

Forum:[Hack Forums](#)

Thread: [Evil Twin or WPA Cracking?](#)

PurpleMoss - April 30, 2023, 6:07 am

Wondered if anyone had more success with one or the other? If you had a network to get into, what would your approach be? Let's say it's using the default WiFi password which is 10 lower case alphanumeric characters.

Would you capture the handshake and try to get the password cracker, or would you spend the time performing an evil twin attack?

I don't have the hardware for cracking passwords so would pay for someone to crack it if it were possible.

Platinum Stargazer - April 30, 2023, 11:02 am

My facebook acct got hacked once. Hacker used it to spread funny pictures of cute smiling piggies. I think he must have used a dict attack tool like jack the ripper (john the ripper?)

PurpleMoss - April 30, 2023, 12:37 pm

(Apr 30, 2023 11:02 AM)Platinum Stargazer Wrote: [\[CITE\]](#) My facebook acct got hacked once. Hacker used it to spread funny pictures of cute smiling piggies. I think he must have used a dict attack tool like jack the ripper (john the ripper?)

I've never tried a brute force against something like FB but just based on the websites I test at work, it's very likely that FB would have rate limiting of some sort on accounts. That means you'd get blocked (IP or account lockout) after X amount of failed attempts.

What's more than likely is they've gotten your password for something else, and as most people use the same password, they've successfully logged into FB using that password.

pasnger57 - April 30, 2023, 1:51 pm

The only real issue with clone/twin is that is can lid to a null in the association farm and that leave the possibility of a false + true

PurpleMoss - April 30, 2023, 1:58 pm

(Apr 30, 2023 01:51 PM)pasnger57 Wrote: [\[CITE\]](#) The only real issue with clone/twin is that is can lid to a null in the association farm and that leave the possibility of a false + true

Either I'm thick in this subject or that didn't make sense ?. Do you mind explaining what you mean sorry.

pasnger57 - April 30, 2023, 2:06 pm

(Apr 30, 2023 01:58 PM)PurpleMoss Wrote: [\[CITE\]](#) Either I'm thick in this subject or that didn't make sense ?. Do you mind explaining what you mean sorry.

depending on the Clone and capture meth you go about you can do web portal or ask for credentials or just catch the handshake on network you are manipulating to broadcast the same credentials of the (target) to trick its client to connection your rouge twin (then crack handshake (empty authentication)

Ducky - April 30, 2023, 10:15 pm

(Apr 30, 2023 06:07 AM)PurpleMoss Wrote: [\[CITE\]](#) Wondered if anyone had more success with one

or the other? If you had a network to get into, what would your approach be? Let's say it's using the default WiFi password which is 10 lower case alphanumeric characters.

Would you capture the handshake and try to get the password cracker, or would you spend the time performing an evil twin attack?

I don't have the hardware for cracking passwords so would pay for someone to crack it if it were possible.

I assume you're asking for educational purposes, attacking your own network or one that you have specific permission to target and attack.

I've had success with both. It mostly depends on the security of the network you're targeting.

If you're targeting a residential network, I'd aim for cracking first. I've cracked so many residential networks with rockyou, or by guessing the default passwords with ADJWORD123; I have cracking hardware that speeds up the process.

Shoot me a convo if you want help cracking it. If it's a residential network I can probably get it done for you in a day or less. I accept XMR.

2xTheTap115 - May 3, 2023, 12:24 pm

(Apr 30, 2023 06:07 AM)PurpleMoss Wrote: [\[CITE\]](#) Wondered if anyone had more success with one or the other? If you had a network to get into, what would your approach be? Let's say it's using the default WiFi password which is 10 lower case alphanumeric characters.

Would you capture the handshake and try to get the password cracker, or would you spend the time performing an evil twin attack?

I don't have the hardware for cracking passwords so would pay for someone to crack it if it were possible.

I have used both techniques, successfully (personalized dictionary attacks and evil twin + deauth) However, it's hard for me to point out which one is more effective, for me the answer is: It depends, even despite the fact that by far more often evil twin attacks, in my case, were successful. Let's assume that during the reconnaissance phase you learned that the manufacturer of the AP you are attacking generates secure 15-character passwords. You also know that your target has not changed anything in the default configuration. In such a case, you certainly won't waste your time fruitlessly cracking a complex password but will apply a different attack vector here, for example, impersonation (well, unless you have an exclusive decent GPU cluster, however, such considerations are well beyond the topic of the thread?) Following this line of thought, if you find out that your target, has some kind of password creation policy or you simply have an assumption that the password may be predictable, it would be reasonable to use a dictionary attack or other targeted attack.

kohut124 - June 8, 2023, 10:52 am

Personally since you need a handshake for evil twin+captive portal I usually just slap it on to a phone number dict list then if that fails go to evil twin/social engineering but while evil twin is running, use a separate machine for wordlists as you need a client for evil twin and TXpower can be an issue sometimes.

TLDR;

Cracking is better if you have the machine power.

If not and you know the client is active then Evil Twin as no one likes having no Wi-Fi :)