CN Assignment 2
Aayush Tete
202200403
TY-A
Rn 5

Title : Study of Linux and Windows Network commands

Problem Statement Studying Linux and Windows network commands. [ping, pathping, ipconfig/ifconfig, arp, netstat, nbtstat, nslookup, route, traceroute/tracert, nmap, etc]

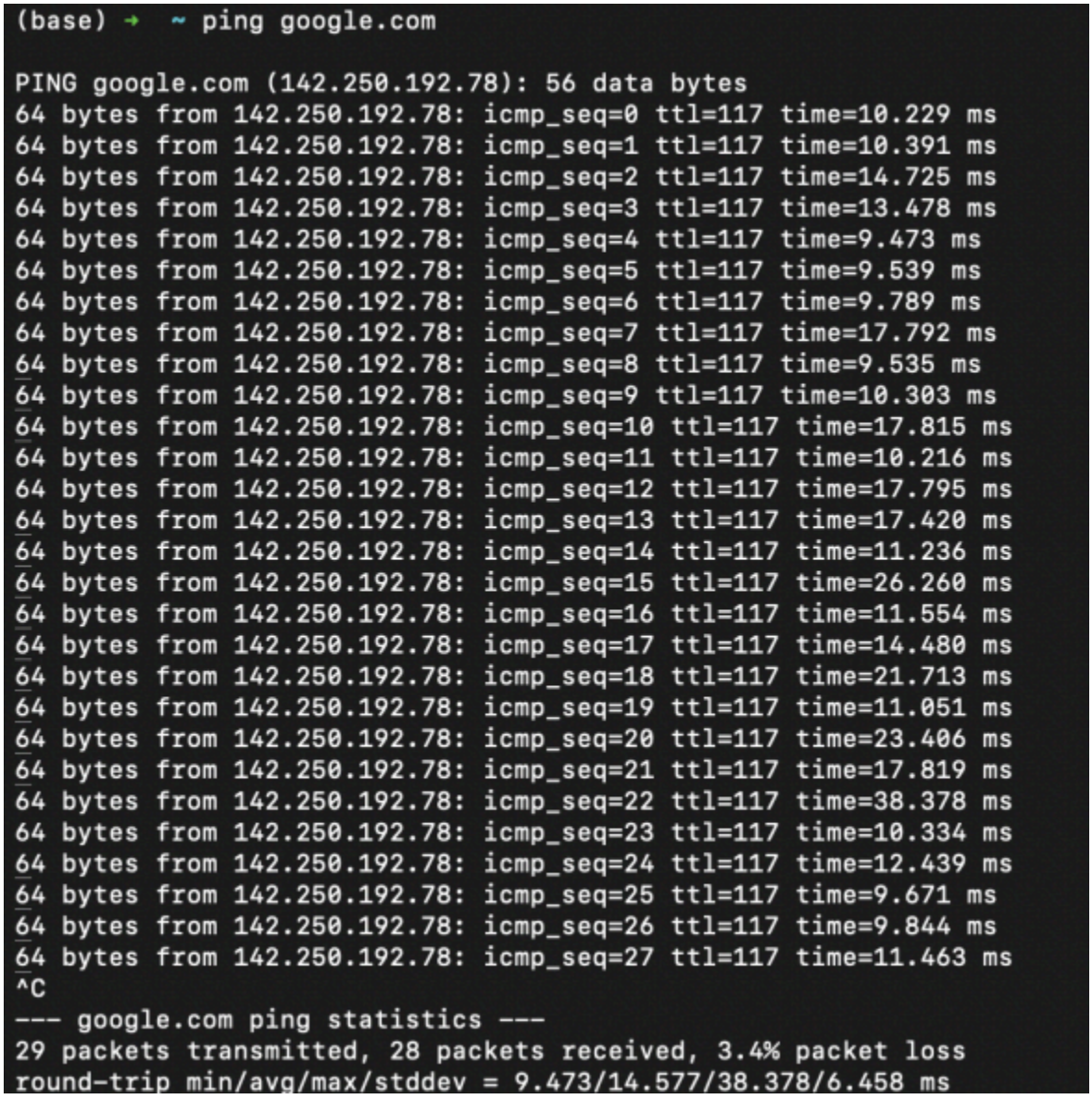
Commands used on Mac

1)ifconfig:Displays network interface configurations, including IP addresses, MAC addresses, and interface statuses, helping you understand the network setup of your machine.

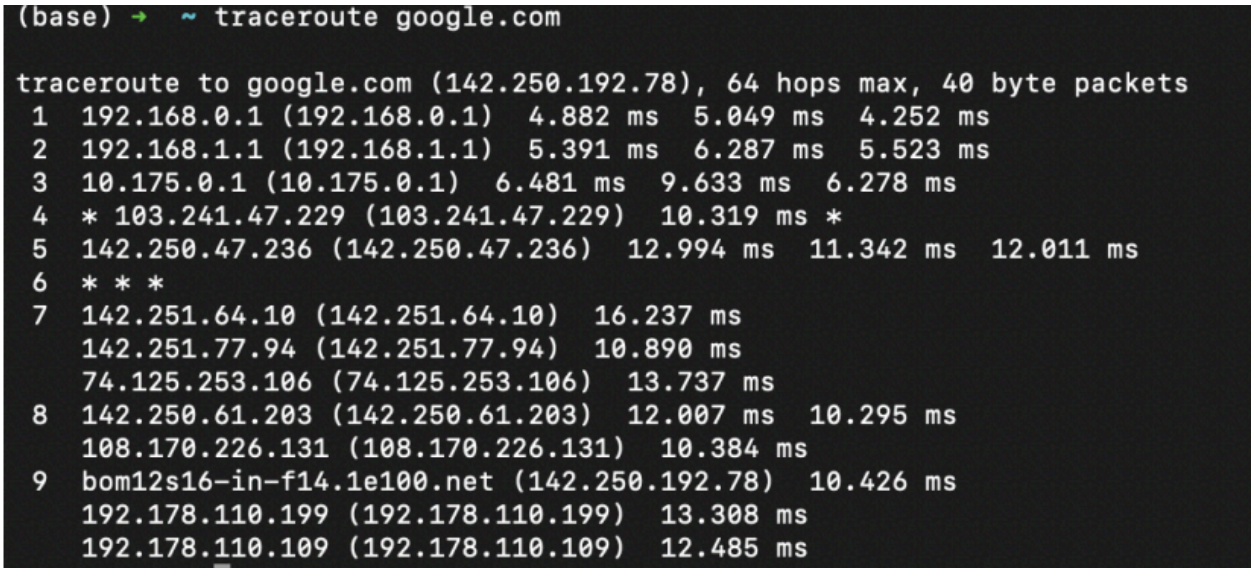
```
(base) ➜  ~ ifconfig

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
anpi1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 4e:f4:56:ea:94:6c
        media: none
        status: inactive
anpi0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 4e:f4:56:ea:94:6b
        media: none
        status: inactive
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 4e:f4:56:ea:94:4b
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 4e:f4:56:ea:94:4c
        nd6 options=201<PERFORMNUD,DAD>
        media: none
        status: inactive
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:97:0d:7d:c9:80
        media: autoselect <full-duplex>
        status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=460<TSO4,TSO6,CHANNEL_IO>
        ether 36:97:0d:7d:c9:84
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 36:97:0d:7d:c9:80
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x0
        member: en1 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 8 priority 0 path cost 0
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 9 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
ap1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 82:4a:0d:4a:e9:36
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (none)
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 8a:8f:43:53:03:3b
        inet6 fe80::1c5f:1e8d:456b:7080%en0 prefixlen 64 secured scopeid 0xb
        inet 192.168.0.2 netmask 0xffffff00 broadcast 192.168.0.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
awdl0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
```

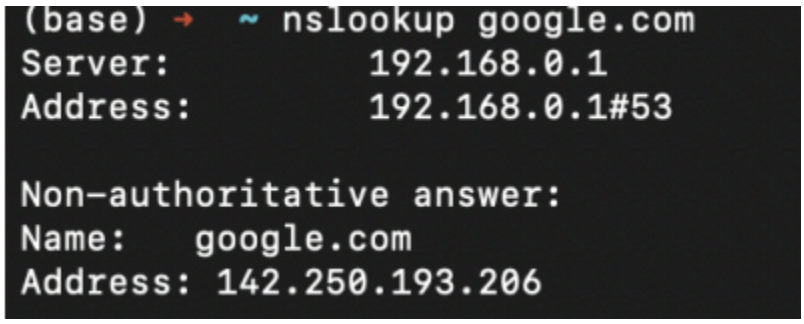
2) Ping:Tests connectivity to a specified host or IP address by sending ICMP echo requests. It measures round-trip time and packet loss, helping diagnose network issues.



3)Traceroute:Traces the path packets take to a destination, showing each hop along the way. It helps identify where delays or failures occur in the network path.



4)nslookup: Queries the Domain Name System (DNS) to obtain domain name or IP address mapping, allowing you to troubleshoot DNS-related issues.



5)netstat: Provides information about active connections, listening ports, and routing tables. It’s useful for monitoring network activity and diagnosing network problems.

```
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  192.168.0.2.51960      162.247.243.29.https   ESTABLISHED
tcp4       0      0  192.168.0.2.51959      162.247.243.29.https   ESTABLISHED
tcp4       0      0  192.168.0.2.51957      162.247.241.14.https   ESTABLISHED
tcp4       0      0  192.168.0.2.51949      101.126.69.5.http      CLOSE_WAIT
tcp4      31      0  192.168.0.2.51946      42.56.77.10.https      CLOSE_WAIT
tcp4      31      0  192.168.0.2.51945      42.56.77.10.https      CLOSE_WAIT
tcp4      31      0  192.168.0.2.51941      server-18-66-41-.https CLOSE_WAIT
tcp4      31      0  192.168.0.2.51940      server-18-66-41-.https CLOSE_WAIT
tcp4       0      0  192.168.0.2.51939      154.85.69.48.http      CLOSE_WAIT
tcp4       0      0  192.168.0.2.51938      154.85.69.48.http      CLOSE_WAIT
tcp4       0      0  192.168.0.2.51937      ecs-124-70-69-14.http  CLOSE_WAIT
tcp4       0      0  192.168.0.2.51936      ecs-124-71-231-1.http  CLOSE_WAIT
tcp4       0      0  192.168.0.2.51935      sd-in-f188.1e100.5228  ESTABLISHED
tcp4       0      0  192.168.0.2.51934      237.240.199.104..4070  ESTABLISHED
tcp4       0      0  192.168.0.2.51931      24.224.186.35.bc.https ESTABLISHED
tcp4       0      0  192.168.0.2.51929      22.224.186.35.bc.https ESTABLISHED
tcp4       0      0  192.168.0.2.51928      40.224.186.35.bc.https ESTABLISHED
tcp4       0      0  192.168.0.2.51920      40.224.186.35.bc.https ESTABLISHED
tcp4       0      0  192.168.0.2.53607      17.248.239.64.443      TIME_WAIT
tcp4       0      0  192.168.0.2.53606      17.248.239.64.443      TIME_WAIT
tcp4       0      0  192.168.0.2.53605      17.248.239.64.443      TIME_WAIT
tcp4       0      0  192.168.0.2.53604      17.248.239.64.443      TIME_WAIT
tcp4       0      0  192.168.0.2.53603      bom12s14-in-f14..443   TIME_WAIT
tcp4       0      0  192.168.0.2.53602      del12s06-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53598      del12s05-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53597      del12s03-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53596      del11s18-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53595      del12s07-in-f10..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53594      del12s10-in-f1.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53593      del11s04-in-f1.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53592      del11s04-in-f1.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53589      del11s11-in-f5.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53588      del11s09-in-f10..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53587      del12s06-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53586      del12s08-in-f4.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53585      del11s15-in-f5.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53584      sa-in-f84.1e100..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53583      del12s03-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53582      del11s17-in-f10..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53581      del12s06-in-f10..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53580      del11s14-in-f10..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53579      bom07s37-in-f3.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53577      del12s04-in-f10..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53575      del11s15-in-f5.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53574      del11s15-in-f3.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53567      del11s12-in-f10..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53564      del11s04-in-f1.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53552      del03s16-in-f10..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53526      del12s07-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53522      del12s05-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53510      104.18.32.47.443       ESTABLISHED
tcp4       0      0  192.168.0.2.53508      104.18.32.47.443       ESTABLISHED
tcp4       0      0  192.168.0.2.53491      whatsapp-chatd-e.5222  ESTABLISHED
tcp4       0      0  192.168.0.2.53335      del11s08-in-f1.1.443   ESTABLISHED
tcp4       0      0  192.168.0.2.53328      del11s21-in-f14..443   ESTABLISHED
tcp4       0      0  192.168.0.2.53281      17.188.169.198.443     ESTABLISHED
udp4       0      0  192.168.0.2.64921      del11s22-in-f10..https
```

6)hostname: Displays or sets the name of the computer on the network, which is useful for identifying devices in a networked environment

```
(base) ➜  ~ hostname
```

7)nmap: A powerful network scanning tool that discovers hosts and services on a network. It can identify open ports, running services, and operating systems, making it useful for security assessments

```
(base) ➜  ~ nmap google.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-08-12 22:39 IST
Nmap scan report for google.com (142.250.193.206)
Host is up (0.038s latency).
rDNS record for 142.250.193.206: del11s17-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 49.98 seconds
```

8)arp: Displays and manages the Address Resolution Protocol (ARP) table, which maps IP addresses to MAC addresses on the local network. This helps troubleshoot network issues and understand local network traffic

```
(base) ➜  ~ arp -a
? (192.168.0.1) at a0:ab:1b:1e:c9:eb on en0 ifscope [ethernet]
? (192.168.0.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

9)whois: Retrieves registration information about domain names and IP addresses. It’s useful for identifying the owner and registration details of a domain.

```
(base) ➜  ~ whois google.com
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.verisign-grs.com

domain:       COM

organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)

contact:      administrative
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

contact:      technical
name:         Registry Customer Service
organisation: VeriSign Global Registry Services
address:      12061 Bluemont Way
address:      Reston VA 20190
address:      United States of America (the)
phone:        +1 703 925-6999
fax-no:       +1 703 948 3978
e-mail:       info@verisign-grs.com

nserver:      A.GTLD-SERVERS.NET 192.5.6.30 2001:503:a83e:0:0:0:2:30
nserver:      B.GTLD-SERVERS.NET 192.33.14.30 2001:503:231d:0:0:0:2:30
nserver:      C.GTLD-SERVERS.NET 192.26.92.30 2001:503:83eb:0:0:0:0:30
nserver:      D.GTLD-SERVERS.NET 192.31.80.30 2001:500:856e:0:0:0:0:30
nserver:      E.GTLD-SERVERS.NET 192.12.94.30 2001:502:1ca1:0:0:0:0:30
nserver:      F.GTLD-SERVERS.NET 192.35.51.30 2001:503:d414:0:0:0:0:30
nserver:      G.GTLD-SERVERS.NET 192.42.93.30 2001:503:eea3:0:0:0:0:30
nserver:      H.GTLD-SERVERS.NET 192.54.112.30 2001:502:8cc:0:0:0:0:30
nserver:      I.GTLD-SERVERS.NET 192.43.172.30 2001:503:39c1:0:0:0:0:30
nserver:      J.GTLD-SERVERS.NET 192.48.79.30 2001:502:7094:0:0:0:0:30
nserver:      K.GTLD-SERVERS.NET 192.52.178.30 2001:503:d2d:0:0:0:0:30
nserver:      L.GTLD-SERVERS.NET 192.41.162.30 2001:500:d937:0:0:0:0:30
nserver:      M.GTLD-SERVERS.NET 192.55.83.30 2001:501:b1f9:0:0:0:0:30
ds-rdata:     19718 13 2 8acbb0cd28f41250a80a491389424d341522d946b0da0c0291f2d3d771d7805a
```

Conclusion

These commands are essential tools for network administration and troubleshooting. They provide valuable insights into network configurations, connectivity, and security, allowing users to effectively diagnose and resolve network-related issues. Familiarity with these commands enhances your ability to manage and monitor network environments efficiently.