**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

Text

Description automatically generated

To display: Command:

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

Text

Description automatically generated

To display: Command:

## Unusual and suspicious processes and services ps -eaf

A screenshot of a computer

Description automatically generated with medium confidence

To display: Command:

## Network connections lsof -i

To display: Command:

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

Text

Description automatically generated

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

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

Graphical user interface, text

Description automatically generated

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

Text

Description automatically generated

To display: Command:

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

Text

Description automatically generated

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

Text

Description automatically generated with low confidence

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

Text

Description automatically generated

To display: Command:

## Show free disk space df

To display: Command:

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

Graphical user interface, text

Description automatically generated

# ACTIVITY 2: LINUX MEMORY ACQUISITION

## 1) Insert the kernel module ang get a memory dump:

## 2) Search the memory dump file for the strings starting with “forensics” (potential password in the memory).

Text

Description automatically generated

# 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.