**DNS SPOOFING**

**CONTROLLING DNS REQUESTS ON THE NETWORK**

**DNS == server that converts domain names such as google.com, to the IP of the server that is hosting this website**

**So when you type google.com in your web browser, the request goes to a DNS server, the server responds with the IP where google.com files are stored and the browser will load the website from this IP**

**When we are the man in the middle, the requests for google.com will pass through us first before it goes to the DNS server**

Therefore, instead of giving the IP of the server that is hosting google.com, we can give any IP we want so we can redirect them to a fake website with a backdoor or with evil code, hijack software updates and much more

Lets run **basic DNS spoofing attack** in which we redirect requests from a specific website to our own website or our own web server

**We must decide on where to redirect our target to**

**We can redirect them to any website we want**, for example when someone requests google.com, we can redirect them to Yahoo but what we want to do is we want to redirect them to our own website, to a local website that we are going to start on Kali

**Kali comes with its own web server so we can actually use it as a website and to do this, all we have to do is just start the web server:**

service apache2 start

**apache2 is the name of the web server and we are saying that we want to start this service**

To access this website, to access this server, we have to go to Kali's IP

**To get our IP, as we know, we can do ifconfig and our IP for example is inet:**

**10.0.2.15**

**So if we go to a web browser and go to 10.0.2.15 we will get the default page of this website**

**The pages for this default website are stored in var/www/html**

So if we type **/var/www/html** we can see the files for our website, so if we want to install a fake website or any type of website, all we have to do is put the files in the directory

**index.html is the file that gets loaded by default**

So we will redact the main page by right clicking index.html and open it with text redactor and delete everything and put smiley face for example :)

**Lets run the DNS spoof attack by opening BetterCAP and use the same command we have been doing so far:**

bettercap -iface eth0 -caplet /root/spoof.cap

**Now the module that we want to use is called - dns.spoof**

**If we type help dns.spoof to modify the options for the module, we can see dns.spoof.address**

**This is the address that the user will be redirected to**

**If we want to redirect them to another website, we have to put the IP of this other website here**

In our case we want to redirect them to our local website which is running at **10.0.2.15**, therefore we are not going to have to modify the option because by default the option is set to the IP of our interface

**The next thing we want to modify is the dns.spoof.all**

**We want to set this to true so that BetterCAP responds to any DNS request**

**Now we will set it on true:**

set dns.spoof.all true

**The next thing we want to modify is the dns.poof.domains == this will specify the domains that we want to target - to spoof**

**And we can use a comma( , ) to separate more than one domain and if we want to target zsecurity.org and redirect that to our own website running on Kali**

**And to do this we modify the option like that:**

set dns.spoof.domains zsecurity.org,\*.zsecurity.org

**The star is a wildcard nad it basically means that we want to target any subdomain .zsecurity.org**

**All we need to do now is start the DNS spoof and to do this, we just need to run dns.spoof:**

dns.spoof on

**BetterCAP will tell us that its going to spoof zsecurity.org to 10.0.2.15 which is our IP and it did it automatically**

We can now test this with Win10 VM but keep in mind we might need to **wait a minute or two for the changes to update**

**Now after the target tries to go in zsecurity.org it will redirect him to our smiley face :)**

**!! This will work against all websites even if they use HTTPS but wont work on HSTS sites !!**

**The reason is because the browser has a list of these websites, the lists are stored locally on the target computer so it doesnt send any requests and it will only load these websites over HTTPS so even though the attack will work, the browser will refuse to load the website that we are spoofing them to**

DNS spoofing is very very useful in so many scenarios

You can use it, for example, when someone is trying to go to a login page and show them a fake page or if they are trying to go to zsecurity for example and just show them another zsecurity website with some malware embedded into it

We can also use it to serve fake updates, so whenever they have a software that is going to check for updates we can DNS spoof that request and send them a fake update with a backdoor