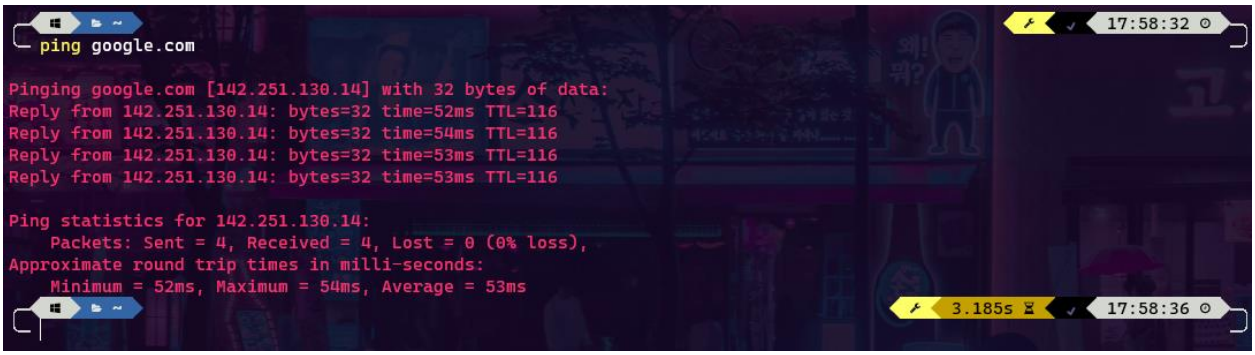
Lab Exer 2 : Familiarizing Network Commands

A. Give the definition and/or usage of the following networking commands in Windows. Also, provide a screenshot of a successful usage of these commands.

1. ping

The ping command sends a series of ICMP ECHO request to a target hostname or IP address, wherein the target host receives the request packets and sends back ICMP Echo reply packets. The command displays the measure of time (e.g. time=52ms) that it takes for a request packet to travel from your computer to the target address.



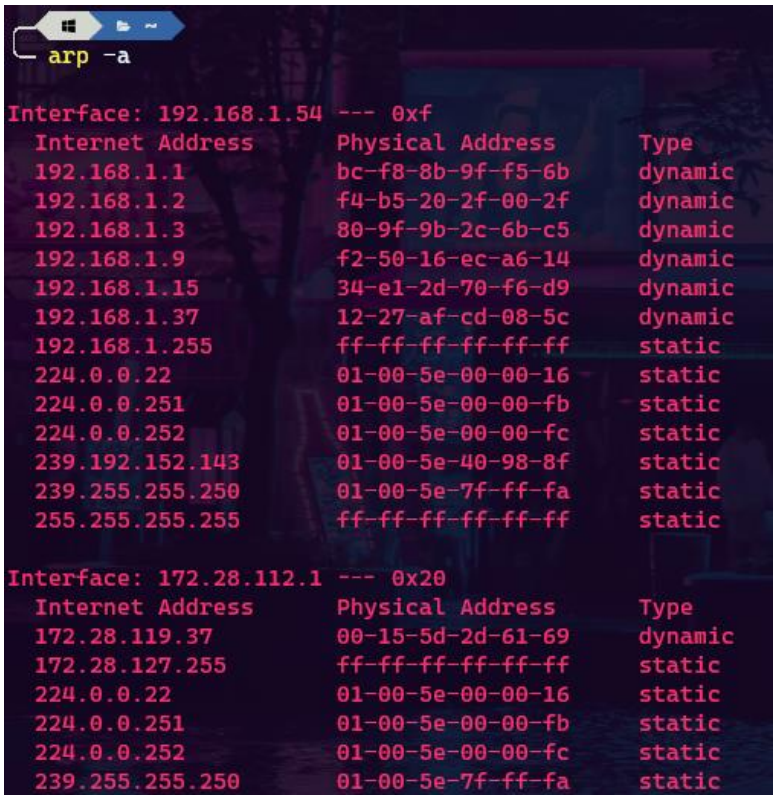
2. netstat

the netstat command displays a list of all active network connections on the local machine, including information like the local address and port the connection is established, the protocol, the connecting foreign address, the connection state, and so on. By default, the -all parameter is implicitly applied when running the command without parameters. With additional parameters, other details can be shown.

```
netstat
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:3662         kubernetes:65001       ESTABLISHED
  TCP    127.0.0.1:3667         kubernetes:3668        ESTABLISHED
  TCP    127.0.0.1:3668         kubernetes:3667        ESTABLISHED
  TCP    127.0.0.1:3687         kubernetes:41661       ESTABLISHED
  TCP    127.0.0.1:8959         kubernetes:8960        ESTABLISHED
  TCP    127.0.0.1:8960         kubernetes:8959        ESTABLISHED
  TCP    127.0.0.1:17871        kubernetes:27060       ESTABLISHED
  TCP    127.0.0.1:27060        kubernetes:17871       ESTABLISHED
  TCP    127.0.0.1:41661        kubernetes:3687        ESTABLISHED
  TCP    127.0.0.1:49693        kubernetes:49694       ESTABLISHED
  TCP    127.0.0.1:49694        kubernetes:49693       ESTABLISHED
  TCP    127.0.0.1:49695        kubernetes:49696       ESTABLISHED
  TCP    127.0.0.1:49696        kubernetes:49695       ESTABLISHED
  TCP    127.0.0.1:49699        kubernetes:49700       ESTABLISHED
  TCP    127.0.0.1:49700        kubernetes:49699       ESTABLISHED
  TCP    127.0.0.1:51809        kubernetes:51810       ESTABLISHED
  TCP    127.0.0.1:51810        kubernetes:51809       ESTABLISHED
  TCP    127.0.0.1:65001        kubernetes:3662        ESTABLISHED
  TCP    192.168.1.54:3663      52.226.139.180:https   ESTABLISHED
  TCP    192.168.1.54:3706      103-10-124-123:27034   ESTABLISHED
  TCP    192.168.1.54:3724      47:https               ESTABLISHED
  TCP    192.168.1.54:8971      170-114-244:https      ESTABLISHED
  TCP    192.168.1.54:8972      170-114-14-72:https    ESTABLISHED
  TCP    192.168.1.54:17897     161:https              CLOSE_WAIT
  TCP    192.168.1.54:17898     17:https               CLOSE_WAIT
  TCP    192.168.1.54:17973     170.114.15.22:https    CLOSE_WAIT
  TCP    192.168.1.54:17974     170.114.15.22:https    CLOSE_WAIT
  TCP    192.168.1.54:34845     edge-star-shv-01-mnl1:https  ESTABLISHED
  TCP    192.168.1.54:34851     edge-dgw-shv-01-mnl1:https  ESTABLISHED
  TCP    192.168.1.54:34852     edge-star-shv-01-mnl1:https  ESTABLISHED
  TCP    192.168.1.54:34856     52.139.250.209:https   ESTABLISHED
  TCP    192.168.1.54:34863     edge-z-p3-shv-01-mnl1:https  ESTABLISHED
  TCP    192.168.1.54:34882     edge-star-shv-01-mnl1:https  ESTABLISHED
  TCP    192.168.1.54:35280     60-241-151-21:44113    ESTABLISHED
  TCP    192.168.1.54:35368     162.159.135.234:https  ESTABLISHED
  TCP    192.168.1.54:35499     104.24.137.8:https     ESTABLISHED
  TCP    192.168.1.54:35501     104.17.24.14:https     ESTABLISHED
  TCP    192.168.1.54:35505     lb-140-82-113-25-iad:https  ESTABLISHED
  TCP    192.168.1.54:35531     ec2-3-235-96-61:https  CLOSE_WAIT
  TCP    192.168.1.54:35563     hkg07s46-in-f5:https   ESTABLISHED
  TCP    192.168.1.54:35607     hosted-by:57690        TIME_WAIT
  TCP    192.168.1.54:35608     server-108-158-213-19:https  ESTABLISHED
  TCP    192.168.1.54:35609     server-108-158-213-67:https  ESTABLISHED
  TCP    192.168.1.54:35610     server-18-65-3-72:https  ESTABLISHED
  TCP    192.168.1.54:35611     server-18-172-21-40:https  ESTABLISHED
  TCP    192.168.1.54:35612     ec2-3-222-102-97:https  ESTABLISHED
  TCP    192.168.1.54:35613     ec2-3-222-102-97:https  ESTABLISHED
  TCP    192.168.1.54:35614     156.59.126.78:https    ESTABLISHED
  TCP    192.168.1.54:35615     168.195.227.244:41963  SYN_SENT
  TCP    192.168.1.54:35616     109-93-33-4:15129      SYN_SENT
  TCP    192.168.1.54:35617     c-69-244-63-61:50160   SYN_SENT
  TCP    192.168.1.54:35618     85.203.21.96:25413     SYN_SENT
  TCP    192.168.1.54:35619     5-15-249-207:6881      SYN_SENT
  TCP    192.168.1.54:35620     13.70.73.107:https     ESTABLISHED
  TCP    192.168.1.54:35621     ua-83-226-92-64:16881  TIME_WAIT
  TCP    192.168.1.54:35622     ho1-32-1-3:51413       SYN_SENT
  TCP    192.168.1.54:62737     52.98.65.2:https       ESTABLISHED
```

3. arp

The arp command is a is a network utility tool used to view and manipulate the Address Resolution Protocol (ARP) cache on a Windows machine. ARP is a protocol used to map an IP address to a physical (MAC) address on a local network. The ARP cache is a table that keeps track of these mappings for devices on the same network segment. When the command is run with no additional parameters, the ARP cache table is shown, with details such as the foreign address, physical MAC address, and the routing type.



```
arp -a

Interface: 192.168.1.54 --- 0xf
  Internet Address      Physical Address      Type
  192.168.1.1           bc-f8-8b-9f-f5-6b     dynamic
  192.168.1.2           f4-b5-20-2f-00-2f     dynamic
  192.168.1.3           80-9f-9b-2c-6b-c5     dynamic
  192.168.1.9           f2-50-16-ec-a6-14     dynamic
  192.168.1.15          34-e1-2d-70-f6-d9     dynamic
  192.168.1.37          12-27-af-cd-08-5c     dynamic
  192.168.1.255         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
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.28.112.1 --- 0x20
  Internet Address      Physical Address      Type
  172.28.119.37         00-15-5d-2d-61-69     dynamic
  172.28.127.255        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
```

4. hostname

The hostname command simply shows the hostname of the current device.

```
hostname
LAPTOP-CL8DNQ0H
```

5. tracert

The command tracert traces the route that packets take from your computer to a target address entered as a parameter. It provides a report of each hop or change of address that the packet encounters along the way.

```
tracert hackthebox.org

Tracing route to hackthebox.org [162.55.161.171]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  192.168.1.1 [192.168.1.1]
  2     4 ms     3 ms     3 ms  100.126.48.1
  3     7 ms    15 ms     *     172.20.80.21 [172.20.80.21]
  4     *        5 ms     *     161.49.4.104.convergeict.com [161.49.4.104]
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7   244 ms   304 ms   306 ms  hetzner.interxionfra11.nl-ix.net [193.239.117.110]
  8   230 ms   304 ms   305 ms  core24.fsn1.hetzner.com [213.239.224.93]
  9   212 ms   259 ms   305 ms  spine1.cloud2.fsn1.hetzner.com [213.239.239.134]
 10   212 ms   243 ms   211 ms  spine8.cloud2.fsn1.hetzner.com [213.239.239.38]
 11     *        *        *     Request timed out.
 12   283 ms   228 ms   210 ms  15833.your-cloud.host [49.12.25.100]
 13   210 ms   209 ms   272 ms  webforward.gr [162.55.161.171]

Trace complete.
```

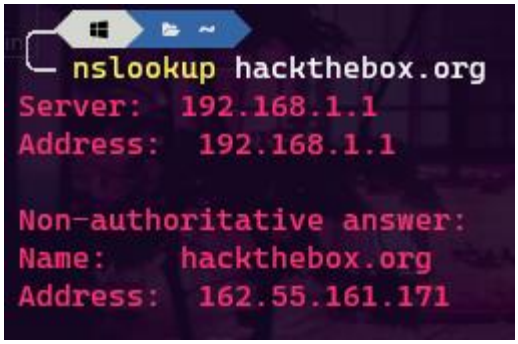
6. ipconfig

The ipconfig command is used to view and manage the network configuration of a Windows machine, providing information about the machine's network interfaces, IP addresses, subnet masks, default gateway, DNS servers and more. There is a suite of details the ipconfig command can provide given certain parameters.

```
ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (WSL):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::aed5:e871:4116:f3e1%32
   IPv4 Address. . . . . . . . . . . : 172.28.112.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1e8b:5f55:53c2:9a18%15
   IPv4 Address. . . . . . . . . . . : 192.168.1.54
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Ethernet:

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

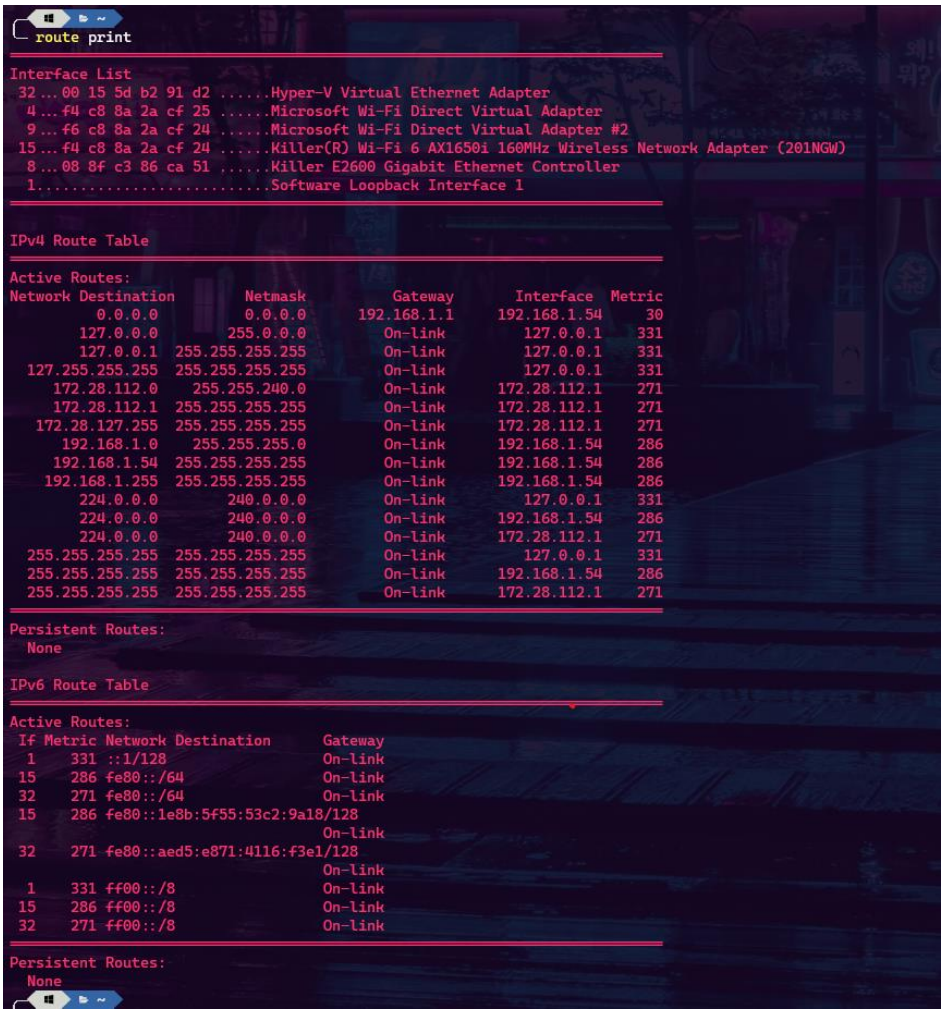
7. nslookup

The nslookup command simply queries the target Domain Name System's server to obtain information, showing details like the domain IP address and proxy.



8. route

The route command, similar to the arp command, shows the routing table on the local machine when run without parameters. It produces the same result as the netstat -rn command. It can also be used to add new routes to the routing table with additional parameters.



9. pathping

The pathping command combines ping and tracert, wherein foreach address hop that a packet encounters, a ping command is sent to that address. The pathping command then shows several statistic, similar to the ping command.

```
pathping hackthebox.org

Tracing route to hackthebox.org [162.55.161.171]
over a maximum of 30 hops:
  0  LAPTOP-CL8DNQ0H [192.168.1.54]
  1  192.168.1.1 [192.168.1.1]
  2  100.126.48.1
  3  172.20.80.21 [172.20.80.21]
  4     *     161.49.4.104.convergeict.com [161.49.4.104]
  5     *        *        *
Computing statistics for 100 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           LAPTOP-CL8DNQ0H [192.168.1.54]
                                 0/ 100 =  0%   |
  1    1ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.1 [192.168.1.1]
                                 0/ 100 =  0%   |
  2    2ms     0/ 100 =  0%     0/ 100 =  0%  100.126.48.1
                                 0/ 100 =  0%   |
  3    5ms     0/ 100 =  0%     0/ 100 =  0%  172.20.80.21 [172.20.80.21]
                                 0/ 100 =  0%   |
  4    2ms     0/ 100 =  0%     0/ 100 =  0%  161.49.4.104.convergeict.com [161.49.4.104]

Trace complete.
```

10. getmac

The command getmac simply displays the physical Media Access Control (MAC) addresses of all network interfaces in the local machine.

```
getmac /v                                                                    00:01:24

Connection Name Network Adapter Physical Address    Transport Name
=============== ===============  ================   ==========================================
Wi-Fi           Killer(R) Wi-Fi  F4-C8-8A-2A-CF-24  \Device\Tcpip_{811B980C-522F-42C1-A70B-5B689993423C}
Ethernet        Killer E2600 Gi  08-8F-C3-86-CA-51  Media disconnected
Ethernet 2      VirtualBox Host  Disabled           Disconnected
Ethernet 3      VirtualBox Host  0A-00-27-00-00-36  \Device\Tcpip_{87087132-DAD0-4900-924E-FEB6804D5062}
                                                                    1.021s   00:01:26
```

B. For each of the commands in A, look for their equivalent in Linux and do the same things as done in A.

1. ping → ping

The ping command in Linux is functionally the same as the ping command in windows, with the exception that the command continually sends an ICMP Echo request to the target address unless manually stopped (^C or more specifically ctrl + C).

```
❯ ping google.com
PING google.com (142.251.130.14) 56(84) bytes of data.
64 bytes from hkg07s54-in-f14.1e100.net (142.251.130.14): icmp_seq=1 ttl=115 time=53.7 ms
64 bytes from hkg07s54-in-f14.1e100.net (142.251.130.14): icmp_seq=2 ttl=115 time=55.0 ms
64 bytes from hkg07s54-in-f14.1e100.net (142.251.130.14): icmp_seq=3 ttl=115 time=53.4 ms
64 bytes from hkg07s54-in-f14.1e100.net (142.251.130.14): icmp_seq=4 ttl=115 time=56.8 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 53.377/54.722/56.765/1.335 ms
                                                          took 3s at 17:57:55
❯
```

2. netstat → netstat

The command is functionally the same as in Windows, with the addition that the Linux counterpart displays additional details without entering any parameters, such as the executable that started the connection, the reference count of the connection, the protocol used, and other details.

```
❯ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    17421    /var/run/chrony/chronyd.sock
unix  2      [ ]         DGRAM                    28866    /run/user/1000/systemd/notify
unix  3      [ ]         DGRAM      CONNECTED     28675    /run/systemd/notify
unix  5      [ ]         DGRAM      CONNECTED     28688    /run/systemd/journal/dev-log
unix  6      [ ]         DGRAM      CONNECTED     28690    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTED     28870    @31b5e8385c0dd795/bus/systemd/bus-system
unix  3      [ ]         STREAM     CONNECTED     18870    @c1c4256a547633f3/bus/systemd/bus-api-system
unix  3      [ ]         STREAM     CONNECTED     23657    @357639f8d8f2be87/bus/systemd-logind/system
unix  3      [ ]         STREAM     CONNECTED     28838
unix  3      [ ]         STREAM     CONNECTED     27667
unix  3      [ ]         STREAM     CONNECTED     17488    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     29706    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     27679    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     18953
unix  3      [ ]         STREAM     CONNECTED     21564
unix  3      [ ]         STREAM     CONNECTED     19664    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     29707    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM      CONNECTED     18806
unix  3      [ ]         STREAM     CONNECTED     17468
unix  3      [ ]         DGRAM      CONNECTED     28867
unix  2      [ ]         DGRAM      CONNECTED     19521
unix  3      [ ]         STREAM     CONNECTED     19720
unix  3      [ ]         STREAM     CONNECTED     26653
unix  3      [ ]         STREAM     CONNECTED     31765
unix  3      [ ]         DGRAM      CONNECTED     28676
unix  3      [ ]         STREAM     CONNECTED     21565    /tmp/dbus-uszpnBP7bQ
unix  3      [ ]         STREAM     CONNECTED     21563
unix  3      [ ]         STREAM     CONNECTED     17437    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM      CONNECTED     18808
unix  2      [ ]         DGRAM      CONNECTED     22577
unix  3      [ ]         DGRAM      CONNECTED     28868
unix  3      [ ]         STREAM     CONNECTED     17489    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     17485
unix  3      [ ]         STREAM     CONNECTED     21559
unix  2      [ ]         DGRAM      CONNECTED     28847
unix  3      [ ]         STREAM     CONNECTED     26652
unix  3      [ ]         STREAM     CONNECTED     21561
unix  3      [ ]         STREAM     CONNECTED     216
unix  3      [ ]         STREAM     CONNECTED     29726    /tmp/.X11-unix/X0
unix  2      [ ]         DGRAM      CONNECTED     23591
unix  3      [ ]         DGRAM      CONNECTED     28677
unix  3      [ ]         STREAM     CONNECTED     23569
unix  3      [ ]         DGRAM      CONNECTED     18809
unix  3      [ ]         STREAM     CONNECTED     18797
unix  2      [ ]         STREAM     CONNECTED     27702
unix  2      [ ]         DGRAM      CONNECTED     22626
unix  3      [ ]         STREAM     CONNECTED     17484
unix  3      [ ]         STREAM     CONNECTED     17523    /mnt/wslg/PulseAudioRDPSink
unix  3      [ ]         STREAM     CONNECTED     21558
unix  2      [ ]         DGRAM      CONNECTED     28855
unix  3      [ ]         STREAM     CONNECTED     21560
unix  3      [ ]         STREAM     CONNECTED     26642    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     23568
unix  2      [ ]         DGRAM      CONNECTED     23646
```

3. arp → arp
   Similar to its Windows counterpart, the arp command in linux displays the ARP cache on the machine. In this screenshot, the -e parameter is used to display all hosts, and the -v parameter is used to produce verbose results.

```
❯ arp -e -v
Address                  HWtype  HWaddress           Flags Mask            Iface
LAPTOP-CL8DNQ0H.mshome.  ether   00:15:5d:b2:91:d2   C                     eth0
Entries: 1      Skipped: 0      Found: 1
at ⊙ 18:05:00
❯
```

4. hostname → hostname
   Functionally similar to its Windows counterpart, the command simply displays the hostname of the local machine when entered without additional parameters. However, the hostname command in Linux is much more versatile in that it offers more functionalities when additional parameters are entered.

```
❯ hostname
LAPTOP-CL8DNQ0H
❯
```

```
❯ hostname -h
Usage: hostname [-b] {hostname|-F file}         set host name (from file)
       hostname [-a|-A|-d|-f|-i|-I|-s|-y]       display formatted name
       hostname                                 display host name

       {yp,nis,}domainname {nisdomain|-F file}  set NIS domain name (from file)
       {yp,nis,}domainname                      display NIS domain name

       dnsdomainname                            display dns domain name

       hostname -V|--version|-h|--help          print info and exit

Program name:
       {yp,nis,}domainname=hostname -y
       dnsdomainname=hostname -d

Program options:
    -a, --alias            alias names
    -A, --all-fqdns        all long host names (FQDNs)
    -b, --boot             set default hostname if none available
    -d, --domain           DNS domain name
    -f, --fqdn, --long     long host name (FQDN)
    -F, --file             read host name or NIS domain name from given file
    -i, --ip-address       addresses for the host name
    -I, --all-ip-addresses all addresses for the host
    -s, --short            short host name
    -y, --yp, --nis        NIS/YP domain name

Description:
   This command can get or set the host name or the NIS domain name. You can
   also get the DNS domain or the FQDN (fully qualified domain name).
   Unless you are using bind or NIS for host lookups you can change the
   FQDN (Fully Qualified Domain Name) and the DNS domain name (which is
   part of the FQDN) in the /etc/hosts file.
❯ hostname -I
172.28.119.37
❯
```

5. tracert → traceroute
   Functionally similar to its Windows counterpart, the traceroute traces the route that packets take from your computer to a target address entered as a parameter. It provides a report of each hop or change of address that the packet encounters along the way. The only difference is that the tracert command stops when the packet reaches the target address, while the traceroute command continues until the set amount of hops (which can be modified via parameter) is reached.

6. ipconfig → ifconfig (deprecated) or ip addr
   The ifconfig command is functionally similar to its Windows counterpart, with the difference being how it displays data. The ifconfig is a deprecated command in favor of ip addr, which is a sub command of the ip network utility tool.

```
❯ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.28.119.37  netmask 255.255.240.0  broadcast 172.28.127.255
        inet6 fe80::215:5dff:fe2d:6169  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:2d:61:69  txqueuelen 1000  (Ethernet)
        RX packets 27285  bytes 38647065 (36.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2773  bytes 194095 (189.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

~/.config                                                    at ⊙ 20:08:23
❯
```

7. nslookup → host
   The host command is functionally exactly similar to its Windows counterpart, with the host command having more parameter options to customize the way the command works.

```
❯ host hackthebox.org
hackthebox.org has address 162.55.161.171
~
❯
```

8. route → netstat -rn (deprecated) or ip route
   Similar to its Windows counterpart, netstat -rn or ip route displays the routing table of the local machine the ip route is a subtool of the ip network utility tool.

```
❯ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         172.28.112.1    0.0.0.0         UG        0 0          0 eth0
172.28.112.0    0.0.0.0         255.255.240.0   U         0 0          0 eth0
~
❯
```

```
❯ ip route
default via 172.28.112.1 dev eth0 proto kernel
172.28.112.0/20 dev eth0 proto kernel scope link src 172.28.119.37
~
```

9. pathping → traceroute -I or mtr
   Functionally similar to its Windows counterpart, the traceroute function with the -I parameter sends an ICMP Echo request to each address hop the packet encounters. However, it does not show additional statistics like that of the pathping command. To replicate the functionalities of the pathping command in Windows, a network utility tool called My traceroute (command: mtr) can be installed and used.

```
❯ sudo traceroute hackthebox.org -I
traceroute to hackthebox.org (162.55.161.171), 30 hops max, 60 byte packets
 1  LAPTOP-CL8DNQ0H.mshome.net (172.28.112.1)  0.512 ms  0.497 ms  0.496 ms
 2  192.168.1.1 (192.168.1.1)  3.034 ms  3.032 ms  3.031 ms
 3  100.126.48.1 (100.126.48.1)  3.502 ms  3.502 ms *
 4  172.20.80.21 (172.20.80.21)  6.113 ms * *
 5  * * *
 6  161.49.4.96.convergeict.com (161.49.4.96)  14.282 ms * *
 7  161.49.11.227.convergeict.com (161.49.11.227)  41.234 ms * *
 8  hetzner.interxionfra11.nl-ix.net (193.239.117.110)  205.564 ms  204.793 ms  205.330 ms
 9  core24.fsn1.hetzner.com (213.239.224.93)  208.999 ms  209.208 ms  208.999 ms
10  spine1.cloud2.fsn1.hetzner.com (213.239.239.134)  210.849 ms  210.395 ms  210.377 ms
11  spine8.cloud2.fsn1.hetzner.com (213.239.239.38)  210.380 ms  211.874 ms  211.872 ms
12  * * *
13  15833.your-cloud.host (49.12.25.100)  210.432 ms  209.254 ms  209.734 ms
14  webforward.gr (162.55.161.171)  209.754 ms  209.610 ms  208.936 ms
~/Meth                                                          took ⌛ 3s at ⊙ 21:58:18
❯
```

```
                                   My traceroute  [v0.95]
LAPTOP-CL8DNQ0H (172.28.119.37) -> hackthebox.org (162.55.161.171)          2023-08-29T21:56:23+0800
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                      Packets               Pings
 Host                                               Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. LAPTOP-CL8DNQ0H.mshome.net                       0.0%    52    0.2   0.6   0.2   0.9   0.2
 2. 192.168.1.1                                      0.0%    51    1.6   1.9   1.5   3.5   0.4
 3. 100.126.48.1                                     0.0%    51    3.4   3.9   2.8  10.0   1.1
 4. 172.20.80.21                                    21.6%    51    7.4   5.9   4.0  11.5   1.8
 5. 161.49.4.104.convergeict.com                    84.0%    51    5.3   6.3   5.3  10.6   1.8
 6. (waiting for reply)
 7. 161.49.11.227.convergeict.com                   98.0%    51   41.7  41.7  41.7  41.7   0.0
 8. hetzner.interxionfra11.nl-ix.net                 0.0%    51  205.7 206.0 205.0 214.9   1.7
 9. core24.fsn1.hetzner.com                          0.0%    51  208.8 209.7 208.8 213.6   0.7
10. spine1.cloud2.fsn1.hetzner.com                   0.0%    51  210.7 213.2 210.1 238.9   7.0
11. spine8.cloud2.fsn1.hetzner.com                   0.0%    51  210.6 211.6 210.3 236.0   3.5
12. (waiting for reply)
13. 15833.your-cloud.host                            0.0%    51  209.6 210.1 209.5 211.9   0.6
14. webforward.gr                                    0.0%    51  213.7 210.2 209.2 213.8   1.0
```

10. getmac → ifconfig (deprecated) or ip addr
    While there is no direct equivalent to getmac in Linux, the ip addr command shows the MAC address of the network devices beside the link/loopback or link/ether sections.

```
❯ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:2d:6b:08 brd ff:ff:ff:ff:ff:ff
    inet 172.28.119.37/20 brd 172.28.127.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe2d:6b08/64 scope link
       valid_lft forever preferred_lft forever
~
❯
```