USAGE OF DIG COMMAND.

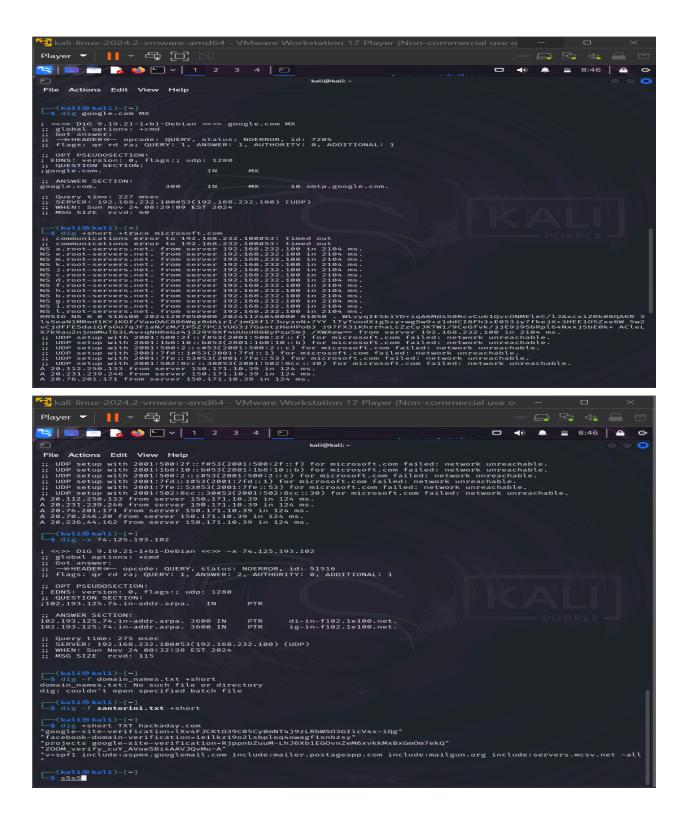
Tools : DIG on KALI Site : google.com

DIG command (short for "Domain Information Groper") is a network administration tool used for querying DNS (Domain Name System) servers. It is typically used to gather information about DNS records, including A records (IP addresses), MX records (mail exchanges), CNAME records (canonical names), and more.

INPUT from DIG:

```
🔁 kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use o
🔇 🛄 🗀 🍃 🐞 🖸 🗸 1 2 3 4 🕒
                                                                                                               □ 4) ≜ 8:45 △
                                                                  kali@kali: ~
File Actions Edit View Help
DiG 9.19.21-1+b1-Debian
(kali@ kali)-[~]
$ dig google.com
;; QUESTION SECTION:
                                        IN
;google.com.
;; ANSWER SECTION:
                                             A 142.250.185.14
                                      IN
;; Query time: 15 msec
;; SERVER: 192.168.232.100#53(192.168.232.100) (UDP)
;; WHEN: Sun Nov 24 08:23:14 EST 2024
;; MSG SIZE rcvd: 44
(kali@ kali)-[~]
$ dig google.com +short
142.250.185.14
[kali⊛ kali)-[~]
$ dig google.com +noall +answer
google.com. 138 IN
___(kali⊗ kali)-[~]

$ dig @8.8.8.8 google.com
; <<>> DiG 9.19.21-1+b1-Debian <<>> @8.8.8.8 google.com; (1 server found)
; (1 Server found)
;; global options: +cmd
;; Got answer:
;; ->>> HEADER - opcode: QUERY, status: NOERROR, id: 5826
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512 ;; QUESTION SECTION:
                                        IN
;google.com.
;; ANSWER SECTION: google.com.
                                      IN A
                                                            172.217.17.14
;; Query time: 147 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Nov 24 08:26:25 EST 2024
```



PROCEDURES AND SOME EXAMPLES OF HOW TO USE DIG COMMAND

We would begin by checking its version by using the following command: dig -v Then, We will begin by performing a simple dig command. Type the following into a terminal: dig google.com

The above command will include several pieces of information. There may be a time when you only want the result of the query. This can be achieved in dig with the following command:dig google.com +short

As you can see, there can be more than one IP for a host record.

This next command will get rid of all information before the answer section, for easier reading. We can specify this using the following command: dig google.com +noall +answer

We can also specify the nameservers we wish to query using the following command: dig @8.8.8.8 google.com This command queries the "google.com" record from the Name Server with IP address 8.8.8.8.

If we want to query all DNS record types, we can use the "ANY" option. This will display all the available record types in the output: dig google.com ANY

We can also look up a specific record. For example, if we want to get only the mail exchange section associated with a domain, we can use the following command: dig google.com MX We can query a number of specific record types using the following tags in place of MX: TXT, CNAME, NS, A

Dig +short +trace {site of your choice}

We can trace the DNS path, similar to traceroute, using the following command: dig -x 74.125.193.102 It is also possible to make DNS queries for IP addresses.

Dig has a useful feature which allows you to perform a number of DNS lookups for a list of domains instead of doing the same for each one individually. This can be done by performing a lookup using a file: dig -f{ domain_names}.txt +short

Dig +short TXT hackaday.com It is possible to access domain verification data by making a DNS TXT query. Dig is a tool with multiple uses and can be very useful for gathering a broad range of DNS information about a target site.