Experiment no.2: Study the use of network reconnaissance tools/commands like ping, traceroute, whois, etc. to gather information about networks and domain registrars

Learning Objective: Student should be able to understand about network information discovery & various basic network commands to gather network information.

Tools: Networking Commands

Theory:

Reconnaissance is a set of processes and techniques used to covertly discover and collect information about a target system. During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible.

Active reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities. This may be through automated scanning or manual testing using various tools like ping, traceroute, netcat etc. ... (Intrusion Detection Systems, network firewalls, etc.)

When one is conducting **Passive reconnaissance**, one is not interacting directly with the target and as such, the target has no way of knowing, recording, or logging activity. The reconnaissance is aimed at collecting as much information as possible on a target.

Some of the networking commands used to gather information:

1. Ping:

Ping is a basic Internet program that allows a user to verify that a particular IP address exists and can accept requests. Ping is used diagnostically to ensure that a host computer the user is trying to reach is actually operating. Ping works by sending an Internet Control Message Protocol (ICMP) Echo Request to a specified interface on the network and waiting for a reply. Ping can be used for troubleshooting to test connectivity and determine response time.

Tells when the IP has been on network for long & can be discarded or not

2. Traceroute:

Traceroute prints the route that packets take to a network host. Traceroute utility uses the TTL field in the IP header to achieve its operation. The TTL field, describes how much hops a particular packet will take while traveling on network. So, this effectively outlines the lifetime of the packet on network. This field is usually set to 32 or 64. Each time the packet is held on an intermediate router, it decreases the TTL value by 1. When a router finds the TTL value of 1 in a received packet then that packet is not forwarded but instead discarded. After discarding the packet, router sends an ICMP error message of —Time exceeded, back to the source from where packet generated. The ICMP packet that is sent back contains the IP address of the router. So now it can be easily understood that traceroute operates by sending packets with TTL value starting from 1 and then incrementing by one each time. Each time a router receives the packet, it checks the TTL field, if TTL field is 1 then it discards the packet and sends the ICMP error packet containing its IP address. So, traceroute incrementally fetches the IP of all the routers between the source and the destination.

3. **Nslookup:** The nslookup command is used to query internet name servers interactively for information. nslookup, which stands for "name server lookup", is a useful tool for finding out information about a domain name. By default, nslookup will translate a domain name to an IP address (or vice versa).

4. **WHOIS:** WHOIS is the Linux utility for searching an object in a WHOIS database. The WHOIS database of a domain is the publicly displayed information about a domains ownership, billing, technical, administrative, and nameserver information. Running a WHOIS on your domain will look the domain up at the registrar for the domain information. All domains have WHOIS information. WHOIS database can be queried to obtain the following information via WHOIS:

- Administrative contact details, including names, email addresses, and telephone numbers
- Mailing addresses for office locations related to the target organization
- Details of authoritative name servers for each given domain

Output:

```
C:\Users\gauta>getmac

Physical Address    Transport Name
=================== ==========================================================
0A-00-27-00-00-0F   \Device\Tcpip_{952C35D7-FBD6-4D42-BB2E-846403EDC0D4}
28-D2-44-74-A9-9F   Media disconnected
7C-7A-91-97-CC-BE   \Device\Tcpip_{0B4935AE-976D-49CC-BE57-7C6B16A8CAC9}
00-FF-4E-58-F7-51   Media disconnected
N/A                 Media disconnected
```