

48436/32309

Week 08 Linux Live as User Report

Name: Huynh Lam

Student ID: 13264763

Date: 03/09/2021

Activity No.: Cmp1/03

Here we will only use user (non sudo) access commands.

This Lab is for WSL on Windows 10.

If you use another Linux device, such as Terminal on MacOS or a Linux VM, answers may vary.

Reminder: To get the Thorough mark, you need to answer as a Forensics Investigator. (Week 1 module)

Part 1: Examine the device volatile data

Preparation

Logon to your laptop. Open a Terminal shell using ubuntu. CD to your desktop.

Q1) Log your activity

Confirm your OS version.

`cat /etc/issue` Yours may be different.

Then `cat /etc/issue > evidence_start.txt`

Type `pwd` to confirm your location.

Type `whoami` to confirm your connection

`pwd >> evidence_start.txt`

`whoami >> evidence_start.txt` # record your name

`date >> evidence_start.txt` # append the date and time

Check the file by typing:

`cat evidence_start.txt`

You should see the OS version, user name and the start date and time in the text file.

Take a screenshot to upload the contents of evidence_start.txt

```
huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ cat evidence_start.txt
Ubuntu 20.04.2 LTS \n \l
/mnt/c/Users/Huynh/Desktop
huynh
Sun Sep 19 21:26:30 AEST 2021
```

Q2) Check network Details.

To identify the dns server, check `/etc/resolv.conf`

Type `cat /etc/resolv.conf` Is it a public or private address? **Private**

Take [a screen shot for upload](#).

```
huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ cat /etc/resolv.conf
# This file was automatically generated by WSL. To stop automatic generation of this file, add the following entry to /etc/wsl.conf:
# [network]
# generateResolvConf = false
nameserver 192.168.60.2
search localdomain
```

In your shell, type `ip addr` . Which interfaces are active? <UP>

- **eth0**
- **lo**

What are your active IPv4 addresses?

- **192.168.60.129**
- **127.0.0.1**

Q3) Check Processes

An attacker or virus may set up its own process or hijack an existing process.

We use `ps` to show running tasks.

Type `ps --help simple`. What do the `-a`, `-A` and the `-r` flags do?

- **-a: All with tty, except session leaders**
- **-A: All processes**
- **-r: Only running processes**

Let us run a suspicious process, say ping.

In another cmd window start another copy of ubuntu.

Ping a dns.

`ping 1.1.1.1` the ping should keep pinging.

Switch back to your original ubuntu shell.

Type `ps -Af` You should see the ping.

Take [a screen shot for upload](#).

```

huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ ps -Af
UID          PID    PPID  C STIME TTY          TIME CMD
root           1        0  0  21:21 ?           00:00:00 /init
root           6          1  0  21:21 tty1          00:00:00 /init
huynh          7          6  0  21:21 tty1          00:00:00 -bash
root        159          1  0  21:33 tty2          00:00:00 /init
huynh        160        159  0  21:33 tty2          00:00:00 -bash
huynh        173        160  0  21:33 tty2          00:00:00 ping 1.1.1.1
huynh        174          7  0  21:33 tty1          00:00:00 ps -Af

```

Q4) Check Services

We can see installed services by looking at [init.d](#), the service launcher.

`ls /etc/init.d` Take a screen shot for upload.

```

huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ ls /etc/init.d/
apparmor      cryptdisks      iscsid          multipath-tools  procps          udev
apport        cryptdisks-early keyboard-setup.sh open-iscsi        rsync           ufw
atd           dbus            kmod            open-vm-tools    rsyslog         unattended-upgrades
console-setup.sh hwclock.sh      lvm2            plymouth          screen-cleanup  uuid
cron          irqbalance      lvm2-lvmpolld  plymouth-log     ssh             x11-common

```

Which ones in the table are running on your device?

- **cron**
- **ssh**
- **x11**

Part 2: Examine the device non-volatile data

Q5) System Information – cmd line

5a) The basic system info is revealed by [uname](#)

48436/32309

Week 08 Linux Live as User Report

Type `uname -a` to see the system summary.

Type `uname -v` to see the kernel version

Type `wsl.exe --update --status`

Take a screenshot of all three for upload.

```
huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ uname -a
Linux DESKTOP-LD37I00 4.4.0-19041-Microsoft #1151-Microsoft Thu Jul 22 21:05:00 PST 2021 x86_64 x86_64 x86_64 GNU/Linux
huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ uname -v
#1151-Microsoft Thu Jul 22 21:05:00 PST 2021
```

Comment on the difference shown for the kernel version

- `-a` prints all the system information in the command `uname` whereas using `-v` argument will only print the kernel version which you can see both commands print out the kernel version in their output.

5b) What Linux knows about the hardware is kept in `/proc`

`cat /proc/cmdline` # This shows you how the boot image is loaded.

`cat /proc/cpuinfo` # This shows you the CPU details – some will be virtual if this is a VM.

`cat /proc/meminfo` # Memory management details

Repeat the `cat /proc` commands with `grep` as shown on the lecture slide to show the number of processors, cpu model, total and free Memory. Take a screenshot for upload.

```
huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ cat /proc/cmdline
BOOT_IMAGE=/kernel init=/init
```

48436/32309

Week 08 Linux Live as User Report

```

huynh@DESKTOP-LD37100:/mnt/c/Users/Huynh/Desktop$ cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 142
model name     : Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
stepping       : 12
microcode      : 0xffffffff
cpu MHz        : 1992.000
cache size     : 256 KB
physical id    : 0
siblings       : 2
core id        : 0
cpu cores      : 2
apicid         : 0
initial apicid : 0
fpu            : yes
fpu_exception  : yes
cpuid level    : 6
wp             : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss ht syscall nx pdpe1gb rdtscp lm pni pclmuldq sse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer
bogomips       : 3984.00
clflush size   : 64
cache alignment : 64
address sizes   : 36 bits physical, 48 bits virtual
power management:

processor       : 1
vendor_id      : GenuineIntel
cpu family     : 6
model          : 142
model name     : Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
stepping       : 12
microcode      : 0xffffffff
cpu MHz        : 1992.000
cache size     : 256 KB
physical id    : 0
siblings       : 2
core id        : 1
cpu cores      : 2
apicid         : 0
initial apicid : 0
fpu            : yes
fpu_exception  : yes
cpuid level    : 6
wp             : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ss ht syscall nx pdpe1gb rdtscp lm pni pclmuldq sse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer
bogomips       : 3984.00
clflush size   : 64
cache alignment : 64
address sizes   : 36 bits physical, 48 bits virtual
power management:

```

```

huynh@DESKTOP-LD37100:/mnt/c/Users/Huynh/Desktop$ cat /proc/meminfo
MemTotal:        4095448 kB
MemFree:         2043408 kB
Buffers:         34032 kB
Cached:         188576 kB
SwapCached:      0 kB
Active:         167556 kB
Inactive:       157876 kB
Active(anon):    103104 kB
Inactive(anon):  17440 kB
Active(file):    64452 kB
Inactive(file):  140436 kB
Unevictable:     0 kB
Mlocked:         0 kB
SwapTotal:       7864060 kB
SwapFree:        7731508 kB
Dirty:           0 kB
Writeback:       0 kB
AnonPages:       102824 kB
Mapped:          71404 kB
Shmem:           17720 kB
Slab:            13868 kB
SReclaimable:    6744 kB
SUnreclaim:     7124 kB
KernelStack:    2848 kB
PageTables:      2524 kB
NFS_Unstable:    0 kB
Bounce:          0 kB
WritebackTmp:    0 kB
CommitLimit:    515524 kB
Committed_AS:   3450064 kB
VmallocTotal:   122880 kB
VmallocUsed:     21296 kB
VmallocChunk:   66044 kB
HardwareCorrupted: 0 kB
AnonHugePages:  2048 kB
HugePages_Total: 0
HugePages_Free:  0
HugePages_Rsvd:  0
HugePages_Surp:  0
Hugepagesize:   2048 kB
DirectMap4k:    12280 kB
DirectMap4M:    897024 kB

```

5c) We can see the Linux file structure with df

48436/32309

Week 08 Linux Live as User Report

`whatis df ?` [Show information about the file system on which each FILE resides, or all file systems by default.](#)

Type `df -ahT` [Take a screen shot for upload](#)

```
huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ df -ahT
Filesystem      Type      Size  Used Avail Use% Mounted on
rootfs          wslfs     60G   31G   30G   51% /
none           tmpfs     60G   31G   30G   51% /dev
sysfs           sysfs      0      0      0    - /sys
proc            proc       0      0      0    - /proc
devpts          devpts     0      0      0    - /dev/pts
none           tmpfs     60G   31G   30G   51% /run
none           tmpfs     60G   31G   30G   51% /run/lock
none           tmpfs     60G   31G   30G   51% /run/shm
none           tmpfs     60G   31G   30G   51% /run/user
binfmt_misc     binfmt_misc 0      0      0    - /proc/sys/fs/binfmt_misc
tmpfs           tmpfs     60G   31G   30G   51% /sys/fs/cgroup
cgroup          cgroup     0      0      0    - /sys/fs/cgroup/devices
C:\             drvfs     60G   31G   30G   51% /mnt/c
```

What is the Linux root mount symbol ? [/](#)

What is this filesystem type? [wslfs](#)

5d) User Accounts

We can see the user accounts in [/etc/passwd](#).

`cat /etc/passwd | grep bash`

[Take a screenshot](#) of the users for your report.

```
huynh@DESKTOP-LD37I00:/mnt/c/Users/Huynh/Desktop$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
huynh:x:1000:1000:::/home/huynh:/bin/bash
```

Comment on the results.

There are only 2 users in the system. The root account and my personal account Huynh

Close all windows and shells when done.

Bring an empty USB for the week 9 Lab.