Why do we need port security?

Well, one open port is an opportunity to take advantage of someone. There are tons on tool out there that allow you to know all the details of a Network by just plugging it in, and it takes less than on minute. To receive a message to your phone with all that info, like a **Shark Jack** from Hak5.

So how do we protect from attacks like those?

First let’s take a look into the Shark Jack.

**Shark Jack** is actually a Linux server running inside a very little device and as every Linux server we can configure it by SSHing into it by connecting it to your computer in the neutral configuration.

Microsoft Windows [Version 10.0.19041.1052]

(c) Microsoft Corporation. All rights reserved.

C:\Users\chuck>ssh root@172.16.24.1

root@172.16.24.1’s password:

BusyBox v1.28.4 () built-in shell (ash)

\\_\_\_\_\_\_)\\_\_\_\_\_ Shark Jack \_\_\_\_\_\_/(\_\_\_\_\_\_/

/--V\_\_\_\_\_ \_\_°< by Hak5 >°\_\_\_ \_\_\_\_\_V--\

)/ \(

root@shark:~# █

So, this is an actual Linux server, and we can use all Linux commands:

root@shark:~# ls

VERSION loot payload

root@shark:~# █

The loot folder is the result of our attacks. Is where the nmap search results go.

root@shark:~# cd loot/nmap

root@shark:~loot/nmap# ls

nmap scan\_1.txt

root@shark:~# █

If we want to see the information, we just have to use cat and voila.

root@shark:~loot/nmap# cat nmap scan\_1.txt

root@shark:~# “””ALL INFO GOES HERE”””█

Now the payload folder is where we have the script that does the work

root@shark:~# ls

VERSION loot payload

root@shark:~# cd payload

root@shark:~/payload# ls

payload.sh

root@shark:~/payload# cat payload.sh

(...)

HERE GOES THE SCRIPT

(...)

root@shark:~/payload# █

So, how do we stop it:

First thing you want to do is to shut down the ports you are not using so the Device can’t get an IP address and access the data.

If we still must have some ports open something else we can do is put them into a VLAN, a virtual local area network, so it is in its own isolated network, and it cant access the other devices or the other parts of the network.

**PORT SECURITY:**

Here what we want to do is say to the switch that only the device that has a certain MAC address can connect to a certain port. (O\/0)//. Problem Solved.