

Forum:[Hack Forums](#)

Thread: [Has anyone used fern wifi cracker to succesfully crack a wifi password?](#)

javinzplayer - September 12, 2017, 6:44 pm

This tool comes with kali and im wondering if this tool can crack wifi networks. Thanks! If you know any good alternatives to this tool please also tell me! ?

pasnger57 - September 13, 2017, 4:42 am

yes but it only works for Simple one's the you can get from a list .

As it ues CPU to calculate hash's it was simple to use to use to get .cap files but Farm management protections

but this can be solved by setting the mac address to a client on the AP

its just a GUI for

aircrack-ng and reaver

Jopemeister - September 13, 2017, 4:46 am

(Sep 13, 2017 04:42 AM)pasnger57 Wrote: [\[CITE\]](#) yes but it only reilly works for Simple once the you can get from a list as it ues CPU to calculate has's it was simple to use to use to get .cap files but Farm management protections

but this can be solved by setting the mac address to a client on the AP

dude what

pasnger57 - September 13, 2017, 5:11 am

the question was about fern wifi cracker

and if you can use it to crack a WiFi

short answer is yes its just SLOW and only Simple passwords will fall to this based on the List you have set

javinzplayer - September 15, 2017, 4:10 pm

(Sep 13, 2017 04:42 AM)pasnger57 Wrote: [\[CITE\]](#) yes but it only works for Simple one's the you can get from a list .

As it ues CPU to calculate hash's it was simple to use to use to get .cap files but Farm management protections

but this can be solved by setting the mac address to a client on the AP

its just a GUI for

aircrack-ng and reaver

Do you know any crackers like fern?

pasnger57 - September 15, 2017, 6:39 pm

fern is just a GUI for the tools that have ben in use for some time and better tools like hashcat or pyrit - opencl are now a better option

i use hashcat as myself and have much luck with critical thinking and a few good list and researching the target is key to

the more data you can get about what/soeone may use for a kay is ida

if you tryin to beet something generated by the router itself then a dump of the Fw and its working helps ALOT understanding Key space and complexity and reducing possibility that are Most likely false

if you nex READ alot more ALORE MORE
a god page read is

<https://hashcat.net/forum/thread-6170.html?highlight=wpa2>

roosiinfidel09 - May 12, 2019, 4:03 am

(Sep 12, 2017 06:44 PM)javinzplayer Wrote: [\[CITE\]](#) This tool comes with kali and im wondering if this tool can crack wifi networks. Thanks! If you know any good alternatives to this tool please also tell me! ?

What exactly can one do after hacking wi-fi? apart from the free internet? Please keep HSTS in mind. For me it has been useless. You can't redirect traffic, can't sniff passwords, all you can do is capture packets on wireshark. What good is that? or just see the links of pages being browsed using bettercap etc. If the victim is using an App..it is even more useless not that you can do anything with the browser as such.

TxRx - May 12, 2019, 1:52 pm

When i learned how to crack wifi, i started with the basics. All i had was BackTrack 3 and my AWUS036H. No GUI tools like fern. The aircrack suite is such an excellent and intriguing tool, as it has so many options and variants you can use to modify your attacks. I always recommend to learn the hard way, using command line. At the end, it will pay off.

The point is not getting the signal cracked, its learning how it got cracked... how the process works.

Pawnhub - May 13, 2019, 3:24 am

Fern in my opinion is only good for cracking WEP anything else use the programs that people already commented about.

s3n-py - May 13, 2019, 12:49 pm

(May 12, 2019 04:03 AM)roosiinfidel09 Wrote: [\[CITE\]](#) What exactly can one do after hacking wi-fi? apart from the free internet? Please keep HSTS in mind. For me it has been useless. You can't redirect traffic, can't sniff passwords, all you can do is capture packets on wireshark. What good is that? or just see the links of pages being browsed using bettercap etc. If the victim is using an App..it is even more useless not that you can do anything with the browser as such.

You can do SO much!... What do you mean you can't redirect traffic? Once you are on the network you do a arp or dns spoof and direct them to a crafted page of your own. You can do a MiTM and steal creds. You could even set up a evil twin where you control the whole network. If being on the network is useless then what is the point of invading a network at all???? It's not magic. It takes preparation.

tycho - May 13, 2019, 3:29 pm

(May 13, 2019 12:49 PM)s3n-py Wrote: [\[CITE\]](#) You can do SO much!... What do you mean you can't redirect traffic? Once you are on the network you do a arp or dns spoof and direct them to a crafted page of your own. You can do a MiTM and steal creds. You could even set up a evil twin where you control the whole network. If being on the network is useless then what is the point of invading a network at all???? It's not magic. It takes preparation.

That's correct. There are a lot of sophisticated attacks you can do while on the network. With the right setup, you can capture the data from every device that uses the network. HTTPS and the like have made attacks like these a bit harder, but more than easily bypassed.

TxRx - May 14, 2019, 1:10 am

(May 13, 2019 12:49 PM)s3n-py Wrote: [\[CITE\]](#) You can do SO much!... What do you mean you can't redirect traffic? Once you are on the network you do a arp or dns spoof and direct them to a crafted page of your own. You can do a MiTM and steal creds. You could even set up a evil twin where you control the whole network. If being on the network is useless then what is the point of invading a network at all???? It's not magic. It takes preparation.

Lmao. You certainly do not know the steps of penetration testing then... the holy grail of pentesting is actually getting INSIDE the network. From there, you exploit the machines inside that network.

Recon, Scan/Profiling, Penetrate, Backdooring, Destroy the evidence...

roosiinfidel09 - May 14, 2019, 11:44 pm

(May 13, 2019 12:49 PM)s3n-py Wrote: [\[CITE\]](#) You can do SO much!... What do you mean you can't redirect traffic? Once you are on the network you do a arp or dns spoof and direct them to a crafted page of your own. You can do a MiTM and steal creds. You could even set up a evil twin where you control the whole network. If being on the network is useless then what is the point of invading a network at all???? It's not magic. It takes preparation.

Pfft...Have you tried any of these lately?..Please go ahead and do so. Let me know what happens. It seems you have just read about these and haven't actually done anything.

You can't sniff SHIT. If sniffing means looking at URLs ..good for you.

You can't redirect SHIT. HSTS would not allow the browser to connect to your website unless the victim is trying to browse to a really really really shitty site.

You can't MiTM SHIT. in case you are referring to hooks, SSLStrip, Beef Injections etc. Either the browser needs to be shitty IE5 or something or again the victim needs to be browsing a really really really shitty website.

If it is a normal user who uses FB.Google and Insta 90% of the time (which is like 95% of the users)..you can't do SHIT.

Recon??...Looking at Mac addresses of devices? and their OS? ...what good is that?

Evil Twin? really. Ok. Let us say the victim connects to YOUR evil twin and you give him internet access. All the above conditions still stand. Now, go and actually DO any of these and not come back here after watching YT videos.

(May 13, 2019 03:29 PM)FleetFoxes Wrote: [\[CITE\]](#) That's correct. There are a lot of sophisticated attacks you can do while on the network. With the right setup, you can capture the data from every device that uses the network. HTTPS and the like have made attacks like these a bit harder, but more than easily bypassed.

Yeah?...what are these "sophisticated attacks" and what is the "right set up"...and how is HSTS "easily bypassed"? ...Let's hear it.

S2K - May 15, 2019, 5:45 am

I hacked wifi networks first time today, I was in need of internet.

I used airgeddon toll and pixie-dust strategy. 5 wifi passwords cracked out of 15 in total. 33% success rate in my case. AND the good thing is it's easy to use and it takes seconds

pasnger57 - May 15, 2019, 3:42 pm

(May 15, 2019 05:45 AM)Ms-DOs Wrote: [\[CITE\]](#) I hacked wifi networks first time today, I was in need of internet.

I used airgeddon toll and pixie-dust strategy. 5 wifi passwords cracked out of 15 in total. 33% success rate in my case. AND the good thing is it's easy to use and it takes seconds
wow that sorta sad considering how OLD pixie dust is

sc0re - May 15, 2019, 6:35 pm

(May 15, 2019 03:42 PM)pasnger57 Wrote: [\[CITE\]](#) wow that sorta sad considering how OLD pixie dust is

Ya, I have no luck in my areas with the pixie dust attack....even other areas of my city I have tried

with no luck yet. I tried the airgeddon and it is a pretty nifty utility he put together!

s3n-py - May 17, 2019, 7:06 am

(May 14, 2019 11:44 PM)roosiinfidel09 Wrote: [\[CITE\]](#) Pfft...Have you tried any of these lately?..Please go ahead and do so. Let me know what happens. It seems you have just read about these and haven't actually done anything.

You can't sniff SHIT. If sniffing means looking at URLs ..good for you.

You can't redirect SHIT. HSTS would not allow the browser to connect to your website unless the victim is trying to browse to a really really really shitty site.

You can't MiTM SHIT. in case you are referring to hooks, SSLStrip, Beef Injections etc. Either the browser needs to be shitty IE5 or something or again the victim needs to be browsing a really really really shitty website.

If it is a normal user who uses FB.Google and Insta 90% of the time (which is like 95% of the users)..you can't do SHIT.

Recon??...Looking at Mac addresses of devices? and their OS? ...what good is that?

Evil Twin? really. Ok. Let us say the victim connects to YOUR evil twin and you give him internet access. All the above conditions still stand. Now, go and actually DO any of these and not come back here after watching YT videos.

Yeah?...what are these "sophisticated attacks" and what is the "right set up"...and how is HSTS "easily bypassed"? ...Let's hear it.

Dude calm down.... read a little bit, there is always a way. As far as FB and Insta goes anyway, who cares about that information anyway? If I wanted to get into someones FB I would use the username in the html and just read through there timeline for the password. The information worth getting isn't FB and Insta anyway.

(May 14, 2019 01:10 AM)TxRx Wrote: [\[CITE\]](#) Lmao. You certainly do not know the steps of penetration testing then... the holy grail of pentesting is actually getting INSIDE the network. From there, you exploit the machines inside that network.

Recon, Scan/Profiling, Penetrate, Backdooring, Destroy the evidence...

That is exactly what I was saying.... ????

roosiinfidel09 - May 20, 2019, 9:28 am

(May 17, 2019 07:06 AM)s3n-py Wrote: [\[CITE\]](#) Dude calm down.... read a little bit, there is always a way. As far as FB and Insta goes anyway, who cares about that information anyway? If I wanted to get into someones FB I would use the username in the html and just read through there timeline for the password. The information worth getting isn't FB and Insta anyway.

That is exactly what I was saying.... ????

Yea...it is always the new members who have ALL the answers. LOL. Yo! Dumbfuck. When you have a way let us know. Fuck your conjecture. We are miles ahead.

(May 15, 2019 06:35 PM)sc0re Wrote: [\[CITE\]](#) Ya, I have no luck in my areas with the pixie dust attack....even other areas of my city I have tried with no luck yet. I tried the airgeddon and it is a pretty nifty utility he put together!

Airgeddon depends on a shitty router. Please dont try and educate me about EVIL TWIN. HSTS fucks it in it's ass. What I wanna know is what you do AFTER you gain access. Jack fucking shit. Have proof. post it. Truth is.... with HSTS...browser hacking is dead. You ain't hacking no apps for sure. All you have is a free internet connection where you see "URLs" being browsed ...You make a video of that and call it "Hacking" to make more fool out of already vulnerable fucks. Truth..again is that...Wi-Fi access to a foreign network amounts to jack fucking shit. Eagerly waiting for a rebuttal.

Robert Elias - November 6, 2019, 11:45 am

I hope someone can help me out. I recently purchased a new wifi router RT-AX88U. Today I was looking at my client lists and did not recognize a Samsung Android Automatic IP CC:B1:1A:11:69:16

This device was connected to my 5g network. Any idea how they were able to connect when it is password protected? I appreciate your follow up on this.

Regards,

txnerd - December 9, 2019, 7:24 am

I've used it for cracking WEP, and been able to get really lucky and find some writers that were vulnerable to the WPS exploit..

OR10N - December 9, 2019, 10:26 am

Personally as far as automated scripts go I'm a really big fan of airgeddon (incl. in parrot / kali) since it manages wps pixiedust, bruteforce and "known" pin attacks as well as helping to automate aircrack-ng suite based attacks like using an aireplay deauth to bounce users off and capture the handshake when they reconnect then aircrack to attempt to match it with a wordlist.

though realistically you're going to have the best luck by far by learning to do a deauth attack manually, targetting a specific wireless client for best results then, if successful. ruining the handshake against something like the rockyou wordlist or some other (there are some decent ones on these forums just look, but rockyou ships with parrot / kali and actually still manages a pretty surprising success rate)