Experiment No 10

Aim: To Study the use of network reconnaissance tools like WHOIS, dig, tracert, nslookup.

Theory:

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.

To use WHOIS in windows we need to install WhoIs from Microsoft site and extract its folder and to switch to its directory in cmd.

Dig

Dig (Domain Information Groper) is a powerful command-line tool for querying DNS name servers.

The dig command, allows you to query information about various DNS records, including host addresses, mail exchanges, and name servers. It is the most commonly used tool among system administrators for troubleshooting DNS problems because of its flexibility and ease of use.

To use dig in windows we need to install Bind and set path for it. Bind also provides other commands support such as tracert and nslookup.

Tracert

This diagnostic tool determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) echo Request or ICMPv6 messages to the destination with incrementally increasing time to live (TTL) field values. Each router along the path is required to decrement the TTL in an IP packet by at least 1 before forwarding it. Effectively, the TTL

is a maximum link counter. When the TTL on a packet reaches 0, the router is expected to return an ICMP time Exceeded message to the source computer.

This command determines the path by sending the first echo Request message with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum number of hops is reached. The maximum number of hops is 30 by default and can be specified using the **-h** parameter.

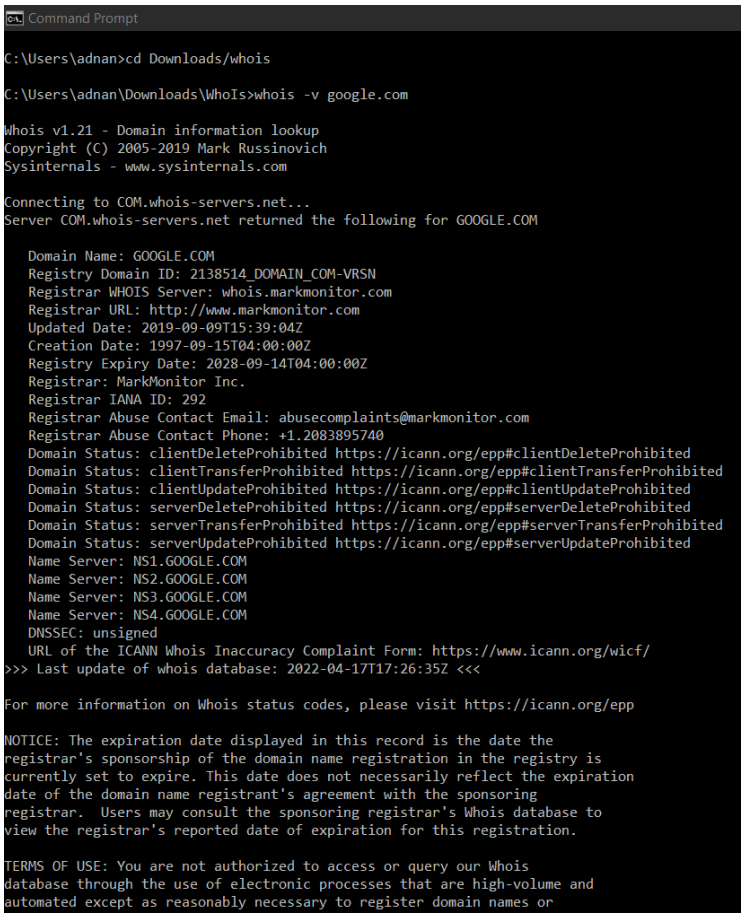
Nslookup

The nslookup command queries internet domain name servers in two modes. Interactive mode allows you to query name servers for information about various hosts and domains, or to print a list of the hosts in a domain. In noninteractive mode, the names and requested information are printed for a specified host or domain.

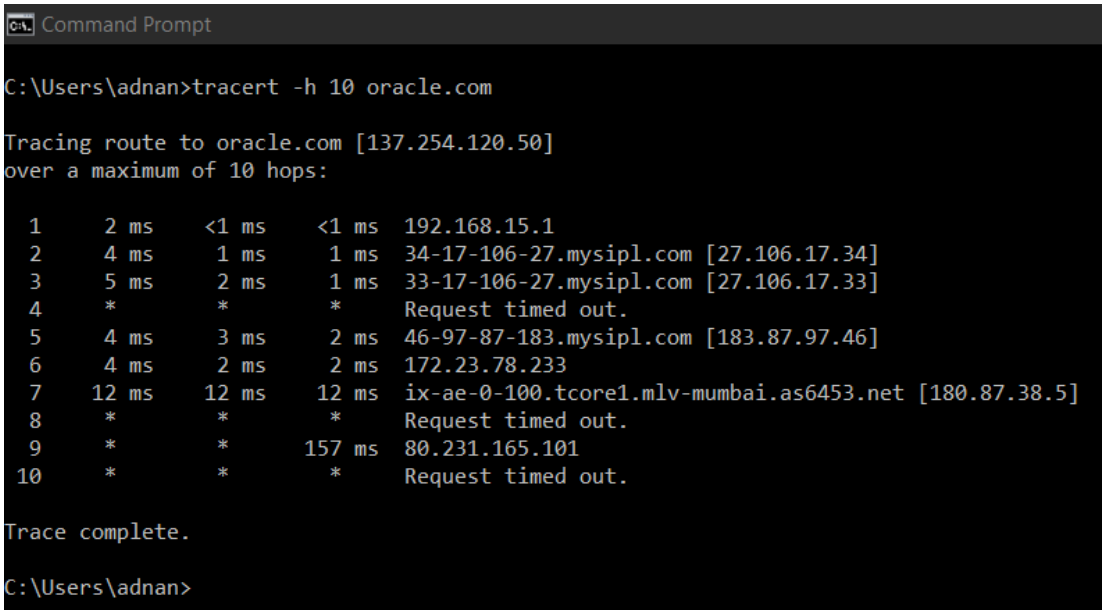
The nslookup command enters interactive mode when no arguments are given, or when the first argument is a - (minus sign) and the second argument is the host name or internet address of a name server. When no arguments are given, the command queries the default name server. The nslookup command enters non-interactive mode when you give the name or internet address of the host to be looked up as the first argument. The optional second argument specifies the host name or address of a name server.

Output:

Whois



Tracert



Dig

```
Command Prompt

C:\Users\adnan>dig yahoo.com trace

; <<>> DiG 9.16.27 <<>> yahoo.com trace
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4583
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 10

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              1237    IN      A       74.6.143.25
yahoo.com.              1237    IN      A       74.6.231.20
yahoo.com.              1237    IN      A       98.137.11.163
yahoo.com.              1237    IN      A       74.6.231.21
yahoo.com.              1237    IN      A       74.6.143.26
yahoo.com.              1237    IN      A       98.137.11.164

;; AUTHORITY SECTION:
yahoo.com.              51952   IN      NS      ns4.yahoo.com.
yahoo.com.              51952   IN      NS      ns3.yahoo.com.
yahoo.com.              51952   IN      NS      ns2.yahoo.com.
yahoo.com.              51952   IN      NS      ns1.yahoo.com.
yahoo.com.              51952   IN      NS      ns5.yahoo.com.

;; ADDITIONAL SECTION:
ns4.yahoo.com.          312358  IN      A       98.138.11.157
ns1.yahoo.com.          312358  IN      A       68.180.131.16
ns1.yahoo.com.          53595   IN      AAAA    2001:4998:1b0::7961:686f:6f21
ns5.yahoo.com.          53166   IN      A       202.165.97.53
ns5.yahoo.com.          53595   IN      AAAA    2406:2000:1d0::7961:686f:6f21
ns2.yahoo.com.          312358  IN      A       68.142.255.16
ns2.yahoo.com.          53595   IN      AAAA    2001:4998:1c0::7961:686f:6f21
ns3.yahoo.com.          1217    IN      A       27.123.42.42
ns3.yahoo.com.          745     IN      AAAA    2406:8600:f03f:1f8::1003

;; Query time: 15 msec
;; SERVER: 192.168.15.1#53(192.168.15.1)
;; WHEN: Sun Apr 17 23:11:01 India Standard Time 2022
;; MSG SIZE  rcvd: 416

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 43794
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

Nslookup

```
Command Prompt

C:\Users\adnan>nslookup -type=ns redhat.com
Server:  UnKnown
Address:  192.168.15.1

Non-authoritative answer:
redhat.com      nameserver = a9-65.akam.net
redhat.com      nameserver = a10-65.akam.net
redhat.com      nameserver = a28-64.akam.net
redhat.com      nameserver = a13-66.akam.net
redhat.com      nameserver = a16-67.akam.net
redhat.com      nameserver = a1-68.akam.net

a13-66.akam.net internet address = 2.22.230.66
a13-66.akam.net AAAA IPv6 address = 2600:1480:800::42
a9-65.akam.net  internet address = 184.85.248.65
a9-65.akam.net  AAAA IPv6 address = 2a02:26f0:117::41
a10-65.akam.net internet address = 96.7.50.65
a16-67.akam.net internet address = 23.211.132.67
a16-67.akam.net AAAA IPv6 address = 2600:1406:1b::43
a28-64.akam.net internet address = 95.100.173.64
```

```
C:\Users\adnan>nslookup -type=any google.com
Server:  UnKnown
Address:  192.168.15.1

Non-authoritative answer:
google.com      AAAA IPv6 address = 2404:6800:4009:810::200e
google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 442195542
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
google.com      internet address = 142.250.183.110
google.com      nameserver = ns1.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns3.google.com

google.com      nameserver = ns3.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns1.google.com
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
```

```
C:\Users\adnan>nslookup -type=mx facebook.com
Server:  UnKnown
Address:  192.168.15.1

Non-authoritative answer:
facebook.com    MX preference = 10, mail exchanger = smtpin.vvv.facebook.com

facebook.com    nameserver = b.ns.facebook.com
facebook.com    nameserver = c.ns.facebook.com
facebook.com    nameserver = d.ns.facebook.com
facebook.com    nameserver = a.ns.facebook.com
a.ns.facebook.com       internet address = 129.134.30.12
a.ns.facebook.com       AAAA IPv6 address = 2a03:2880:f0fc:c:face:b00c:0:35
b.ns.facebook.com       internet address = 129.134.31.12
b.ns.facebook.com       AAAA IPv6 address = 2a03:2880:f0fd:c:face:b00c:0:35
c.ns.facebook.com       internet address = 185.89.218.12
c.ns.facebook.com       AAAA IPv6 address = 2a03:2880:f1fc:c:face:b00c:0:35
d.ns.facebook.com       internet address = 185.89.219.12
d.ns.facebook.com       AAAA IPv6 address = 2a03:2880:f1fd:c:face:b00c:0:35
```