

Forum:[Hack Forums](#)

Thread: [Effective WPA Cracking and Bruteforcing](#)

whitehatblackhat - August 6, 2018, 5:39 pm

This should be a [Quick Thread](#).

Do any of you know of a free and effective way to bruteforce a WiFi password from a .cap file (with multiple networks, all with handshakes)?

Bruteforcing with hashcat and crunch can take years. There has to be a better way to crack WiFi passwords.

Thanks,
whitehatblackhat

CryptixHacking - August 6, 2018, 5:59 pm

(Aug 6, 2018 05:39 PM)whitehatblackhat Wrote: [\[CITE\]](#) This should be a [Quick Thread](#).

Do any of you know of a free and effective way to bruteforce a WiFi password from a .cap file (with multiple networks, all with handshakes)?

Bruteforcing with hashcat and crunch can take years. There has to be a better way to crack WiFi passwords.

Thanks,
whitehatblackhat

Aircrack-ng not working for you ??

Maybe the issue is not with your bruteforcers but with your packet file, It may just be you require more valid handshake sessions to be captured as these are required to crack/brute into a WPA. The more valid handshake packets captured for that target network the easier the bruteforcer can crack it. Have you tried using a De-authentication tool while you capture handshake packets. Usually this can allow you to kick other systems connected to that network off the network forcing them to re connect which gives you a valid handshake packets.

"If only everyone was still using WEP like the old days xD"

whitehatblackhat - August 6, 2018, 6:39 pm

(Aug 6, 2018 05:59 PM)CryptixHacking Wrote: [\[CITE\]](#) Aircrack-ng not working for you ??

Maybe the issue is not with your bruteforcers but with your packet file, It may just be you require more valid handshake sessions to be captured as these are required to crack/brute into a WPA. The more valid handshake packets captured for that target network the easier the bruteforcer can crack it. Have you tried using a De-authentication tool while you capture handshake packets. Usually this can allow you to kick other systems connected to that network off the network forcing them to re connect which gives you a valid handshake packets.

"If only everyone was still using WEP like the old days xD"

That would be great if they all used WEP...

I am using aircrack, but that requires either using a dictionary or simply using something like crunch, which isn't affected too much by the number of packets that are captured. I have deauthorized them to get my handshakes, but bruteforcing alphanumeric characters, lowercase and

uppercase with integers and symbols, is not something any computer can do in any reasonable amount of time. What other methods are there for cracking the actual password itself (Reaver does not work these days) or methods for hacking WiFi in different ways? I could probably pull off the Evil Twin attack even right now, but I am worried, since my neighbors already know that I am a hacker (I revealed to one of them that I was going to pen-test, to which they accepted my request and then denied it afterwards (I still got their password), which clearly would be a memory of theirs if they were to see suspicious WiFi activity). What do I do in this case? There have to be other ways.

Thanks,
whitehatblackhat

Archlights - August 6, 2018, 7:09 pm

(Aug 6, 2018 06:39 PM)whitehatblackhat Wrote: [\[CITE\]](#) That would be great if they all used WEP... I am using aircrack, but that requires either using a dictionary or simply using something like crunch, which isn't affected too much by the number of packets that are captured. I have deauthorized them to get my handshakes, but bruteforcing alphanumeric characters, lowercase and uppercase with integers and symbols, is not something any computer can do in any reasonable amount of time. What other methods are there for cracking the actual password itself (Reaver does not work these days) or methods for hacking WiFi in different ways? I could probably pull off the Evil Twin attack even right now, but I am worried, since my neighbors already know that I am a hacker (I revealed to one of them that I was going to pen-test, to which they accepted my request and then denied it afterwards (I still got their password), which clearly would be a memory of theirs if they were to see suspicious WiFi activity). What do I do in this case? There have to be other ways.

Thanks,
whitehatblackhat

Unless your neighbors are smarter than the average boomer or pen testers themselves I don't think they'd notice an evil twin attack. I know most people would just go fiddle with their router if they notice funky internet stuff.

CryptixHacking - August 6, 2018, 9:50 pm

(Aug 6, 2018 06:39 PM)whitehatblackhat Wrote: [\[CITE\]](#) That would be great if they all used WEP... I am using aircrack, but that requires either using a dictionary or simply using something like crunch, which isn't affected too much by the number of packets that are captured. I have deauthorized them to get my handshakes, but bruteforcing alphanumeric characters, lowercase and uppercase with integers and symbols, is not something any computer can do in any reasonable amount of time. What other methods are there for cracking the actual password itself (Reaver does not work these days) or methods for hacking WiFi in different ways? I could probably pull off the Evil Twin attack even right now, but I am worried, since my neighbors already know that I am a hacker (I revealed to one of them that I was going to pen-test, to which they accepted my request and then denied it afterwards (I still got their password), which clearly would be a memory of theirs if they were to see suspicious WiFi activity). What do I do in this case? There have to be other ways.

Thanks,
whitehatblackhat

Yes this is all true and you are correct with most the statements made here. The WPA cracking at that point just comes down to how well of a crack setup you have for the data. And no I do not know of any such cracking methods that are any better than what you currently seem to have setup. Cracking a WPA usually is a slow process just for those reasons. The only thing I can think of which may speed up the cracking method would be to use multiple systems like a botnet. You could have multiple systems attempting to crack the same cap file from separate points or by splitting/altering the cap file for the multiple systems.

You might try looking into WPS exploits "like reaver" most wifi modems/routers that have a WPA encryption tend to have WPS enabled or most have WPS enabled by default. There are ways to brute force the WPS or inject a payload into the WPS end of the router that allows you to connect to its network without the need of the password. There is a program I tested around with in the past that used WPS exploits and bruteforcing to then connect to the network and once connected could then dump the wifi password without the need to crack the WPA. This might be your best option if you do not wish to crack the WPA.

Another option could be a unique type of attack that uses de-authentication and tricks the target system into thinking its home wifi network is your wifi network much like the hak5 wifi pineapple attack, You can setup your own wifi and mask its network settings and mac in a way so that when you de-auth your target and they auto connect back to the home wifi they are actually connected to your wifi. Once the target system is on your LAN you can use multiple payload methods to dump the wifi password of there home network even though they are not on it.

And for the part about masking "hiding" yourself is to spoof your systems external MAC address as the wifi router logs and tracks MAC addresses of systems that connect to it which is viewable by the network administrator. If you spoof your mac address you are saying yes this computer with this mac address is connected to the network even though your real systems hardware mac address is not the same. This tells the network and administrator that your computer system is not the same computer system that was once connected to it. Though if the network admin is tech savey it wouldnt be to hard to find and detect the real mac address of the user though highly unlikely.

cthulhu1337 - August 11, 2018, 6:18 pm

aircrack should take a day at most