**Experiment no.2:**

**Aim:** Study the use of network reconnaissance tools/commands like ping, traceroute, whois, nmap 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 computer network administration software utility used to test the reachability of a host on an Internet Protocol network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.

# Traceroute:

In computing, traceroute and tracert are computer network diagnostic commands for displaying possible routes and measuring transit delays of packets across an Internet Protocol network.

1. **Nslookup**

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

1. **Whois**

WHOIS 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.

1. **Nmap**

Nmap is a network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

**Result and Discussion**

1. **Ping**

Text

Description automatically generated

# Traceroute:

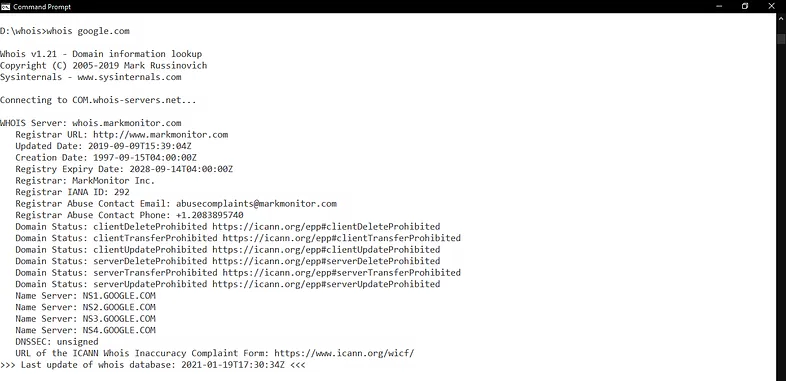
# Text Description automatically generated

1. **Nslookup**

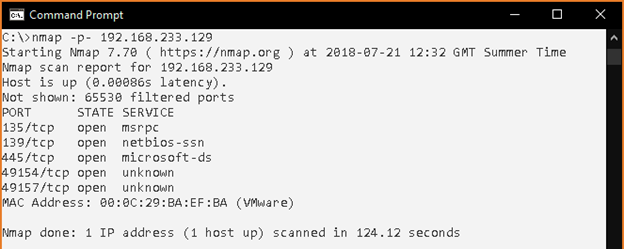
Text, letter

Description automatically generated

1. **Whois**

****

1. **Nmap**



1. **(Analyze the tool nmap and use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc)**

**Learning Outcomes:** The student will be able to

LO1: Understand the use of network reconnaissance tools

LO2: Apply basic network command to gather basic network information.

**Course Outcomes:**

Upon completion of the course students will be able to study the various network reconnaissance tools & how to use them to gather primary network information.

# Conclusion:

In this experiment we used various network commands to gather information about the network host is present in and learned to read and understand their outputs.

# For Faculty Use

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Correction Parameters** | **Formative Assessment [40%]** | **Timely completion of Practical**  **[ 40%]** | **Attendance / Learning Attitude [20%]** |  |
| **Marks Obtained** |  |  |  |