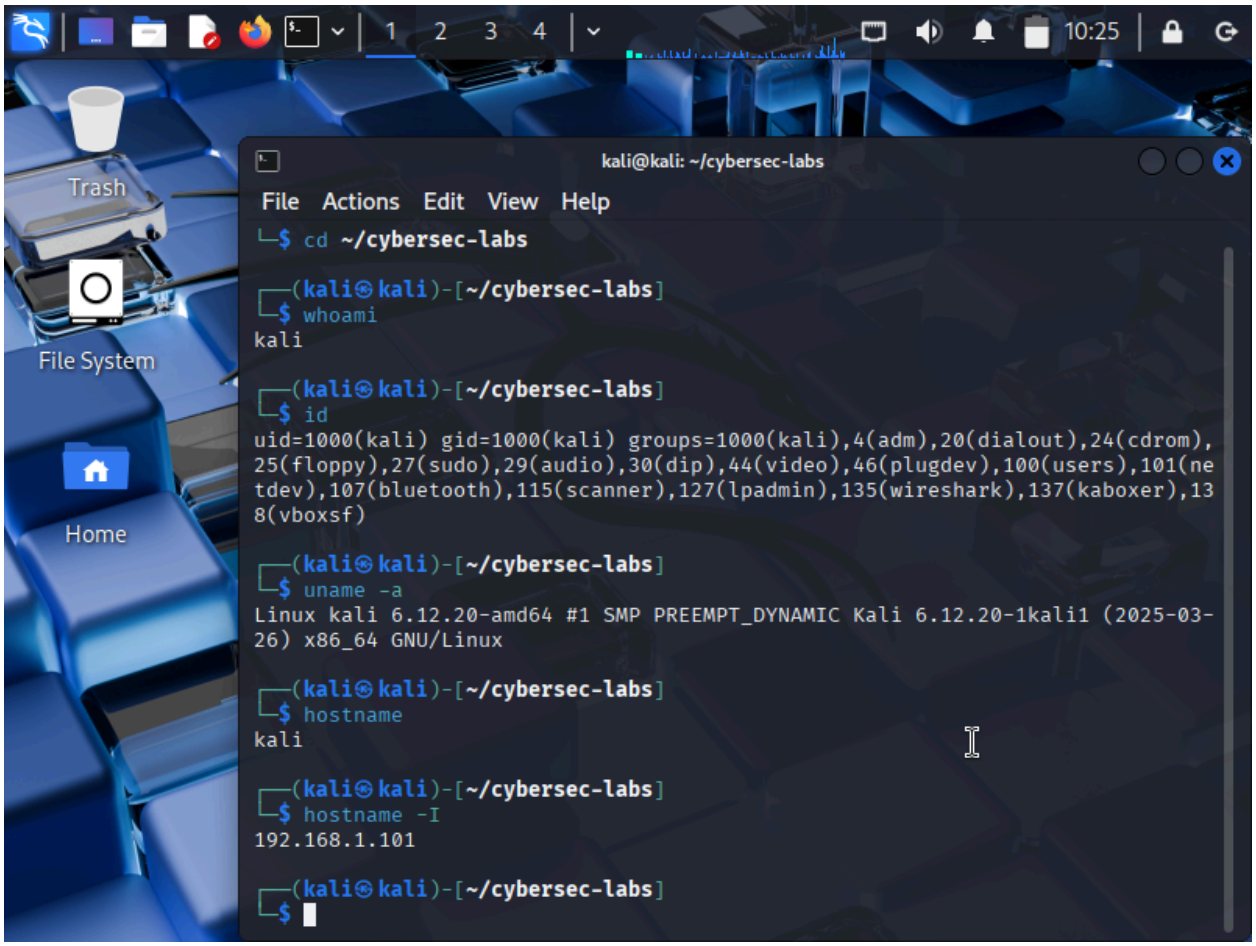
Title: Lab 2: Linux Basics Part 2 - Text Processing and System Information

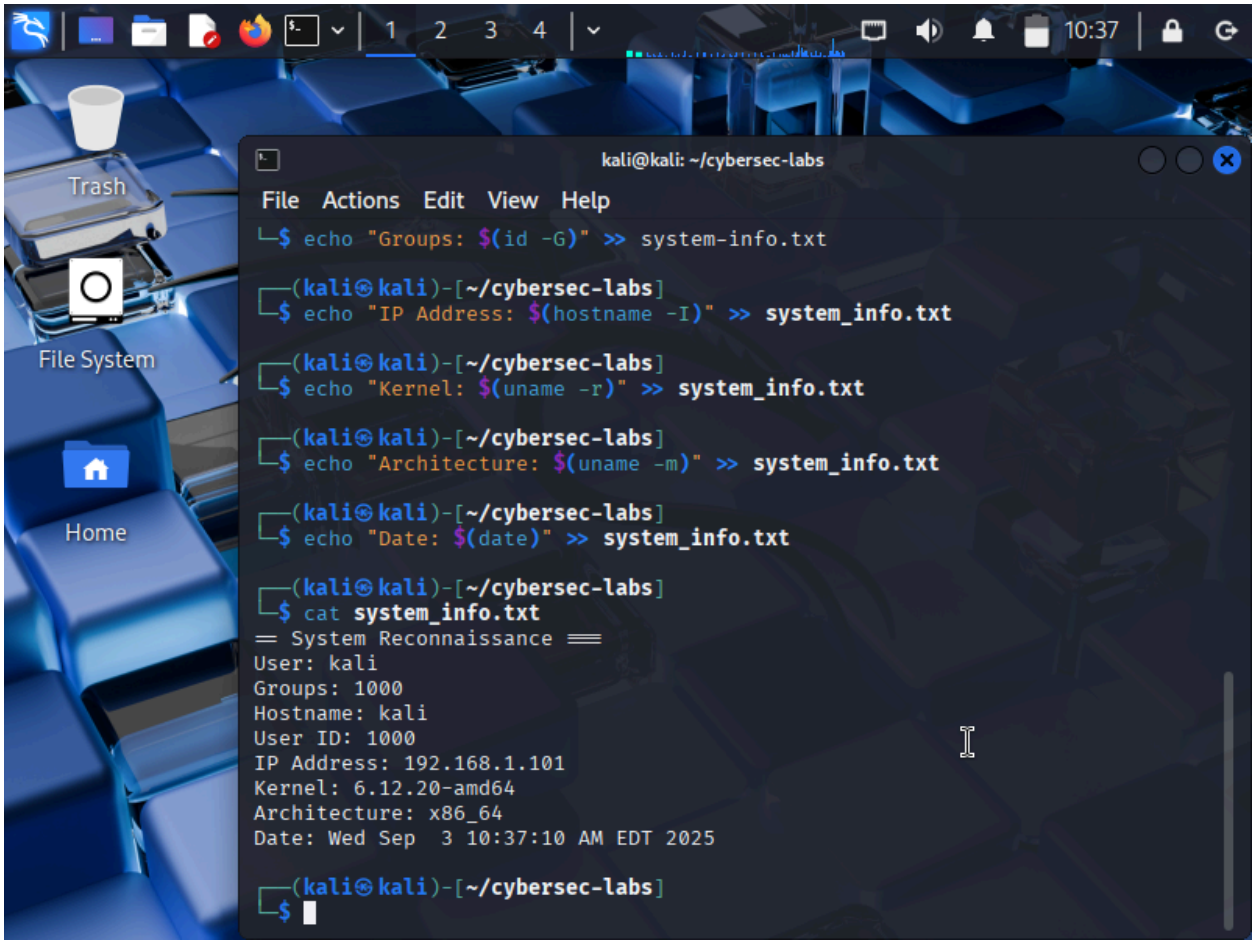
Matthew Cox, COMP325-01, term (Fall 2025)

Introduction: This lab builds upon Lab 1's foundation, introducing powerful text processing tools and system information commands that are essential for security analysis workflows. In this lab, I'll demonstrate processes and analyze text files using essential Linux text processing tools, extract specific information from command outputs and log files, use piping to chain commands for complex data processing, and gather system information for reconnaissance and enumeration.

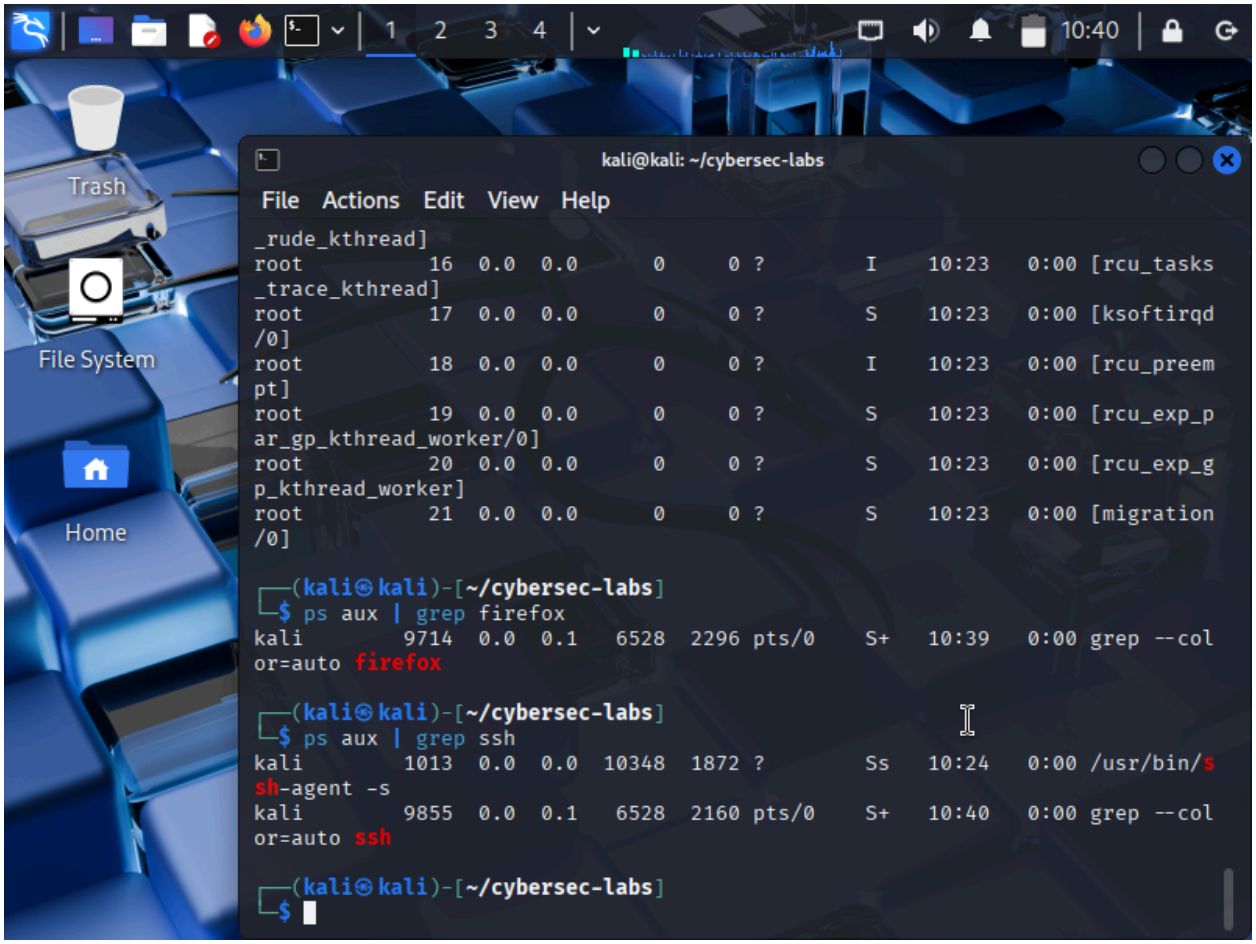
Body:



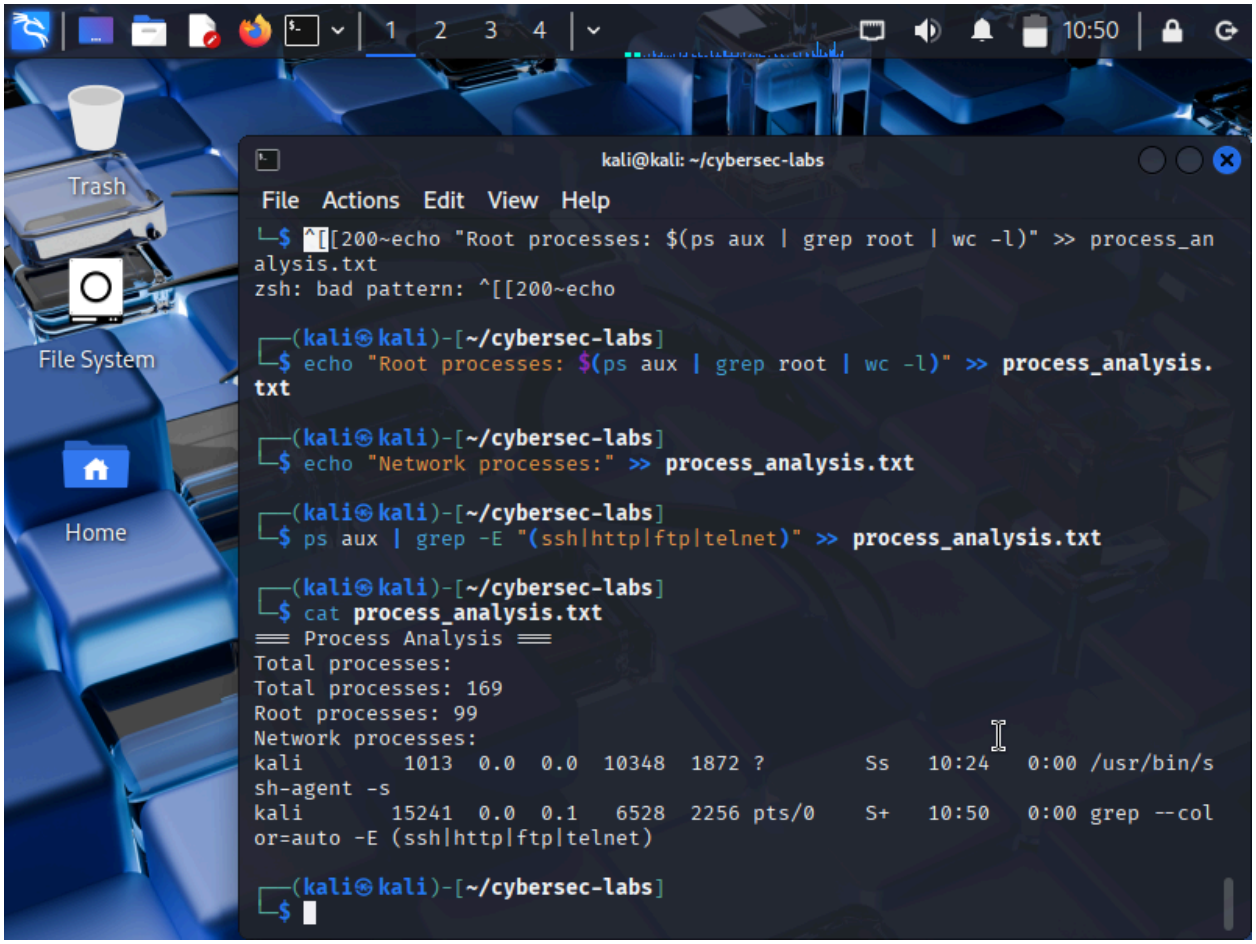
This just shows that I am starting up my environment and checking the host.



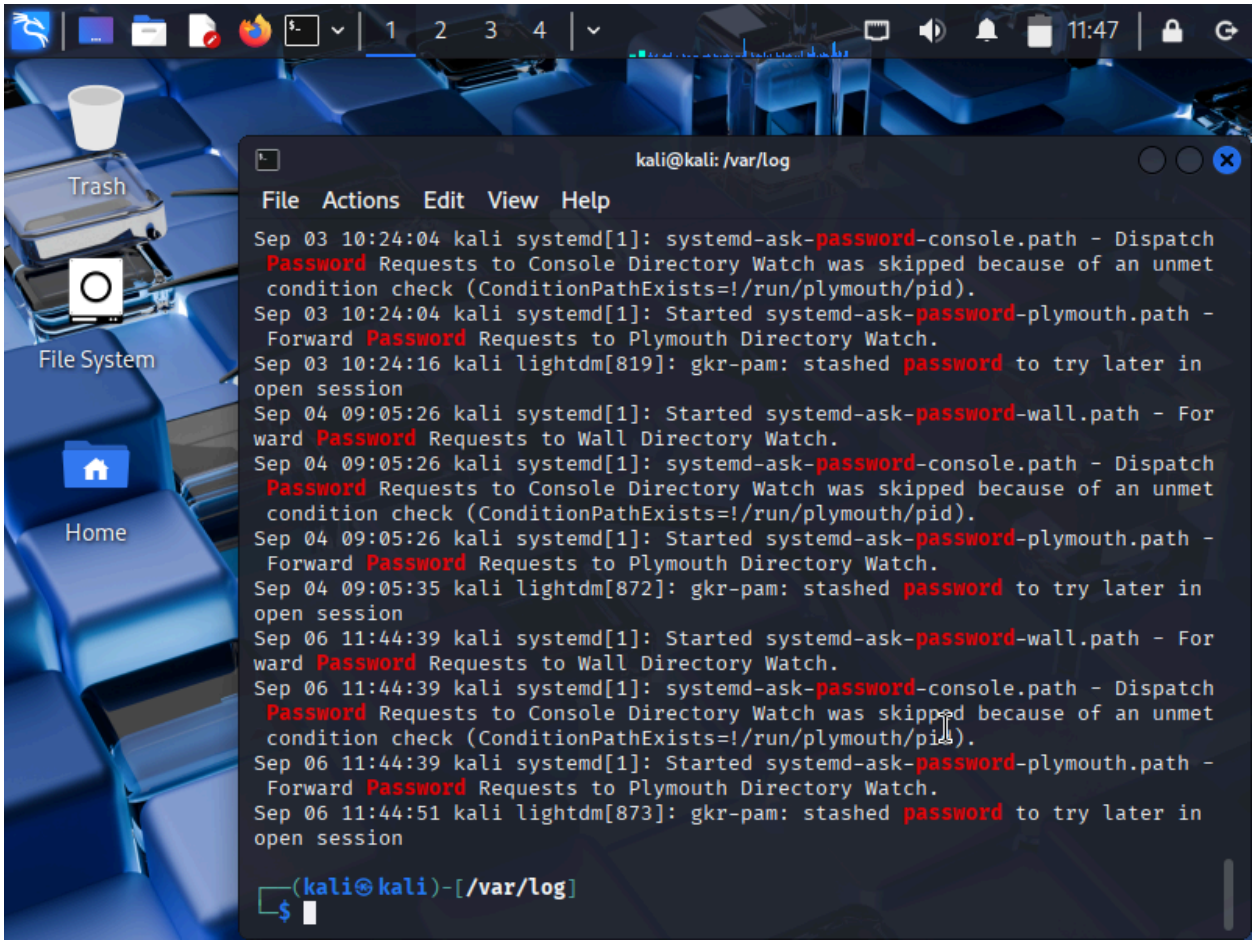
Here, I created the system information and have it displayed for myself to look over.



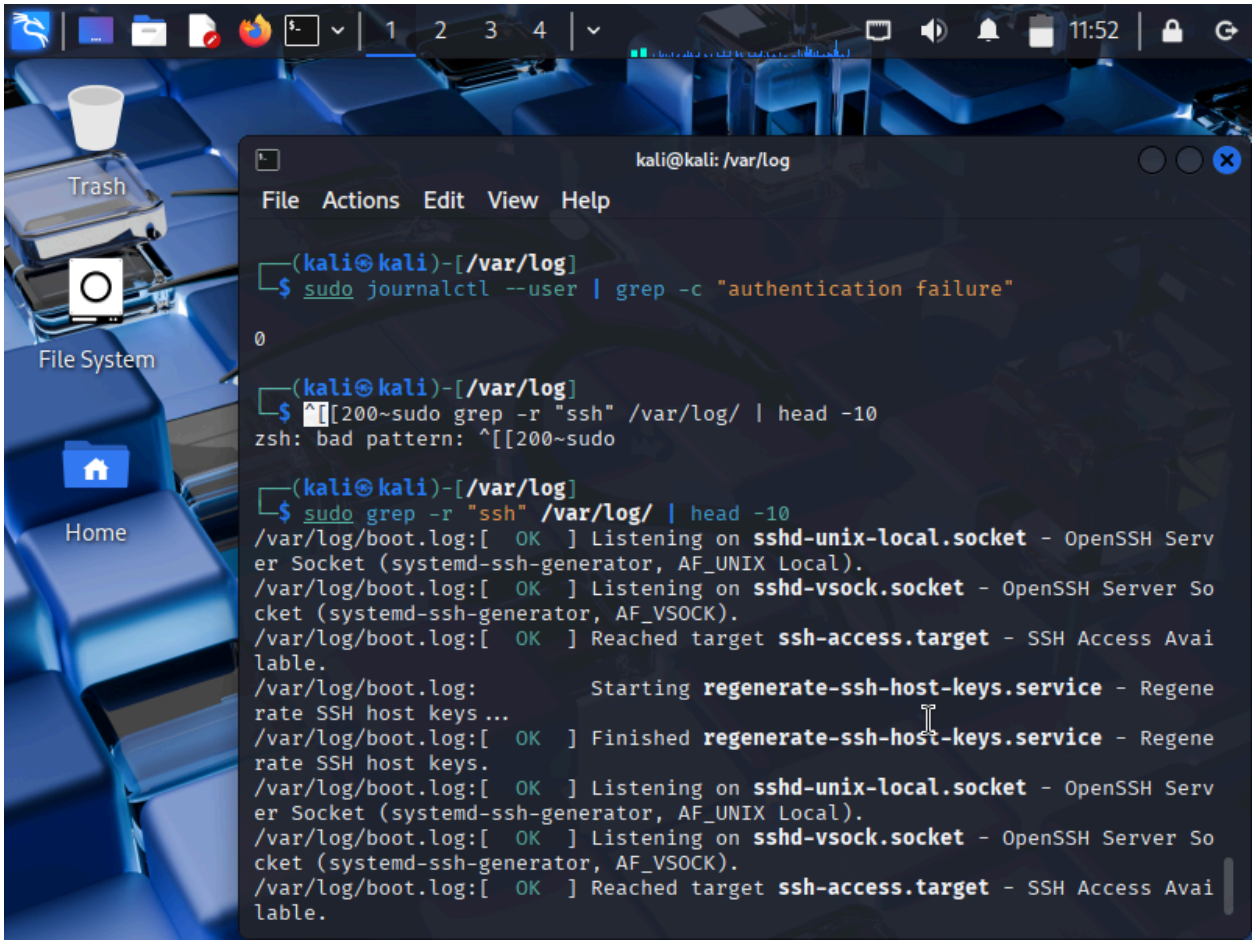
Out of sight, I used the command to view all running processes. In the screenshot, you can see that I used the first twenty processes and then specifically singled out Firefox and the last seek processes using the string ssh.



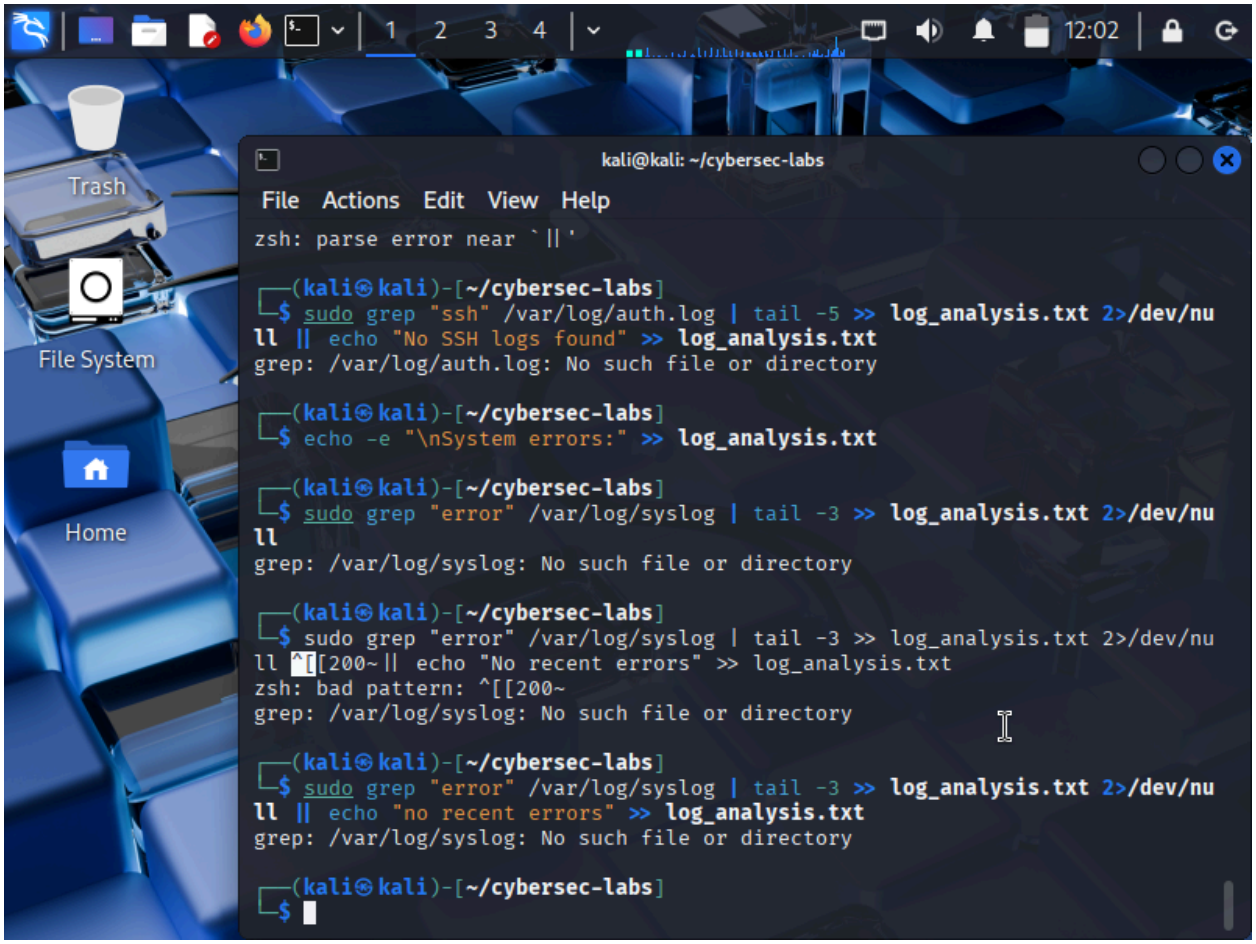
Here, I showed the first 10 processes running as the root user. Then, I created a process monitoring file. This is where I stopped during class recitation. This is the conclusion of Exercise 2.



Here you can specifically see me using the journal and group command to find the entries for “password”, out of view, I used those commands to find the five entries for “error”.

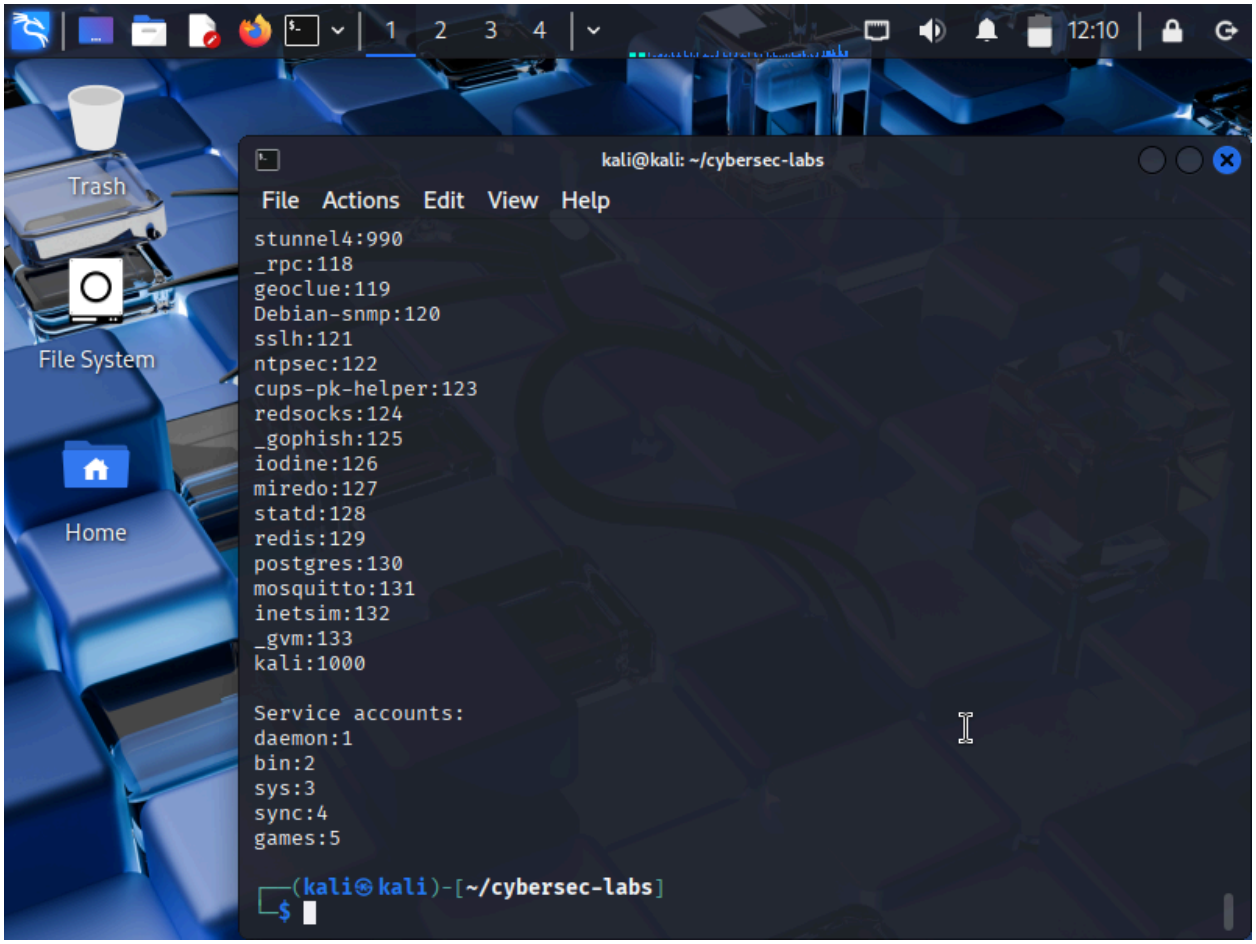


Here, I am counting the occurrences for specific entries and then searching multiple files.

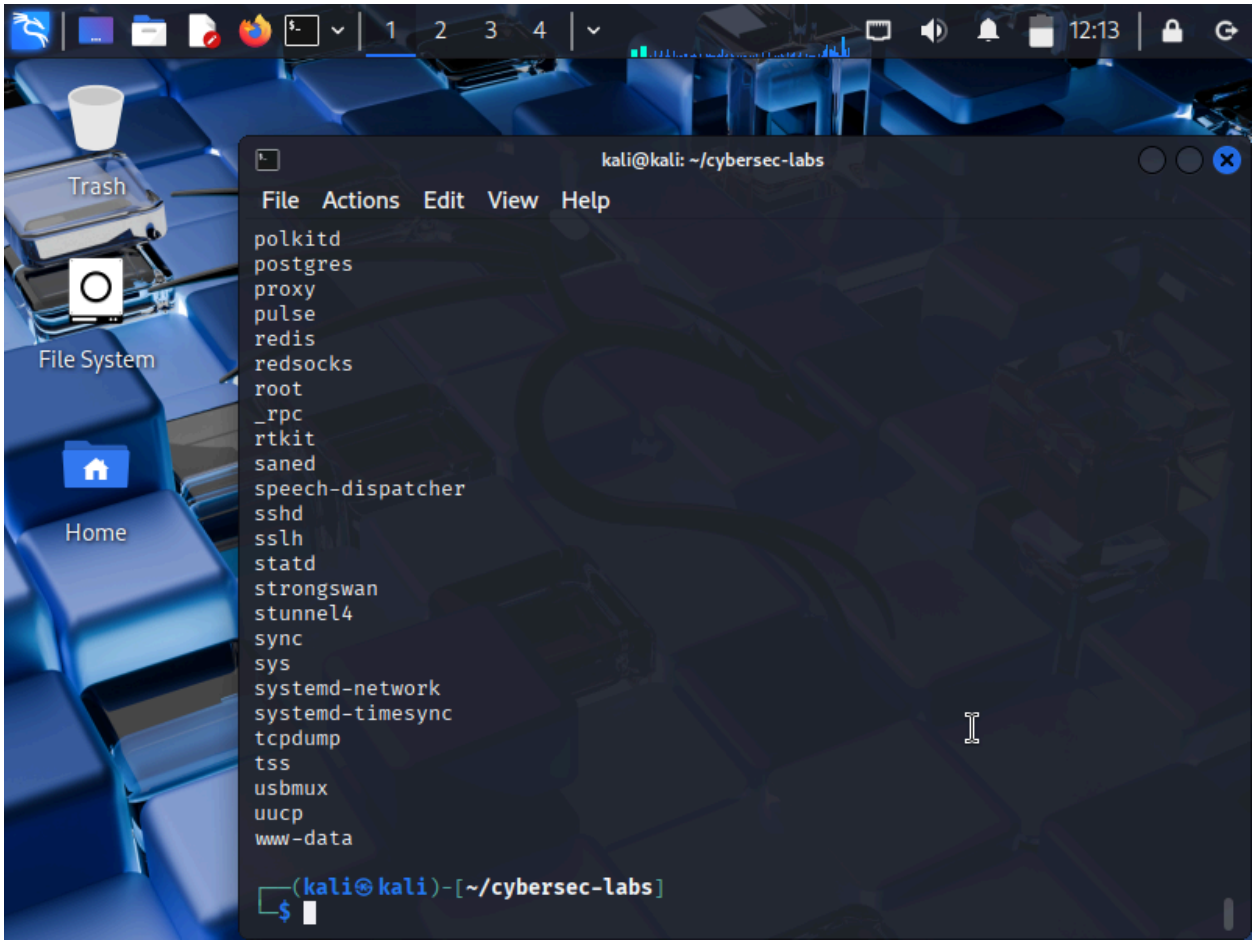


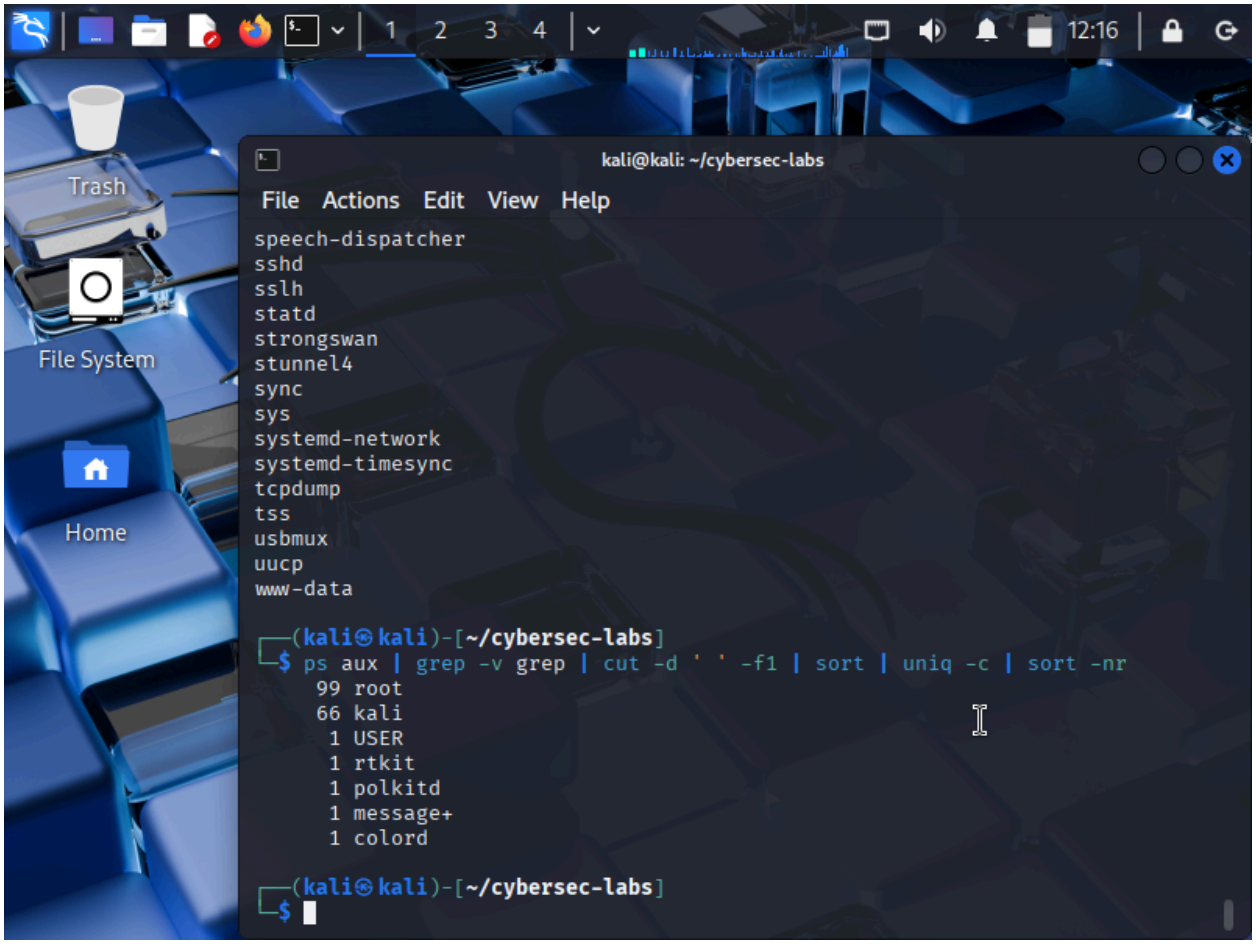
Tried testing this log analysis, but it's not compatible with Kali Linux.

Here, I am extracting various things such as users, specific characters, and more in a specific order.

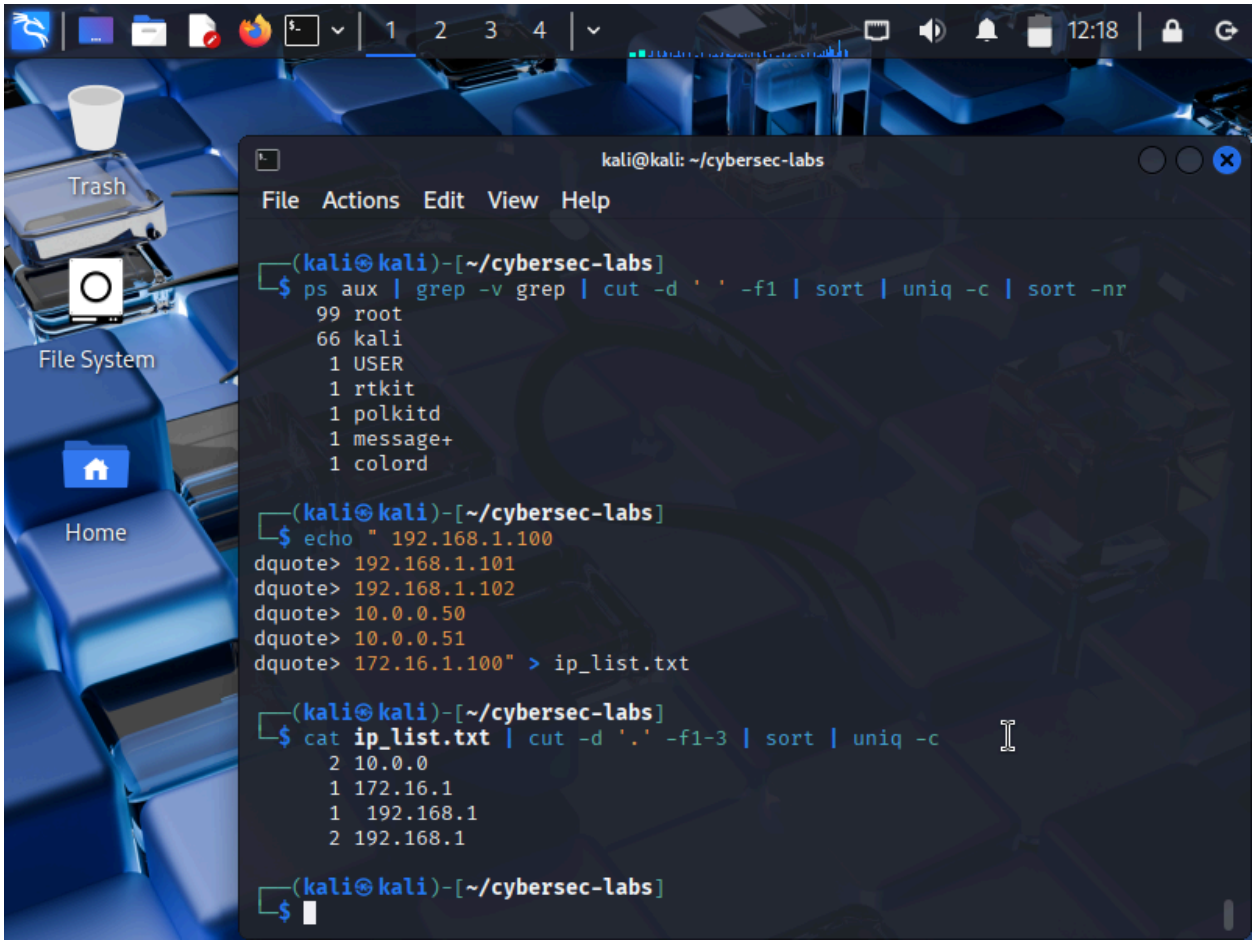


Here, I created a user analysis. This displays the username and user ID for all system users and system accounts in /etc/passwd

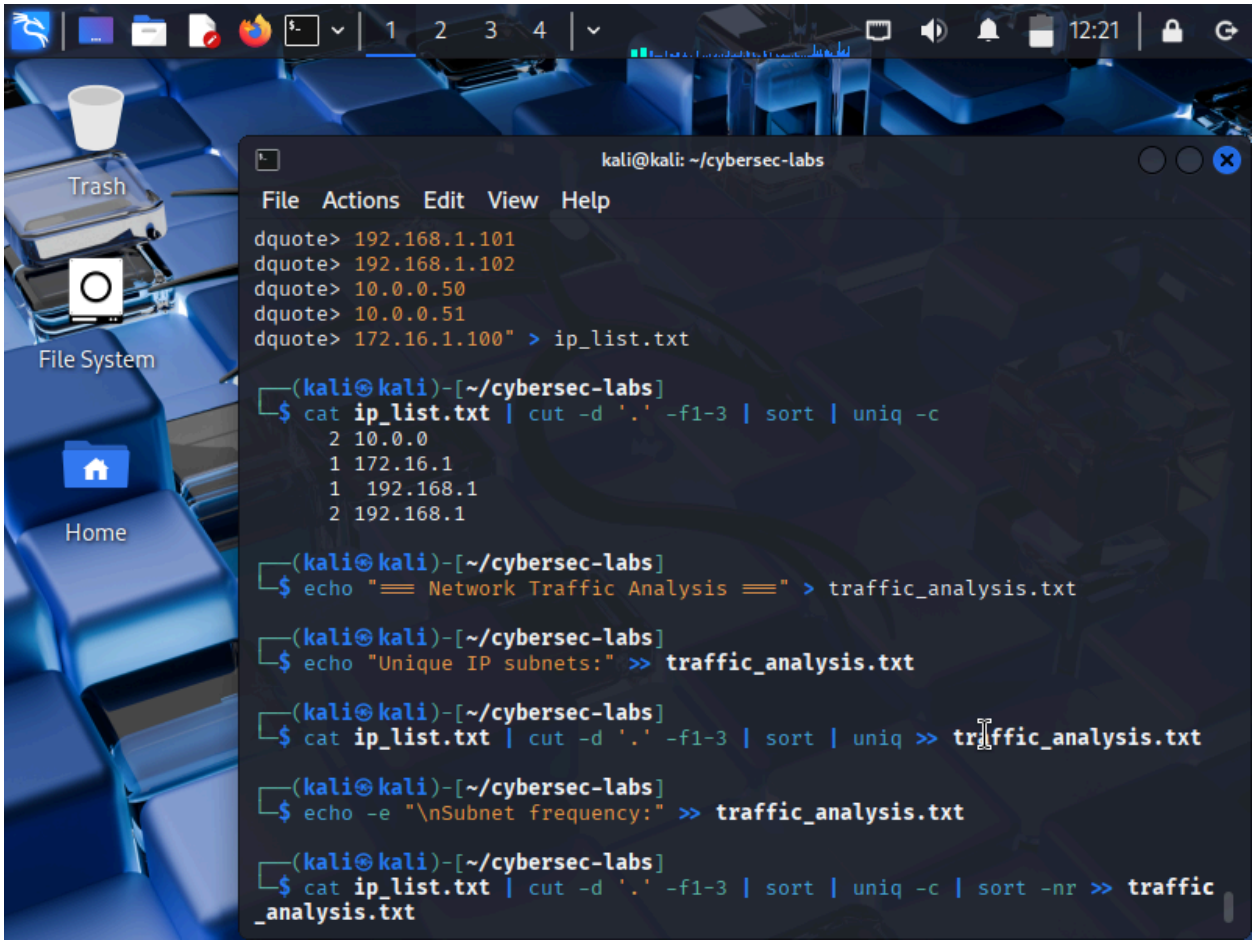

1 2 3 4
12:13
Trash
File System
Home
kali@kali: ~/cybersec-labs
File Actions Edit View Help
polkitd
postgres
proxy
pulse
redis
redsocks
root
_rpc
rtkit
saned
speech-dispatcher
sshd
sslh
statd
strongswan
stunnel4
sync
sys
systemd-network
systemd-timesync
tcpdump
tss
usbmux
uucp
www-data
(kali㉿kali)-[~/cybersec-labs]
$



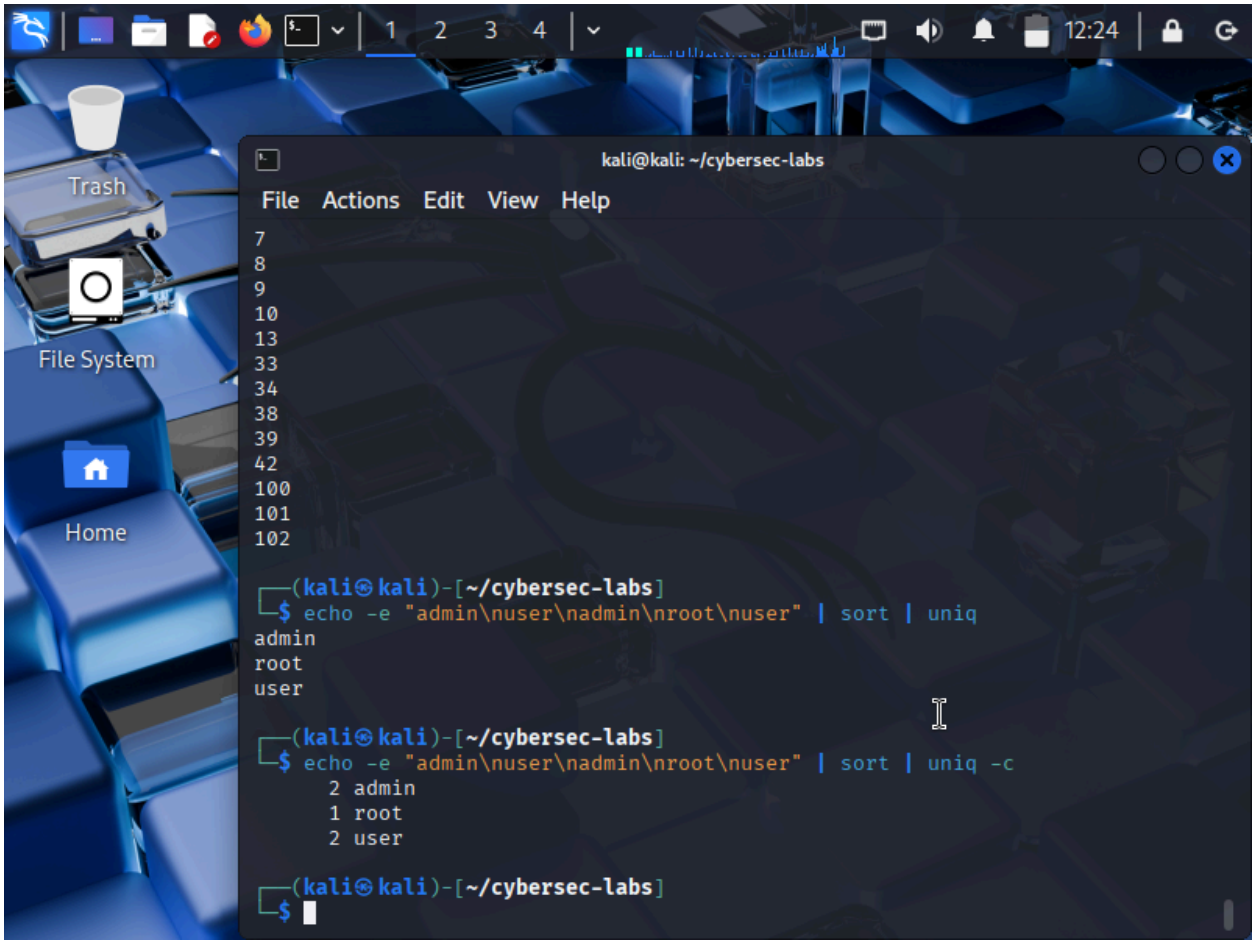
In this image, I executed some basic piping. Then I executed a Multi-stage processing where this counts processes by user and sorts by frequency.



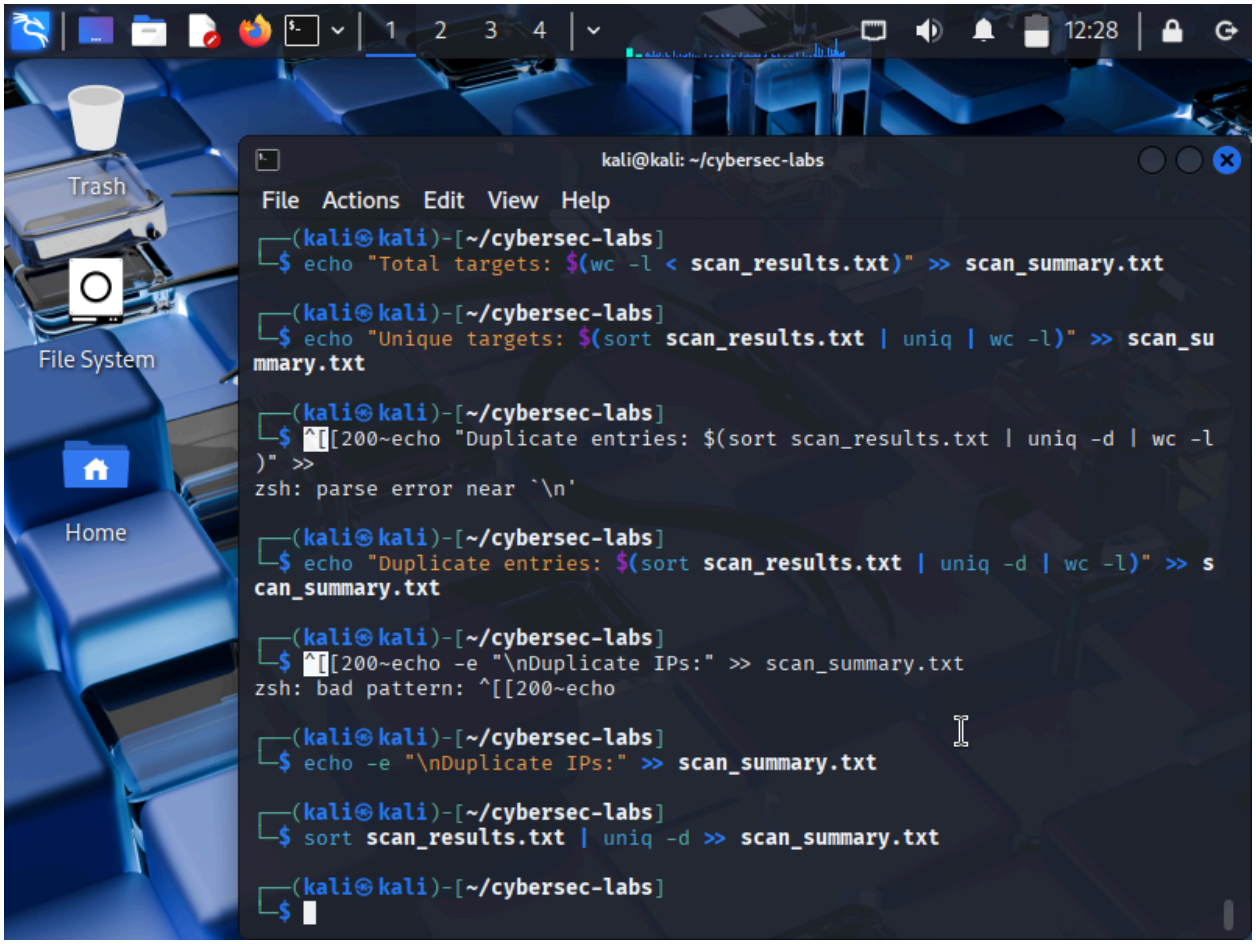
In this portion of the exercise, I got the machine to analyze the IP address ranges.



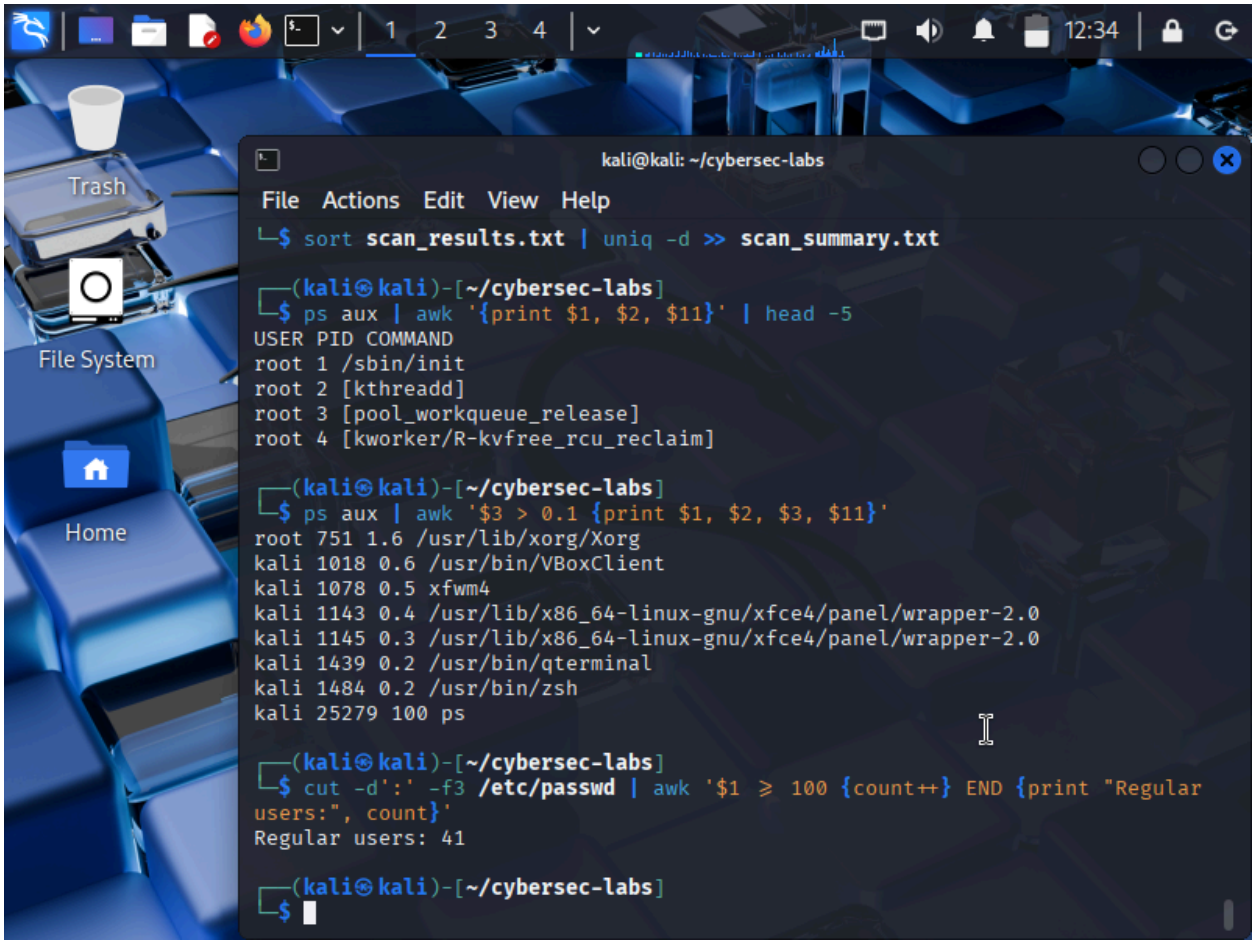
In this, I create a log file analysis pipeline.



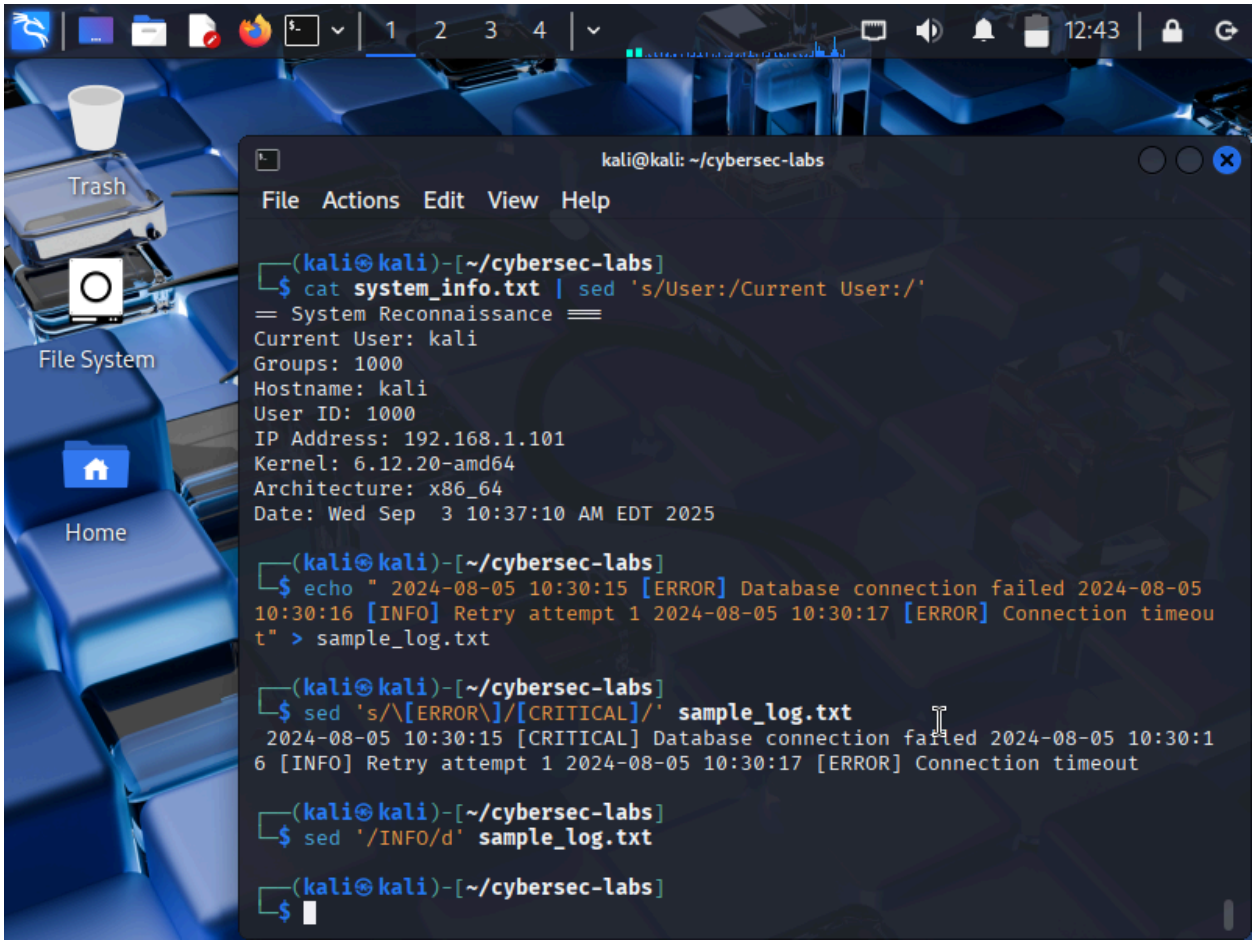
Here, I performed some basic sorting, numerical sorting, and then removed duplicates.



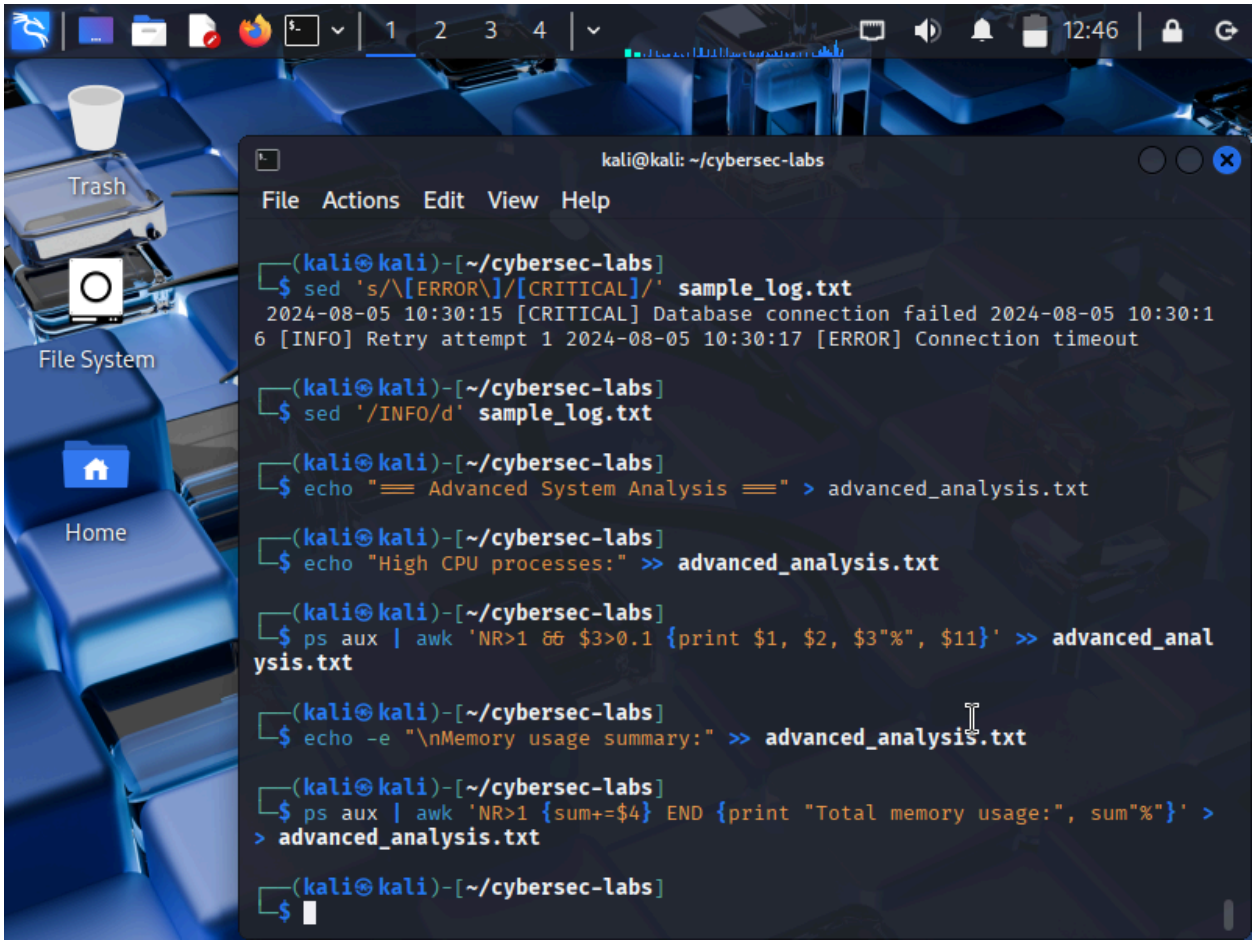
Finally, in exercise 6, I found the two duplicates, then created a comprehensive analysis.



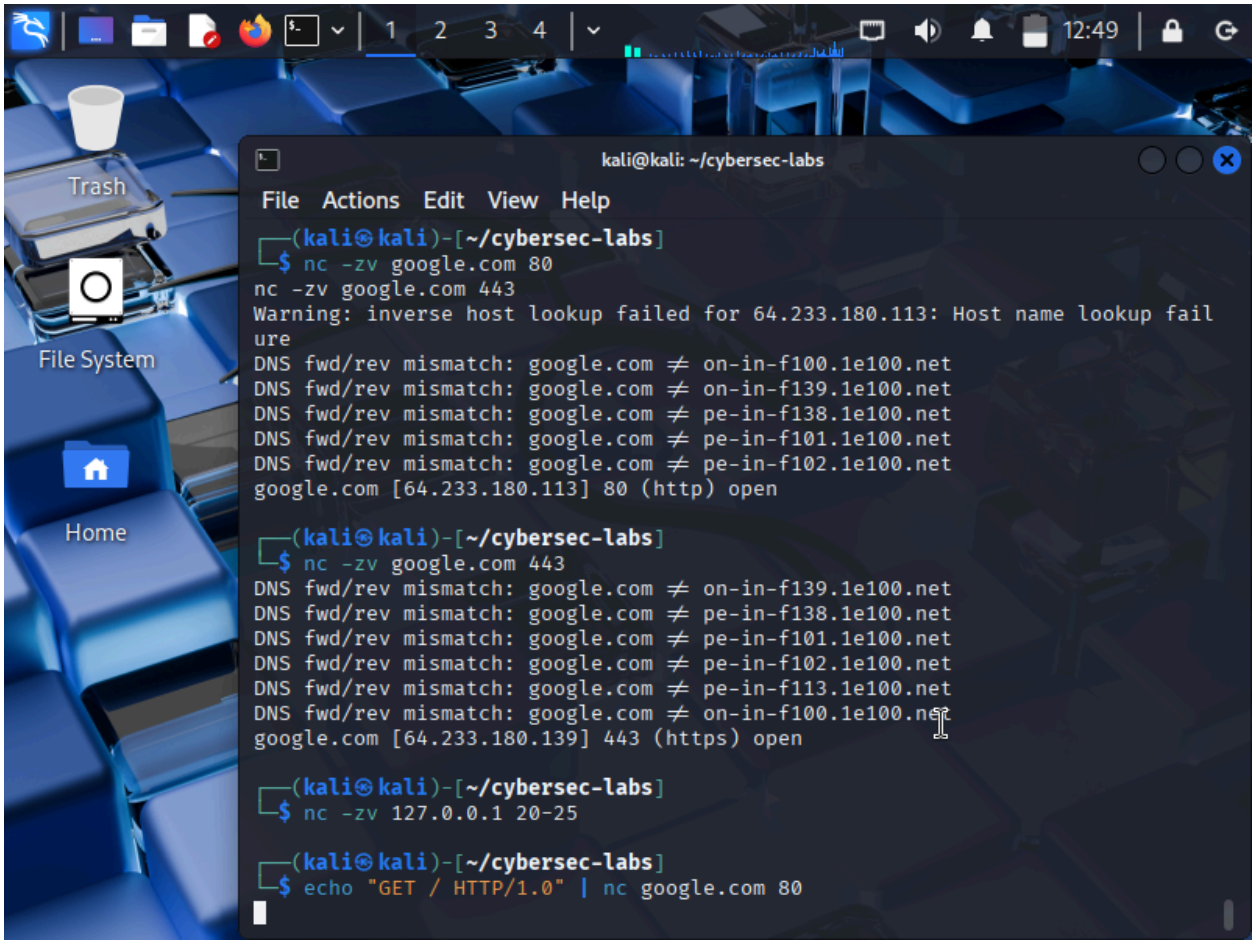
In these few commands, I printed specific columns with clear outputs rather than a cut. Then I used a command to provide me with an output that shows processes using more than 0.1% CPU. Then I used an awk calculation command that counts the number of regular users by seeking user IDs starting at 1000.



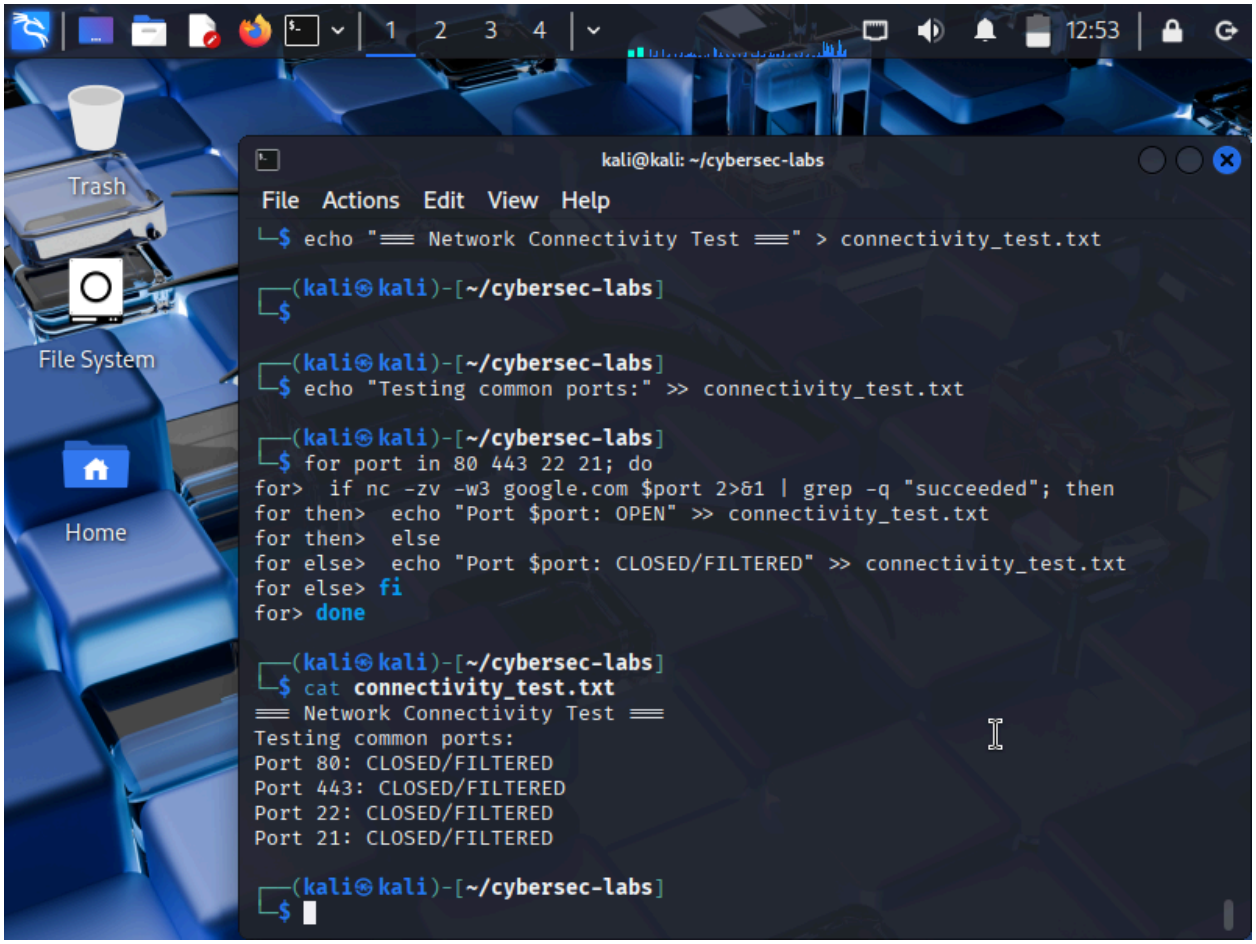
Used a simple string substitution. Then I used a sed command for log cleaning.



Here, I created an advanced analysis.



In this exercise, I tested two ports to see if they were open on Google. Then I scanned through ports 20-25 on the local host.



In this assessment, I completed a banner grab, followed by creating a connectivity test. I can't say that I understand it completely or did it correctly. I may have messed up the indentation on the command fi.

Knowledge Assessment:

Question 1: True or False: The command ps aux | grep ssh | wc -l counts the number of SSH-related processes currently running.

False

Question 2: Which command combination would extract only the usernames from the/etc/passwd file?

a) cat /etc/passwd | cut -d':' -f1

Question 3: True or False: The uniq command removes duplicate lines even if the input is not sorted.

False

Question 4: What does the command nc -zv google.com 80 accomplish?

b) Tests if port 80 is open on google.com

Question 5: Which command would show processes using more than 1% CPU?

b) ps aux | awk '$3 > 1'

Conclusion:

With the conclusion of lab 2, I am now well acquainted with Kali Linux. After building off of Lab 1, I am now comfortable with the previous commands and exercises committed in Lab 1. After the conclusion of Lab 2, I have a greater understanding of extracting and processing text data using grep, cut, awk, and sed. Gather comprehensive system information, use piping to create complex data processing workflows, and analyze processes and network connectivity.