Lab 2

Understanding and Practice on basic Networking commands such as ping, ipconfig, tracert, nslookup, arp, tcpdump, netstat, dnsip, hostname, route

Objective

To understand and practice the basic networking commands.

Apparatus: Command Prompt, Linux and Packet Tracer.

Background:

Networking commands are used at the command prompt to get network information like the IP address of the system, MAC address, network route traversed by a packet and the IP address of the server in which a website or URL is hosted. Some basic networking commands are:

a. ping: The ping command is used to test connectivity between two hosts.
b. ipconfig: View the IP addresses on the computers that are configured to obtain their IP address automatically.
c. tracert: This command is used to diagnose path-related problems.
d. nslookup: display the name and IP address of the device's default DNS server.
e. arp: To send IP packets, a computer needs two addresses.
f. tcpdump: used to analyze network traffic by intercepting and displaying packets that are being created or received by the computer it's running on.
g. netstat: This command displays active connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, and IP statistics.
h. dnsip : configures the source IP address for the DNS client to communicate with a server.
i. hostname: returns the local computer name.
j. route: allows to view the device's routing tables.

Procedure / Experiment:

To do this experiment, all the basic command should enter to the command line interface and the result of respective command will appear on windows.

a. Ping:

Syntax: ping *destination host IP or name*

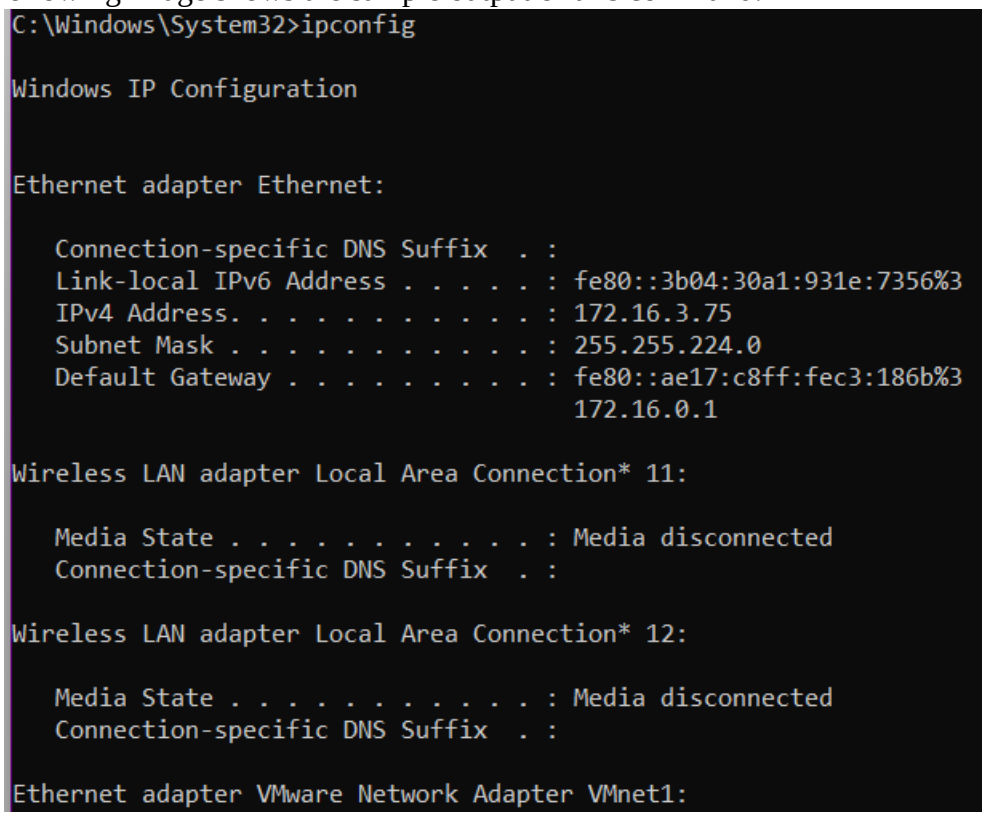
The following command tests connectivity between the host computer and hackthebox's server.

```
C:\Windows\System32>ping www.hackthebox.com

Pinging www.hackthebox.com [104.18.21.126] with 32 bytes of data:
Reply from 104.18.21.126: bytes=32 time=5ms TTL=59
Reply from 104.18.21.126: bytes=32 time=58ms TTL=59
Reply from 104.18.21.126: bytes=32 time=36ms TTL=59
Reply from 104.18.21.126: bytes=32 time=17ms TTL=59

Ping statistics for 104.18.21.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 58ms, Average = 29ms
```

b. Ipconfig:

This command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings.

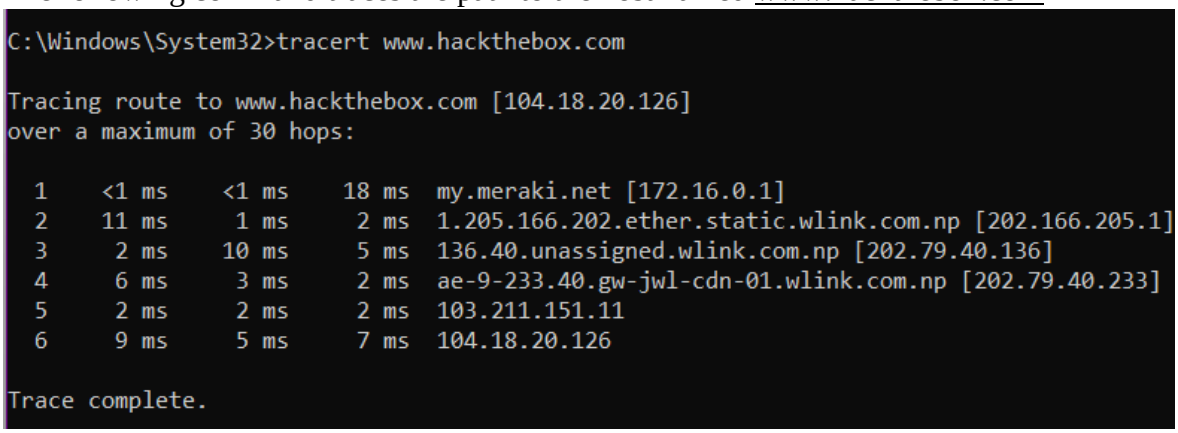
The following image shows the sample output of this command.



c. Tracert

Syntax: tracert *Destination Name or IP address*

The following command traces the path to the host named www.hackthebox.com



Options for tracert Command are as follows:

- **target** : This is the destination, either an IP address or hostname.
- **-w** : A timeout value must be specified while executing this ping command. It adjusts the amount of time in milliseconds.

- -d : Do not resolve the IP addresses of intermediate routers to their names.
- -h the : Specifies the maximum number of hops (routers) to search on path. The default is 30 hops

d. nslookup

Syntax: *nslookup [domain_name]*

The nslookup, which stands for name server lookup command, is a network utility command used to obtain information about internet servers. It provides name server information for the DNS (Domain Name System), i.e. the default DNS server's name and IP Address.

```
C:\Windows\System32>nslookup www.freecodecamp.org
Server:  my.meraki.net
Address:  172.16.0.1

Non-authoritative answer:
Name:    www.freecodecamp.org
Addresses:  2606:4700:20::681a:321
          2606:4700:20::ac43:4695
          2606:4700:20::681a:221
          172.67.70.149
          104.26.2.33
          104.26.3.33
```

,

e. arp

Syntax: *arp*

By default, this command displays the ARP table of the active NIC. If multiple NICs are installed on the computer, you can use the **-a** option with this command. If the -a option is used, the ARP command displays all ARP tables.

```
C:\Windows\System32>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]
```

f. tcpdump

Syntax: *tcpdump –[flag/options]*

tcpdump has a feature to capture and save the file in a .pcap format, to do this just execute the command with -w option.

```
kafleaz@kafleaz:~$ tcpdump -D
1.ens33 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
kafleaz@kafleaz:~$
```

Options for tracert Command are as follows:

- -A : prints each packets
- -b : Print the AS number in BGP packets in ASDOT notation
- -c count: Exit after receiving count packets
- -D : List interfaces

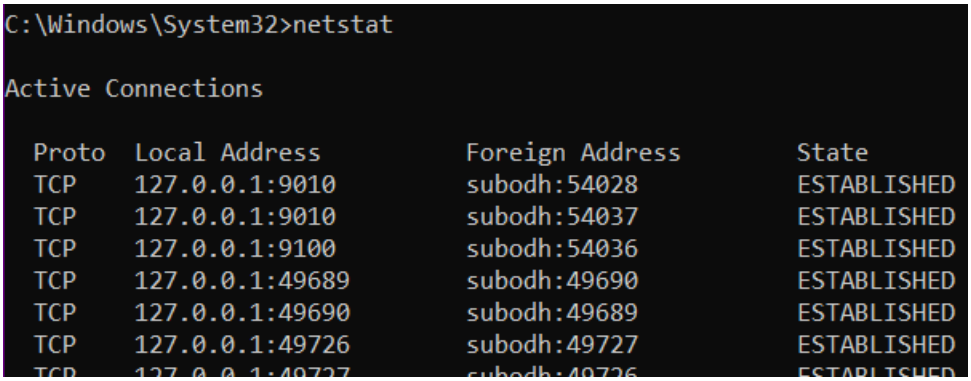
  And so on…

g. netstat

Syntax: *netstat*

The output of this command is organized in rows and columns. Each row represents a new connection or an entry in the output. It contains four columns. These columns provide the following information about the row.

Proto: - This column displays the name of the protocol (TCP or UDP).
Local Address: - This column displays the IP address of the local computer and the port number being used. If the port is not yet established, the port number is shown as an asterisk (*).
Foreign Address: - This column displays the IP address and port number of the remote computer to which the port is connected.
State: - This column displays the status of the connection.



h. dnsip

Syntax: *dnsip (option)*

It configures the source IP address for the DNS client to communicate with a server.

Options for dnsip Command are as follows:

- -h : prints help
- -b : use new output style
- -v : Print version information

i. Hostname

Syntax: *hostname –(option) (file)*

Hostname command in Linux is used to obtain the DNS (Domain Name System) name and set the system's hostname or NIS (Network Information System) domain name. A hostname is a name which is given to a computer and it attached to the network. Its main purpose is to uniquely identify over a network.

```
user@user:~/Desktop$ hostname
user
```

Options for hostname Command are as follows:

- -a : It is used to display the alias name of the host
- -A : used to display the FQDNs of the system.
- -b : allows to set a hostname for always
- -F : print the FQDN (Fully Qualified Domain Name)

And so on..

j. Route

Syntax: *route print*

In IP networks, routing tables are used to direct packets from one subnet to another. The Route command provides the device's routing tables. To get this result, just type route print. The Route command returns the routing table, and the user can make changes by Commands such as Route Add, Route Delete, and Route Change, which allows modifying the routing table as a requirement.

```
C:\Windows\System32>route print
===========================================================================
Interface List
  3...08 8f c3 51 9f d7 ......Killer E2600 Gigabit Ethernet Controller
 19...4c 03 4f e5 a7 14 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 12...4e 03 4f e5 a7 13 ......Microsoft Wi-Fi Direct Virtual Adapter #4
 13...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
  8...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 10...4c 03 4f e5 a7 13 ......Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network Adapter (201NGW)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.0.1      172.16.3.75     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
       172.16.0.0    255.255.224.0         On-link      172.16.3.75    281
      172.16.3.75  255.255.255.255         On-link      172.16.3.75    281
    172.16.31.255  255.255.255.255         On-link      172.16.3.75    281
```

Conclusion

Hence, by Knowing about networking command can identifies all TCP connections and UDP open on a machine. Besides this, it allows us to know the following information: Routing tables to meet our network interfaces and its outputs.