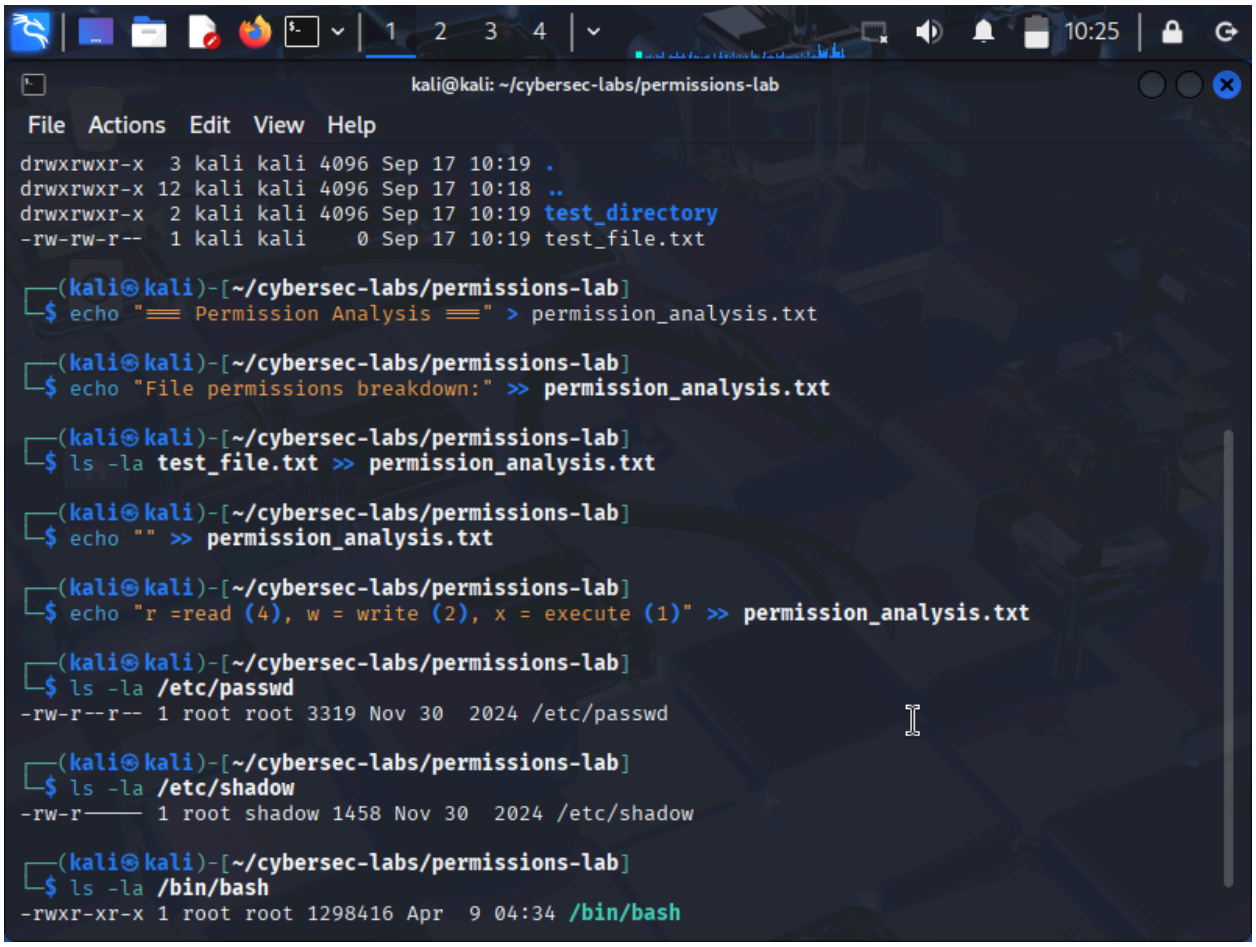
Lab 4: Linux Basics Part 4 - Permissions and File Discovery
Matthew Cox, COMP325-01, term (Fall 2025)

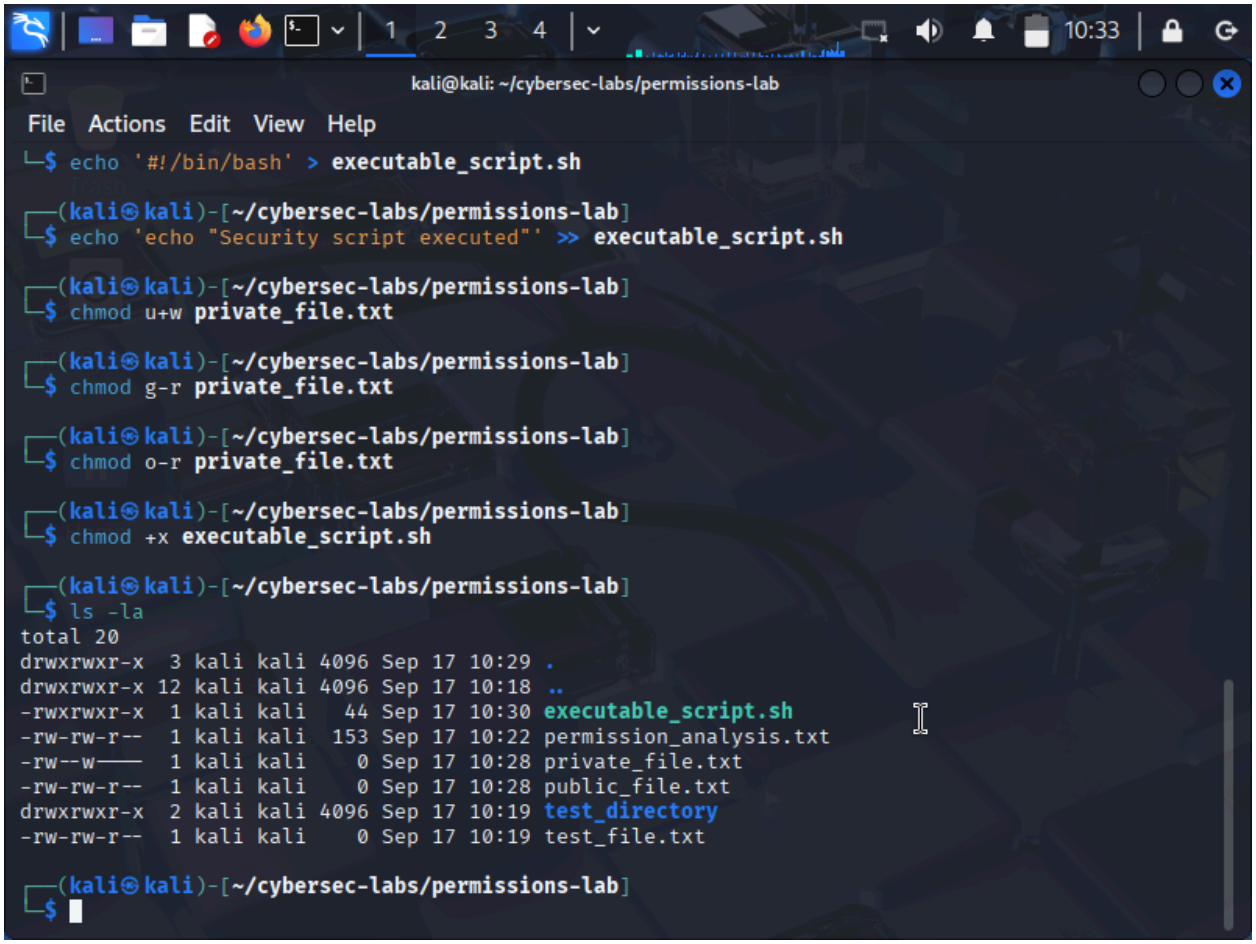
Introduction:

This lab will focus on Linux file permissions, analyzing SUID/SGID files, and locating files and directories. I will gain a greater understanding of how hackers might exploit misconfigured files. At the same time, I will be learning more in-depth about how Security Analysts need these skills to investigate incidents.

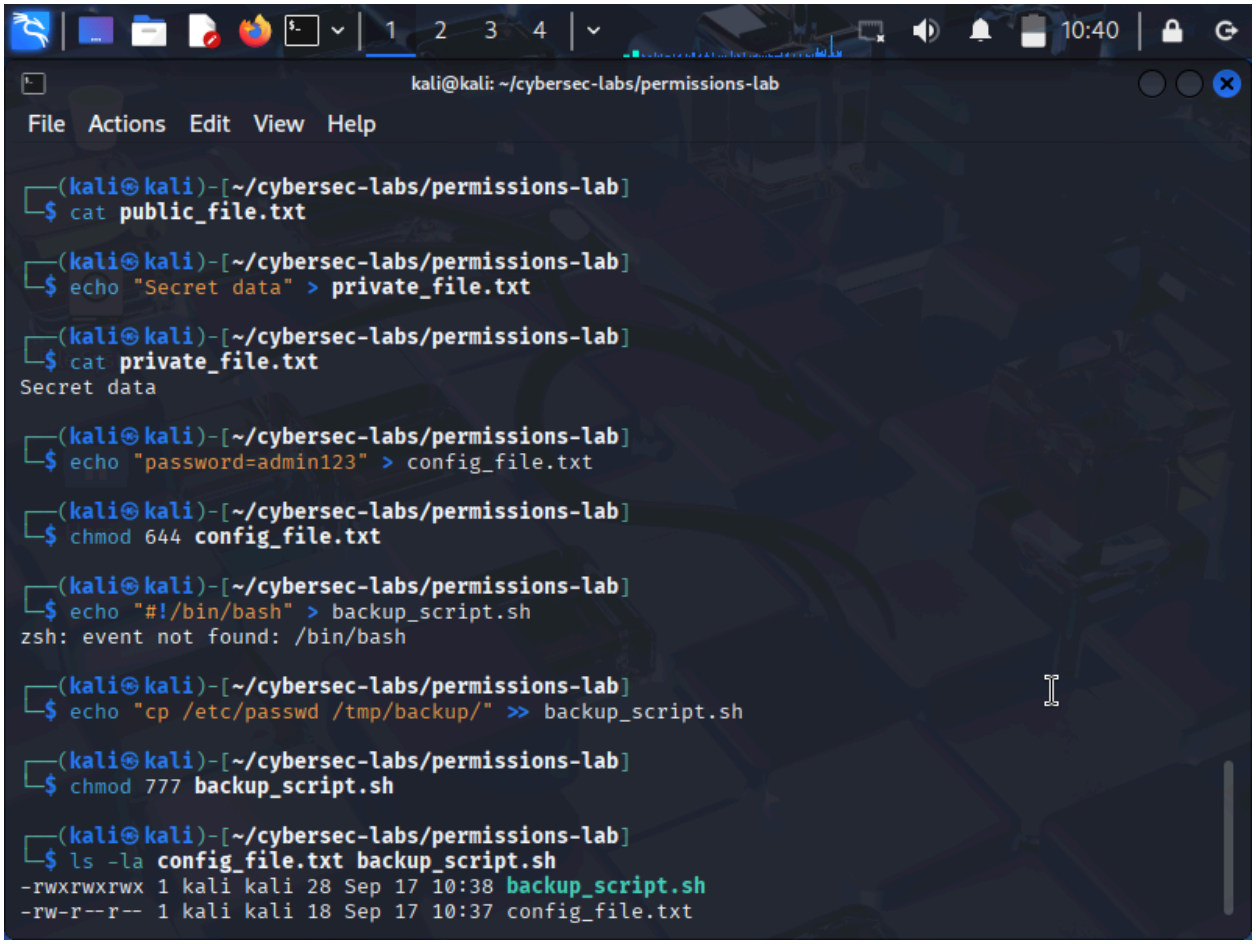
Body:



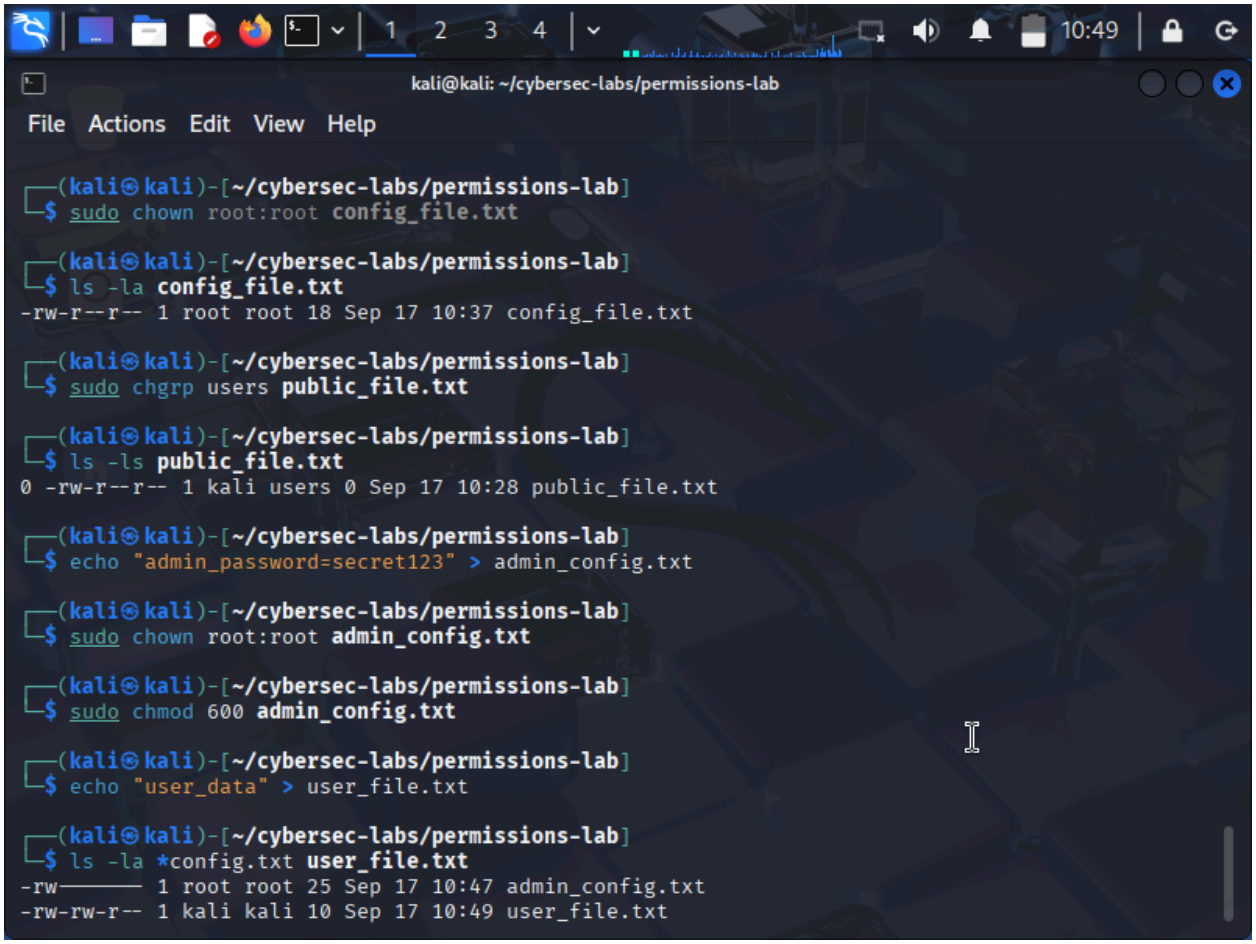
Here, I was just setting the start of this lab. I ran a couple of test files and created a log to get a grasp of permission notation. Then, I ran some commands to view the system file permissions.



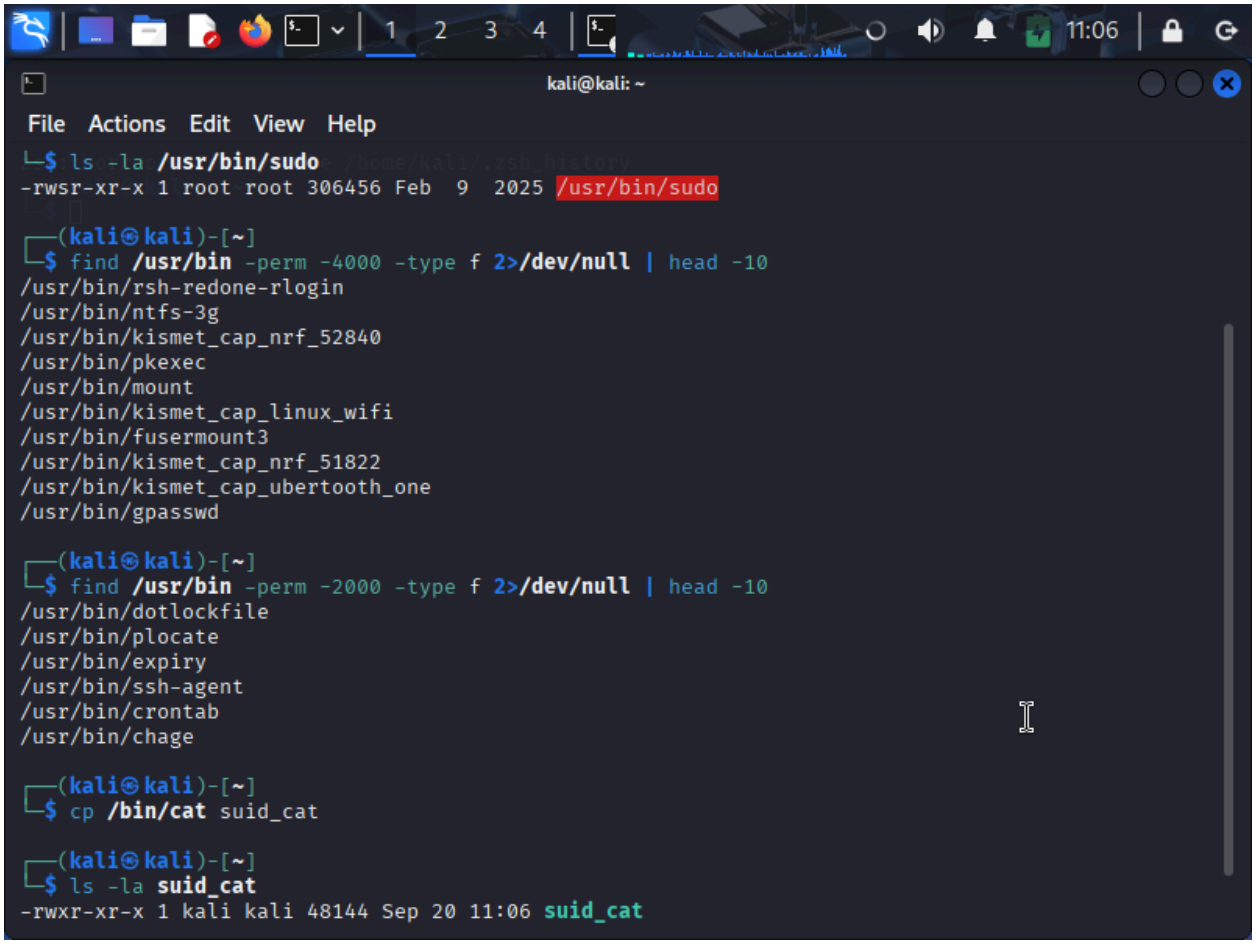
I created some permission examples. Then, I used symbolic notations with the command chmod.



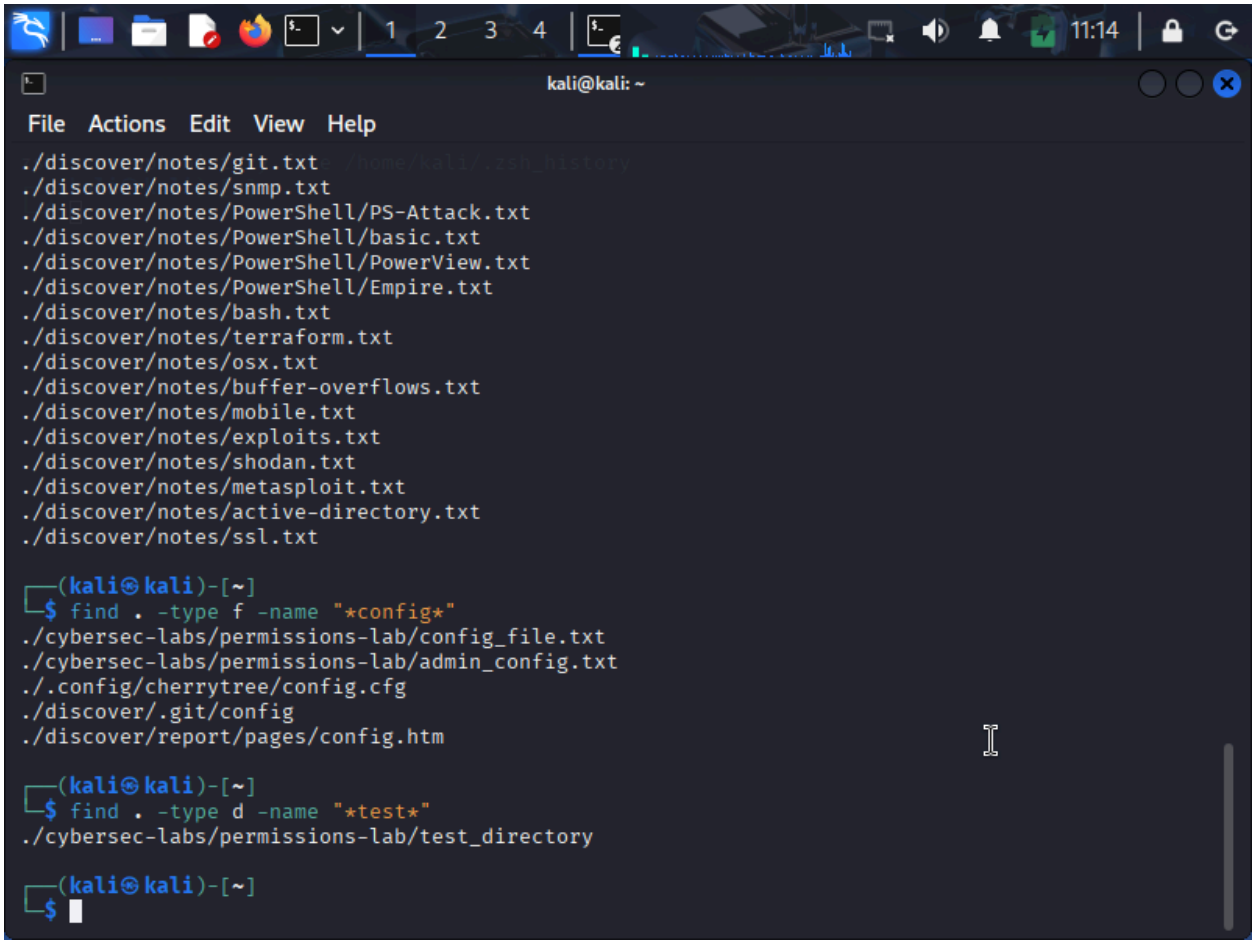
I used numeric notations with chmod. Afterwards, I used some text permission effects. Then, I created some security-relevant scenarios. I'm going to document the permission analysis and examine some file ownerships.



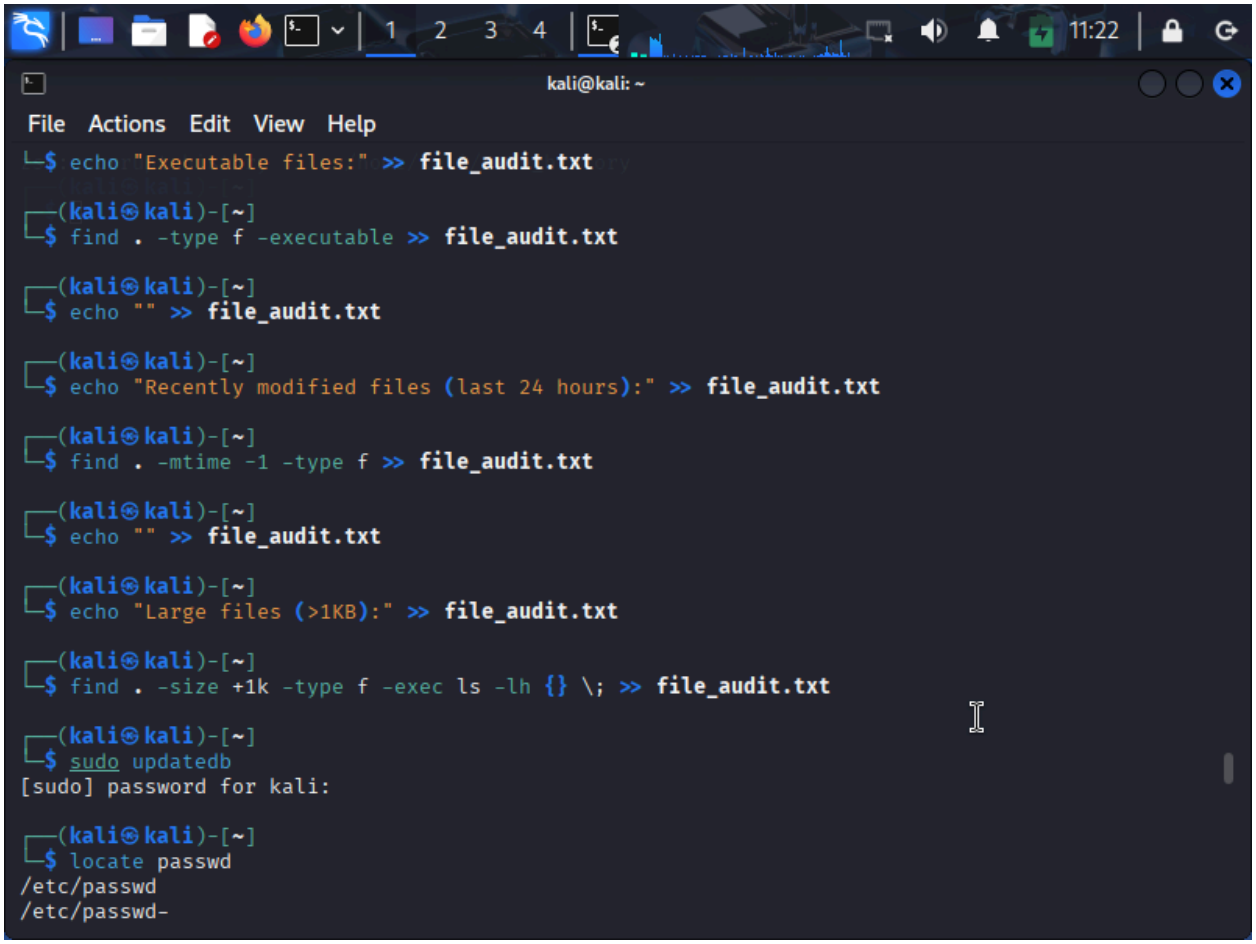
Initially, I examined the current ownership. After, I changed the ownership as well as the group ownership. Then I created a few ownership scenarios. Next, I will be making an ownership analysis. That will then cover this section. For then I will gain a greater understanding of the sudo command in the next exercise.



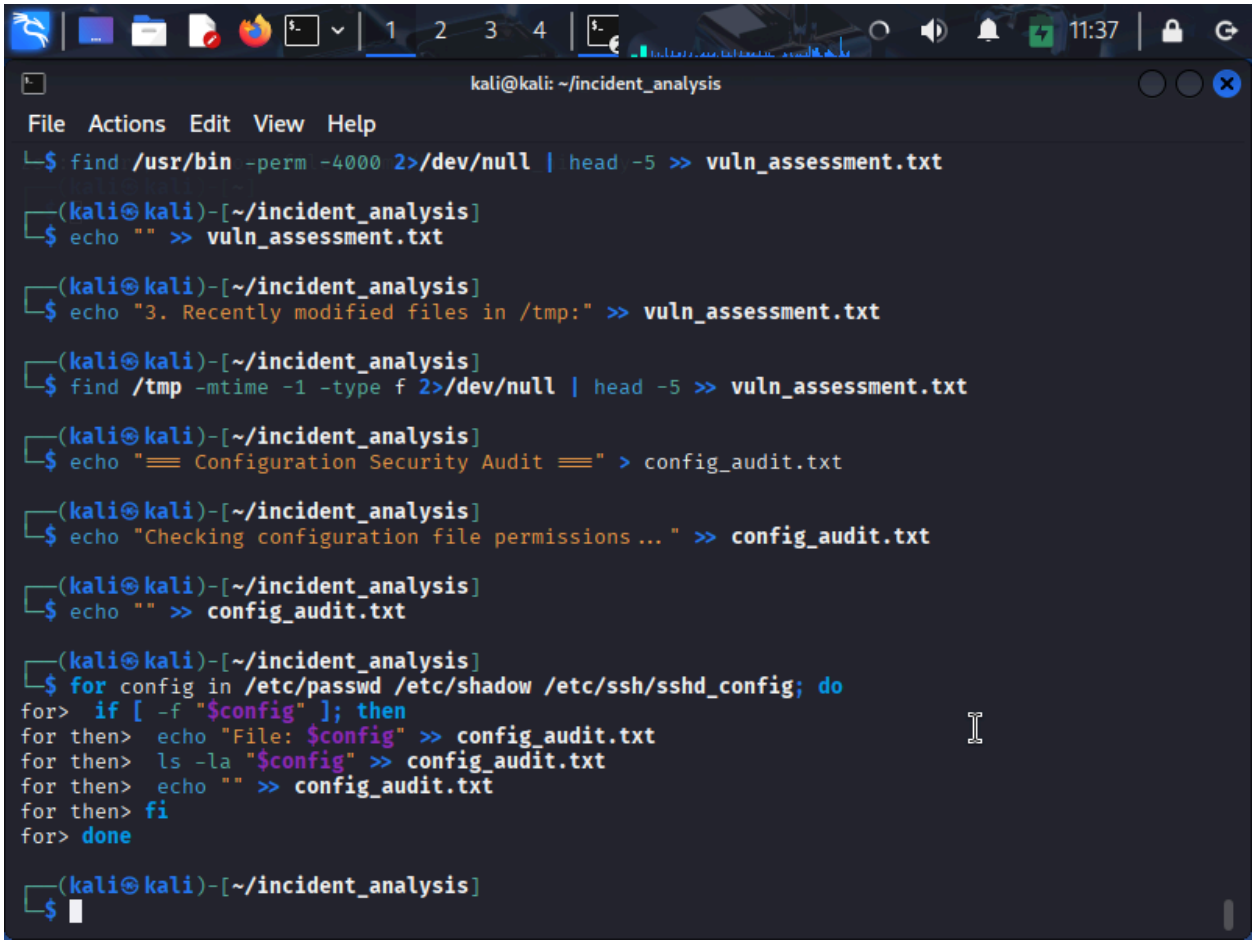
Here, I have gotten familiar with SUID and SGID. I then created a SUID example as a demonstration.



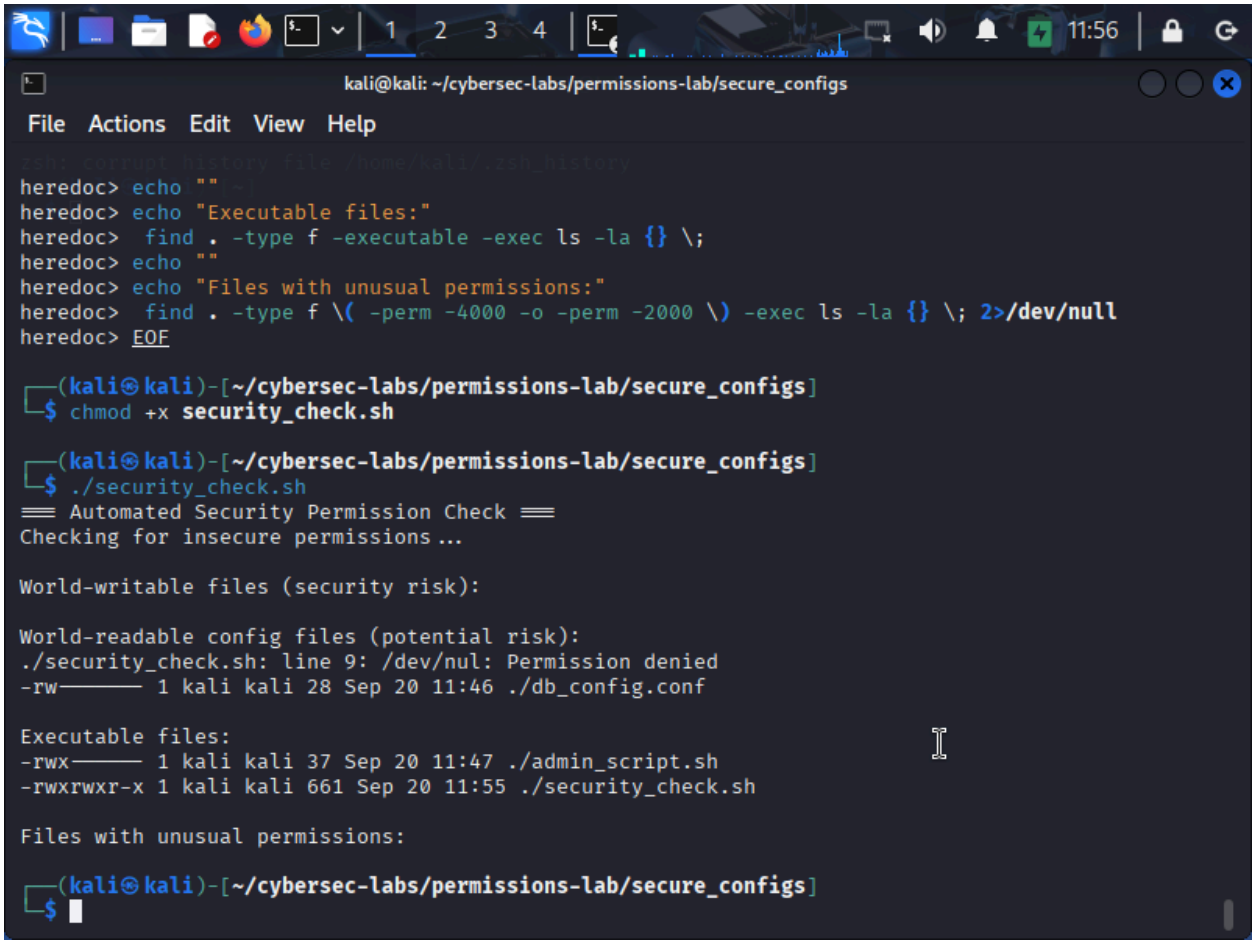
Out of frame, I created a SUID and SGID analysis. Now, I used some basic find operations.



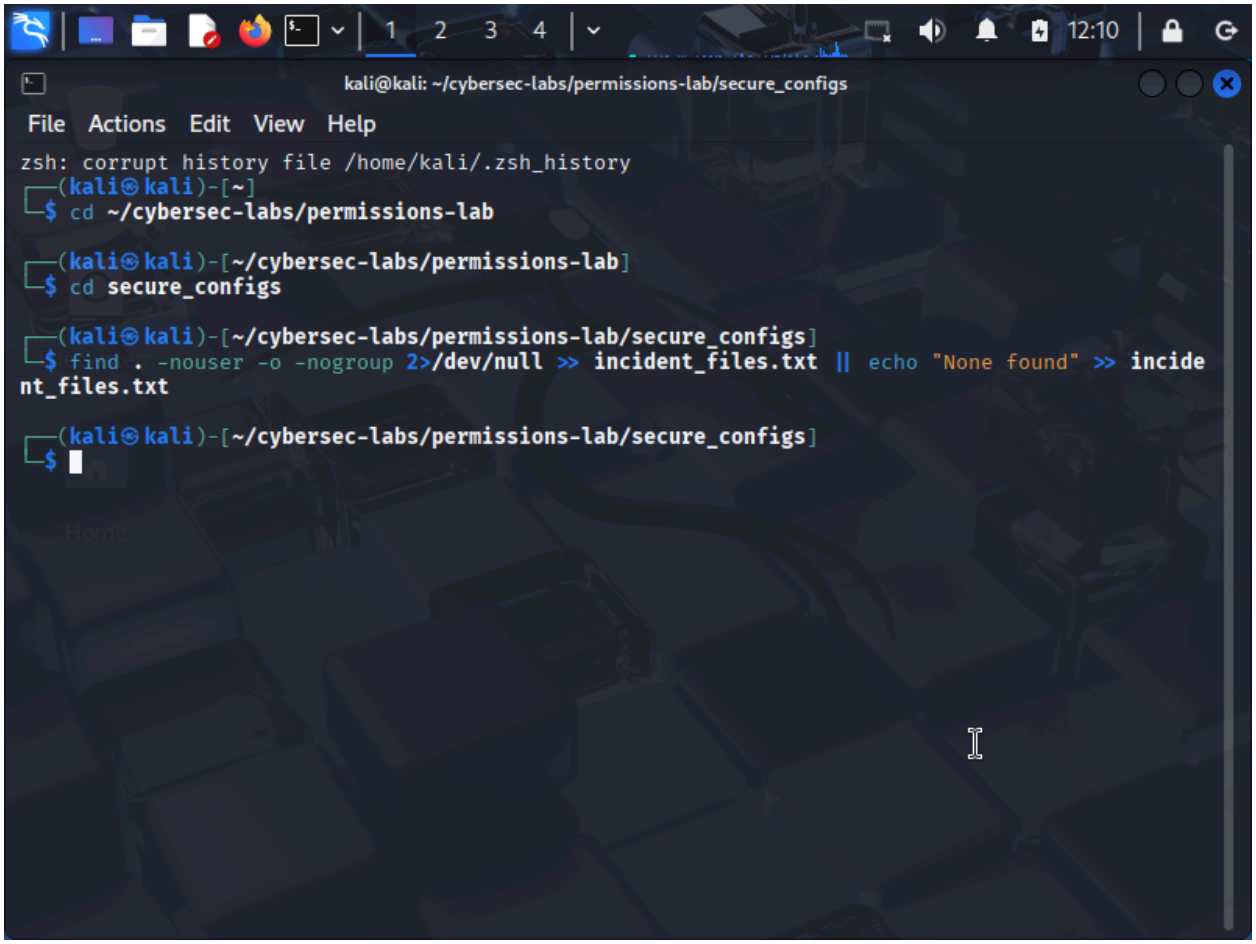
Following the last slide, I used a command to conduct further file discovery. I used commands to find permissions, size, and time. Then I did a deeper search with security-focused operations and an advanced file with actions. Afterwards, I created a comprehensive file audit. Now I'm executing some basic locate operations.



Following the series of basic locate operations, I then moved to comparing find vs locate operations. After that, I created a security reconnaissance with locate operations. Then, I made an incident file analysis and a permission vulnerability assessment. Following that, I made a configuration file audit.



To recap what I've done: I created a private escalation reconnaissance, secure file structure, permission remediation examples, and automated security check scripts. I verified the secure permissions. When I performed the security check, I obtained the output shown above. I did have one hiccup when creating the automated security check script. The output doesn't look correct to me.



I know the screenshot doesn't show much. I messed up on the very last line of the incident response file patterns and had to close my terminal. But to recap what I've done from the last slide, I found files using multiple different criteria. I then used some security-focused file patterns and complex logical operations.

Knowledge Assessment:

Question 1: True or False: A file with permissions 644 (rw-r--r--) allows the group and others to modify the file.
False

Question 2: Which command would find all SUID files in the /usr/bin directory?
b) find /usr/bin -perm -4000 -type f

Question 3: True or False: The locate command searches the filesystem in real-time, making it slower than find but more accurate.
False

Question 4: What does the command chmod u+s filename accomplish?
b) Sets the SUID bit on the file

Question 5: Which find command would locate world-writable files?
b) find. -perm -002

Conclusion:

With the completion of this lab, I have a greater understanding of manipulating file permissions with various commands. I have now discovered and learned about how to identify and analyze SUID/SGID files for security assessment. I am now able to apply advanced find techniques for security analysis and incident response, as well as locate files with both locate and find commands. After this lab and week of class time, I'm very intrigued by jobs within Digital Forensics. I like the thought of working with local law enforcement and actively investigating and making the world a better place.