
Querying the domain registration information

After you know the target domain name, the first thing you would want to do is query the `Whois` database about that domain to look for the domain registration information. The `Whois` database will give information about the DNS server and the contact information of a domain.

`WHOIS` is a protocol for searching Internet registrations, databases for registered domain names, IPs, and autonomous systems. This protocol is specified in RFC 3912 (https://www.ietf.org/rfc/rfc3912.txt).

By default, Kali Linux already comes with a `whois` client. To find out the `Whois` information for a domain, just type the following command:

```
# whois example.com
```

The following is the abridged result of the `Whois` information:

```
Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: EXAMPLE.COM
   Registrar: REGISTRAR.COM
   Whois Server: whois.registrar.com
   Referral URL: http://registrar.com
   Name Server: NS.HOSTING.COM
   Name Server: NS2.HOSTING.COM
   Status: clientDeleteProhibited
   Status: clientRenewProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Updated Date: 08-apr-2012
   Creation Date: 08-apr-2012
   Expiration Date: 08-apr-2015

>>> Last update of whois database: Wed, 25 Jul 2012 02:15:41 UTC <<<

Please note: the registrant of the domain name is specified
in the "registrant" field.  In most cases, registrar.com
is not the registrant of domain names listed in this database.
The Registrant:
   Jalan Sudirman No. 1
   DKI Jakarta
   Indonesia 12345

   Domain Name: EXAMPLE.COM
      Created on: 08-Apr-12
      Expires on: 08-Apr-15
      Last Updated on: 08-Apr-12
```

```
Administrative Contact:
   The Registrant
   Jalan Sudirman No. 1
   DKI Jakarta
   Indonesia 12345
   62 2112345678
Technical Contact:
   The Registrant registrant@example.com
   Jalan Sudirman No. 1
   DKI Jakarta
   Indonesia 12345
   62 2112345678

Domain servers in listed order:
   NS.HOSTING.COM
   NS2.HOSTING.COM
```

From the preceding `Whois` result, we can get the information of the DNS server and the contact person of a domain. This information will be useful at the later stages of penetration testing.

Besides using the command-line `whois` client, the `Whois` information can also be collected via the following websites, which provide the `whois` client:

- www.whois.net
- www.internic.net/whois.html

Or, you can also go to the top-level domain registrar for the corresponding domain:

- America: www.arin.net/whois/
- Europe: www.db.ripe.net/whois
- Asia-Pacific: www.apnic.net/apnic-info/whois_search2

> **Note**
>
> Beware, that to use the top-level domain registrar `whois`, the domain needs to be registered through their own system. For example, if you use ARIN `WHOIS`, it only searches in the `ARIN WHOIS` database and will not search in the `RIPE` and `APNIC Whois` databases.

After getting information from the `Whois` database, next we want to gather information about the DNS entries of the target domain.