

SUBJECT: NTAL

Experiment 1

Name :

Roll No:

Aim: Study, installation and working of the network reconnaissance tools for gathering information about networks and domain registrars.

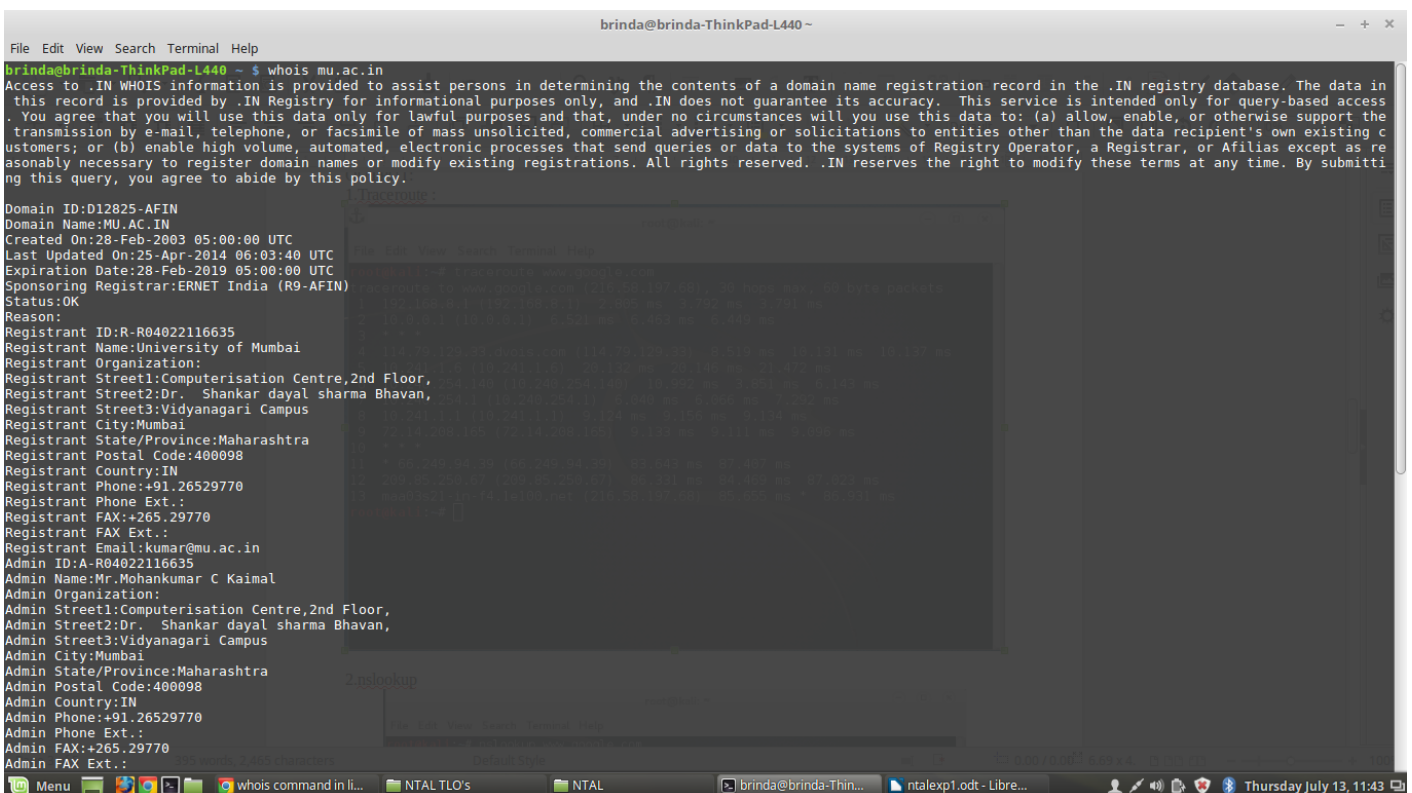
• whois • dig • traceroute • nslookup

Theory:

1. whois

The whois command looks up the registration record associated with a domain name. This can show you more information about who registered and owns a domain name, including their contact information.

whois searches for an object in a **WHOIS** database. **WHOIS** is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information.



```
brinda@brinda-ThinkPad-L440 ~ $ whois mu.ac.in
Access to .IN WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the .IN registry database. The data in this record is provided by .IN Registry for informational purposes only, and .IN does not guarantee its accuracy. This service is intended only for query-based access. You agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of Registry Operator, a Registrar, or Afilias except as reasonably necessary to register domain names or modify existing registrations. All rights reserved. .IN reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.

Domain ID:D12825-AFIN
Domain Name:MU.AC.IN
Created On:28-Feb-2003 05:00:00 UTC
Last Updated On:25-Apr-2014 06:03:40 UTC
Expiration Date:28-Feb-2019 05:00:00 UTC
Sponsoring Registrar:ERNET India (R9-AFIN)
Status:OK
Reason:
Registrant ID:R-R04022116635
Registrant Name:University of Mumbai
Registrant Organization:
Registrant Street1:Computerisation Centre,2nd Floor,
Registrant Street2:Dr. Shankar dayal sharma Bhavan,
Registrant Street3:Vidyanagari Campus
Registrant City:Mumbai
Registrant State/Province:Maharashtra
Registrant Postal Code:400098
Registrant Country:IN
Registrant Phone:+91.26529770
Registrant Phone Ext.:
Registrant FAX:+265.29770
Registrant FAX Ext.:
Registrant Email:kumar@mu.ac.in
Admin ID:A-R04022116635
Admin Name:Mr.Mohankumar C Kaimal
Admin Organization:
Admin Street1:Computerisation Centre,2nd Floor,
Admin Street2:Dr. Shankar dayal sharma Bhavan,
Admin Street3:Vidyanagari Campus
Admin City:Mumbai
Admin State/Province:Maharashtra
Admin Postal Code:400098
Admin Country:IN
Admin Phone:+91.26529770
Admin Phone Ext.:
Admin FAX:+265.29770
Admin FAX Ext.:
```

2. dig

Dig stands for (Domain Information Groper) is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried. dig is part of the BIND domain name server software suite. dig command replaces older tool such as nslookup and the host. dig tool is available in major Linux distributions.

```
brinda@brinda-ThinkPad-L440 ~ $ dig mu.ac.in
; <<>> DiG 9.10.3-P4-Ubuntu <<>> mu.ac.in Linux Foundation's LFCS and LFCE Certification Preparation Guide (530)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 2114
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;mu.ac.in.                IN      A
;; ANSWER SECTION:
mu.ac.in.                141     IN      A      121.241.25.1
mu.ac.in.                141     IN      A      121.241.25.2
mu.ac.in.                141     IN      A      14.139.125.195
;; Query time: 1 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Jul 13 11:45:46 IST 2017
;; MSG SIZE rcvd: 74
```

Just to display server names:

```
brinda@brinda-ThinkPad-L440 ~ $ dig mu.ac.in +short
121.241.25.1
121.241.25.2
14.139.125.195
brinda@brinda-ThinkPad-L440 ~ $
```

Tip: Only display answer section with using +short.

```
# dig -x 72.30.38.140 +short
ir1.fp.vip.sp2.yahoo.com
```

9. Querying Multiple DNS Records

Query multiple websites DNS specific query viz. MX, NS etc. records.

```
# dig yahoo.com mx +noall +answer redhat.com ns +noall +answer
```

10. Top Command Examples in Linux

3. traceroute / tracert / tracepath

The traceroute, tracert, or tracepath command is similar to ping, but provides information about the path a packet takes. traceroute sends packets to a destination, asking each Internet router along the way to reply when it passes on the packet. This will show you the path packets take when you send them between your location and a destination.

This tool can help troubleshoot connection problems. For example, if you can't communicate with a server, running traceroute may show you where the problem is occurring between your computer and the remote host.

```
brinda@brinda-ThinkPad-L440 ~ $ traceroute mu.ac.in
traceroute to mu.ac.in (121.241.25.1), 30 hops max, 60 byte packets
 1  172.16.16.1 (172.16.16.1)  0.472 ms  0.445 ms  0.669 ms
 2  1.22.55.121 (1.22.55.121)  4.792 ms  5.257 ms  6.264 ms
 3  218.100.48.78 (218.100.48.78)  130.182 ms  130.171 ms  130.118 ms
 4  172.23.78.225 (172.23.78.225)  124.185 ms  124.183 ms  124.162 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

4. nslookup

The nslookup command will look up the IP addresses associated with a domain name. For example, you can run **nslookup howtogeek.com** to see the IP address of How-To Geek’s server.

Your computer is constantly querying its DNS servers to translate domain names to IP addresses This command just allows you to do it manually. nslookup also allows you to perform a reverse lookup to find the domain name associated with an IP address.

```
brinda@brinda-ThinkPad-L440 ~ $ nslookup howtogeek.com
Server:      127.0.1.1
Address:     127.0.1.1#53

Non-authoritative answer:
Name:   howtogeek.com
Address: 23.92.23.113
```

Conclusion :