Vivekanand Education Society's Institute of Technology

Department of AI & DS Engineering

Subject: Cryptography and System Security

Class: D11AD

Roll No: 46	**Name: Ashish Patil**
Practical No:7	**Title:**
DOP:	**DOS:**
Grades:	**LOs Mapped:**
Signature:	

Title: Network reconnaissance tools like WHOIS, dig, traceroute

DOP: /3/24

DOS: /3/24

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

Theory:(Execute commands and attach screenshots)

Steps:

1.Open ubuntu terminal.

2.Get root access by typing "sudosu root". Put the pc password.

3.Install the tool using the following command

#apt-get install whois

#apt-get install dig

#apt-get install traceroute

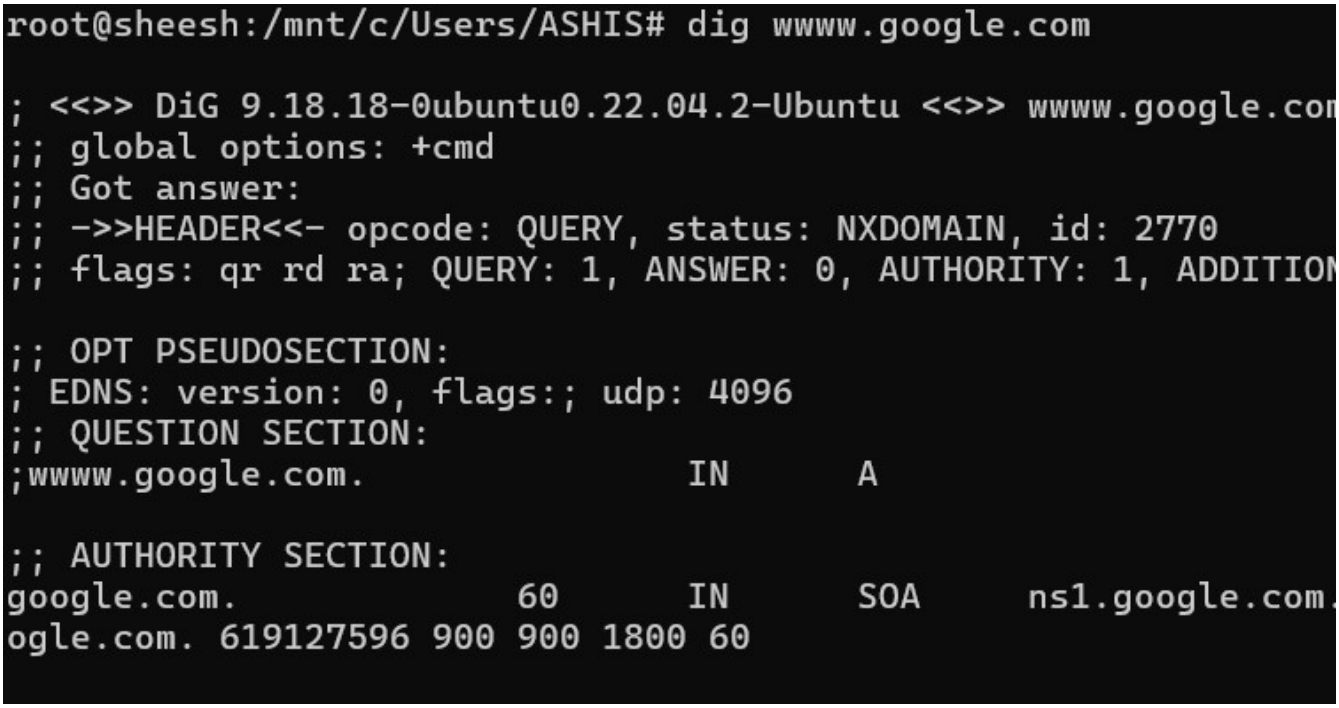
#apt-get install nslookup

whois

Example: Querying tsec.edu

student@lab:~#whoistsec.edu

dig 1. Simple dig Command Usage



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

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

```
root@sheesh:/mnt/c/Users/ASHIS# dig wwww.google.com +noquestion

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> wwww.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 55641
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITION

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; AUTHORITY SECTION:
google.com.             60      IN      SOA     ns1.google.com.
ogle.com. 619127596 900 900 1800 60

;; Query time: 149 msec
```

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.

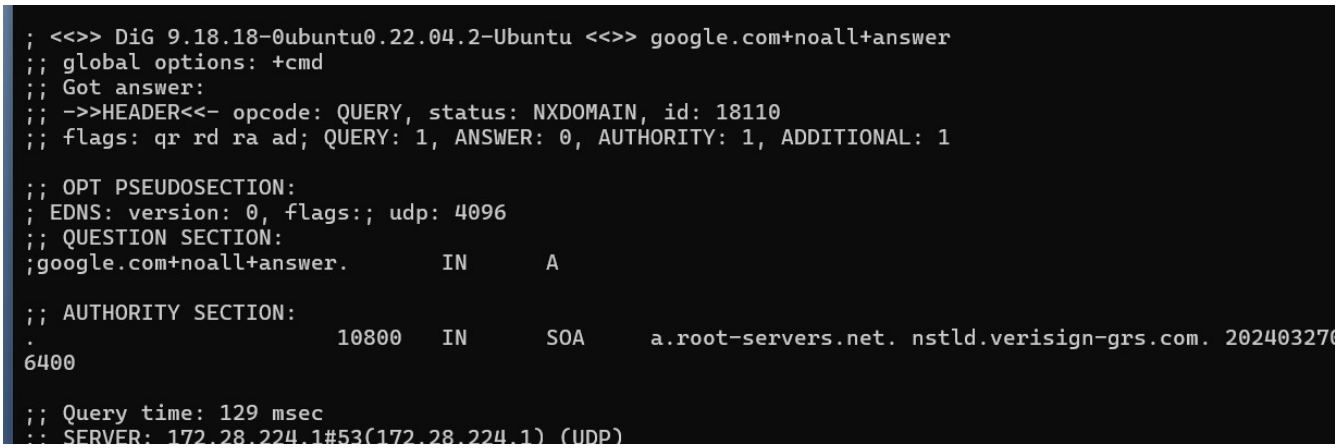
i)student@lab:~ #dig google.com +noquestion

ii)student@lab:~ #dig google.com +nocomments – Turn off the comment lines iii) student@lab:~ # dig google.com +noauthority – Turn off the authority section iv) student@lab:~ #dig google.com +noadditional – Turn off the additional section

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

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

3. Query MX Records Using dig MX

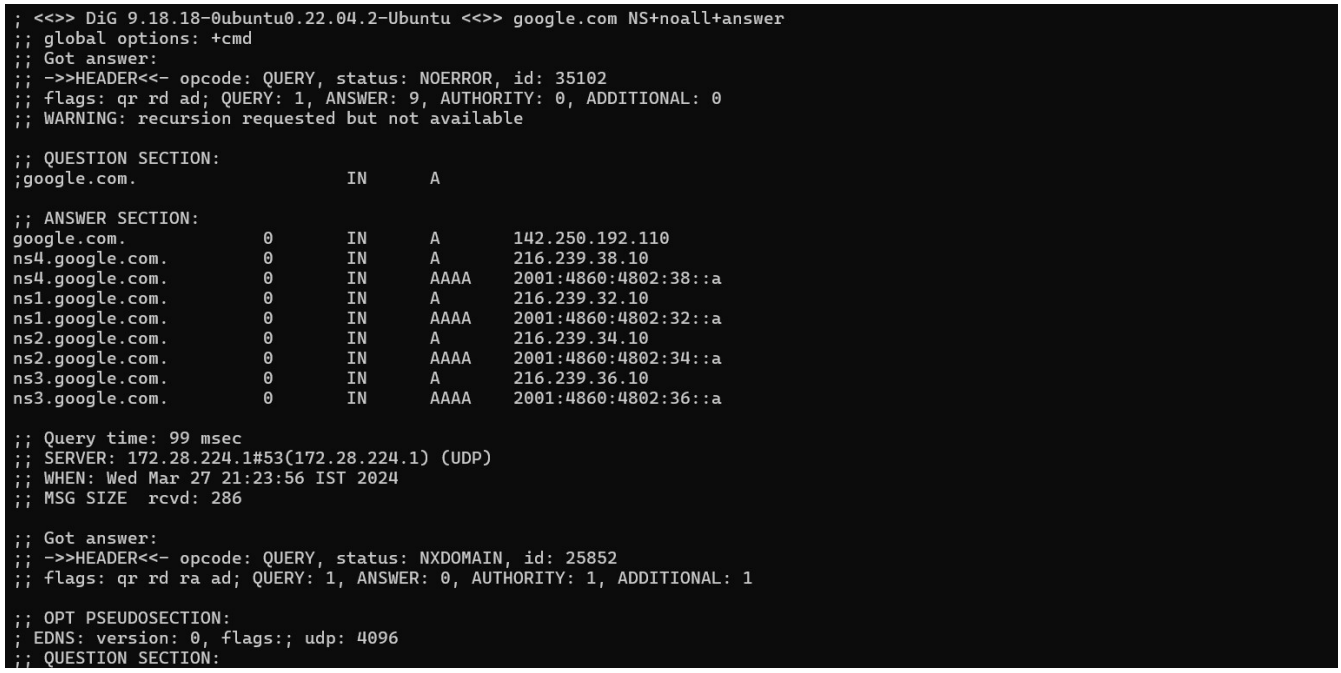


```
; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> google.com+noall+answer
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 18110
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 20240327
6400

;; Query time: 129 msec
;; SERVER: 172.28.224.1#53(172.28.224.1) (UDP)
```

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

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

4. Query NS Records Using dig NS



```
; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> google.com NS+noall+answer
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35102
;; flags: qr rd ad; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             0       IN      A       142.250.192.110
ns4.google.com.         0       IN      A       216.239.38.10
ns4.google.com.         0       IN      AAAA    2001:4860:4802:38::a
ns1.google.com.         0       IN      A       216.239.32.10
ns1.google.com.         0       IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         0       IN      A       216.239.34.10
ns2.google.com.         0       IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         0       IN      A       216.239.36.10
ns3.google.com.         0       IN      AAAA    2001:4860:4802:36::a

;; Query time: 99 msec
;; SERVER: 172.28.224.1#53(172.28.224.1) (UDP)
;; WHEN: Wed Mar 27 21:23:56 IST 2024
;; MSG SIZE  rcvd: 286

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 25852
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
```

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

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

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

6. View Short Output Using dig +short

```
^Croot@sheesh:/mnt/c/Users/ASHIS# dig google.com +short
142.250.192.110
216.239.38.10
2001:4860:4802:38::a
216.239.32.10
2001:4860:4802:32::a
216.239.34.10
2001:4860:4802:34::a
```

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

```
; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> -x 209.132.183.81
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 30960
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;81.183.132.209.in-addr.arpa.   IN      PTR

;; AUTHORITY SECTION:
183.132.209.in-addr.arpa. 3598  IN      SOA     dns1.p01.nsone.net. hostmaster.nsone.net. 1677108684 200 7200 1209

;; Query time: 1119 msec
```

traceroute

```
traceroute to google.com (142.250.192.110), 30 hops max, 60 byte packets
 1  sheesh.mshome.net (172.28.224.1)  0.286 ms  0.261 ms  0.252 ms
 2  192.168.0.1 (192.168.0.1)  1.732 ms  2.773 ms  2.007 ms
 3  100.76.80.1 (100.76.80.1)  12.630 ms  14.009 ms  12.608 ms
 4  114.79.129.117.dvois.com (114.79.129.117)  16.774 ms  16.763 ms  15.756 ms
 5  10.241.1.6 (10.241.1.6)  8.190 ms  7.409 ms  7.396 ms
 6  10.240.254.150 (10.240.254.150)  15.713 ms  18.802 ms  15.515 ms
 7  10.240.254.1 (10.240.254.1)  6.923 ms  38.705 ms *
 8  10.241.1.1 (10.241.1.1)  203.092 ms  192.280 ms  191.856 ms
 9  72.14.208.165 (72.14.208.165)  82.689 ms  82.674 ms  82.659 ms
```

Command:

student@lab:~#traceroute google.com

nslookup

```
root@sheesh:/mnt/c/Users/ASHIS# nslookup google.com
Server:         172.28.224.1
Address:        172.28.224.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.192.110
Name:   ns4.google.com
Address: 216.239.38.10
Name:   ns4.google.com
Address: 2001:4860:4802:38::a
Name:   ns1.google.com
Address: 216.239.32.10
Name:   ns1.google.com
Address: 2001:4860:4802:32::a
Name:   ns2.google.com
Address: 216.239.34.10
Name:   ns2.google.com
Address: 2001:4860:4802:34::a
Name:   ns3.google.com
Address: 216.239.36.10
Name:   ns3.google.com
Address: 2001:4860:4802:36::a
Name:   google.com
Address: 2404:6800:4009:82a::200e
Name:   ns4.google.com
Address: 216.239.38.10
Name:   ns4.google.com
```

1. **Simple nslookup command**

student@lab:~#nslookup google.com

2.Query the MX Record using -query=mx

student@lab:~#nslookup -query = mx

google.com

```
Server:         172.28.224.1
Address:        172.28.224.1#53

Non-authoritative answer:
google.com      mail exchanger = 10 smtp.google.com.
Name:   smtp.google.com
Address: 64.233.170.27
Name:   smtp.google.com
Address: 74.125.68.27
Name:   smtp.google.com
Address: 142.251.175.26
Name:   smtp.google.com
Address: 142.251.175.27
Name:   smtp.google.com
Address: 64.233.170.26
Name:   smtp.google.com
Address: 2404:6800:4003:c1a::1a
Name:   smtp.google.com
Address: 2404:6800:4003:c1a::1b
Name:   smtp.google.com
Address: 2404:6800:4003:c1c::1b
Name:   smtp.google.com
Address: 2404:6800:4003:c02::1a
Name:   ns4.google.com
Address: 216.239.38.10
Name:   ns4.google.com
Address: 2001:4860:4802:38::a
Name:   ns1.google.com
Address: 216.239.32.10
Name:   ns1.google.com
```

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

3. Query the NS Record using -type=ns

```
root@sheesh:/mnt/c/Users/ASHIS# dig google.com MX +noall +answer
google.com.             0       IN      MX      10 smtp.google.com.
smtp.google.com.        0       IN      A       142.251.10.27
smtp.google.com.        0       IN      A       142.251.12.26
smtp.google.com.        0       IN      A       142.251.12.27
smtp.google.com.        0       IN      A       172.217.194.26
smtp.google.com.        0       IN      A       172.217.194.27
smtp.google.com.        0       IN      AAAA    2404:6800:4003:c11::1a
smtp.google.com.        0       IN      AAAA    2404:6800:4003:c11::1b
smtp.google.com.        0       IN      AAAA    2404:6800:4003:c04::1b
smtp.google.com.        0       IN      AAAA    2404:6800:4003:c0f::1a
ns4.google.com.         0       IN      A       216.239.38.10
ns4.google.com.         0       IN      AAAA    2001:4860:4802:38::a
ns1.google.com.         0       IN      A       216.239.32.10
ns1.google.com.         0       IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         0       IN      A       216.239.34.10
```

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.

4. Query the SOA Record using -type=soa

```
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36426
;; flags: qr rd ad; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;google.com.                    IN      SOA

;; ANSWER SECTION:
google.com.             0       IN      SOA     ns1.google.com. dns-admin.google.com. 619127596 900 900
ns4.google.com.         0       IN      A       216.239.38.10
ns4.google.com.         0       IN      AAAA    2001:4860:4802:38::a
ns1.google.com.         0       IN      A       216.239.32.10
ns1.google.com.         0       IN      AAAA    2001:4860:4802:32::a
ns2.google.com.         0       IN      A       216.239.34.10
ns2.google.com.         0       IN      AAAA    2001:4860:4802:34::a
ns3.google.com.         0       IN      A       216.239.36.10
ns3.google.com.         0       IN      AAAA    2001:4860:4802:36::a
```

student@lab: ~ #nslookup -type = soagoogle.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

5. View available DNS records using -

query=anystudent@lab: ~ #nslookup -type = any google.

```
root@sheesh:/mnt/c/Users/ASHIS# nslookup -type=any google.com
;; Connection to 172.28.224.1#53(172.28.224.1) for google.com failed: timed out.
```

Conclusion: We have successfully done a walkthrough of the dig module to perfom various analysis related to certain domains.