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.

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
```

```
C:\Users\gauta>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=6ms TTL=53
Reply from 8.8.8.8: bytes=32 time=5ms TTL=53
Reply from 8.8.8.8: bytes=32 time=5ms TTL=53
Reply from 8.8.8.8: bytes=32 time=5ms TTL=53

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 6ms, Average = 5ms

C:\Users\gauta>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     1 ms    <1 ms     1 ms  reliance.reliance [192.168.29.1]
  2     3 ms     2 ms     2 ms  10.31.48.1
  3     3 ms     4 ms     4 ms  172.31.2.22
  4     4 ms     3 ms     3 ms  192.168.70.18
  5     4 ms     3 ms     3 ms  172.26.76.165
  6     3 ms     3 ms     3 ms  172.26.76.131
  7     4 ms     3 ms     3 ms  192.168.7.246
  8     6 ms     6 ms     5 ms  192.168.7.247
  9     5 ms     5 ms     5 ms  172.31.3.23
 10     4 ms     6 ms     4 ms  72.14.217.206
 11     8 ms     9 ms    16 ms  142.251.76.27
 12     5 ms     4 ms     4 ms  142.251.64.11
 13     5 ms     5 ms     5 ms  dns.google [8.8.8.8]

Trace complete.

C:\Users\gauta>hostname
GSCs-Thinkpad
```

```
C:\Users\gauta>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter ProtonVPN TUN:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

```
C:\Users\gauta>nslookup 8.8.8.8
Server:  reliance.reliance
Address:  192.168.29.1

Name:    dns.google
Address:  8.8.8.8


C:\Users\gauta>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.29.26:60642    170-114-14-65:https    ESTABLISHED
  TCP    192.168.29.26:60649    170.114.15.37:https    ESTABLISHED
  TCP    192.168.29.26:60664    20.198.162.76:https    ESTABLISHED
  TCP    192.168.29.26:60669    se-in-f188:5228        ESTABLISHED
  TCP    192.168.29.26:60680    20.195.65.202:https    ESTABLISHED
  TCP    192.168.29.26:60691    104.18.188.55:https    ESTABLISHED
  TCP    192.168.29.26:60692    151.101.66.217:https   ESTABLISHED
  TCP    192.168.29.26:60693    151.101.154.49:https   ESTABLISHED
  TCP    192.168.29.26:60697    151.101.154.137:https  ESTABLISHED
  TCP    192.168.29.26:60699    104.20.59.209:https    ESTABLISHED
  TCP    192.168.29.26:60706    server-13-227-178-25:https  ESTABLISHED
  TCP    192.168.29.26:60707    58:https               ESTABLISHED
  TCP    192.168.29.26:60709    server-13-227-166-122:https  ESTABLISHED
  TCP    192.168.29.26:60710    172.67.73.184:https    ESTABLISHED
  TCP    192.168.29.26:60711    104.26.6.134:https     ESTABLISHED
```

```
C:\Users\gauta>arp /a

Interface: 192.168.29.26 --- 0x3
  Internet Address      Physical Address      Type
  192.168.29.1          18-82-8c-f1-79-bd     dynamic
  192.168.29.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0xf
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Result and Discussion:

1. **Ping** - This command allows you to test the reachability of a device on a network. Pinging a host should return four data packets if no network anomaly is present.
2. **hostname -** This command returns the name of the host.
3. **getmac -** A user can determine the MAC address of their various network devices using this command.
4. **arp** – Displays entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved physical addresses.
5. **nslookup** - The NSLookUp Windows 10 network command displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Using NSLookUp without a parameter will show the DNS server your PC is currently using to resolve domain names into IP addresses.
6. **tracert** - This command will trace the route a data packet takes before reaching its destination, displaying information on each hop along the route. Each hop of the route will display the latency between your device and that particular hop and the IP address of the hop.
7. **ipconfig** - The IPConfig command displays basic IP address configuration information for the current host.
8. **netstat -** The Netstat command displays active TCP connections, ports on which the computer is listening.

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				