

A **whois Kali linux command** is a utility as a part of the information gathering used in all of the Linux-based operating systems. this tool is part of **information security assessment**, and one of **information gathering techniques**. there are a lot of **information gathering strategies**. It is used to identify domain information and more.

- Unknown and distant hosts
- Networks
- Even Netadmins if you use the command the right way and you are lucky enough

IN TECHNICAL TERMS:

“WHOIS is a database managed by local internet registrar, availing to us the personal information about the owner for example: his contact details, his organization, and his IP as well as his geographical location ” we can use **whois command** to retrieve that information.

The usage of whois kali linux

The usage of the ‘whois’ varies widely from system to system, but nevertheless, a common ground is established where you have to give the IP address after the command. The usage of the command in Kali Linux systems is as follows:

whois <ip address/name of the website you want to access the information to>

for example

whois 74.125.68.106

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# whois 74.125.68.106  
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/whois\_tou.html  
#  
#  
# The following results may also be obtained via:  
# http://whois.arin.net/rest/nets;q=74.125.68.106?showDetails=true&showARIN=false&ext=netref2  
#  
NetRange:          74.125.0.0 - 74.125.255.255  
CIDR:              74.125.0.0/16  
OriginAS:  
NetName:           GOOGLE  
NetHandle:         NET-74-125-0-0-1  
Parent:            NET-74-0-0-0-0  
NetType:           Direct Allocation  
RegDate:           2007-03-13  
Updated:           2012-02-24  
Ref:               http://whois.arin.net/rest/net/NET-74-125-0-0-1
```

or

whois www.google.com

```
root@kali: ~  
File Edit View Search Terminal Help  
# available at: https://www.arin.net/whois_tou.html  
#  
root@kali:~# whois www.google.com  
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.  
  
Server Name: WWW.GOOGLE.COM.AR  
Registrar: ENOM, INC.  
Whois Server: whois.enom.com  
Referral URL: http://www.enom.com  
  
Server Name: WWW.GOOGLE.COM.AU  
Registrar: MELBOURNE IT, LTD. D/B/A INTERNET NAMES WORLDWIDE  
Whois Server: whois.melbourneit.com  
Referral URL: http://www.melbourneit.com  
  
Server Name: WWW.GOOGLE.COM.BR  
Registrar: ENOM, INC.  
Whois Server: whois.enom.com
```

In the above pictorials, you note one thing==> whois kali linux command is behaving differently for IP address and site name

- For the IP addresses, the information is much more substantial. Here you got addresses, phone numbers, organization handles and everything
- For the site name, you got the server name registrar and the referral URL which is of course for the whois command. as you can notice that the information is certainly less substantial but fun and relevant if you are just starting.

Typing `whois -help` will grant you further information on the command on the Linux itself.

```
root@kali: ~
File Edit View Search Terminal Help
Registrars.
root@kali:~# whois --help
Usage: whois [OPTION]... OBJECT...

-l          one level less specific lookup [RPSL only]
-L          find all Less specific matches
-m          find first level more specific matches
-M          find all More specific matches
-c          find the smallest match containing a mnt-irt attribute
-x          exact match [RPSL only]
-d          return DNS reverse delegation objects too [RPSL only]
-i ATTR[,ATTR]... do an inverse lookup for specified ATTRibutes
-T TYPE[,TYPE]... only look for objects of TYPE
-K          only primary keys are returned [RPSL only]
-r          turn off recursive lookups for contact information
-R          force to show local copy of the domain object even
            if it contains referral
-a          search all databases
-s SOURCE[,SOURCE]... search the database from SOURCE
-g SOURCE:FIRST-LAST find updates from SOURCE from serial FIRST to LAST
-t TYPE     request template for object of TYPE
-v TYPE     request verbose template for object of TYPE
-q [version|sources|types] query specified server info [RPSL only]
-F          fast raw output (implies -r)
```

The modern versions of whois try to guess the specific object. If no conclusive result is found the query goes straight to whois.arin.net for ipv4 addresses(like we can do anything with ipv6 just yet!! huh SARCASM) or whois.networksolutions.com for NIC handles. Basically, NIC is network interface controller used to connect the computer to the computer network. Further information is available on the WIKI(The blue link I gave).