

Forum:[Hack Forums](#)

Thread: [Things someone can do if he has access to admin router page](#)

ilija - January 1, 2019, 3:52 am

Hello there! I'm wondering what someone could do if he had admin privileges in my router configuration page. I know he could change DNS settings or SSID or password , but could he spoof the traffic or scan the devices connected for further exploitation? ?

FriendZone - January 1, 2019, 9:28 am

(Jan 1, 2019 04:52 AM)ilija Wrote: [\[CITE\]](#) Hello there! I'm wondering what someone could do if he had admin privileges in my router configuration page. I know he could change DNS settings or SSID or password , but could he spoof the traffic or scan the devices connected for further exploitation? ? Spoofing and scanning don't require admin privileges, a wifi access is enough.

CyberError - January 1, 2019, 9:29 am

well you can enable WPS and save that key so you can have your backdoor open if router wifi password get changed , and i dont think you can do much

Baud - January 1, 2019, 10:50 am

I'm surprised nobody mentioned one of the most fun things to do: backdooring the firmware. It's not always possible if the router performs sanity checks over files upon upload or if the firmware files are encrypted, but when you can it allows you to have complete control and access to the actual file system instead of just the web interface, and that opens a lot more options.

PerfectStorm - January 1, 2019, 10:52 am

Not too much to be done that I know of. I mean its just a router configuration page.

webdev77 - January 1, 2019, 10:53 am

Flashing new firmware onto the router is a real possibility. Changing over to DD-WRT or similar could disable the physical reset button on the router then. Good luck fixing that problem.

FriendZone - January 1, 2019, 11:11 am

(Jan 1, 2019 11:50 AM)Baud Wrote: [\[CITE\]](#) I'm surprised nobody mentioned one of the most fun things to do: backdooring the firmware. It's not always possible if the router performs sanity checks over files upon upload or if the firmware files are encrypted, but when you can it allows you to have complete control and access to the actual file system instead of just the web interface, and that opens a lot more options.

You're right but what Op asked if spoofing and scanning were possible with admin privileges.

I guess he doesn't know how exactly this kind of attacks work, because admin privileges are not a requirement for spoofing or scanning in a common LAN. That s probably the first thing he should understand to protect himself

Angelis - January 1, 2019, 11:26 am

Use of the router can lead to many possible results, primarily you control the routing you can tell shit where to go.

IE you can route google to yahoo if you were so inclined.

This can lead to many MITM attacks, such as logging pages or key grabbers.

CyberStrike - January 1, 2019, 1:21 pm

You can do any number of things already mentioned, as well as for example SOHO routers you can tunnel and route traffic through the router basically using their IP. Providing that you have ssh and access to iptables/netfilter. BGP hijacking there are tons of options, and yes the hope is that you have a VPS somewhere hopefully in an important place (this is done by governments). Also SOHO devices after a reboot will just have the iptables/netfilter rules you setup cleared from memory. Backdooring the firmware as mentioned by BAUD is actually a decent idea using binwalk and dd (since some times you get different file types eg trx) you can really get it done.

biggioturbomaster - January 1, 2019, 2:46 pm

DNS poisoning could be pretty annoying and powerful to get more control.

Asdethprime - January 1, 2019, 2:47 pm

If you are already in the wifi box as admin you can change what the box is meant to do.

Scanning for vulnerability is not something wifi does but it's most likely running Linux ; and you may be able to download these scanners directly there and with a bit of editing get it to scan the computer that connects to it next.

You are unlikely to be able to sniff much as everything is encrypted and your wifi box is never given the key used for https (which is used virtually everywhere)

Scanning too ; scanning a personal computer likely won't get u far as these computers are , by nature , designed not to accept any traffic unless one is initiated from the computer.

The kind of things u want to get at ; your barrier is ENCRYPTION (when trying to sniff) and the built in OS protecting (for scanning)

ilija - March 11, 2019, 3:49 pm

(Jan 1, 2019 03:47 PM)Asdethprime Wrote: [\[CITE\]](#) If you are already in the wifi box as admin you can change what the box is meant to do.

Scanning for vulnerability is not something wifi does but it's most likely running Linux ; and you may be able to download these scanners directly there and with a bit of editing get it to scan the computer that connects to it next.

You are unlikely to be able to sniff much as everything is encrypted and your wifi box is never given the key used for https (which is used virtually everywhere)

Scanning too ; scanning a personal computer likely won't get u far as these computers are , by nature , designed not to accept any traffic unless one is initiated from the computer.

The kind of things u want to get at ; your barrier is ENCRYPTION (when trying to sniff) and the built in OS protecting (for scanning)

I was thinking about changing the dns server to my own and then dns poisoning the requests, although I'm not quite sure how to

Fallenour - March 12, 2019, 7:35 am

(Jan 1, 2019 04:52 AM)ilija Wrote: [\[CITE\]](#) Hello there! I'm wondering what someone could do if he had admin privileges in my router configuration page. I know he could change DNS settings or SSID

or password , but could he spoof the traffic or scan the devices connected for further exploitation? ?

Stop thinking configuration, and start thinking data. All of your internet connections go over that router. All the data, all the logins, all the sessions. Data is far more valuable than locking someone out of a device.

ilija - June 24, 2019, 5:56 pm

(Mar 12, 2019 07:35 AM)Fallenour Wrote: [\[CITE\]](#) Stop thinking configuration, and start thinking data. All of your internet connections go over that router. All the data, all the logins, all the sessions. Data is far more valuable than locking someone out of a device.

How could i collect the data tho