Vulnerabilities:

Usually, the network we have at home has a router, this router does all the functions we need to connect to the internet, is a router, a switch and a WAP ( wireless access point ). This router is connected then somehow to the internet, and then all of your devices on its network can access to the internet through itself.

There are four main vulnerable points in your home network:

* Internet (external attacks directly from the router way)
* WAP ( Anyone can have access to your network via your WAP )
* Devices (everything that is connected to your network)
* Company ( how are you connected to your company )

Internet:

Now that we know a little more about networking, we know that the internet is just the pool of al the devices that exist in the world, all connected at once, and each one of them are different in two aspects: the first one is something that will never change, the MAC address. The second one can variate in time, because this address the IP address is given by the router, or whatever device that is connecting you to the internet, or to any kind of network. The problem is that for any moment in time, if we are connected to the internet, we WILL always have an IP address and if someone with enough knowledge about hacking and networking knows that info, can use it to hack the device.

The public IP address is something that we can easily know by just typing in google “What is my IP address”. With this information a hacker, for example might try to break in by any weak point that our network has. Let’s use an online tool as an example of it: <https://pentest-tools.com/> which you have to pay, but you can do some free scans.

What we are looking here are open ports. Ports are the ways in and out in a server and that is what hackers target.

How do we access?

People usually have firewall. What a firewall does is that closes all the ports in a way that nothing can come in unless you expressly request it. If we want to get in a device that device need to have at least an open port, like for example, when you have a website running in your laptop and you have port 80 or port 443 for HTTP or HTTPS protocols. If you do, then that is a hole and someone can easily get in.

Other way of scan you network:

A free way to do a complete scan is to use **nmap** using a Linux server outside your network so it can work. First, we have to go to linode.com, which is a website where we can go and play with a free Linux server for free, for approximately 20 months.

Nmap:

Nmap is a tool we can use in Linux that allow us to know which ports are open in a determined IP address. Also gives us the possible attacks we can use to hack a device with a concrete settings structure. What is dangerous about nmap is that people usually use it in ranges of IP addresses and if you are in one of those, and your network is weak, you can get hacked.

Nmap has a lot of things that I need to know and study, and I am going to dedicate just a whole folder for this kind of stuff but ill do that in my Linux VBox computer. For now, let’s say that ports are what is important here, and nmap helps you find those ports, also tells you which attack you can use, how to use them by referencing its documentation. That’s fucking SICK!!!

How to protect yourself?

A screenshot of a computer

Description automatically generatedBasically, if we want to protect ourselves from this kind of attacks we just have to install a VPN service. Mine for example comes pre-installed with the Anti-Virus and this is how **ipconfig** looks like when we use it:

Figure 1

IMPORTANT

Now this doesn’t mean that I’m completely protected, because in my network, exist more devices that aren’t using a VPN, like an Alexa, for example; or another computer, or a phone for example. But this is not always the best way of securing yourself because these people are using the nmap in ranges of IP addresses and if yours happens to be there, your real one, not the one provided by your VPN, and you have an open port, or your router’s settings are pointing to a weak structure, you might also get hacked.

Router’s Settings (WAP):

Now that ewe know that our router needs better settings combinations, what are those combinations?

* **Firewall active**
  + This is mostly on, so is very probable that this will not be a big deal
* **NAT Forwarding / Port Forwarding**
  + Even if we have or firewall active, we might be letting some traffic in or out by having any open port. When we go to these settings, we can see which ports are being allowed.
* **Disable Remote Management**
  + This is an option that might be enabled, and hackers can easily use this to get in and manipulate your device remotely.
* **Change Default Credentials**
  + Routers have software, and if a hacker has your credentials, or, if you have a default set of credentials, is like you are giving them the keys to enter you home.
* **Upgrade Always**
  + If there is a software upgrade for the router is always convenient to get it.
* **Wireless Settings**
  + **Security** : WPA/**WPA2**
  + **Password**: Recommendable to use a strong password
  + **Network Name**: If a hacker sees the default name, which is the router type you have, that can give him lots of info about how to get you data easily. **Always change it**.
  + **Gest Network**: It is never good to give your network, the one that you use for your stuff for someone else. Is better to just buy on router that has this feature or buy two routers for two networks. This way your home network remains “private”.
* **Disable the Ping response**:
  + **Respond to Pings from LAN** : Disabled
  + **Respond to Pings from WAN** : Disabled
  + If this is on, someone can ping your network and if your router responds a hacker can know that there is a device there.

Devices:

Even if our network and its traffic from outside is being monitored, we still have no-smart for calling them that way, devices that are always using internet. A light-ball, a very simple and inoffensive device, can be used to get into your networks since it might have no firewall, and well, he has a MAC address and its own IP address and if there is no protection there…Dude, you’re so fucked!

And we are not just talking about these, no no, there is also other kind of devices that might use a Wi-Fi connection, like a TV, for example, or a toilet (-\_-).

So how do we work on this?

What we can do is simple, just separate the devices. If we classify our devices in different categories, and then connect each category to its own category network no device from the Secret-Stuff-Category can interact of have access to the Alexa-Tv-light-Ball-Category.

This ISOLATION is the best way of doing this. This principle is also applied in the gest Wi-Fi setting that we saw before.

VLAN:

The isolation system we saw before can become very expensive if we think of having 4 or 5 categories that’s why we get a device that is able to create VLANs or Virtual Local Area Networks. Other option is to take the standard router that we usually get and use a software called -DD-WRT. The Unifi is the device we can use for this task.