The Sn0wF0x Doks

Domain Name System [DNS]

What is DNS?

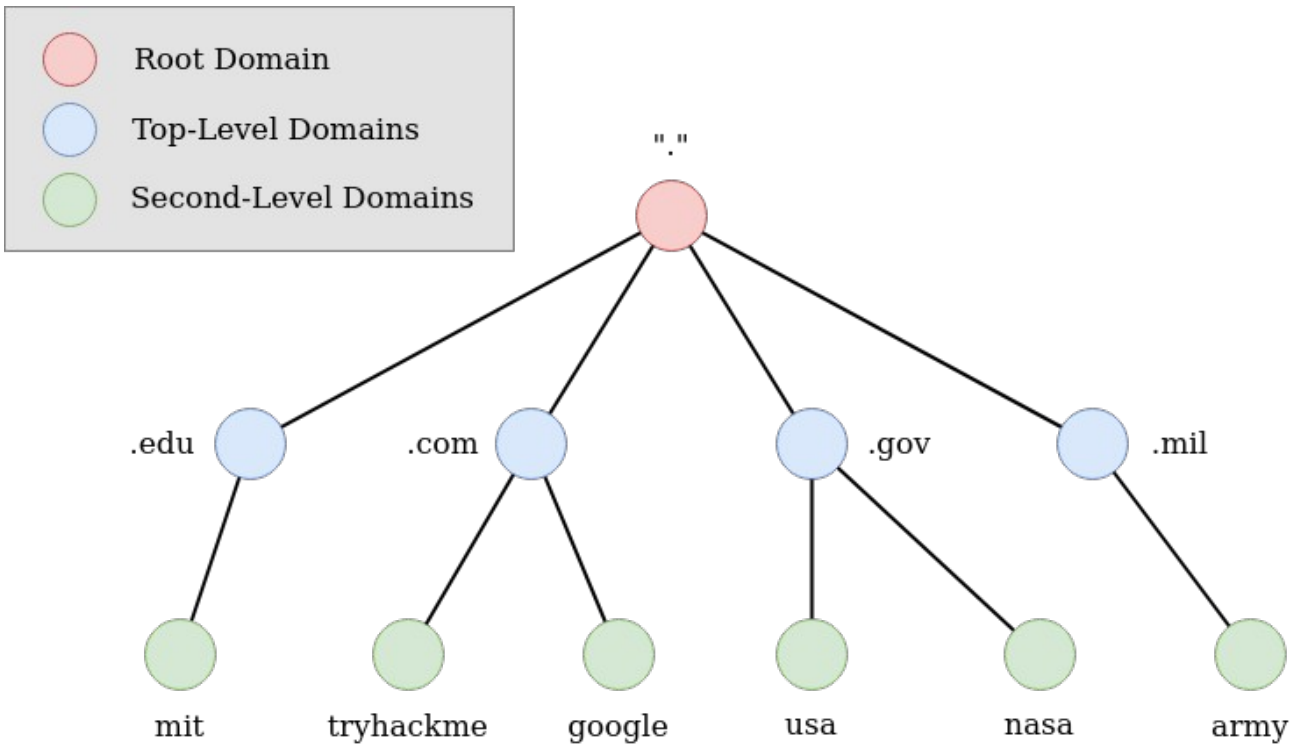
When using the Internet, every website avaible has a unique **IP Adress**.

This IP Adress is an 4 Digits Set Ranging from 0-255 which makes the following Range:

0.0.00 => 255.255.255.255

Remembering every of the IP Adresses would be Kinda Insane. In Todays standarts we all save our Phone numbers under Names so why would we do something else with Websites? Thats where DNS Comes in. DNS helps us to remember the Websites names instead of IP Adresses.

But what are Domains and how are they constructed?



The First thing we are Gonna Analyze are the Top Level Domains (aka TLD):

Lets Take the Following example: http://www.google.com

In this case, the TLD is ».com «

There are 2 Types of TLD.

First of all the gTLD (Generetic Top Level). These were supposted to tell us what the Domains Purpose was.

The Second Type was ccTLD (Country Code Top Level Domain). You might already know what this leads to. Geographic Purposes.

Now we come to Second-Level Domain:

Back to our Example: http://www.google.de

The Second-Level Domain is »google« and is limited to 63 Characters + TLD. The Limit is a-z0-9.

Now to the Last Part, the So Called „Subdomain“.

Doing CTF you will always meet one of thoose. A Subdomain s more or less a Part of the Second Level Domain. Lets asume that http://www.google.de has an admin panel. Then the Sub-Domain would be http://www.admin.google.de where »admin« would be the subdomain part. It follows the same rules as a Second Level Domains, but the amount of Subdomains that are abled to create is infinite.

Now lets talk about DNS-Record-Types.

A Record	These Records resolve the IPv4 Adresses, for example 10.2.3.4
AAAA Record	The Same as Above but with IPv6
CNAME Record	Sometimes its possible that an Subdomain leads to another Domain, like online Shops. The CNAME Record gives you the EXACT Domain Location.
MX Record	More or less the E-Mail for your Domain.
TXT Record	Those are Free Text Fields for any Text-Based Data.

And now for the Finale of this Document:

What Happends when you make a DNS Request [aka Looking for a Name fit to the Destined IP]?

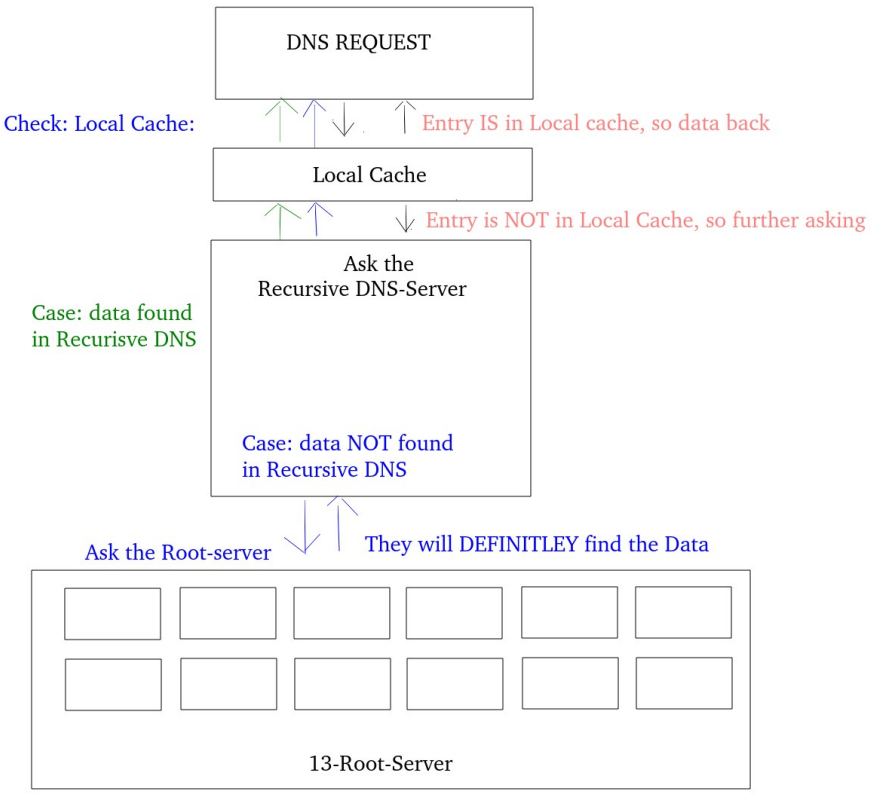
Step 1 : You start a Request for any Domain Name.

Step 2: Your Computers checks the Local Cache if you previously looked for this exact Adress., if he wont find it a request to your recursive DNS Server will be made

Step 3: The Next step depends on your Configuration. If you have choosen your own DNS Server, it will be asked. If you use the one Provided by the ISP, then this one will be asked. No matter who of the Both is now in work, it also has a local cache of recently looked up domain names. In Best Case your requested Domain is here and will be send back. IF NOT, however we go one instance further and coming to the „Root Server“. Theese are 13 Servers all around the world and thoose are more or less what we call the Internet Nowadays

Step 4: The Root server now takes the TLD of your request and gives it to the right TDL Server to find out how to continue

Step 5: The TLD Server finally gives the Data back to the Recursive DNS with the Nessesary Informations and the Request is complete



Credits:

I Hope this might Help Someone on their Journey through Infosec :)

If so, feel free to contact me on Twitter : https://twitter.com/MarcusChachuls1

Created by Sn0wF0x