Aim: Use of network reconnaisaance tools like WHOIS, dig, nslookup to gather information about networks and domain registrars

Theory:-

Steps:

1. Open ubuntu terminal.

2. Get root access by typing “sudo su root”. Put the pc password.

3. Install the tool using the following command

```
#apt-get install whois

#apt-get install dnsutils

#apt-get install traceroute

#apt-get install nslookup
```

Theory:

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. Reconnaissance is also known as information gathering and, in most cases, precedes an actual access or DoS attack. First, the malicious intruder typically conducts a ping sweep of the target network to determine which IP addresses are alive. Then the intruder determines which services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the type and version of the application and operating system running on the target host. Reconnaissance is somewhat analogous to a thief investigating a neighborhood for vulnerable homes, such as an unoccupied residence or a house with an easy-to-open door or window. In many cases, intruders look for vulnerable services that they can exploit later when less likelihood that anyone is looking exists.

WHOIS:

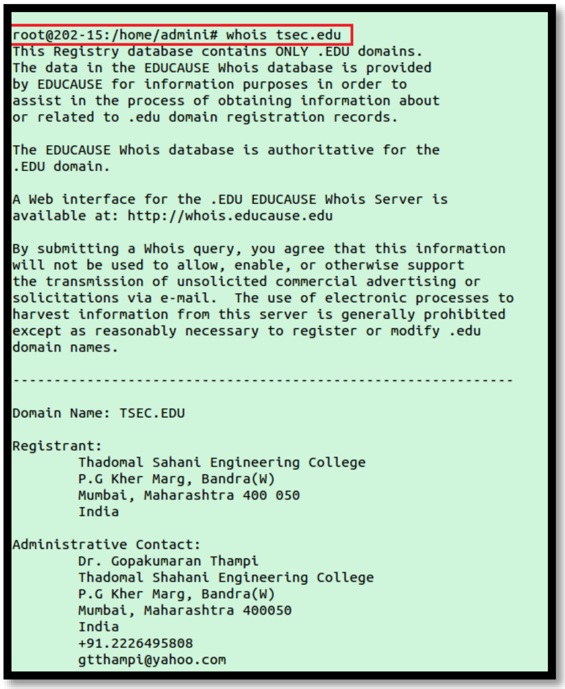
WHOIS is the Linux utility for searching an object in a WHOIS database. The WHOIS database of a domain is the publicly displayed information about a domains ownership, billing, technical, administrative, and nameserver information. Running a WHOIS on your domain will look the domain up at the registrar for the domain information. All domains have WHOIS information. WHOIS database can be queried to obtain the following information via WHOIS:

- Administrative contact details, including names, email addresses, and telephone numbers
- Mailing addresses for office locations relating to the target organization

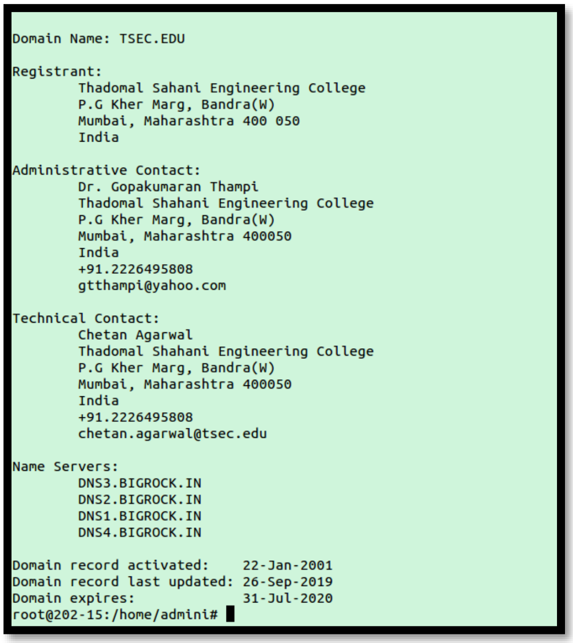
Details of authoritative name servers for each given domain

Example: Querying tsec.edu

student@lab:~# whois tsec.edu



```
root@202-15:/home/admini# whois tsec.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-------------------------------------------------------------

Domain Name: TSEC.EDU

Registrant:
        Thadomal Sahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400 050
        India

Administrative Contact:
        Dr. Gopakumaran Thampi
        Thadomal Shahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400050
        India
        +91.2226495808
        gtthampi@yahoo.com
```



```
Domain Name: TSEC.EDU

Registrant:
        Thadomal Sahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400 050
        India

Administrative Contact:
        Dr. Gopakumaran Thampi
        Thadomal Shahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400050
        India
        +91.2226495808
        gtthampi@yahoo.com

Technical Contact:
        Chetan Agarwal
        Thadomal Shahani Engineering College
        P.G Kher Marg, Bandra(W)
        Mumbai, Maharashtra 400050
        India
        +91.2226495808
        chetan.agarwal@tsec.edu

Name Servers:
        DNS3.BIGROCK.IN
        DNS2.BIGROCK.IN
        DNS1.BIGROCK.IN
        DNS4.BIGROCK.IN

Domain record activated:    22-Jan-2001
Domain record last updated: 26-Sep-2019
Domain expires:             31-Jul-2020
root@202-15:/home/admini#
```

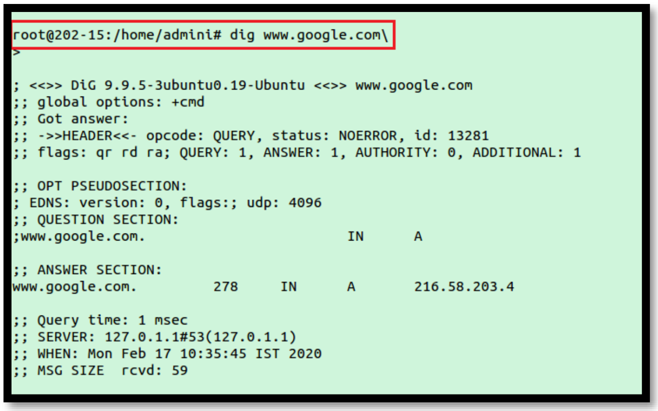
DIG:

Dig (domain information groper) is a network administration command-line tool for querying Domain Name System (DNS) name servers. Dig is useful for network troubleshooting and for educational purposes.

When you pass a domain name to the dig command, by default it displays the A record (the ip-address of the site that is queried) as shown below.

1. Simple dig Command Usage

student@lab:~# dig www.google.com



```
root@202-15:/home/admini# dig www.google.com\
>
; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13281
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         278     IN      A       216.58.203.4

;; Query time: 1 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Feb 17 10:35:45 IST 2020
;; MSG SIZE  rcvd: 59
```

The dig command output has the following sections:

Header: This displays the dig command version number, the global options used by the dig command, and few additional header information.

QUESTION SECTION: This displays the question it asked the DNS. i.e. input. Since we said ‘dig google.com’, it indicates in this section that we asked for the record of the google.com website.

ANSWER SECTION: This displays the answer it receives from the DNS. i.e This is your output. This displays the record of google.com.

AUTHORITY SECTION: This displays the DNS name server that has the authority to respond to this query. Basically this displays available name servers of google.com.

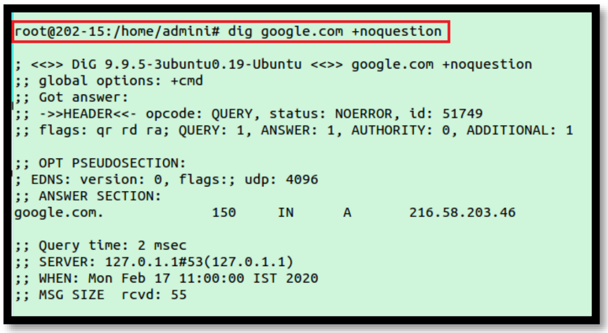
ADDITIONAL SECTION: This displays the ip address of the name servers listed in the AUTHORITY SECTION.

Stats section at the bottom displays few dig command statistics including how much time it took to execute this query

2. Display Only the ANSWER SECTION of the Dig command Output

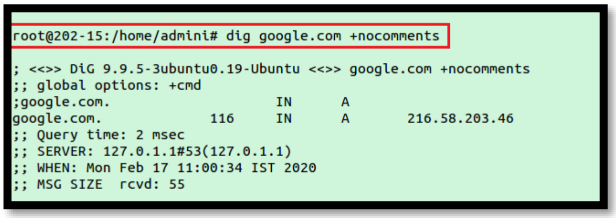
All you need to look at is the “ANSWER SECTION” of the dig command. So, we can turn off all other sections as shown below.

i) student@lab:~ #dig google.com +noquestion



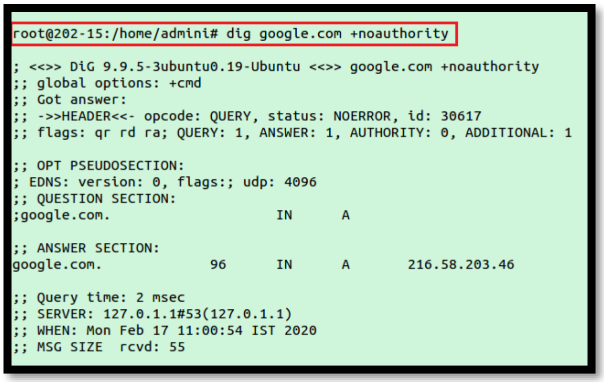
```
root@202-15:/home/admini# dig google.com +noquestion

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com +noquestion
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51749
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; ANSWER SECTION:
google.com.             150     IN      A       216.58.203.46

;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Feb 17 11:00:00 IST 2020
;; MSG SIZE  rcvd: 55
```

ii) student@lab:~ #dig google.com +nocomments – Turn off the comment lines



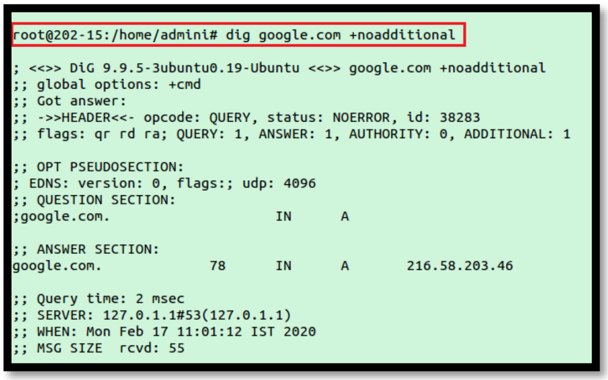
```
root@202-15:/home/admini# dig google.com +nocomments

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com +nocomments
;; global options: +cmd
;google.com.                    IN      A
google.com.             116     IN      A       216.58.203.46
;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Feb 17 11:00:34 IST 2020
;; MSG SIZE  rcvd: 55
```

iii) student@lab:~ # dig google.com +noauthority – Turn off the authority section



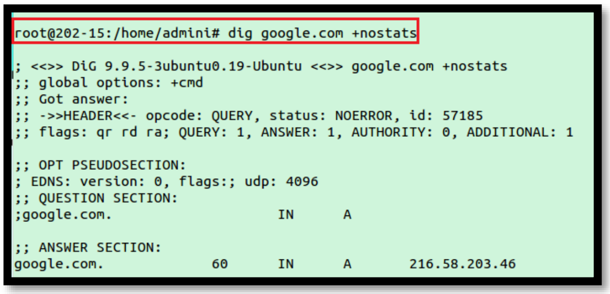
```
root@202-15:/home/admini# dig google.com +noauthority

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com +noauthority
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30617
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             96      IN      A       216.58.203.46

;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Feb 17 11:00:54 IST 2020
;; MSG SIZE  rcvd: 55
```

iv) student@lab:~ #dig google.com +noadditional – Turn off the additional section



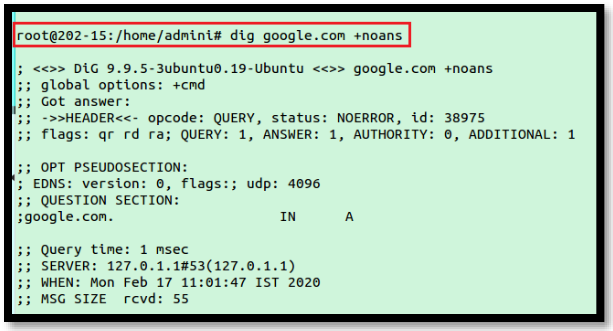
```
root@202-15:/home/admini# dig google.com +noadditional

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com +noadditional
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38283
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             78      IN      A       216.58.203.46

;; Query time: 2 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Feb 17 11:01:12 IST 2020
;; MSG SIZE  rcvd: 55
```

v) student@lab:~ #dig google.com +nostats – Turn off the stats section



```
root@202-15:/home/admini# dig google.com +nostats

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com +nostats
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57185
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             60      IN      A       216.58.203.46
```

vi) student@lab:~ #dig google.com +noanswer – Turn off the answer section

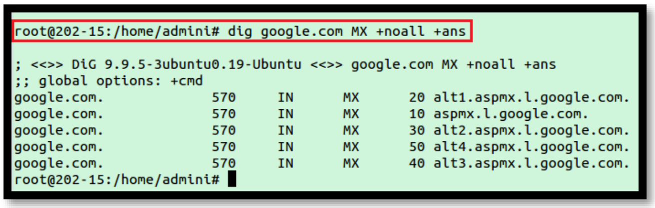


```
root@202-15:/home/admini# dig google.com +noans

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com +noans
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38975
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.                    IN      A

;; Query time: 1 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Mon Feb 17 11:01:47 IST 2020
;; MSG SIZE  rcvd: 55
```

3. Query MX Records Using dig MX

To query MX records, pass MX as an argument to the dig command as shown below.

student@lab:~ #dig google.com MX +noall +answer

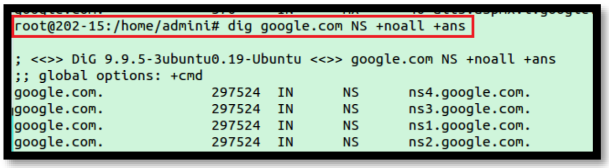


```
root@202-15:/home/admini# dig google.com MX +noall +ans

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com MX +noall +ans
;; global options: +cmd
google.com.             570     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             570     IN      MX      10 aspmx.l.google.com.
google.com.             570     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             570     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             570     IN      MX      40 alt3.aspmx.l.google.com.
root@202-15:/home/admini# █
```

4. Query NS Records Using dig NS

To query the NS record use the type NS as shown below.

student@lab:~ #dig google.com NS +noall +answer

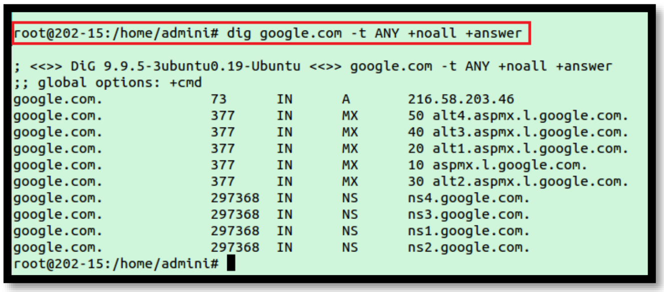


```
root@202-15:/home/admini# dig google.com NS +noall +ans

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com NS +noall +ans
;; global options: +cmd
google.com.             297524  IN      NS      ns4.google.com.
google.com.             297524  IN      NS      ns3.google.com.
google.com.             297524  IN      NS      ns1.google.com.
google.com.             297524  IN      NS      ns2.google.com.
```

5. View ALL DNS Records Types Using dig -t ANY

To view all the record types (A, MX, NS, etc.), use ANY as the record type as shown below.

student@lab:~ #dig -t ANY google.com +noall +answer



```
root@202-15:/home/admini# dig google.com -t ANY +noall +answer

; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> google.com -t ANY +noall +answer
;; global options: +cmd
google.com.             73      IN      A       216.58.203.46
google.com.             377     IN      MX      50 alt4.aspmx.l.google.com.
google.com.             377     IN      MX      40 alt3.aspmx.l.google.com.
google.com.             377     IN      MX      20 alt1.aspmx.l.google.com.
google.com.             377     IN      MX      10 aspmx.l.google.com.
google.com.             377     IN      MX      30 alt2.aspmx.l.google.com.
google.com.             297368  IN      NS      ns4.google.com.
google.com.             297368  IN      NS      ns3.google.com.
google.com.             297368  IN      NS      ns1.google.com.
google.com.             297368  IN      NS      ns2.google.com.
root@202-15:/home/admini# █
```

6. View Short Output Using dig +short

To view just the ip-address of a web site (i.e the A record), use the short form option as shown below.

student@lab:~ #dig google.com +short

7. DNS Reverse Look-up Using dig –x

To perform a DNS reverse look up using the ip address using dig -x as shown below

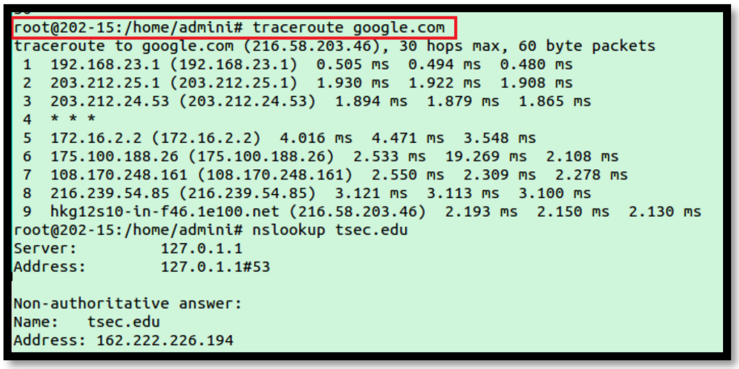
student@lab:~ #dig -x 209.132.183.81

Traceroute:

Traceroute prints the route that packets take to a network host. Traceroute utility uses the TTL field in the IP header to achieve its operation. TTL field describes how much hops a particular packet will take while traveling on network. So, this effectively outlines the lifetime of the packet on network. This field is usually set to 32 or 64. Each time the packet is held on an intermediate router, it decreases the TTL value by 1. When a router finds the TTL value of 1 in a received packet then that packet is not forwarded but instead discarded. After discarding the packet, router sends an ICMP error message of ―Time exceeded‖ back to the source from where packet generated. The ICMP packet that is sent back contains the IP address of the router. So now it can be easily understood that traceroute operates by sending packets with TTL value starting from 1 and then incrementing by one each time. Each time a router receives the packet, it checks the TTL field, if TTL field is 1 then it discards the packet and sends the ICMP error packet containing its IP address and this is what traceroute requires. So traceroute incrementally fetches the IP of all the routers between the source and the destination.

Command:

student@lab:~ #traceroute google.com



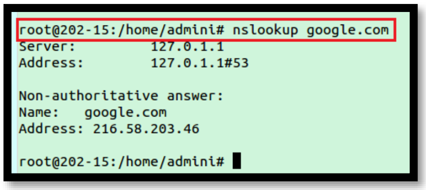
```
root@202-15:/home/admini# traceroute google.com
traceroute to google.com (216.58.203.46), 30 hops max, 60 byte packets
 1  192.168.23.1 (192.168.23.1)  0.505 ms  0.494 ms  0.480 ms
 2  203.212.25.1 (203.212.25.1)  1.930 ms  1.922 ms  1.908 ms
 3  203.212.24.53 (203.212.24.53)  1.894 ms  1.879 ms  1.865 ms
 4  * * *
 5  172.16.2.2 (172.16.2.2)  4.016 ms  4.471 ms  3.548 ms
 6  175.100.188.26 (175.100.188.26)  2.533 ms  19.269 ms  2.108 ms
 7  108.170.248.161 (108.170.248.161)  2.550 ms  2.309 ms  2.278 ms
 8  216.239.54.85 (216.239.54.85)  3.121 ms  3.113 ms  3.100 ms
 9  hkg12s10-in-f46.1e100.net (216.58.203.46)  2.193 ms  2.150 ms  2.130 ms
root@202-15:/home/admini# nslookup tsec.edu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   tsec.edu
Address: 162.222.226.194
```

Nslookup:

The ***nslookup*** command is used to query internet name servers interactively for information. Nslookup, which stands for "name server lookup”. It is a useful tool for finding out information about a named domain. By default, nslookup will translate a domain name to an IP address (or vice versa). Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.

1. Simple nslookup command

student@lab:~ #nslookup google.com

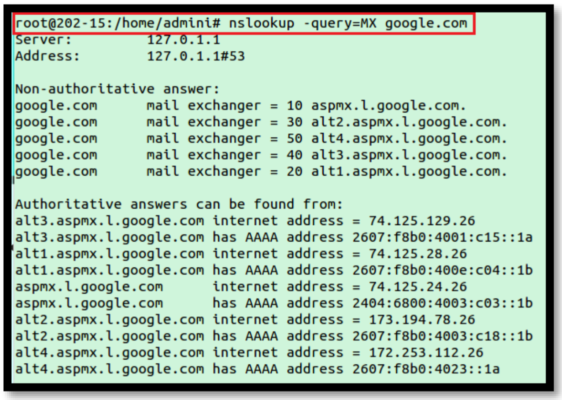


```
root@202-15:/home/admini# nslookup google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.203.46

root@202-15:/home/admini# █
```

2. Query the MX Record using -query=mx

student@lab:~ #nslookup -query = mx google.com

MX (Mail Exchange) record maps a domain name to a list of mail exchange servers for that domain.

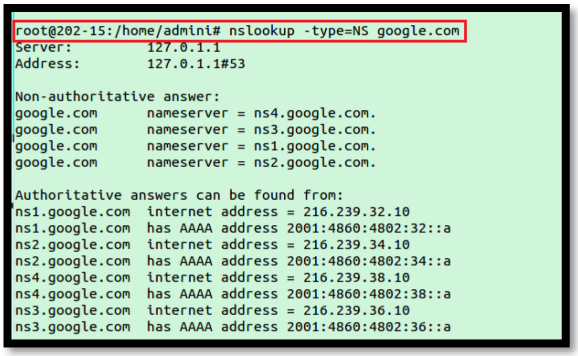


```
root@202-15:/home/admini# nslookup -query=MX google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
google.com      mail exchanger = 10 aspmx.l.google.com.
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
alt3.aspmx.l.google.com internet address = 74.125.129.26
alt3.aspmx.l.google.com has AAAA address 2607:f8b0:4001:c15::1a
alt1.aspmx.l.google.com internet address = 74.125.28.26
alt1.aspmx.l.google.com has AAAA address 2607:f8b0:400e:c04::1b
aspmx.l.google.com      internet address = 74.125.24.26
aspmx.l.google.com      has AAAA address 2404:6800:4003:c03::1b
alt2.aspmx.l.google.com internet address = 173.194.78.26
alt2.aspmx.l.google.com has AAAA address 2607:f8b0:4003:c18::1b
alt4.aspmx.l.google.com internet address = 172.253.112.26
alt4.aspmx.l.google.com has AAAA address 2607:f8b0:4023::1a
```

3. Query the NS Record using -type=ns

student@lab: ~ #nslookup -type = ns google.com

NS (Name Server) record maps a domain name to a list of DNS servers authoritative for that domain.

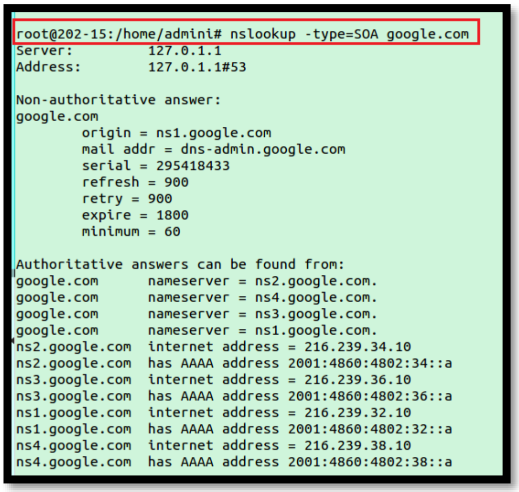


```
root@202-15:/home/admini# nslookup -type=NS google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.

Authoritative answers can be found from:
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
```

4. Query the SOA Record using -type=soa

student@lab: ~ #nslookup -type = soa google.com

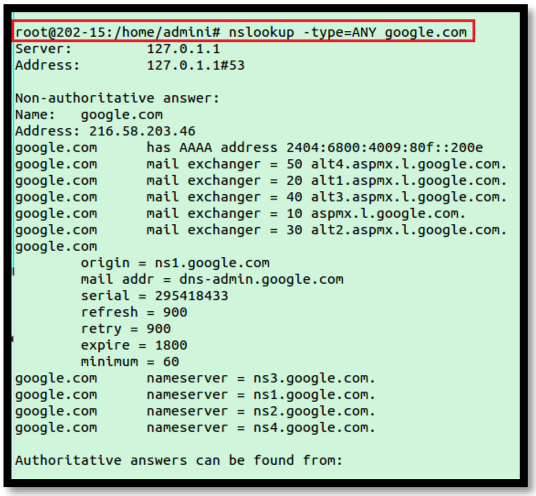
SOA record (start of authority) provides the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number, etc



```
root@202-15:/home/admini# nslookup -type=SOA google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 295418433
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60

Authoritative answers can be found from:
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
```

5. View available DNS records using -query=any

student@lab: ~ #nslookup -type = any google.com



```
root@202-15:/home/admini# nslookup -type=ANY google.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.203.46
google.com      has AAAA address 2404:6800:4009:80f::200e
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
google.com      mail exchanger = 10 aspmx.l.google.com.
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 295418433
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60
google.com      nameserver = ns3.google.com.
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns4.google.com.

Authoritative answers can be found from:
```