Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Information Technology

Experiment No: 04				
Date of Performance:	30/08/2024			
Date of Submission:	**07/09/2024**			
Program Formation/ Execution/ Correction (06)	**Timely Submission (01)**	**Viva (03)**	**Experiment Marks (10)**	**Teacher Signature with date**

EXPERIMENT - 04

Aim : Network Reconnaissance tools like WHOIS , dig , traceroute , nslookup , to gather information

Theory :

1. WHOIS: Domain Registration Lookup

Purpose:
WHOIS is a query/response protocol used to retrieve details about domain name registrations and IP address ownership. It provides information such as:

- The domain registrar
- Domain owner (registrant)
- Administrative and technical contact details

How It Works:
When a domain is registered, the domain owner's details are stored in a WHOIS database. The WHOIS tool queries this database and provides publicly available details of the registration. WHOIS databases are managed by domain registries and ICANN (Internet Corporation for Assigned Names and Numbers).

Example:
Let's say you want to find the registration details of example.com.

You could perform a WHOIS query, and the result would show:

- **Registrar**: The name of the company that registered the domain (e.g., GoDaddy).
- **Registrant**: The individual or organization that owns the domain.
- **Admin Contact**: Contact details for administrative issues.

2. dig: DNS Information Lookup

Purpose:
dig (Domain Information Groper) is a tool used to query Domain Name System (DNS) servers. It provides detailed information about DNS records, such as:

- A records (IPv4 addresses)
- AAAA records (IPv6 addresses)
- MX records (Mail servers)
- NS records (Name servers)

- SOA records (Start of Authority, which provides information about DNS zones)

How It Works:
dig queries the DNS for specific records associated with a domain. For example, when you use dig example.com, it will contact DNS servers to retrieve the IP address (A record) linked to the domain.

Example:
For example.com, using dig example.com might return the following:

- **A Record**: 93.184.216.34 (the IPv4 address associated with example.com).
- **MX Record**: The mail server responsible for handling emails for that domain.

This allows you to verify which servers are being used for a domain, check DNS propagation, or troubleshoot DNS-related issues.

3. traceroute: Network Path Tracing

Purpose:
traceroute shows the path that packets take from your computer to a remote destination, such as a server or website. It helps you identify the number of hops (intermediate routers) between your device and the destination and the time taken for each hop. This tool is useful for diagnosing network delays, congestion, or routing issues.

How It Works:
traceroute sends packets with increasing TTL (Time to Live) values. Each router that the packet passes through decreases the TTL, and when it reaches 0, the router sends an ICMP "Time Exceeded" message back. This process is repeated for each hop until the destination is reached.

Example:
If you run traceroute for example.com, it will return the list of routers (hops) that the data travels through to reach the destination.

4. nslookup: Query DNS for Specific Records

Purpose:
nslookup is a simpler DNS lookup tool that retrieves IP addresses or DNS records (A, MX, CNAME, etc.) for a domain. It’s a basic way to check if a domain resolves correctly to an IP address and if the DNS records are correctly configured.

How It Works:
You specify the domain, and nslookup will query the DNS to return the corresponding IP address or the specified DNS record. It’s particularly useful for troubleshooting DNS issues, checking DNS propagation, or verifying DNS records.

nslookup Example:

Let’s say you want to find the IP address for the domain example.com.

You could perform an **nslookup** query, and the result would show:

- **Domain Name**: example.com
- **IP Address**: 93.184.216.34 (This is the IPv4 address the domain resolves to)
- **DNS Server**: The DNS server used to resolve the domain (e.g., Google's public DNS 8.8.8.8)

Implementation

1.) **WHOIS :**

```
owner@owner-Virtual-Machine:~$ whois cnn.com
```

```
Domain Name: cnn.com
Registry Domain ID: 3269879_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2018-04-10T16:43:38Z
Creation Date: 1993-09-22T04:00:00Z
Registrar Registration Expiration Date: 2026-09-21T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Name Manager
Registrant Organization: Turner Broadcasting System, Inc.
Registrant Street: One CNN Center
Registrant City: Atlanta
Registrant State/Province: GA
Registrant Postal Code: 30303
Registrant Country: US
Registrant Phone: +1.4048275000
Registrant Phone Ext:
Registrant Fax: +1.4048271995
Registrant Fax Ext:
Registrant Email: tmgroup@turner.com
Registry Admin ID:
Admin Name: Domain Name Manager
Admin Organization: Turner Broadcasting System, Inc.
Admin Street: One CNN Center
Admin City: Atlanta
Admin State/Province: GA
Admin Postal Code: 30303
Admin Country: US
Admin Phone: +1.4048275000
Admin Phone Ext:
Admin Fax: +1.4048271995
Admin Fax Ext:
Admin Email: tmgroup@turner.com
Registry Tech ID:
Tech Name: TBS Server Operations
```

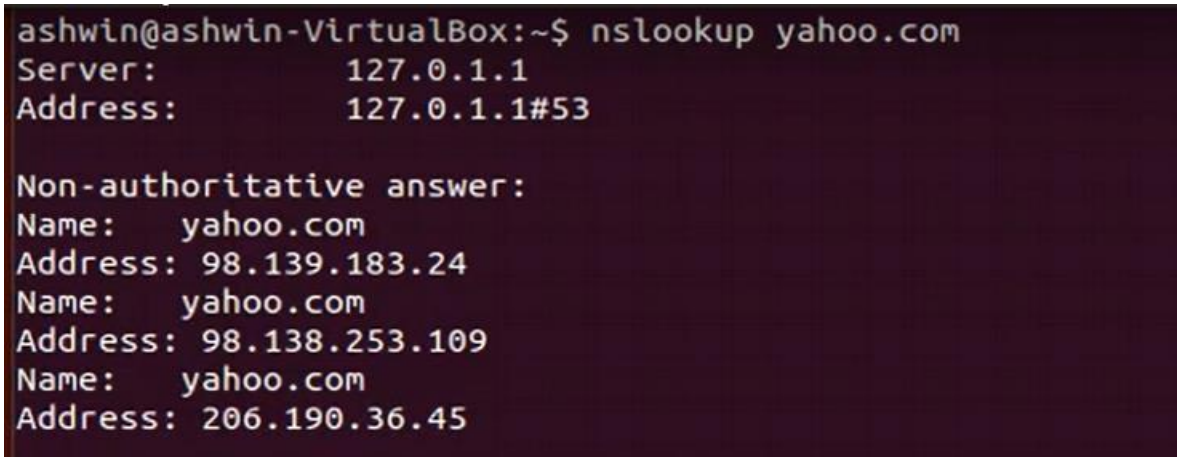
2.) **Dig :**

```
ashwin@ashwin-VirtualBox:~$ dig www.redhat.com

; <<>> DiG 9.9.5-3-Ubuntu <<>> www.redhat.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38526
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.redhat.com.                        IN      A

;; ANSWER SECTION:
www.redhat.com.         60      IN      CNAME   wildcard.redhat.com.edgekey.net.
wildcard.redhat.com.edgekey.net. 7147 IN CNAME  wildcard.redhat.com.edgekey.net.globalredir.akadns.net.
wildcard.redhat.com.edgekey.net.globalredir.akadns.net. 549 IN CNAME e1890.b.akamaiedge.net.
e1890.b.akamaiedge.net. 20      IN      A       172.230.231.100

;; Query time: 57 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Dec 09 17:34:49 PST 2014
;; MSG SIZE  rcvd: 202
```

3.) Traceroute

```
ashwin@ashwin-VirtualBox:~$ traceroute www.google.com
traceroute to www.google.com (74.125.28.104), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.569 ms  0.344 ms  0.998 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

4.) nslookup



Conclusion :

- **WHOIS**: Retrieves domain ownership and registration details (e.g., registrar, owner, contact details).
- **dig**: Queries DNS for specific records (e.g., IP addresses, mail servers).
- **traceroute**: Maps the path data takes from your computer to the destination server, showing all the hops.
- **nslookup**: Quickly retrieves DNS records for a domain, such as the IP address.

These tools are essential for gathering network information, troubleshooting DNS issues, and understanding the structure of domain and IP relationships. Let me know if you'd like to dive deeper into any particular tool!