**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 command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable.

# Traceroute: The traceroute command attempts to trace the route an IP packet follows to an Internet host by launching UDP probe packets with a small maximum time-to-live (Max\_ttl variable), then listening for an ICMP TIME\_EXCEEDED response from gateways along the way.

1. **Nslookup**: The nslookup command queries internet domain name servers in two modes. Interactive mode allows you to query name servers for information about various hosts and domains, or to print a list of the hosts in a domain.
2. **Whois**: The whois command tries to reach ARPANET host internic.net where it examines a user-name database to obtain information. The whois command should be used only by users on ARPANET.
3. **Nmap:** Nmap is Linux command-line tool for network exploration and security auditing. This tool is generally used by hackers and cybersecurity enthusiasts and even by network and system administrators. It is used for the following purposes:

* Real time information of a network
* Detailed information of all the IPs activated on your network

**Result and Discussion**

1. **Ping:**

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]

[-r count] [-s count] [[-j host-list] | [-k host-list]]

[-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]

[-4] [-6] target\_name

Options:

-t Ping the specified host until stopped.

To see statistics and continue - type Control-Break;

To stop - type Control-C.

-a Resolve addresses to hostnames.

-n count Number of echo requests to send.

-l size Send buffer size.

-f Set Don't Fragment flag in packet (IPv4-only).

-i TTL Time To Live.

-v TOS Type Of Service (IPv4-only. This setting has been deprecated

and has no effect on the type of service field in the IP

Header).

-r count Record route for count hops (IPv4-only).

-s count Timestamp for count hops (IPv4-only).

-j host-list Loose source route along host-list (IPv4-only).

-k host-list Strict source route along host-list (IPv4-only).

-w timeout Timeout in milliseconds to wait for each reply.

-R Use routing header to test reverse route also (IPv6-only).

Per RFC 5095 the use of this routing header has been

deprecated. Some systems may drop echo requests if

this header is used.

-S srcaddr Source address to use.

-c compartment Routing compartment identifier.

-p Ping a Hyper-V Network Virtualization provider address.

-4 Force using IPv4.

-6 Force using IPv6.

# Traceroute:

Usage: tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout]

[-R] [-S srcaddr] [-4] [-6] target\_name

Options:

-d Do not resolve addresses to hostnames.

-h maximum\_hops Maximum number of hops to search for target.

-j host-list Loose source route along host-list (IPv4-only).

-w timeout Wait timeout milliseconds for each reply.

-R Trace round-trip path (IPv6-only).

-S srcaddr Source address to use (IPv6-only).

-4 Force using IPv4.

-6 Force using IPv6.

1. **Nslookup**

Default Server: dns.google

Address: 8.8.8.8

1. **Whois**

whois techbuzzonline.com

Whois v1.14 - Domain information lookup

Copyright (C) 2005-2016 Mark Russinovich

Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

Domain ID: 1663819488\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: http://www.godaddy.com

Updated Date: 2017-10-26T16:55:43Z

Creation Date: 2011-06-26T05:36:06Z

Registry Expiry Date: 2022-06-26T05:36:06Z

Registrar: GoDaddy.com, LLC

1. **Nmap**

nmap -iL input.txt

$ cat input.txt

server.shellhacks.com

192.168.1.0/24

192.168.2.1,2,3

192.168.3.0-200

**(**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 Parameter s** | **Formative Assessment [40%]** | **Timely completion of Practical** | **Attendance / Learning Attitude [20%]** |  |
|  |  | **[ 40%]** |  |
| **Marks Obtained** |  |  |  |