**SPYING ON NETWORK DEVICES**

**USING BETTERCAP ARP SPOOFING ATTACK**

Assuming we are already in the middle of the connection and this data is already flowing through our computer

So all we have to do is just use a program to capture this data and analyze it

We can do this using **Wireshark** but now we will be using a Module that comes with **BetterCAP** **that will automatically capture all of this data, analyze it and show us the interesting stuff**

So all we have to do now is to tell **BetterCAP** to capture all of the data that is flowing through this computer and analyze it for us

**To do this, we can use the net.sniff Module**

We can do help **net.sniff** to see all the options that you can set for this Module but we wont do that now so we are just going to do:

**net.sniff on**

**Now everything that is going to flow through our computer will be captured and analyzed by the net.sniff Module**

**!! What we are doing right now will not work against HTTPS but later we will bypass HTTPS and why this wont work !!**

**We can still test it by going to vulnweb.com that doesnt use HTTPS**

If we open this site through our target and if we go to the Kali machine we will see that every request that we sent was actually captured by this computer

We will see we made a request for this website **vulnweb.com**, we can also see all of the other files that this website loaded

If we open a site in **vulnweb.com that has login** and we log into the site and if we go back to the Kali machine, we can see we captured a login that was sent to this website - **testhtml.vulnweb.com**

**We can see that the username was test and the password was 1q2w3e4r**