Whois Records

What is Whois?

Whois is a query and response protocol that allows us to access databases containing information about registered domain names, IP addresses, and other internet resources.

So, Whenever we purchase a domain from a domain registrar like godaddy.com or namecheap. We have to provide some information about us as the owner. Whois database contains all the records of all the domains that is registered.

Now, lets check the whois records for our target - zomato.com

So, there are two ways of doing this, one is by the terminal and the other one is from the web.

Let's see the web one first.

- WHO IS records - https://viewdns.info/whois/
- Whois - https://who.is/

Now that we have seen the web method. Let see the terminal one. So, in linux there is a whois command line tool that comes pre-installed with every linux distribution. With the help of this, we can get the same result that we got from the online websites.

```
whois zomato.com
```

Now as you can see we have some really interesting sections here like the registrar email, phone no and address. However we are not getting any relevant information there. This is because of the privacy guard which most of the registrar provides to the domain owners. Because of this privacy guard, we are not able to get the actual owner details.

But whois records have to be checked while performing recon as sometimes people don't bother to turn on the privacy guard.

Historical Whois Records

If in case, the target has enabled the privacy guard recently. We can query the historical Whois data rather than the new one and if we are lucky, we might get the target details even if the privacy guard is turned ON.

To do this, we have some online tools with us.

-> Whoxy - https://whoxy.com/domain.com
-> Whoisology - https://whoisology.com
-> Domain Big Data - https://domainbigdata.com
-> Security Trails - https://securitytrails.com [Need API KEY]
-> Whois XML API - https://whoisxmlapi.com [Need API KEY]

We can also find other websites that belongs to the same registrar using reverse whois lookup.

```
https://viewdns.info/reversewhois/?q=zomato.com
```
