

Don Bosco Institute of Technology, Mumbai 400070
Department of Information Technology

Experiment No. : 7

Name : Avadhoot Pawaskar
Rollno.: 43

Date: 10/09/2024

Title : Network Reconnaissance tools/commands

Problem Definition : Use following Network Reconnaissance tools/commands to gather information about network and domain registrars.

WHOIS, dig, traceroute, nslookup

Pre-requisite : Networking commands

Theory :

WHOIS: It searches for an object in a RFC 3912 database. This version of the whois client tries to guess the right server to ask for the specified object. If no guess can be made it will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

dig (domain information groper): It is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.

Traceroute: It tracks the route packets taken from an IP network on their way to a given host. It utilizes the IP protocol's time to live (TTL) field and attempts to elicit an ICMP TIME_EXCEEDED response from each gateway along the path to the host.

Nslookup: It is a program to query Internet domain name servers. 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. Noninteractive mode is used to print just the name and requested information for a host or domain.

Results :

1. WHOIS

```
kali@kali:~$ whois host
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:      HOST
organisation: Radix Technologies Inc.
address:     Services Cayman Limited, P.O. Box 10000, Willow House, Cricket Square, Grand Cayman
address:     KY1-1001
address:     Cayman Islands (the)

contact:     administrative
name:        Director
organisation: Radix Technologies Inc.
address:     Services Cayman Limited, P.O. Box 10000, Willow House, Cricket Square, Grand Cayman
address:     KY1-1001
address:     Cayman Islands (the)
phone:       +971 44487934
e-mail:      admin@radix.email

contact:     technical
name:        CTO
organisation: CentralNIC
address:     Saddlers House, 4th Floor
address:     44 Gutter Lane
address:     London EC2V 6BN
address:     United Kingdom of Great Britain and Northern Ireland (the)
phone:       +44 20 33 88 0000
fax-no:      +44 20 33 88 0001
e-mail:      tld.ops@centralnic.com

nsrserver:   A.NIC-HOST 194.169.210.53 2001:67c:13cc:0:0:0:1:53
nsrserver:   B.NIC-HOST 185.24.64.53 2a04:2b00:13cc:0:0:0:1:53
nsrserver:   E.NIC-HOST 212.18.240.53 2a04:2b00:13cc:0:0:0:1:53
nsrserver:   F.NIC-HOST 212.18.240.53 2a04:2b00:13ff:0:0:0:1:53
ds-rdata:    61162 8 2 d15742398f5291b062642bee5da6eddef3f4497c85bac8f5a6c9c8ff495cf286
ds-rdata:    1897 8 2 720c3c1ba71ba983360e0cd34270d42d1ec30ec79a1843c7c014f81dcdf38f0
```

2. DIG

```
kali@kali:~$ dig nic.host

;; global options: +cmd
;; Got answer:
;; --HEADER-- opcode: QUERY, status: NOERROR, id: 60791
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: 0, udp: 1280
;; QUESTION SECTION:
;nic.host. IN A
;; ANSWER SECTION:
nic.host. 282 IN A 142.251.42.78

;; Query time: 8 msec
;; SERVER: 192.168.29.1#53(192.168.29.1) (UDP)
;; WHEN: Fri Sep 13 23:27:35 IST 2024
;; MSG SIZE rcvd: 56

(kali@kali)~$
```

3. TRACEROUTE

```
kali@kali:~$ traceroute google
google: No address associated with hostname
Cannot handle 'host' cmdline arg 'google' on position 1 (argc 1)

(kali@kali)~$ traceroute Youtube.com
traceroute to Youtube.com (142.251.42.78), 30 hops max, 60 byte packets
 1 reliance.reliance (192.168.29.1)  2.770 ms  7.754 ms  8.539 ms
 2 10.27.32.1 (10.27.32.1)  8.160 ms  9.060 ms  9.038 ms
 3 172.31.2.22 (172.31.2.22)  9.015 ms  8.992 ms  172.31.2.24 (172.31.2.24)  8.972 ms
 4 192.168.70.14 (192.168.70.14)  8.961 ms  8.925 ms  192.168.70.16 (192.168.70.16)  8.910 ms
 5 172.26.76.165 (172.26.76.165)  8.895 ms  8.879 ms  8.862 ms
 6 172.26.76.131 (172.26.76.131)  8.857 ms  7.548 ms  6.512 ms
 7 192.168.7.244 (192.168.7.244)  6.447 ms  192.168.7.250 (192.168.7.250)  5.847 ms  192.168.7.248 (192.168.7.248)  7.279 ms
 8 * * *
 9 * * *
10 209.85.168.26 (209.85.168.26)  10.060 ms  74.125.51.166 (74.125.51.166)  10.683 ms  173.194.121.8 (173.194.121.8)  9.936 ms
11 * 192.178.110.227 (192.178.110.227)  9.879 ms  192.178.110.129 (192.178.110.129)  94.195 ms
12 142.250.62.152 (142.250.62.152)  7.115 ms  142.251.69.103 (142.251.69.103)  8.138 ms  209.85.142.84 (209.85.142.84)  7.177 ms
13 bom1221-in-f14.1e100.net (142.251.42.78)  7.568 ms  8.014 ms  192.178.111.60 (192.178.111.60)  9.347 ms

(kali@kali)~$
```

4. NSLOOKUP

```
kali@kali:~$ nslookup Youtube.com
Server: 192.168.29.1
Address: 192.168.29.1#53

Non-authoritative answer:
Name: Youtube.com
Address: 142.251.42.78
Name: Youtube.com
Address: 2404:6800:4009:831::200e

(kali@kali)~$
```

References:

- <https://centralops.net/co/>
- <https://www.howtogeek.com/190148/8-common-network-utilities-explained/>