

Forum:[Hack Forums](#)

Thread: [taking over devices on the local network \(help\)](#)

To*kOv% - May 21, 2022, 9:50 am

i'm new to hacking, how do I take over devices on a local network for which I know the password?

darktechspec - May 21, 2022, 2:45 pm

OK, first look at the DHCP pool, find the connected devices, grab the mac address then google "mac address lookup" then search each mac, that will tell u the company that made it, usually intel are pc's and laptops, broadcoms are usually phones, netgear are routers, some companies make access control, some make epos. Sometimes the names of the devices make sense, and you can work out windows devices.

Note down the IP addresses you will need this later

Now check the NAT settings, look for IP addresses and if the device you want to access is not on the list, enable it lol. eg, if you see windows running, setup portforwarding on terminal services and smb then connect using that password. Do this will all the devices on the network.

If fails, try exploits from public sources

skull - May 22, 2022, 2:32 am

There is no simple way to do this.

You will have to lookup the different connected devices and see if there are any known security exploits for them.

However, MITM-attacks are an option if you control the network. But this topic is not allowed here on HF I think.

darktechspec - May 22, 2022, 3:12 am

mitm attacks are useful, dns poisoning is useful too