

# Experiment No - 1

**Aim:** To study Network reconnaissance commands.

## Theory:

### 1) Trace route

The tracer command is a Command Prompt command that's used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify.

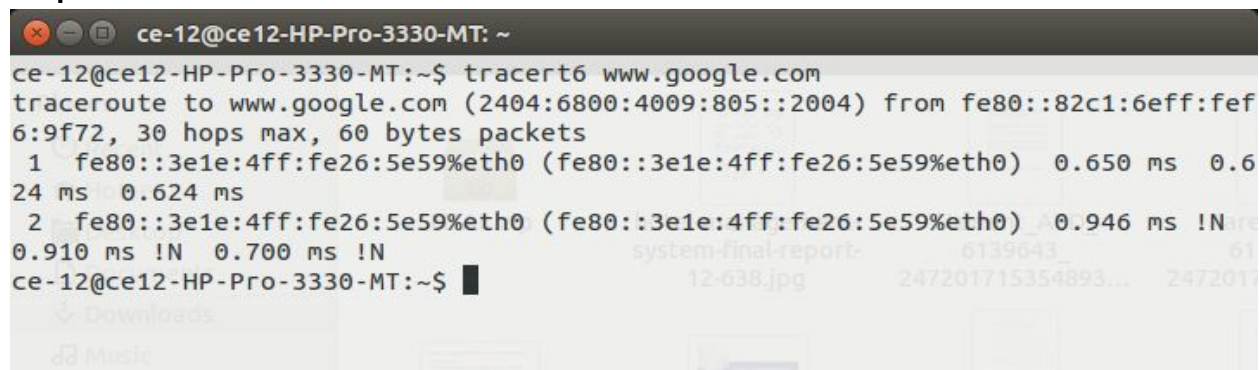
You might also sometimes see the tracer command referred to as the trace route command or traceroute command.

### Syntax:

```
tracert [-d] [-h MaxHops] [-w Timeout] [-4] [-6] target [/?]
```

- -d = This option prevents tracer from resolving IP addresses to hostnames, often resulting in much faster results.
- -h MaxHops = This tracer option specifies the maximum number of hops in the search for the target. If you do not specify MaxHops, and target has not been found by 30 hops, tracer will stop looking.
- -w Timeout = You can specify the time, in milliseconds, to allow each reply before timeout using this tracer option.
- -4 = This option forces tracer to use IPv4 only.
- -6 = This option forces tracer to use IPv6 only.
- target = This is the destination, either an IP address or hostname.

### Output:



```
ce-12@ce12-HP-Pro-3330-MT: ~  
ce-12@ce12-HP-Pro-3330-MT:~$ tracert6 www.google.com  
traceroute to www.google.com (2404:6800:4009:805::2004) from fe80::82c1:6eff:fef  
6:9f72, 30 hops max, 60 bytes packets  
 1  fe80::3e1e:4ff:fe26:5e59%eth0 (fe80::3e1e:4ff:fe26:5e59%eth0)  0.650 ms  0.6  
24 ms  0.624 ms  
 2  fe80::3e1e:4ff:fe26:5e59%eth0 (fe80::3e1e:4ff:fe26:5e59%eth0)  0.946 ms !N  
0.910 ms !N  0.700 ms !N  
ce-12@ce12-HP-Pro-3330-MT:~$
```

### 2) Nslookup

Nslookup is a network utility program used to obtain information about Internet servers. As its name suggests, the utility finds name server information for domains by querying the Domain Name Service (DNS).

The name "nslookup" means "name server lookup". nslookup does not use the operating system's local Domain Name System resolver library to perform its queries, and thus may behave differently from dig (which does). Additionally, vendor-provided versions can confuse matters by using or including output of other sources of name information (such as host files, Network Information Service). Some behaviors of nslookup may be modified by the contents of resolv.conf

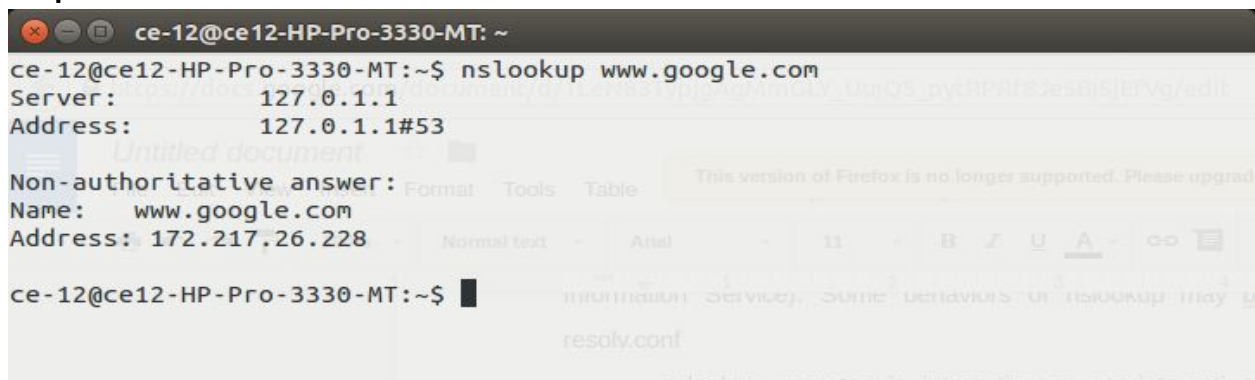
nslookup operates in interactive or non-interactive mode. When used interactively by invoking it without arguments or when the first argument is - (minus sign) and the second argument is a hostname or Internet address of a name server, the user issues parameter configurations or requests when presented with the nslookup prompt (>). When no arguments are given, then the command queries the default server. The - (minus sign) invokes subcommands which are specified on the command line and should precede nslookup commands. In non-interactive mode, i.e. when the first argument is a name or Internet address of the host being searched, parameters and the query are specified as command line arguments in the invocation of the program. The non interactive mode searches the information for a specified host using the default name server.

#### Syntax:

**nslookup [-SubCommand ...] [{ComputerToFind}[-Server]]**

- Parameters:
- SubCommand: Specifies one or more nslookup subcommands as a command-line option. For a list of subcommands, see Related Topics.
- ComputerToFind: Looks up information for ComputerToFind using the current default DNS name server, if no other server is specified. To look up a computer not in the current DNS domain, append a period to the name.
- Server: Specifies to use this server as the DNS name server. If you omit -Server, the default DNS name server is used.
- { help | ? }: Displays a short summary of nslookup subcommands.

#### Output:



```
ce-12@ce12-HP-Pro-3330-MT: ~  
ce-12@ce12-HP-Pro-3330-MT:~$ nslookup www.google.com  
Server:      127.0.1.1  
Address:     127.0.1.1#53  
  
Non-authoritative answer:  
Name:   www.google.com  
Address: 172.217.26.228  
  
ce-12@ce12-HP-Pro-3330-MT:~$
```

### 3) Dig

#### Description:

Dig is a networking tool that can query DNS servers for information. It can be very helpful for diagnosing problems with domain pointing and is a good way to verify that your configuration is working.

We will discuss how to use dig to verify your domain name settings and return data about how the internet sees your domain. We will also examine a few other related tools like "whois" and "ping".

We will be using an Ubuntu 12.04 VPS to test the commands in this guide, but any modern Linux distribution should function in a similar way.

#### Syntax:

**dig duckduckgo.com**

## Output:

```
ce-12@ce12-HP-Pro-3330-MT:~$ dig
; <<> DiG 9.9.5-3ubuntu0.4-Ubuntu <<>
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 10351
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;
;                IN      NS
;; ANSWER SECTION:
.      236431 IN      NS      k.root-servers.net.
.      236431 IN      NS      c.root-servers.net.
.      236431 IN      NS      j.root-servers.net.
.      236431 IN      NS      e.root-servers.net.
.      236431 IN      NS      m.root-servers.net.
.      236431 IN      NS      l.root-servers.net.
.      236431 IN      NS      a.root-servers.net.
.      236431 IN      NS      h.root-servers.net.
.      236431 IN      NS      f.root-servers.net.
.      236431 IN      NS      g.root-servers.net.
.      236431 IN      NS      i.root-servers.net.
.      236431 IN      NS      b.root-servers.net.
.      236431 IN      NS      d.root-servers.net.
;; Query time: 5 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Jul 27 10:17:49 IST 2017
;; MSG SIZE rcvd: 239

ce-12@ce12-HP-Pro-3330-MT:~$
```

## 4) WHOIS

### Description:

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.

Most modern versions of whois try to guess the right server to ask for the specified object. If no guess can be made, whois will connect to whois.networksolutions.com for NIC handles or whois.arin.net for IPv4 addresses and network names.

## Output:

```
ce-12@ce12-HP-Pro-3330-MT: ~
WHOIS(1)                                Debian GNU/Linux                                WHOIS(1)

NAME
whois - client for the whois directory service

SYNOPSIS
whois [ { -h | --host } HOST ] [ { -p | --port } PORT ] [ -abBcdGHK-
lLmMrRx ] [ -g SOURCE:FIRST-LAST ] [ -i ATTR[,ATTR]... ]
[ -s SOURCE[,SOURCE]... ] [ -T TYPE[,TYPE]... ] [ --verbose ] OBJECT

whois -q KEYWORD

whois -t TYPE

whois -v TYPE

whois --help

whois --version

DESCRIPTION
whois searches for an object in a RFC 3912 database.

Manual page whois(1) line 1 (press h for help or q to quit)
```

## 5) ping

### Ping Command Syntax

**ping** [-t] [-a] [-n *count*] [-l *size*] [-f] [-i *TTL*] [-v *TOS*] [-r *count*] [-s *count*] [-w *timeout*] [-R] [-S *srcaddr*] [-p] [-4] [-6] *target* [/?]

### DESCRIPTION

ping uses the ICMP protocol's mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from a host or gateway. ECHO\_REQUEST datagrams ("pings") have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of "pad" bytes used to fill out the packet.

ping6 is IPv6 version of ping, and can also send Node Information Queries (RFC4620). Intermediate hops may not be allowed, because IPv6 source routing was deprecated (RFC5095).

### OPTIONS

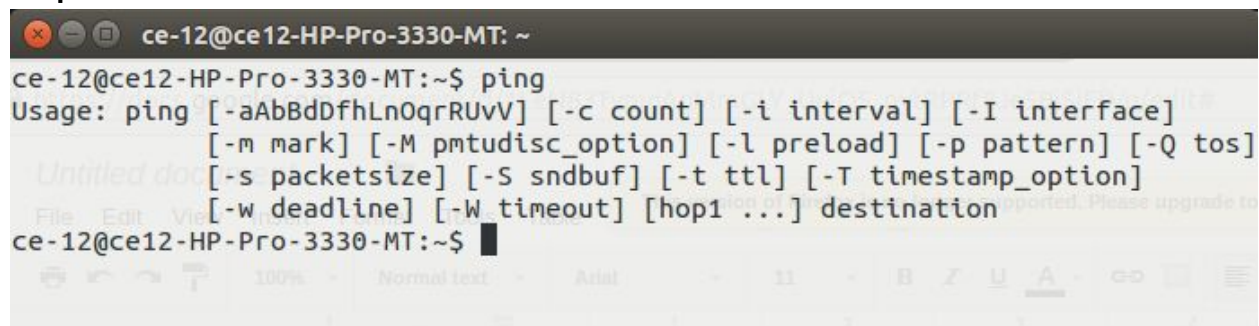
-a Audible ping.

-A Adaptive ping. Interpacket interval adapts to round-trip time, so that effectively not more than one (or more, if preload is set) unanswered probe is present in the network. Minimal interval is 200msec for not super-user. On networks with low rtt this mode is essentially equivalent to flood mode.

-b Allow pinging a broadcast address.

-B Do not allow ping to change source address of probes. The address is bound to one selected when ping starts.

### Output:

A screenshot of a terminal window with a dark background. The title bar shows a window icon, a close button, and the text 'ce-12@ce12-HP-Pro-3330-MT: ~'. The terminal content shows the command 'ce-12@ce12-HP-Pro-3330-MT:~\$ ping' followed by the usage text: 'Usage: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface] [-m mark] [-M pmtudisc\_option] [-l preload] [-p pattern] [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp\_option] [-w deadline] [-W timeout] [hop1 ...] destination'. The prompt 'ce-12@ce12-HP-Pro-3330-MT:~\$' is visible at the bottom of the terminal output. A faint 'Untitled doc' window is visible in the background.

**Conclusion:** Hence, we've studied use of network reconnaissance tool like WHOIS, dig, traceroute, nslookup to gather information about network and domain registrars.