

Forum:[Hack Forums](#)

Thread: [Tutorial - Bruteforcing WPA/WPA2 with Crunch](#)

Spagnum - June 11, 2011, 6:41 am

Disclaimer

I know brute forcing is stupid, but I still see all these questions asking how to brutefore WPA and WAP2 passwords. So I decided to give it a try. From now on you can referee to this tread if someone wants proof of brute forcing beening stupid.?

What this guide will show you:

How to install and use Crunch to do a bruteforce attack against a WPA or WPA2 network.

What this guide will not show you:

How to capture a handshake file from a WPA og WPA2 network. There is plenty of other guides to show you how to do this. I recommend [this](#) one by Middle.

Getting and installing Crunch:

I'm using Backtrack 4 here, and it's pretty strate forward getting and installing Crunch.
(If you are one another distro like Ubuntu or something you might need to install the gcc compiler first)

Open the console and use the following commands one by one:

Code wget

`http://sourceforge.net/projects/crunch-wordlist/files/crunch-wordlist/crunch-3.0.tgz/download`

`tar -zxvf crunch-3.0.tgz`

`cd crunch3.0/`

`gcc -c crunch.c`

`gcc -lm -lpthread -o crunch crunch.o`

[img]<http://i57.photobucket.com/albums/g207/Spagnum/e89cf38a.jpg>[img]

Crunch should now be installed and you should be in the Crunch3.0 directory.

We will need to tell Crunch the minimum and maximum characters in the password, we do this like this:

Code `crunch <min-len> <max-len>`

We also need to tell crunch which carters to try with. This is simply done by typing all the carters you want it to use:

Code `abcdefghijklmnopqrstu`

Finally we need to pipe crunch to Aircrack-ng which will do the actually cracking. Aircrack-ng will need two things, path to the handshake file and the ESSID of the AP. My handshake file is called WPAtest.pcap and the name of the AP is "Wireless AP" (the quotes are only necessary if there is a space in the ESSID)

All together the command looks like this:

Code `./crunch 8 8 abcdefghijklmnopqrstu`

Aircrack-ng starts trying the all the possible password one by one:

[img]<http://i57.photobucket.com/albums/g207/Spagnum/1-1.jpg>[img]

Notice that Aircrack-ng cracks around 620 k/s. Now lets take a look at how long that would take, accounting to [Online Password Calculator](#).

[img]<http://i57.photobucket.com/albums/g207/Spagnum/2-1.jpg>[img]

Okay so you see that bruteforce is stupid??

Just for the fun of it, let's help out crunch by limiting the characters to use as well as giving it the first part of the password. We need to tell crunch the first part of the password, like this:

Code -t knownpassword@@@

All together the command looks like this:

Code ./crunch 8 8 1234 -t test@@@@ | aircrack-ng /root/WPAtest.pcap -e "Wireless AP" -w -

[img]<http://i57.photobucket.com/albums/g207/Spagnum/3-2.jpg>[img]

My first tutorial at HF, please forgive me for any grammar mistakes!

captainmark - June 11, 2011, 2:21 pm

Nice tut man.

I have a question and i dont rember if have been answered before so
is it possible to pipe crunch to pyrit?

Cause if its a yes then we all might still not be alive to see the "KEY FOUND"

but atleast our grand children will have free internet lol

No seriously it would be very interesting if it could colaborate with pyrit and 4 hi-end GPUs

Spagnum - June 11, 2011, 4:24 pm

Thanks!

I haven't tried Pyrit yet, but it's on my "To do list". I remember having read somewhere that you can combine Pyrit with crunch, but I'm not sure...

ziggycat - June 12, 2011, 1:46 am

@spagnum - bruteforcing is not stupid.

Pyrit is the only way forward if you plan to try and crack wpa. You can pipe the ouput directly from crunch and depending on the graphics card you are using instead of the 620 keys a second you can do 90,000+ a second.

Middle - June 12, 2011, 4:49 am

(Jun 12, 2011 01:46 AM)ziggycat Wrote: [\[CITE\]](#) @spagnum - bruteforcing is not stupid.

Pyrit is the only way forward if you plan to try and crack wpa. You can pipe the ouput directly from crunch and depending on the graphics card you are using instead of the 620 keys a second you can do 90,000+ a second.

Brute forcing is stupid

Only exception is if you know 1 or two characters and know its only 8 characters long (Phone number perhaps)

Spagnum - June 12, 2011, 5:32 am

(Jun 12, 2011 01:46 AM)ziggycat Wrote: [\[CITE\]](#) @spagnum - bruteforcing is not stupid.

Well in the case that you using "normal" hardware like most users would. I conclude brute forcing is stupid.?

Ph0x - June 12, 2011, 5:49 am

Pyrit isn't yet configured to work with Aircrack-ng unfortunately.

http://www.backtrack-linux.org/documents/BACKTRACK_CUDA_v2.0.pdf

<page 22> states that aircrack doesn't currently support the option for the passthrough from Pyrit, however, there are options to build aircrack with CUDA capabilities <page 28>.

Still trying to get the cowpatty one working at the moment though! :-D

ziggycat - June 12, 2011, 9:09 am

(Jun 12, 2011 04:49 AM)~Middle Wrote: [\[CITE\]](#) Brute forcing is stupid

Only exception is if you know 1 or two characters and know its only 8 characters long (Phone number perhaps)

Sorry mate I disagree,

Most people who don't change the ssid have a tendency to leave everything on default settings.

As we have discussed on other threads:

BTHH - 10 characters, comprising (a-f & 2-9) = 289 254 654 976 perms

SKY - 8 characters comprising (A-Z) = 208 827 064 576 perms

I am now using 2 machines, and 3 x 5850's. I'm not using pyrit serve but currently I'm achieving a combined total of 210K pmk's a sec, and plan to add a 5870 at the end of the month pushing this to over 300K.

(all 5850's have been purchased second hand at a total cost of £245, each card has been flashed with a 5870 bios. This enables me to push past the 775 overdrive limit).

Although this could potentially take 11 days for BTHH, and 8 days for sky I defend my position that bruteforcing is not stupid (these are the maximum times, it's very possible that the key is found much earlier in the process)

Currently crunch does not have the ability to drop any number of repeating characters (although there is a feature request ticket for this on sf). I'm looking at something in perl or C to accomplish this, by accepting output from crunch and piping it to pyrit. The ability to drop 5 or more repeating characters on the fly will significantly reduce the number of permutations and therefore the overall processing time.

Middle - June 12, 2011, 9:58 am

But even with 300,000 keys/s it could still take you 8 days, and for most people that is really not an option...

I think that pursuing brute forcing attacks past the point where you are all ready aware of some of

the characters (i.e i know it starts with 44 and is 8 characters long, so it can't take long to do 44xx) is just silly!

But hey if you have the resources and time there is nothing stopping you, my main concern is just that the newbies will think that they can get a 100% success rate with this awesome tool, whereas in fact unless they shell out several hundreds of pounds and rack up a massive electricity bill its not happening. Where as a pro like yourself who understands the attack doesn't need a tutorial on it...

Thanks why i don't like this tutorial!

EDIT: @Spagnum i just read the tutorial and it is nicely written and put in good context, good job! Oh and the bruteforce calculator is a great find! And spell my name right XD

theboyz - June 12, 2011, 4:07 pm

Great tutorial Thanks you very much :)

MaXoNe - June 13, 2011, 4:25 am

Great tutorial , there is a bash script that generates passwords based on data you provide [Pet name , date of birth etc] that shit got me 2 WPA networks , but it took me some time to do the research [it is a part of zer0day's Linux Script Collection] :)

Middle - June 13, 2011, 7:49 am

CUPP.py

CommonUserPasswordsProfiler

Counter440 - June 13, 2011, 7:53 am

Excellent tutorial, thx ?

Spagnum - June 13, 2011, 10:05 am

(Jun 12, 2011 09:58 AM)~Middle Wrote: [\[CITE\]](#) EDIT: @Spagnum i just read the tutorial and it is nicely written and put in good context, good job! Oh and the bruteforce calculator is a great find! And spell my name right XD

Thanks! - sorry about the name ? - can't edit it now.

Gates - June 13, 2011, 11:25 am

Thanks For Posting...Nice Tutorial and layout. I'm waiting for amd to release it's 8-core cpu this fall and paring it with my GTX 460 2GB to see what I can get.

m317down - June 20, 2011, 6:02 am

Why should I download it, when John is already installed on BT? I dont see any advantages using Crunch.

Spagnum - June 20, 2011, 6:30 am

(Jun 20, 2011 06:02 AM)m317down Wrote: [\[CITE\]](#) Why should I download it, when John is already installed on BT? I dont see any advantages using Crunch.

I not that familiar with john (john the ripper I guess). but if that works for you stick to that. ?

Das_Virus - June 20, 2011, 1:05 pm

You could use JtR instead of Crunch.

zerocool - June 21, 2011, 4:28 am

nice post an well expained many thanks

Spagnum - June 25, 2011, 5:25 pm

I had a look at John The Ripper just for the fun of it. The speeds seems pretty much the same.

I'm using this command:

Code `./john --increment --stdout | aircrack-ng /root/WPAtest.pcap -e "Wireless AP" -w -`

I looked at the tutorials in here about JTR, but still I have problems defining min and max characters. Can anyone explain to me how to make the program do the same thing as I did in the tutorial with Crunch?

get - June 30, 2011, 7:48 am

Does this method means its done on the fly. could crunch be used on an asus 701 witch as a 4 gb drive. Also if am not in a rush would it be safe to leave it on 27/7 fot mouths at a time?

Spagnum - June 30, 2011, 4:04 pm

can't see why it wouldn't work on that one. dunno about leaving it on 24/7 i guess that wordlist could get pretty huge over time...

Da_Devil - August 23, 2011, 3:05 pm

Thanks a lot Spagnum, very nice tool that can be pretty useful in some scenarios.

RedDevil08 - November 15, 2011, 6:02 am

Great tutorial, thanks

The message is . Please enter a message longer than 35 characters

The_Defiant_One - November 19, 2011, 12:44 am

Nice tutorial here!!! Thanks for writing it!!!!

e6to - February 20, 2012, 7:42 pm

Great tut and conversation. Thanks Spagnum! No need to worry about grammar issues except possibly in a command. I don't think there are any English teachers on here... :)

bruteforge - March 4, 2012, 11:57 am

Great! Thanks! How i put like that password for check "1GH1V89E8G5G" this is algorithm 1 numeric 2 letter , 1 numeric 1 letter and etc.. because 5 year is very long time :P

`./crunch 12 12 ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890`

Crunch will now generate the following amount of data: 6258725177052364800 bytes

5968785454800 MB

5828892045 GB

5692277 TB

5558 PB

Crunch will now generate the following number of lines: 4738381338321616896

^CCrunch ending at

yacked2 - January 22, 2013, 12:02 pm

Bruteforcing is not stupind, using aircrack to crack it is stupid. use hashcat