

Forum:[Hack Forums](#)

Thread: [how to collect data from a public network ?](#),

Nanaciel - December 7, 2021, 4:40 pm

Hello, I would like to conduct an experiment but you see, I am new in the "hacking" I know computer security in general. Proxy, vpn etc. the classic.

My question is quite simple... how can we try to retrieve data from a public network such as McDonald's? I would like to make people in my neighborhood aware of the risk of not being well protected, I myself have suffered in the past from a data leak in a restaurant with free wifi and I would like to avoid this happening to people I know.

But in fact, I can only tell them that it is possible, like a VPN commercial on TV... so I would like to know more about it to be able to popularize the subject and to be able to bring them proofs and arguments by an experiment in the McDonald's of my neighborhood.

So I would like to try to collect some basic data, such as one or two passwords, to alert people to the potential danger of being poorly protected. When I talk about being "poorly protected" I mean the fact of not having for example a two-factor verification or of having left active the option "one-click purchase" on their mobile or computer.

So i come here in order to have potential information on the steps to follow to realize my experiment ?.

Nanaciel - December 8, 2021, 3:59 pm

(Dec 8, 2021 11:11 AM)forfeit Wrote: [CITE](#) it usually doesnt happen because they containerize each login but maybe the one you visited was an independently franchised store that has free wireless

in any case if they're not containerized someone can just run a mitm atk or something but most sites now require ssl so youd have to break the encryption to get anything worthwhile

then again i guess people can make internal phishing portals etc that's probably most likely waht happens

I heard about a way to create a public network similar to "Mcdonald's free wifi" in English to fool people, is it possible? I live in a francophone province so the network names are in French so people could be prepared for a movement to encourage linguistic diversity I think.

The networks are free and without password there is simply a message asking to accept to receive mail from McDonald's Canada or not by entering an email but nothing forces us to do so.

So how can I do it? ?

LXST1741 - December 19, 2021, 7:59 pm

(Dec 8, 2021 11:11 AM)forfeit Wrote: [CITE](#) it usually doesnt happen because they containerize each login but maybe the one you visited was an independently franchised store that has free wireless

in any case if they're not containerized someone can just run a mitm atk or something but most sites now require ssl so you'd have to break the encryption to get anything worthwhile

then again i guess people can make internal phishing portals etc that's probably most likely what happens

what does it mean to "containerize each login" ?

Perciville5241 - December 30, 2021, 2:33 pm

(Dec 19, 2021 08:59 PM)LXST1741 Wrote: [\[CITE\]](#) what does it mean to "containerize each login" ? each node that goes on the network is segregated from the other so if billy bob connects his phone, his traffic isn't heard by Eve who is eavesdropping and trying to Wireshark other devices on the network.

Unless you're at the local cafe run by a granny with a standard home hub set up for everyone to "connect to".

Having said that though - if it's an open no authentication wifi AP then you can MITM with a Pineapple or another OpenWRT router, hell you could even use an Alfa if you have one.

jessepinkman420 - August 8, 2022, 8:15 am

(Dec 8, 2021 05:20 PM)shatter Wrote: [\[CITE\]](#) it's called a fake access point

Can this be done digitally or will you always need to be present physically to create a fake access point?

Toe Jam - August 16, 2022, 3:57 pm

(Dec 8, 2021 05:20 PM)shatter Wrote: [\[CITE\]](#) it's called a fake access point

I think you mean "evil twin attack"

Ryzeaf - January 9, 2025, 9:23 pm

Thanks twin i appreciate it <3