

## **PRACTICAL-8**

### **AIM**

Gather information of any domain/website/IP address using following Information Gathering Tools.

- Nslookup
- Whois
- Tracert

### **THEORY**

#### **NSLOOKUP:**

- nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address or domain name system (DNS) record.

#### **WHOIS:**

- WHOIS is a TCP-based query and response protocol that is commonly used to provide information services to Internet users.
- It returns information about the registered Domain Names, an IP address block, Name Servers and a much wider range of information services.

#### **TRACERT:**

- The traceroute command is used to determine the path between two connections. Often a connection to another device will have to go through multiple routers.
- The traceroute command will return the names or IP addresses of all the routers between two devices.

## IMPLEMENTATION

### Nslookup:

```
(kalichanga@kalichanga)-[~]
$ nslookup www.charusat.ac.in
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name:   www.charusat.ac.in
Address: 185.151.30.139
Name:   www.charusat.ac.in
Address: 2a07:7800::139
```

### Whois:

```
(kalichanga@kalichanga)-[~]
$ whois 185.151.30.139
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '185.151.30.0 - 185.151.30.255'

% Abuse contact for '185.151.30.0 - 185.151.30.255' is 'abuse@20i.com'

inetnum:        185.151.30.0 - 185.151.30.255
netname:        CDN
descr:          Cloud Platform
country:        GB
admin-c:        HI825-RIPE
tech-c:         HI825-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-20i
created:        2018-09-19T13:27:19Z
last-modified:  2020-07-27T11:58:38Z
source:         RIPE

role:           Hosting Infrastructure
address:        Hawthorn House
admin-c:        AR36293-RIPE
nic-hdl:        HI825-RIPE
mnt-by:         MNT-20i
created:        2020-07-27T11:58:11Z
last-modified:  2020-07-27T11:59:21Z
source:         RIPE # Filtered

% Information related to '185.151.30.0/24AS48254'

route:          185.151.30.0/24
origin:         AS48254
mnt-by:         MNT-20i
created:        2018-09-20T12:52:20Z
last-modified:  2018-09-21T09:16:52Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.103 (ANGUS)
```

**Tracert:**

```
C:\Users\Parth Patel>tracert www.charusat.ac.in

Tracing route to www.charusat.ac.in [185.151.30.139]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms  192.168.0.1
  2   70 ms   14 ms   18 ms  100.67.0.1
  3   24 ms   17 ms   26 ms  vad-core01.youbroadband.in [203.187.193.1]
  4   29 ms   16 ms   14 ms  118.185.43.222
  5   61 ms   22 ms   23 ms  182.19.106.200
  6  169 ms  166 ms  191 ms  ae11-100-xcr1.mar.cw.net [213.185.219.53]
  7  136 ms  118 ms  123 ms  4.68.111.209
  8  140 ms  138 ms  137 ms  ae3.3202.edge3.London15.level3.net [4.69.143.246]
  9  139 ms  136 ms  138 ms  lon-tel-01gw.voxility.net [217.163.113.54]
 10  136 ms  145 ms  139 ms  lon-tel-02c.voxility.com [185.242.206.2]
 11  196 ms  191 ms  194 ms  212.119.4.229
 12  154 ms  455 ms  149 ms  et1-1-1-cr1-lon-rdg.as48254.net [185.146.164.19]
 13  146 ms  140 ms  142 ms  185-151-30-139.ptr4.stackcp.net [185.151.30.139]

Trace complete.
```

**CONCLUSION**

In this practical, we used different tools and frameworks to gather information of websites.