

Forum: [Hack Forums](#)

Thread: [Which way is most suitable for me?](#)

UnicornJap - November 24, 2018, 8:43 pm

Hi, I have been trying to read through many threads but there is so many different approaches and most stuff are too technical for me (I am very basic in this regard).

I want to get log-in information on someone, this person usually use my Wifi, so I figure it might be easier that way.

I am mostly interested in Facebook and Instagram, facebook might be easy since they use their computer at my place a lot but instagram is only through the phone, is that still possible?

Which approach do you guys recommend to me? I am open to every alternative as long as it does not cost too much.

SysAdmin - November 25, 2018, 8:36 am

A MiTM Attack that would lead to DNS Poisoning and another attack that I am not at liberty to discuss due to the rules in place on this forum.

Check out my thread on MiTM Framework;

[Influence | Using MiTMf | MiTM, DNS & ARP Spoofing](#)

FriendZone - November 25, 2018, 9:07 am

(Nov 24, 2018 09:43 PM)UnicornJap Wrote: [\[CITE\]](#) Hi, I have been trying to read through many threads but there is so many different approaches and most stuff are too technical for me (I am very basic in this regard).

I want to get log-in information on someone, this person usually use my Wifi, so I figure it might be easier that way.

I am mostly interested in Facebook and Instagram, facebook might be easy since they use their computer at my place a lot but instagram is only through the phone, is that still possible?

Which approach do you guys recommend to me? I am open to every alternative as long as it does not cost too much.

You have many options, you can scan his device for vulnerabilities (metasploit) to own it, then keylogger.

Or Social Engineering and Dns spoofing, you can redirect him to your server, but it's mostly social engineering coz facebook is one of the sites already recorded in the major browsers, it will be hsts protected also. It means to move this kind of attack you will need at least no caches saved and better if you own a trusted Certificate. You can instead poisoning Google with your server which has an http version, from it rework the way he will find facebook (so basically make a fake google result with your server link in this way the browser wont be able to lock it) that just one way an easy one, I was able to spoof even facebook in google chrome which is one of the hardest, but it's definitely not easy

SIM-3429335 - November 25, 2018, 10:17 pm

Research Man-in-the middle attacks and DNS Poisoning. you WILL find your answer there.

UnicornJap - November 27, 2018, 3:54 am

Thank you all! Seems like I have some reading to do

1asdasd1 - November 27, 2018, 11:42 pm

Just what I was searching for :D

Thanks!