Admin2 Lab

1- Identify the current USB devices

```
radwa@radwa-VirtualBox:~$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 005: ID 80ee:0021 VirtualBox USB Tablet
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
radwa@radwa-VirtualBox:~$
```

2-Count how many CPUs on your device

```
radwa@radwa-VirtualBox:~$ nproc
2
radwa@radwa-VirtualBox:~$
```

3-Take a snapshot of current disk statistics 5 times with 2 seconds interval.

```
radwa@radwa-VirtualBox:~$ iostat -d 2 5
Linux 5.15.0-60-generic (radwa-VirtualBox)      04/01/2023      _x86_64_       (
2 CPU)

Device             tps    kB_read/s    kB_wrtn/s    kB_dscd/s    kB_read    kB_w
rtn    kB_dscd
dm-0              0.07         0.42         0.75         3.90      27817      49
372     258052
loop0             0.00         0.00         0.00         0.00         17
  0          0
loop1             0.00         0.02         0.00         0.00       1374
  0          0
loop10            0.00         0.02         0.00         0.00       1372
  0          0
loop11            0.01         0.03         0.00         0.00       2019
 48          0
loop12            0.02         0.59         0.00         0.00      38841
  0          0
loop13            0.00         0.01         0.00         0.00        339
  0          0
loop14            0.00         0.07         0.00         0.00       4366
```

4-measure the network activities

```
radwa@radwa-VirtualBox:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::6d29:1cb2:8049:801d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:fe:8d:d4  txqueuelen 1000  (Ethernet)
        RX packets 404144  bytes 587279984 (587.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34789  bytes 2223800 (2.2 MB)
        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 374  bytes 33541 (33.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 374  bytes 33541 (33.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

radwa@radwa-VirtualBox:~$ nicstat -z -t -n -i enp0s3
04:46:25    InKB   OutKB   InSeg  OutSeg Reset  AttF %ReTX InConn OutCon Drops
TCP         0.00    0.00    0.76    0.52  0.00  0.00 0.000   0.00   0.00  0.00
```

5-List current PCI devices on your device

```
radwa@radwa-VirtualBox:~$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:02.0 VGA compatible controller: VMware SVGA II Adapter
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controll
er (rev 02)
00:04.0 System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Service
00:05.0 Multimedia audio controller: Intel Corporation 82801AA AC'97 Audio Contr
oller (rev 01)
00:06.0 USB controller: Apple Inc. KeyLargo/Intrepid USB
00:07.0 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 08)
00:0b.0 USB controller: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) US
B2 EHCI Controller
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Cont
roller [AHCI mode] (rev 02)
```

6-List all files compressed by zip utilities

```
radwa@radwa-VirtualBox:~$ sudo find / -type f -exec file {} \; | grep "Zip archi
ve data"
/snap/firefox/1635/usr/lib/firefox/browser/features/doh-rollout@mozilla.org.xpi:
 Zip archive data, at least v1.0 to extract, compression method=store
/snap/firefox/1635/usr/lib/firefox/browser/features/formautofill@mozilla.org.xpi
: Zip archive data, made by v2.0 UNIX, extract using at least v1.0, last modifie
d Wed Dec 19 21:00:48 2001, uncompressed size 7323, method=store
/snap/firefox/1635/usr/lib/firefox/browser/features/pictureinpicture@mozilla.org
.xpi: Zip archive data, made by v2.0 UNIX, extract using at least v1.0, last mod
ified Wed Dec 19 21:00:48 2001, uncompressed size 2453, method=store
/snap/firefox/1635/usr/lib/firefox/browser/features/screenshots@mozilla.org.xpi:
 Zip archive data, at least v1.0 to extract, compression method=store
/snap/firefox/1635/usr/lib/firefox/browser/features/webcompat-reporter@mozilla.o
rg.xpi: Zip archive data, at least v1.0 to extract, compression method=store
/snap/firefox/1635/usr/lib/firefox/browser/features/webcompat@mozilla.org.xpi: Z
ip archive data, made by v2.0 UNIX, extract using at least v1.0, last modified W
ed Dec 19 21:00:48 2001, uncompressed size 1248, method=store
/snap/firefox/1635/usr/lib/firefox/browser/omni.ja: Zip archive data, made by v2
.0 UNIX, extract using at least v1.0, last modified Wed Dec 19 21:00:48 2001, un
compressed size 69385, method=store
/snap/firefox/1635/usr/lib/firefox/distribution/extensions/locale-ach/langpack-a
ch@firefox.mozilla.org.xpi: Zip archive data, at least v2.0 to extract, compress
ion method=deflate
/snap/firefox/1635/usr/lib/firefox/distribution/extensions/locale-af/langpack-af
```

7-Using grep and regex list all lines containing hex numbers on a /var/log/syslog

```
radwa@radwa-VirtualBox:~$ grep -e "0x" /var/log/syslog
Feb 22 03:09:27 radwa-VirtualBox NetworkManager[638]: <info>  [1677053367.0540]
dns-mgr[0x55bc1857c2a0]: init: dns=systemd-resolved rc-manager=unmanaged (auto),
 plugin=systemd-resolved
Feb 22 03:09:27 radwa-VirtualBox NetworkManager[638]: <info>  [1677053367.0560]
manager[0x55bc1859d040]: rfkill: Wi-Fi hardware radio set enabled
Feb 22 03:09:27 radwa-VirtualBox NetworkManager[638]: <info>  [1677053367.0560]
manager[0x55bc1859d040]: rfkill: WWAN hardware radio set enabled
Feb 22 03:09:58 radwa-VirtualBox kernel: [   34.617818] audit: type=1326 audit(1
677053398.273:49): auid=1000 uid=1000 gid=1000 ses=3 subj=snap.snapd-desktop-int
egration.snapd-desktop-integration pid=1975 comm="snapd-desktop-i" exe="/snap/sn
apd-desktop-integration/49/usr/bin/snapd-desktop-integration" sig=0 arch=c000003
e syscall=314 compat=0 ip=0x7f39a74f073d code=0x50000
Feb 23 10:24:00 radwa-VirtualBox kernel: [    0.000000] x86/fpu: Supporting XSAV
E feature 0x001: 'x87 floating point registers'
Feb 23 10:24:00 radwa-VirtualBox kernel: [    0.000000] x86/fpu: Supporting XSAV
E feature 0x002: 'SSE registers'
Feb 23 10:24:00 radwa-VirtualBox kernel: [    0.000000] x86/fpu: Supporting XSAV
E feature 0x004: 'AVX registers'
Feb 23 10:24:00 radwa-VirtualBox kernel: [    0.000000] x86/fpu: Enabled xstate
features 0x7, context size is 832 bytes, using 'standard' format.
Feb 23 10:24:00 radwa-VirtualBox kernel: [    0.000000] BIOS-e820: [mem 0x000000
```