**Name: Jigar Siddhpura** **SAPID:** 60004200155

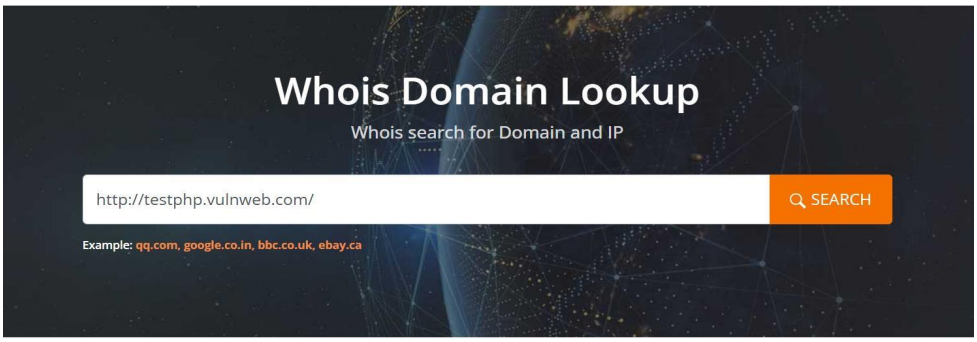
**DIV: C/C2** **Branch:** Computer Engineering

# IS - Experiment 9 - Information Gathering (OSINT)

**Aim:** Perform information Gathering/Footprint using using tools such as: WHOIS, nslookup, traceroute.

**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.




vulnweb.com

Updated 2 hours ago

**Domain Information**

| | |
|---|---|
| Domain: | vulnweb.com |
| Registrar: | EuroDNS S.A. |
| Registered On: | 2010-06-14 |
| Expires On: | 2025-06-13 |
| Updated On: | 2023-05-26 |
| Status: | clientTransferProhibited |
| Name Servers: | ns1.eurodns.com<br>ns2.eurodns.com<br>ns3.eurodns.com<br>ns4.eurodns.com |

**Registrant Contact**

| | |
|---|---|
| Name: | Acunetix Acunetix |
| Organization: | Acunetix Ltd |
| Street: | 3rd Floor,, J&C Building,, Road Town |
| City: | Tortola |
| Postal Code: | VG1110 |
| Country: | VG |
| Phone: | +1.23456789 |
| Email: | administrator@acunetix.com |

## Administrative Contact

| | |
|---|---|
| Name: | Acunetix Acunetix |
| Organization: | Acunetix Ltd |
| Street: | 3rd Floor,, J&C Building,, Road Town |
| City: | Tortola |
| Postal Code: | VG1110 |
| Country: | VG |
| Phone: | +1.23456789 |
| Email: | administrator@acunetix.com |

## Technical Contact

| | |
|---|---|
| Name: | Acunetix Acunetix |
| Organization: | Acunetix Ltd |
| Street: | 3rd Floor,, J&C Building,, Road Town |
| City: | Tortola |
| Postal Code: | VG1110 |
| Country: | VG |
| Phone: | +1.23456789 |
| Email: | administrator@acunetix.com |

## Raw Whois Data

```
Domain Name: vulnweb.com
Registry Domain ID: D16000066-COM
Registrar WHOIS Server: whois.eurodns.com
Registrar URL: http://www.eurodns.com
Updated Date: 2023-05-26T10:04:20Z
Creation Date: 2010-06-14T00:00:00Z
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z
Registrar: Eurodns S.A.
Registrar IANA ID: 1052
Registrar Abuse Contact Email: legalservices@eurodns.com
Registrar Abuse Contact Phone: +352.27220150
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Acunetix Acunetix
Registrant Organization: Acunetix Ltd
Registrant Street: 3rd Floor,, J&C Building,, Road Town
Registrant City: Tortola
Registrant State/Province:
Registrant Postal Code: VG1110
Registrant Country: VG
Registrant Phone: +1.23456789
Registrant Fax:
Registrant Email: administrator@acunetix.com
Registry Admin ID:
Admin Name: Acunetix Acunetix
Admin Organization: Acunetix Ltd
Admin Street: 3rd Floor,, J&C Building,, Road Town
Admin City: Tortola
Admin State/Province:
Admin Postal Code: VG1110
Admin Country: VG
Admin Phone: +1.23456789
Admin Fax:
Admin Email: administrator@acunetix.com
Registry Tech ID:
Tech Name: Acunetix Acunetix
Tech Organization: Acunetix Ltd
Tech Street: 3rd Floor,, J&C Building,, Road Town
Tech City: Tortola
Tech State/Province:
Tech Postal Code: VG1110
Tech Country: VG
Tech Phone: +1.23456789
Tech Fax:
Tech Email: administrator@acunetix.com
Name Server: ns1.eurodns.com
Name Server: ns2.eurodns.com
Name Server: ns3.eurodns.com
Name Server: ns4.eurodns.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2024-02-17T05:16:12Z <<<
```

**TraceRoute:**

Traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. The first column corresponds to the hop count. The second column represents the address of that hop and after that, you see three space-separated time in milliseconds. the traceroute command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop. In windows, alternative for traceroute command is tracert.

```
C:\Users\jsidd>tracert google.com

Tracing route to google.com [142.250.183.206]
over a maximum of 30 hops:

  1    <1 ms     4 ms    <1 ms  192.168.1.1
  2     1 ms     1 ms     1 ms  170.86.179.202.aipl.ankhnet.net [202.179.86.170]
  3     *        *        *     Request timed out.
  4     *        5 ms     5 ms  as15169.bom.extreme-ix.net [103.77.108.82]
  5     4 ms     5 ms     4 ms  142.251.76.23
  6     4 ms     *       71 ms  142.251.64.11
  7    12 ms     *        3 ms  bom07s33-in-f14.1e100.net [142.250.183.206]

Trace complete.
```

**Nslookup:**

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems. nslookup followed by the domain name will display the “A Record” (IP Address) of the domain. Use this command to find the address record for a domain. It queries to domain name servers and get the details

```
sf1@DESKTOP-ST93SJ9:~$ nslookup amazon.com
Server:         192.168.240.1
Address:        192.168.240.1#53

Non-authoritative answer:
Name:   amazon.com
Address: 52.94.236.248
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 205.251.242.103
```

**CONCLUSION**

Thus, we have successfully implemented and studied the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars