

CIS-387: Digital Forensics (4 credits)

With Dr. Jinhua Guo

Lab 1

Demetrius Johnson

September 19, 2022

ACTIVITY 1: PRACTICING LINUX/UNIX COMMANDS

To display: Command:

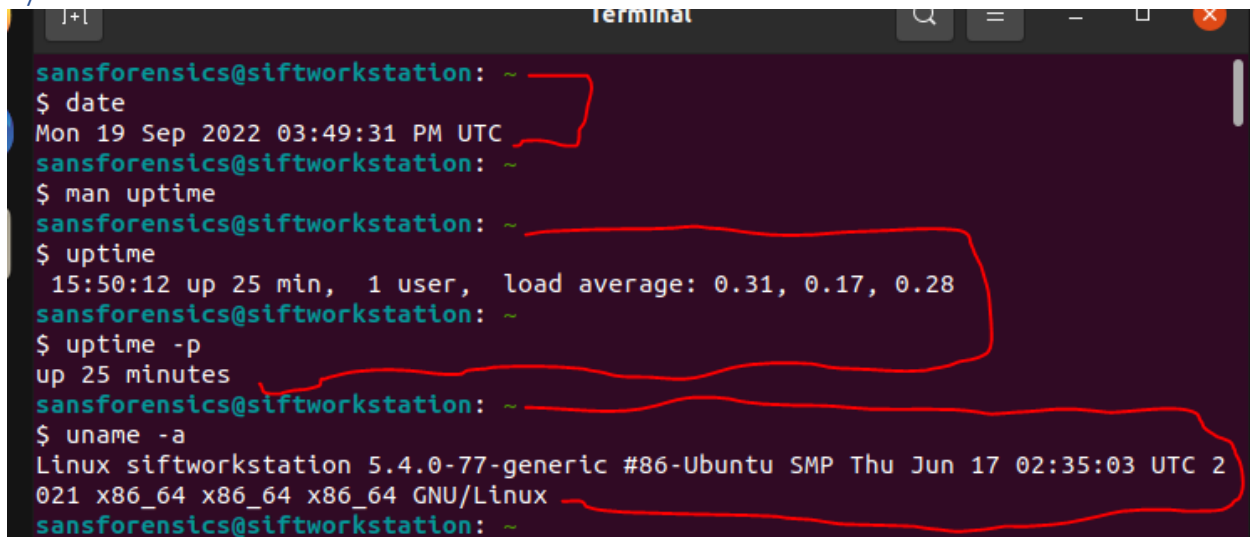
Current system date and time `date`

To display: Command:

When was the system rebooted `uptime -p`

To display: Command:

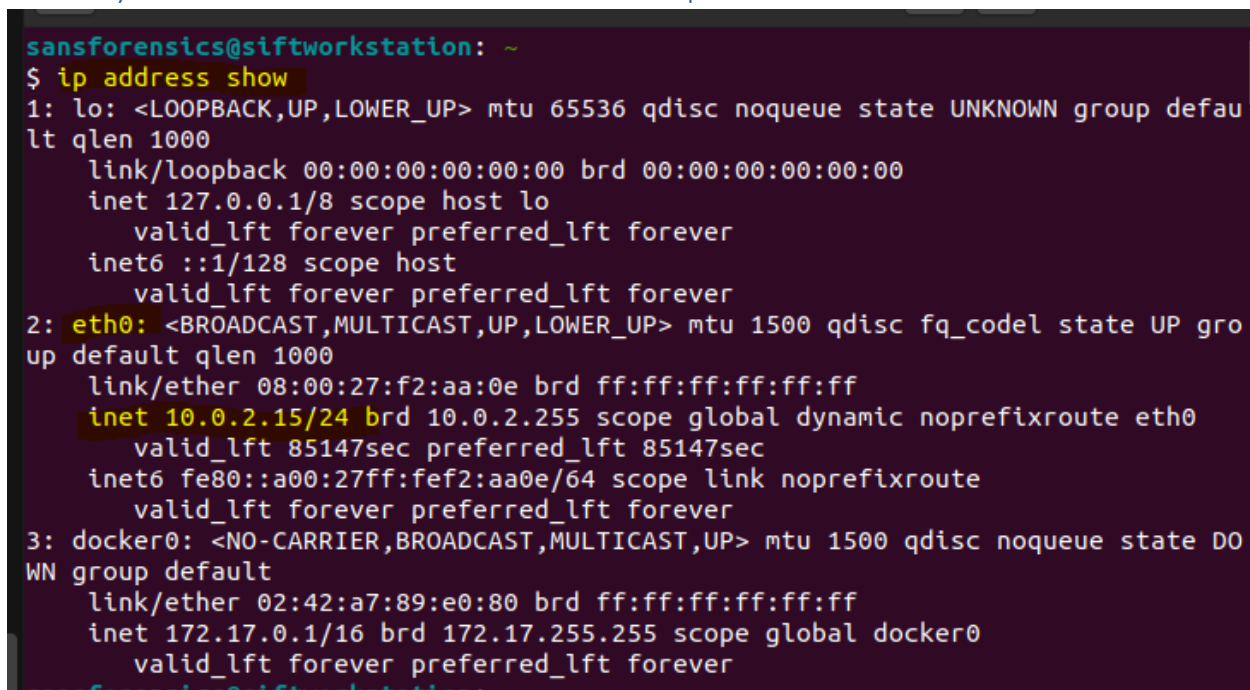
System information `uname -a`



```
sansforensics@siftworkstation: ~  
$ date  
Mon 19 Sep 2022 03:49:31 PM UTC  
sansforensics@siftworkstation: ~  
$ man uptime  
sansforensics@siftworkstation: ~  
$ uptime  
15:50:12 up 25 min, 1 user, load average: 0.31, 0.17, 0.28  
sansforensics@siftworkstation: ~  
$ uptime -p  
up 25 minutes  
sansforensics@siftworkstation: ~  
$ uname -a  
Linux siftworkstation 5.4.0-77-generic #86-Ubuntu SMP Thu Jun 17 02:35:03 UTC 2  
021 x86_64 x86_64 x86_64 GNU/Linux  
sansforensics@siftworkstation: ~
```

To display: Command:

Show layer 3 details of network interfaces `ip address show`



```
sansforensics@siftworkstation: ~  
$ ip address 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 fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:f2:aa:0e brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0  
        valid_lft 85147sec preferred_lft 85147sec  
    inet6 fe80::a00:27ff:fef2:aa0e/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default  
    link/ether 02:42:a7:89:e0:80 brd ff:ff:ff:ff:ff:ff  
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0  
        valid_lft forever preferred_lft forever  
sansforensics@siftworkstation: ~
```

To display:

Command:

Unusual and suspicious processes and services `ps -eaf`

```
sansforensics@siftworkstation: ~  
$ ps -eaf  
UID          PID     PPID  C  STIME TTY          TIME CMD  
root          1         0  0  15:24 ?        00:00:05 /sbin/init  
root          2         0  0  15:24 ?        00:00:00 [kthreadd]  
root          3         2  0  15:24 ?        00:00:00 [rcu_gp]  
root          4         2  0  15:24 ?        00:00:00 [rcu_par_gp]  
root          6         2  0  15:24 ?        00:00:00 [kworker/0:0H-kblockd]  
root          9         2  0  15:24 ?        00:00:00 [mm_percpu_wq]  
root         10         2  0  15:24 ?        00:00:00 [ksoftirqd/0]  
root         11         2  0  15:24 ?        00:00:02 [rcu_sched]  
root         12         2  0  15:24 ?        00:00:00 [migration/0]  
root         13         2  0  15:24 ?        00:00:00 [idle_inject/0]  
root         14         2  0  15:24 ?        00:00:00 [cpuhp/0]  
root         15         2  0  15:24 ?        00:00:00 [cpuhp/1]  
root         16         2  0  15:24 ?        00:00:00 [idle_inject/1]  
root         17         2  0  15:24 ?        00:00:00 [migration/1]  
root         18         2  0  15:24 ?        00:00:00 [ksoftirqd/1]  
root         20         2  0  15:24 ?        00:00:00 [kworker/1:0H-kblockd]  
root         21         2  0  15:24 ?        00:00:00 [kdevtmpfs]  
root         22         2  0  15:24 ?        00:00:00 [netns]  
root         23         2  0  15:24 ?        00:00:00 [rcu_tasks_kthre]  
root         24         2  0  15:24 ?        00:00:00 [kauditd]  
root         25         2  0  15:24 ?        00:00:00 [khungtaskd]
```

To display: Command:

Network connections lsof -i

To display: Command:

Open in memory, but unlinked files (requested for deletion) lsof +L1

```
$ man ps
sansforensics@siftworkstation: ~
$ lsof -i
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
kdeconnec 2018 sansforensics 20u IPV6 36467 0t0 UDP *:1716
kdeconnec 2018 sansforensics 21u IPV6 36468 0t0 TCP *:1716 (LISTEN)
sansforensics@siftworkstation: ~
$ lsof +L1
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NLINK NODE NAME
pulseaudi 1555 sansforensics 6u REG 0,1 67108864 0 30528 /memfd:p
ulseaudio (deleted)
Xorg 1638 sansforensics 37u REG 0,1 4 0 34010 /memfd:x
shmfd (deleted)
Xorg 1638 sansforensics 49u REG 0,1 4 0 35358 /memfd:x
shmfd (deleted)
Xorg 1638 sansforensics 53u REG 0,1 4 0 36497 /memfd:x
shmfd (deleted)
Xorg 1638 sansforensics 58u REG 0,1 4 0 38277 /memfd:x
shmfd (deleted)
gnome-she 1809 sansforensics 23r REG 8,2 64 0 3145768 /home/sa
nsforensics/.local/share/gvfs-metadata/root (deleted)
gnome-she 1809 sansforensics 35r REG 8,2 32768 0 3145876 /home/sa
nsforensics/.local/share/gvfs-metadata/root-3923f3aa.log (deleted)
sansforensics@siftworkstation: ~
```

To display: Command: (ran with sudo (super user) for full output)

Files opened by the process PID lsof -p (PID)

```
systemd denied)
sansforensics@siftworkstation: ~
$ sudo lsof -p 1
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
Output information may be incomplete.
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
systemd 1 root cwd DIR 8,2 4096 2 /
systemd 1 root rtd DIR 8,2 4096 2 /
systemd 1 root txt REG 8,2 1620224 19926208 /usr/lib
/systemd/systemd
systemd 1 root mem REG 8,2 1369352 19928388 /usr/lib
/x86_64-linux-gnu/libm-2.31.so
systemd 1 root mem REG 8,2 178528 19928341 /usr/lib
/x86_64-linux-gnu/libudev.so.1.6.17
systemd 1 root mem REG 8,2 1575112 19926306 /usr/lib
/x86_64-linux-gnu/libunistring.so.2.1.0
systemd 1 root mem REG 8,2 137584 19923679 /usr/lib
/x86_64-linux-gnu/libgpg-error.so.0.28.0
systemd 1 root mem REG 8,2 67912 19924349 /usr/lib
/x86_64-linux-gnu/libjson-c.so.4.0.0
systemd 1 root mem REG 8,2 34872 19926196 /usr/lib
/x86_64-linux-gnu/libargon2.so.1
systemd 1 root mem REG 8,2 431472 19926211 /usr/lib
```

To display:

Command:

Currently logged in users (three options)

w (or who, or users)

To display:

Command: (ran with sudo (super user) for full output)

All root-owned (uid=0) SUID files `find / -uid 0 -perm -4000 -print`

```
temd/journal/stdout type=STREAM
sansforensics@siftworkstation: ~
$ w
17:31:40 up 2:07, 1 user, load average: 0.28, 0.15, 0.10
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
sansfore :0        :0                Wed17    ?xdm?   5:11   0.04s /usr/lib/gdm3/
sansforensics@siftworkstation: ~
$ sudo find / -uid 0 -perm -4000 -print
/opt/VMBoxGuestAdditions-6.1.32/bin/VMBoxDRMClient
/usr/bin/su
/usr/bin/umount
/usr/bin/fusermount
/usr/bin/vmware-user-suid-wrapper
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/chsh
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/gpasswd
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
```

To display:

Command:

Logged general system activities `tail -f /var/log/syslog`

```
sansforensics@siftworkstation: ~
$ tail -f /var/log/syslog
Sep 19 17:31:34 localhost freshclam[669]: Mon Sep 19 17:31:34 2022 -> ^Your ClamAV installation is OUTDATED!
Sep 19 17:31:34 localhost freshclam[669]: Mon Sep 19 17:31:34 2022 -> ^Local version: 0.103.2 Recommended version: 0.103.7
Sep 19 17:31:34 localhost freshclam[669]: Mon Sep 19 17:31:34 2022 -> DON'T PANIC! Read https://www.clamav.net/documents/upgrading-clamav
Sep 19 17:31:34 localhost freshclam[669]: Mon Sep 19 17:31:34 2022 -> daily.cld database is up-to-date (version: 26663, sigs: 2003374, f-level: 90, builder: raynman)
Sep 19 17:31:34 localhost freshclam[669]: Mon Sep 19 17:31:34 2022 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Sep 19 17:31:34 localhost freshclam[669]: Mon Sep 19 17:31:34 2022 -> bytecode.cvd database is up-to-date (version: 333, sigs: 92, f-level: 63, builder: awillia2)
Sep 19 17:34:28 localhost systemd[1]: Started Run anacron jobs.
Sep 19 17:34:28 localhost anacron[3259]: Anacron 2.3 started on 2022-09-19
Sep 19 17:34:28 localhost anacron[3259]: Normal exit (0 jobs run)
Sep 19 17:34:28 localhost systemd[1]: anacron.service: Succeeded.
```

To display:

Command:

A list of all users with last logged in (and logged out) times stored in the log file /var/log/wtmp

last

```
sansforensics@siftworkstation: ~  
$ last  
sansfore :0                :0                Wed Sep 14 17:01      gone - no logout  
reboot   system boot      5.4.0-77-generic Wed Sep 14 16:59      still running  
sansfore :0                :0                Wed Sep 14 16:54 -   down (00:03)  
reboot   system boot      5.4.0-77-generic Wed Sep 14 12:52 -   16:58 (04:05)  
sansfore :0                :0                Wed Sep 14 16:42 -   down (00:04)  
reboot   system boot      5.4.0-77-generic Wed Sep 14 16:36 -   16:47 (00:11)  
sansfore :0                :0                Wed Sep 14 16:26 -   down (00:09)  
reboot   system boot      5.4.0-77-generic Wed Sep 14 12:24 -   16:35 (04:11)  
sansfore :0                :0                Wed Sep 14 16:22 -   down (00:00)  
reboot   system boot      5.4.0-77-generic Wed Sep 14 12:20 -   16:23 (04:03)  
reboot   system boot      5.4.0-77-generic Wed Sep 14 12:14 -   16:18 (04:03)  
sansfore :0                :0                Mon Sep 12 17:01 -   down (00:07)  
reboot   system boot      5.4.0-77-generic Mon Sep 12 12:53 -   17:09 (04:15)  
reboot   system boot      5.4.0-77-generic Mon Sep 12 12:19 -   17:09 (04:49)  
reboot   system boot      5.4.0-77-generic Mon Sep 12 12:10 -   17:09 (04:58)  
reboot   system boot      5.4.0-77-generic Mon Sep 12 11:58 -   17:09 (05:10)  
  
wtmp begins Mon Sep 12 11:58:30 2022  
sansforensics@siftworkstation:
```

To display:

Command:

Any regular files in /directory_path that has been modified within 1 day (24 hours)

find /directory_path -type f -mtime -1 -print

```
sansforensics@siftworkstation: ~  
$ find /home -type f -mtime -1 -print  
/home/sansforensics/.local/share/gvfs-metadata/root-35a08c11.log  
/home/sansforensics/.local/share/gvfs-metadata/root  
/home/sansforensics/.local/share/gnome-shell/application_state  
/home/sansforensics/.config/dconf/user  
/home/sansforensics/.cache/event-sound-cache.tdb.8a90d662a55e473a8f63730aa70af8  
ac.x86_64-pc-linux-gnu  
/home/sansforensics/.cache/update-manager-core/meta-release-lts  
sansforensics@siftworkstation: ~
```

To display:

Command:

Show free disk space

df

To display:

Command:

Show amount of free and used physical and swap memory in system

free

```
sansforensics@siftworkstation: ~  
$ df  
Filesystem      1K-blocks    Used Available Use% Mounted on  
udev            1968724        0    1968724  0% /dev  
tmpfs           403064       2824    400240  1% /run  
/dev/sda2       500946168  8852312  466577520  2% /  
tmpfs           2015308        0    2015308  0% /dev/shm  
tmpfs           5120          4       5116  1% /run/lock  
tmpfs           2015308        0    2015308  0% /sys/fs/cgroup  
share           1939681600  341013816  1598667784  18% /home/sansforensics/host  
tmpfs           403060        28     403032  1% /run/user/1000  
/dev/sr0        59770       59770        0 100% /media/sansforensics/VBox_G  
As_6.1.32  
sansforensics@siftworkstation: ~  
$ free  
              total        used        free      shared  buff/cache   available  
Mem:        4030620       673032    1598068        4220     1759520     3069584  
Swap:       1998844          0     1998844  
sansforensics@siftworkstation: ~  
$
```

ACTIVITY 2: LINUX MEMORY ACQUISITION

- 1) Insert the kernel module and get a memory dump:
- 2) Search the memory dump file for the strings starting with "forensics" (potential password in the memory).

```
strip -x strip -x lime.ko
mv lime.ko lime-5.4.0-77-generic.ko
sansforensics@siftworkstation: ~/Downloads/LiME-master/LiME-master/src
$ ls
deflate.c  hash.o          lime.mod.o  Makefile.sample
deflate.o  lime-5.4.0-77-generic.ko  lime.o      modules.order
disk.c     lime.h          main.c      Module.symvers
disk.o     lime.mod        main.o      tcp.c
hash.c     lime.mod.c      Makefile    tcp.o
sansforensics@siftworkstation: ~/Downloads/LiME-master/LiME-master/src
$ sudo insmod lime-5.4.0-77-generic.ko "path=./mem_dump.bin format=padded"
sansforensics@siftworkstation: ~/Downloads/LiME-master/LiME-master/src
$ strings -n 8 mem_dump.bin | grep ^forensics
forensics
forensics/host vboxsf rw,uid=0,gid=997,dmode=0770,fmode=0770,dmask=0000,fmask=0
0
sansforensics@siftworkstation: ~/Downloads/LiME-master/LiME-master/src
```

Summary/Reflection

In this Lab, I was refreshed about many of the Linux/Unix commands that I used to be very familiar with from CIS-450 Operating Systems course with Dr. Jinhua Guo. I ran into some issues with Virtual Box virtual Ubuntu machine; However, after making some small changes to display card and display memory, it worked. I also installed the extension pack for Virtual Box so that I can have the USB module, which will be used in lab 2. As for the memory dump command, I can see how it is useful, for example, if you know that the password is in memory somewhere you can work with all strings in memory and brute force a password (which is very fast, since the size of memory is way less than all possible combinations for an x-length password where each value can be 26 or more elements). Also, if you know generally where passwords are stored, then by doing memory dump, you can try the strings in that file location.