

Forum:[Hack Forums](#)

Thread: [Wi-Fi post exploitation?](#)

SkunT3llo - August 9, 2022, 7:08 pm

Hello to everyone who's reading this!?

After You get connect to target Wi-Fi and scan whole network (MAC + IPv4 + IPv6 + OS + open ports) and If there is no working public exploit for any open port, what's the next thing You do?

And based on experience, what is in your opinion most effective attack in the network?

ice_c00l - August 11, 2022, 2:30 pm

Personally I'd monitor for unencrypted traffic with Wireshark and also look for POST messages. I would look to use Responder for any user connections if you are on the WiFi. Might be able to pick up some usernames / credentials that way. Use Crackmapexec with any found username/passwords against a range of services of those IPs.

ThrillQuks - September 1, 2022, 5:03 am

(Aug 9, 2022 07:08 PM)SkunT3llo Wrote: [\[CITE\]](#) Hello to everyone who's reading this!?

After You get connect to target Wi-Fi and scan whole network (MAC + IPv4 + IPv6 + OS + open ports) and If there is no working public exploit for any open port, what's the next thing You do?

And based on experience, what is in your opinion most effective attack in the network?

Since you are connected and can access the local panel page, routersploit might be good option

SkunT3llo - September 1, 2022, 8:29 am

(Sep 1, 2022 05:03 AM)ThrillQuks Wrote: [\[CITE\]](#) Since you are connected and can access the local panel page, routersploit might be good option

Yeah, might be, but what if routersploit fails, what are the other ways/options?

AlmightyK - September 1, 2022, 9:52 am

Well if there is no available exploit for the targets then you would have to attack from a different vector. I'd ARP Ban all clients on the network, then, create a duplicate (fake) access point that is identical to the AP I ARP banned. If users connect to the AP. A capture page can be displayed on the victims browser. This page can be whatever you want, it can ask for credentials or anything else you might need. This is only one of many different options.

SIM-5614029 - February 18, 2025, 3:52 am

bumping this thread for more input

Control Alt Elite - March 15, 2025, 9:26 pm

I'd try to deauth the clients and then get them to connect to a WiFi access point that I control - maybe passing them to a captive portal that has an executable that they "need" to download and install. Should be smooth sailing from there.

Depicide - April 26, 2025, 12:31 am

Evil portal is always a good way to collect credentials. If you are on the network already I would start looking into the IP's, and individual connections that are on the network to gain more info. You may

capture a phone or computer or their home security system as well and find an open camera.

Running IP's through programs and sites like shodan.io can speed up your process and help you look for more access points as well and other vulnerabilities in their network.

PhoneSploit is also a great program if you end up catching phone data as well.

<https://github.com/AzeemIdrisi/PhoneSploit-Pro>