Shri Vile Parle Kelavani Mandal's
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC Accredited with "A" Grade (CGPA : 3.18)

# Experiment 9

**Date of Performance:** 7 May 2023 **Date of Submission:** 8 May 2023

**SAP Id:** 60004200132 **Name :** Ayush Jain

**Div:** B **Batch :** B3

## Aim of Experiment

Study the use of network reconnaissance tool

## Theory / Algorithm / Conceptual Description:

Algorithm / Conceptual Description

Network reconnaissance is performed on the target, by an ethical hacker who can learn about the details of the target network and identify potential attack vectors. Reconnaissance efforts can be broken up into two types: passive and active.

In passive reconnaissance, the hacker never interacts directly with the target's network. The tools used for passive reconnaissance take advantage of unintentional data leaks from an organization to provide the hacker with insight into the internals of the organization's network.

Tools for active reconnaissance are designed to interact directly with machines on the target network in order to collect data that may not be available by other means. Active reconnaissance can provide a hacker with much more detailed information about the target but also runs the risk of detection. Network reconnaissance is a crucial part of any hacking operation. Any information that a hacker can learn about the target environment can help in identification of potential attack vectors and targeting exploits to potential vulnerabilities. By using a combination of passive and active reconnaissance tools and techniques, a hacker can maximize the information collected while minimizing their probability of detection.

WHOIS:

WHOIS (pronounced as the phrase "who is") is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.[1] The current iteration of the WHOIS protocol was drafted by the Internet Society, and is documented in RFC 3912

Whois is also the name of the command-line utility on most UNIX systems used to make WHOIS protocol queries.[2] In addition WHOIS has a sister protocol called Referral Whois (RWhois).

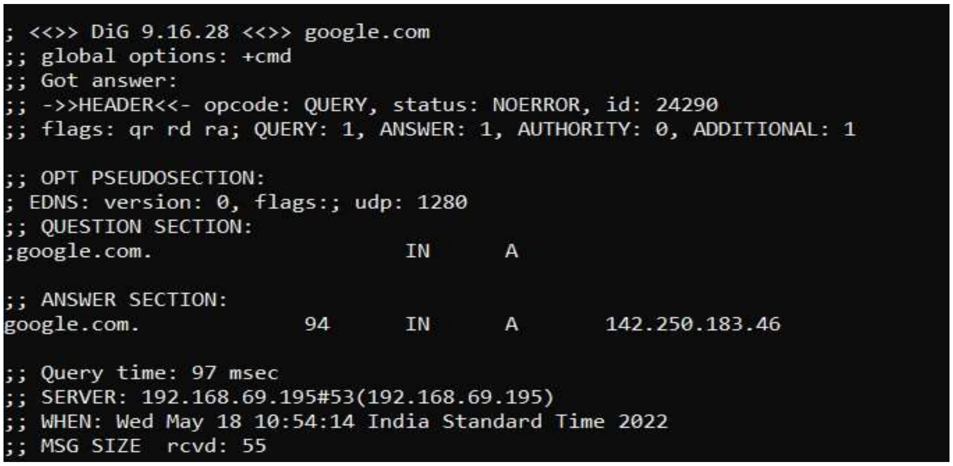
The WHOIS protocol had its origin in the ARPANET NICNAME protocol and was based on the NAME/FINGER Protocol, described in RFC 742 (1977). The

NICNAME/WHOIS protocol was first described in RFC 812 in 1982 by Ken Harrenstien and Vic White of the Network Information Center at SRI International.

WHOIS was originally implemented on the Network Control Program (NCP) but

found its major use when the TCP/IP suite was standardized across the ARPANET and later the Internet.

**Output:**

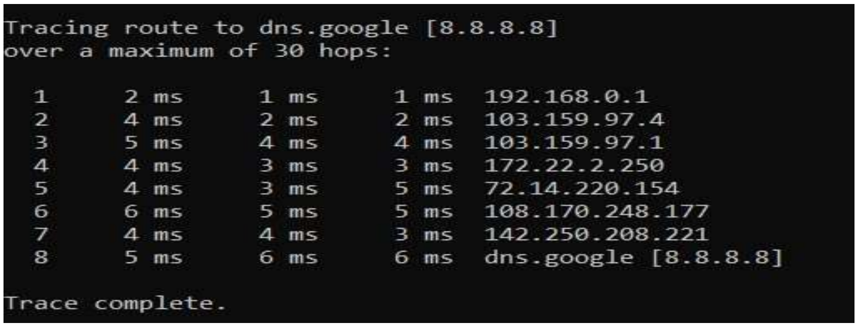


```
; <<>> DiG 9.16.28 <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24290
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             94      IN      A       142.250.183.46

;; Query time: 97 msec
;; SERVER: 192.168.69.195#53(192.168.69.195)
;; WHEN: Wed May 18 10:54:14 India Standard Time 2022
;; MSG SIZE  rcvd: 55
```

**TRACE ROUTE:**

In computing, traceroute and tracert are computer network diagnostic commands for displaying possible routes (paths) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop is a measure of the total time spent to establish the connection. Traceroute proceeds unless all (usually three) sent packets are lost more than twice; then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point.

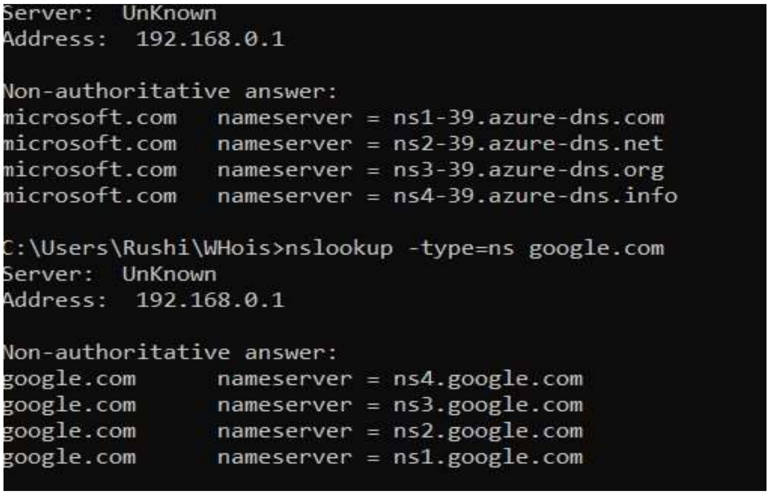
**Output:**



```
Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.0.1
  2     4 ms     2 ms     2 ms  103.159.97.4
  3     5 ms     4 ms     4 ms  103.159.97.1
  4     4 ms     3 ms     3 ms  172.22.2.250
  5     4 ms     3 ms     5 ms  72.14.220.154
  6     6 ms     5 ms     5 ms  108.170.248.177
  7     4 ms     4 ms     3 ms  142.250.208.221
  8     5 ms     6 ms     6 ms  dns.google [8.8.8.8]

Trace complete.
```

**NSLOOKUP:**

nslookup (from name server lookup) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records. 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.



```
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
microsoft.com   nameserver = ns1-39.azure-dns.com
microsoft.com   nameserver = ns2-39.azure-dns.net
microsoft.com   nameserver = ns3-39.azure-dns.org
microsoft.com   nameserver = ns4-39.azure-dns.info

C:\Users\Rushi\WHois>nslookup -type=ns google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
google.com      nameserver = ns4.google.com
google.com      nameserver = ns3.google.com
google.com      nameserver = ns2.google.com
google.com      nameserver = ns1.google.com
```

**Conclusion:** We have successfully studied the use of network reconnaissance tools like WHOIS, dig, trace route, nslookup.