|  |  |
| --- | --- |
| Subject: Cryptography & System Security Lab | Course ID: CSL-602 |
| Semester: VI | Course: AI & DS |
| Laboratory: 302 | Name of teacher: Prof. Gitanjali Korgaonkar |
| Name of Student: Ayush Gupta | Roll No: VU2S2324001 |

**EXPERIMENT NO. 3**

**Aim:**

To study the use of network reconnaissance tools like WHOIS, DIG, Traceroute, and NSLookup to gather information about networks and domain registrars.

**Theory:**

Network reconnaissance is the process of gathering information about a target network or domain before launching attacks or conducting security assessments. This experiment focuses on four widely used command-line tools:

1. **WHOIS:**

WHOIS is a query and response protocol used to obtain domain registration details, including ownership, contact information, and expiration date.

**Attributes:**

* Domain name
* Registrar details
* Creation and expiry dates
* Name servers

**Syntax:** whois <domain>

**Example:** whois google.com

1. **DIG (Domain Information Groper):**

DIG is a DNS lookup utility used to retrieve DNS records, such as A, MX, CNAME, and TXT records, for a domain.

**Attributes:**

* A Record (IP address of the domain)
* MX Record (Mail server information)
* CNAME Record (Alias of a domain)
* TXT Record (Text-based information)

**Syntax:** dig <domain>

**Example:** dig google.com

1. **Traceroute:**

Traceroute maps the path packets take to reach a destination, helping to identify network latency and routing issues.

**Attributes:**

* Number of hops
* Response time
* Intermediate routers

**Syntax:** traceroute <domain>

**Example:** traceroute google.com

1. **NSLookup (Name Server Lookup):**

NSLookup is used to query DNS records and retrieve IP addresses associated with domain names.

**Attributes:**

* IP address of the domain
* DNS server details

**Syntax:** nslookup <domain>

**Example:** nslookup google.com

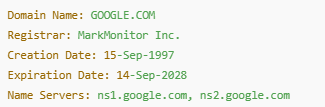
**Conclusion:**

In this experiment, we explored WHOIS, DIG, Traceroute, and NSLookup, which are essential network reconnaissance tools. These tools help gather critical information about domains, IP addresses, and routing paths. Ethical use of these tools is important in cybersecurity for network troubleshooting and security assessments.



**Program and Output:**

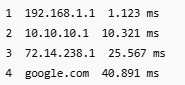
1. **WHOIS:** whois google.com

****

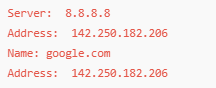
1. **DIG:** dig google.com

****

1. **Traceroute:** traceroute google.com

****

1. **NSLookup:** nslookup google.com

****