

Forum:[Hack Forums](#)

Thread: [evil twin attack doubt](#)

vijayshetty - February 5, 2024, 4:29 pm

1

evil twin mainly done with pineapple device or kali linux
any tool for windows?

2

what if original network is password protected,how get that password?

webdev77 - February 5, 2024, 4:46 pm

1. Windows doesn't have readily available tools for an evil twin type attack. It's drastically harder to do because the network stack isn't as easily accessible. No real reason to do it from windows honestly when a VM with linux works fine. If you want your main OS to be windows still, just use virtualbox to spin up Kali or Windows Subsystem for Linux.

2. Try to crack it, use a fake active portal, or otherwise obtain the passphrase.

DramaKing - February 5, 2024, 8:28 pm

(Feb 5, 2024 05:29 PM)vijayshetty Wrote: [\[CITE\]](#) 1

evil twin mainly done with pineapple device or kali linux
any tool for windows?

Pretty sure there isn't. Microsoft didn't design Windows with access point applications in mind. Even if you had experience with writing Windows applications, I doubt that you would be able to create a working Evil Twin.

(Feb 5, 2024 05:29 PM)vijayshetty Wrote: [\[CITE\]](#) what if original network is password protected,how get that password?

There's only a hundred tutorials here on WiFi hacking, including the pinned thread, as well as as Hacking Tutorials. People frequently post about WiFi passwords. There are completely guides that just require a quick search to find. Don't post questions that have answers available at a glance.

vijayshetty - February 6, 2024, 1:04 pm

There's only a hundred tutorials here on WiFi hacking, including the pinned thread, as well as as Hacking Tutorials. People frequently post about WiFi passwords. There are completely guides that just require a quick search to find. Don't post questions that have answers available at a glance.

[/quote]

yes,but dont want to brute force/dictionary attack password

webdev77 - February 6, 2024, 1:08 pm

Quote: (Feb 6, 2024 02:04 PM)vijayshetty Wrote: [\[CITE\]](#) There's only a hundred tutorials here on WiFi hacking, including the pinned thread, as well as as Hacking Tutorials. People frequently post about WiFi passwords. There are completely guides that just require a quick search to find. Don't post

questions that have answers available at a glance.

yes, but don't want to brute force/dictionary attack password
What exactly do you want to do?

kohut124 - February 6, 2024, 1:37 pm

(Feb 5, 2024 05:29 PM) vijayshetty Wrote: [\[CITE\]](#) 1

evil twin mainly done with pineapple device or kali linux
any tool for windows?

2

what if original network is password protected, how get that password?

Easiest way to do this assuming you have all the right wifi cards that support Master Mode/AP Mode etc needed is

1. Have Kali booted up on a PC
2. Download and install the Lazy Script
3. Navigate through the menu's and use the tool Fluxion
4. Cap the AP's Handshake, create the evil twin
5. Use your Pineapple to de-auth clients mdk3/mdk4/airgeddon
6. Wait for them to connect to your Evil Twin and type in the password.

That's the easy route when trying to hack your own network.

If it's your neighbors then just ask them for the password.

For your second question on getting the password

Evil Twin AP / WPS Pixie (or using reaver)

Capturing a Handshake (WPA3 not supported as of right now if I'm not mistaken) and manually brute force the password via password lists

Krack attack for specific type of networks..

That being said I recommend you look at how aircrack-ng suite, Reaver/Pixie, hostapd and understand how to do everything manually.