

Forum:[Hack Forums](#)

Thread: [A noob friendly guide to WiFi Hacking](#)

Middle - April 17, 2011, 3:17 pm

As i have '7 minutes remaining' on a file transfer i decided i would write a little article that would clear up some myths about wireless cracking. I will not go into specifics here just explain a bit about the concepts and what is actually involved in cracking wireless networks.

WEP and WPA, whats the difference?!

WEP was created shortly after wireless routers became common place for private networks, it stands for 'Wired Equivalent Privacy' and was the standard encryption on routers till about 2006, and is still fairly common. The interesting thing with WEP however is that it has a major design flaw, that allows its key to be cracked very easily. This was PoC'ed in about 2001 and soon tools were developed to make it a very easy task to crack WEP. If you know what you are doing you can crack WEP in less than 5 minutes and if you don't it shouldn't take too much longer!

So WEP we can crack easy, but what about this other one that we see so much of these days, WPA or WPA2, well this new form of encryption that you find on the majority of routers is a lot more secure than WEP but it still has issues. Wireless Protected Access (2) CAN be cracked BUT you will need to all ready have the wireless key stored in a word list for it to be cracked. Think of it like guessing the combination to a lock, you all ready have the combination stored in your head its just a long time till it gets tested and is successful. Now when cracking a WPA network you don't just brute force the 'Please enter the key' box with combinations, but rather the handshake between a machine all ready connected to the network and the network. Once the handshake is captured, we can take it off site and then crack it with essentially a brute force of potential keys, a word list. So you need to have the key in the word list all ready, which means BIG word lists, and BIG computing power. Read more about cracking the WPA handshake [here](#)

How can i do all this?!

Well I'm glad to inform you that the only reasonable solution is to use a Linux based OS, but don't panic its not as bad as it sounds, there are distributions of Linux that are designed solely for 'penetration testing' (Hacking) and in these distributions all of the tools you need are pre-installed so it really is just a case of boot up and play!

Now if you don't know; you don't need to install an operating system to your hard drive to use it you can burn it onto a USB stick or CD/DVD, then you can set your computer to boot straight from the mountable media and then straight into Linux. Or you could even burn the iso to a virtual machine in Virtual Box or VMware, then you could use a Linux environment and tools inside your current OS.

Hardware :(

Unfortunately to crack a WEP or WPA encrypted network you will need a wireless card that is compatible with a suite of programs called aircrack-ng, this is what we use to crack all wireless networks, there are other programs but they are pretty much all based around the aircrack-ng suite. If you wireless card isn't compatible with aircrack-ng or you are using a virtual machine that doesn't detect internal wireless cards, you may need to purchase a new USB wireless adapter, and although spending money sucks it is well worth it, even if you all ready have a compatible card inbuilt in your

PC. The 'industry standard' card is the Alfa AWUS036H it costs about £25/\$30 and it will be fully compatible with every Linux WiFi related hacking app out there! The other reason to get one is even if you all ready have a compatible card it will be lacking in power and range when compared to an AWUS036H.

Before you buy though it is worth testing you wireless card to see if it is compatible you can do this by using these commands in pen-testing distro of Linux:

```
airmon-ng start wlan0 (If a new interface is made called mon0 continue)
aireplay-ng -9 mon0 (If it says 'Packet injection support found etc..' then your card is top notch!)
```

If however you just get a shit ton of errors you will need to buy a new wireless adapter or rethink your incentives to wireless hacking XD

Another thing to note on the hardware side of things is if you want to crack WPA seriously then you are going to need a powerful Ati graphics card for use with a program called pyrit. Remember i said about 'brute forcing' the WPA key, on an average PC you may be able to brute force at about 3000 passphrases every second, but with a well set up system with an Ati GFX card you can start looking at 30,000 - 150,000+ keys a second!

Where to go now?

Well if you are still interested i suggest the next step be to go and read one of the hundreds of WEP cracking tutorials on the forums, or just go and lurk in the WiFi hacking section for a while!

This has been a very vague and general introduction to what WiFi hacking is, i hope it has opened your eyes to what is possible and how it is possible. If you want to read more into the subject or read more from me i suggest giving my signature a click, it is linked to all of the tutorials and tools i have created and should be a great place for you to start you extended reading!

I hope you have enjoyed, feel free to post any questions you have so long as you have taken the initiative to search for your answer before hand!

Love

'The WiFi Guy'

Boxing - April 17, 2011, 3:18 pm

Nice tutorial, you obviously spent a lot of time on it.

Starts reading it

Middle - April 17, 2011, 3:20 pm

Yeah may have lasted slightly longer than 7 minutes :P

Be sure to check out my other indepth tutorials as well!

D4rKn3s5 - April 17, 2011, 3:47 pm

This is a good dulled down version of what you have already put out in the wifi section. If you have any questions about anything wifi related ~Middle will most likely have the answer.

wasabi-kun - April 17, 2011, 4:30 pm

ive been trying to firture out how to do this. this is an really good start. thanks ? very well written

Middle - April 18, 2011, 3:32 am

Thanks, i suppose this should really be moved to the tutorial section....

Galaxy15 - April 18, 2011, 3:35 am

This is perfect for what I'm trying to do right now, thanks for the TuT!
Start's Reading ?

EDIT: Nice, very easy to read and easy for newbs (me) to understand. Well done!

titokanon10 - April 18, 2011, 4:15 am

thnx mate :D really usefull

B3cnoc - April 18, 2011, 5:19 am

i like this thread :). you spent a lot of time on this, and i learned a lot :)

Middle - April 18, 2011, 5:43 am

Didn't take me too long to do this, 20 minutes perhaps, check out my other tutorials that took me several hours XD

creed0113 - April 18, 2011, 6:10 pm

you do this for the hell of it; thx dude learned alot, but do you know anything other then wifi cracking.

Middle - April 19, 2011, 1:53 am

Yeah man i know hellava lot!

But i keep to my turf XD

canyon! - April 19, 2011, 4:08 am

thanx :) thanx :) thanx :) thanx :) thanx :) :D

Middle - April 19, 2011, 4:42 am

Your welcome, i hope this just sheds some light for the newer members who haven't fallen to the plight of skidsie tools etc...

creed0113 - April 19, 2011, 6:16 am

xD do you know anything about USbs such as hiding it from the other people sight except you can see it. And auto running a program once you plug it in the comp.

Middle - April 19, 2011, 6:53 am

You might want to have a look at USBsploit :)

hdawg1280 - July 20, 2011, 10:02 pm

when i did "sudo aireplay-ng -9 mon0" I got this error:

Interface mon0:
ioctl(SIOCGIFINDEX) failed: No such device

I have a 2011 macbook pro laptop with Mac/win7/linux OS's.

I'm guessing that my wireless adaptor is useless for WEP wireless cracking?

If so, I plan to buy this wireless adapter:

http://www.amazon.com/AWUS036H-Wireless-Adapter-Network-Antenna/dp/B000QYGNKQ/ref=sr_1_2?s=electronics&ie=UTF8&qid=1311224533&sr=1-2

what do you think?

legitbiz - July 21, 2011, 1:06 am

thanks mate thats was helpful

Leg - July 21, 2011, 1:15 am

Nice guide and very easy to understand.

I just wish there was more efficient methods of cracking WPA

hdawg1280 - July 21, 2011, 10:51 am

So you still think I should purchas the "Alfa AWUS036H" even though my macbook pro 2011 has pretty good range for wireless? Does the Alfa AWUS036H, do something more than just provide a longer range?

one more thing. My wireless is 802.11n and I noticed that the Alfa AWUS036H is a 802.11b/g. I'm assuming my 802.11n is better/faster than the 802.11b/g? If that's the case then I wouldn't need to purchase the Alfa AWUS036H, right? Or am I wrong on this?

I saw an Alfa AWUSO36NH which is "High Gain USB Wireless G / N Long-Rang WiFi Network Adapter". Should I purchase this one instead?

Middle - July 21, 2011, 12:13 pm

The Alfa AWUS036H is the best adapter to get, as it is completely compatible with everything, and will give you fantastic range as well!

hdawg1280 - July 21, 2011, 2:49 pm

ok, but can someone tell me this....what is the difference between Alfa AWUS036H and Alfa AWUSO36NH. which one is better? IF any at all.

viagrastim - November 8, 2011, 6:03 am

Very well written, this is what I've looking for, thank for the hard work

robry1227 - December 29, 2011, 2:05 am

Really appreciate this thread. I prefer knowing what I am actually doing as opposed to following a list of commands. Keep up the good work middle. I need to set up my mac book pro with some hardware and get started.

Thanks,

Robry1227

.pain - September 11, 2012, 6:31 pm

Extreamly good tutorial for explaining the basics in a way for everyone to understand! Thank you! :)