

Network Security Lab (CY-331L)



Name: Rooshan Riaz
Reg No: 2022506

Lab-01:

Task-01 (Network Commands)

Listing open files using lsof

```
477296 13401015 /usr/lib/x86_64-linux-gnu/libpcr.so.3.13.3
#nautilus 8620 pc-13 mem REG 259,3 126560 13400132 /usr/lib/x86_64-linux-gnu/libdbusmenu-glib.so.4.0.12
nautilus 8620 pc-13 mem REG 259,3 686832 13401386 /usr/lib/x86_64-linux-gnu/libunity.so.9.0.2
nautilus 8620 pc-13 mem REG 259,3 835048 13401345 /usr/lib/x86_64-linux-gnu/libtracker-sparql-3.0.so.0.300.0
nautilus 8620 pc-13 mem REG 259,3 166280 13401230 /usr/lib/x86_64-linux-gnu/libselinux.so.1
nautilus 8620 pc-13 mem REG 259,3 698664 13400621 /usr/lib/x86_64-linux-gnu/libhandy-1.0.so.0
nautilus 8620 pc-13 mem REG 259,3 236880 13400418 /usr/lib/x86_64-linux-gnu/libgnome-desktop-3.19.3.0
nautilus 8620 pc-13 mem REG 259,3 100416 13400410 /usr/lib/x86_64-linux-gnu/libgnome-autoar-0.so.0.1.2
nautilus 8620 pc-13 mem REG 259,3 22736 13369889 /usr/lib/x86_64-linux-gnu/libgmodule-2.0.so.0.7200.4
nautilus 8620 pc-13 mem REG 259,3 940560 13371004 /usr/lib/x86_64-linux-gnu/libm.so.6
nautilus 8620 pc-13 mem REG 259,3 387464 13369917 /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.7200.4
nautilus 8620 pc-13 mem REG 259,3 1928592 13369817 /usr/lib/x86_64-linux-gnu/libgio-2.0.so.0.7200.4
nautilus 8620 pc-13 mem REG 259,3 190840 13372719 /usr/lib/x86_64-linux-gnu/libgdk-pixbuf-2.0.so.0.4200.8
nautilus 8620 pc-13 mem REG 259,3 1203976 13400020 /usr/lib/x86_64-linux-gnu/libcairo.so.2.11600.0
nautilus 8620 pc-13 mem REG 259,3 42920 13400016 /usr/lib/x86_64-linux-gnu/libcairo-gobject.so.2.11600.0
nautilus 8620 pc-13 mem REG 259,3 165968 13399917 /usr/lib/x86_64-linux-gnu/libatk-1.0.so.0.23609.1
nautilus 8620 pc-13 mem REG 259,3 417528 13400988 /usr/lib/x86_64-linux-gnu/libpango-1.0.so.0.5000.6
nautilus 8620 pc-13 mem REG 259,3 8533424 13372829 /usr/lib/x86_64-linux-gnu/libgtk-3.0.so.0.2404.29
nautilus 8620 pc-13 mem REG 259,3 1776 4723353 /var/cache/fontconfig/235ac6f0-c974-4361-ab35-0aba221b980d-le64.cache-7
nautilus 8620 pc-13 mem REG 259,3 1068344 13372827 /usr/lib/x86_64-linux-gnu/libgdk-3.0.so.0.2404.29
nautilus 8620 pc-13 mem REG 259,3 1277712 13369828 /usr/lib/x86_64-linux-gnu/libglib-2.0.so.0.7200.4
nautilus 8620 pc-13 mem REG 259,3 43080 13400863 /usr/lib/x86_64-linux-gnu/libnautilus-extension.so.1.5.0
nautilus 8620 pc-13 mem REG 259,3 12331 27569925 /home/pc-13/.config/dconf/user
nautilus 8620 pc-13 mem REG 0,56 2 239 /run/user/1000/dconf/user
nautilus 8620 pc-13 mem-r REG 259,3 32768 27569917 /home/pc-13/.local/share/nautilus/tags/meta.db-shm
nautilus 8620 pc-13 mem REG 259,3 27002 13372494 /usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
nautilus 8620 pc-13 mem REG 259,3 240936 13370998 /usr/lib/x86_64-linux-gnu/ld-linux-x86-64.so.2
nautilus 8620 pc-13 mem REG 259,3 3328 13919174 /usr/share/locale-langpack/en/LC_MESSAGES/gtk30.mo
nautilus 8620 pc-13 0r CHR 1,3 0t0 5 /dev/null
nautilus 8620 pc-13 1u unix 0x0000000000000000 0t0 35641 type=STREAM
nautilus 8620 pc-13 2u unix 0x0000000000000000 0t0 35641 type=STREAM
nautilus 8620 pc-13 3u a_inode 0,16 0 65 [eventfd]
nautilus 8620 pc-13 4u a_inode 0,16 0 65 [eventfd]
nautilus 8620 pc-13 5u unix 0x0000000000000000 0t0 53774 type=STREAM
nautilus 8620 pc-13 6u a_inode 0,16 0 65 [eventfd]
nautilus 8620 pc-13 7u unix 0x0000000000000000 0t0 53776 type=STREAM
nautilus 8620 pc-13 8ur REG 259,3 303104 27525216 /home/pc-13/.local/share/nautilus/tags/meta.db
nautilus 8620 pc-13 9u REG 259,3 0 27569645 /home/pc-13/.local/share/nautilus/tags/meta.db-wal
nautilus 8620 pc-13 10ur REG 259,3 32768 27569917 /home/pc-13/.local/share/nautilus/tags/meta.db-shm
nautilus 8620 pc-13 11rr REG 259,3 303104 27525216 /home/pc-13/.local/share/nautilus/tags/meta.db
nautilus 8620 pc-13 12u unix 0x0000000000000000 0t0 53835 type=DGRAM
nautilus 8620 pc-13 13u unix 0x0000000000000000 0t0 53778 type=STREAM
```

Running command to check which services are listening to machine

```
pc-13@pop-os:~$ lsof -i -P -n | grep LISTEN
```

Using Netstat to listen to open ports

```
pc-13@pop-os:~$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 10.1.135.96:35594       151.101.193.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:54750       151.101.141.91:443      ESTABLISHED
tcp        15      0 10.1.135.96:60600       10.1.142.76:21          CLOSE_WAIT
tcp        0      0 10.1.135.96:49576       108.139.60.50:443       TIME_WAIT
tcp        0      0 10.1.135.96:60506       172.217.19.227:443      TIME_WAIT
tcp        0      0 10.1.135.96:54740       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:43794       108.139.79.18:443       TIME_WAIT
tcp        0      0 10.1.135.96:54788       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:35682       3.160.77.111:443        TIME_WAIT
tcp        0      0 10.1.135.96:48440       10.1.142.76:57399       ESTABLISHED
tcp        0      0 10.1.135.96:33006       3.160.77.100:443        TIME_WAIT
tcp        0      0 10.1.135.96:35588       151.101.193.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:40598       34.120.208.123:443      TIME_WAIT
tcp        32      0 10.1.135.96:43618       151.101.142.49:443      CLOSE_WAIT
tcp        0      0 10.1.135.96:54712       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:54726       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:54834       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:54794       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:36364       172.217.17.67:443       TIME_WAIT
tcp        0      0 10.1.135.96:54984       10.1.142.76:21          ESTABLISHED
tcp        0      0 10.1.135.96:35698       3.160.77.111:443        TIME_WAIT
tcp        0      0 10.1.135.96:54746       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:54808       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:58604       108.139.60.123:443      TIME_WAIT
tcp        0      0 10.1.135.96:54734       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:54778       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:35184       151.101.65.91:443       ESTABLISHED
tcp        0      0 10.1.135.96:37246       151.101.129.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:35170       151.101.65.91:443       ESTABLISHED
tcp        0      0 10.1.135.96:33494       151.101.1.91:443        ESTABLISHED
tcp        15      0 10.1.135.96:60610       10.1.142.76:21          CLOSE_WAIT
tcp        0      0 10.1.135.96:54822       151.101.141.91:443      ESTABLISHED
tcp        0      0 10.1.135.96:36732       108.139.60.69:443       TIME_WAIT
tcp        0      0 10.1.135.96:36372       172.217.17.67:443       TIME_WAIT
tcp        0      0 10.1.135.96:41100       34.107.243.93:443       ESTABLISHED
tcp        0      0 10.1.135.96:37258       151.101.129.91:443      ESTABLISHED
tcp        0    1106 10.1.135.96:35810       162.247.243.29:443      ESTABLISHED
tcp        0      0 10.1.135.96:51434       162.247.241.14:443      ESTABLISHED
```

Using ping to check network connectivity

```
root@pop-os:/home/pc-13# ping 151.101.129.91
PING 151.101.129.91 (151.101.129.91) 56(84) bytes of data.
64 bytes from 151.101.129.91: icmp_seq=4 ttl=55 time=225 ms
64 bytes from 151.101.129.91: icmp_seq=5 ttl=55 time=157 ms
64 bytes from 151.101.129.91: icmp_seq=6 ttl=55 time=61.0 ms
64 bytes from 151.101.129.91: icmp_seq=7 ttl=55 time=1324 ms
64 bytes from 151.101.129.91: icmp_seq=8 ttl=55 time=306 ms
64 bytes from 151.101.129.91: icmp_seq=9 ttl=55 time=157 ms
64 bytes from 151.101.129.91: icmp_seq=10 ttl=55 time=451 ms
64 bytes from 151.101.129.91: icmp_seq=11 ttl=55 time=573 ms
64 bytes from 151.101.129.91: icmp_seq=13 ttl=55 time=354 ms
64 bytes from 151.101.129.91: icmp_seq=14 ttl=55 time=372 ms
64 bytes from 151.101.129.91: icmp_seq=15 ttl=55 time=212 ms
64 bytes from 151.101.129.91: icmp_seq=16 ttl=55 time=1146 ms
64 bytes from 151.101.129.91: icmp_seq=17 ttl=55 time=365 ms
64 bytes from 151.101.129.91: icmp_seq=18 ttl=55 time=371 ms
64 bytes from 151.101.129.91: icmp_seq=19 ttl=55 time=146 ms
64 bytes from 151.101.129.91: icmp_seq=20 ttl=55 time=361 ms
64 bytes from 151.101.129.91: icmp_seq=21 ttl=55 time=1206 ms
64 bytes from 151.101.129.91: icmp_seq=22 ttl=55 time=763 ms
64 bytes from 151.101.129.91: icmp_seq=23 ttl=55 time=561 ms
64 bytes from 151.101.129.91: icmp_seq=24 ttl=55 time=205 ms
^C
--- 151.101.129.91 ping statistics ---
25 packets transmitted, 20 received, 20% packet loss, time 24260ms
rtt min/avg/max/mdev = 60.952/465.789/1323.782/359.152 ms, pipe 2
root@pop-os:/home/pc-13# hostname -I
10.1.135.96 172.17.0.1
```