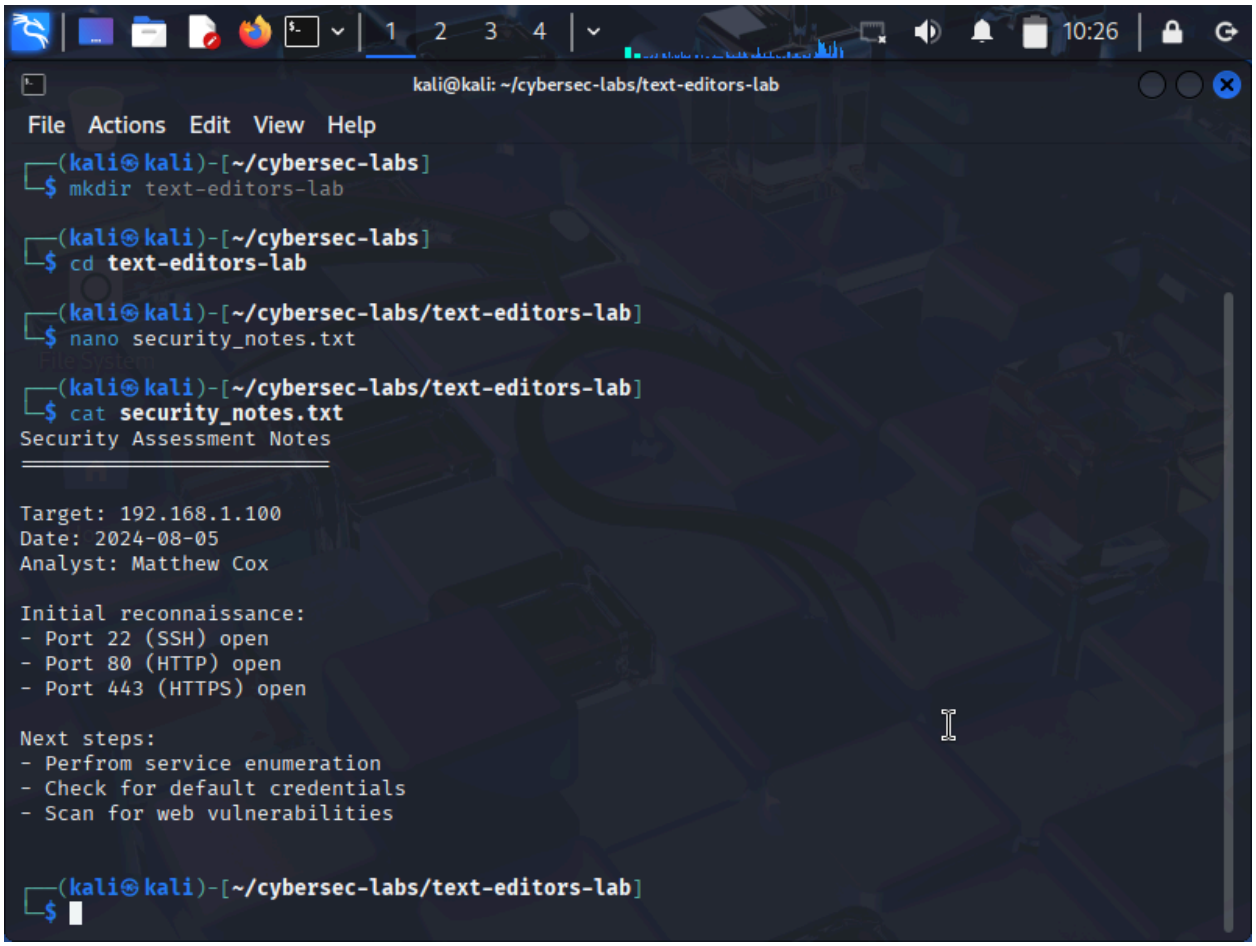
Matthew Cox

COMP 325

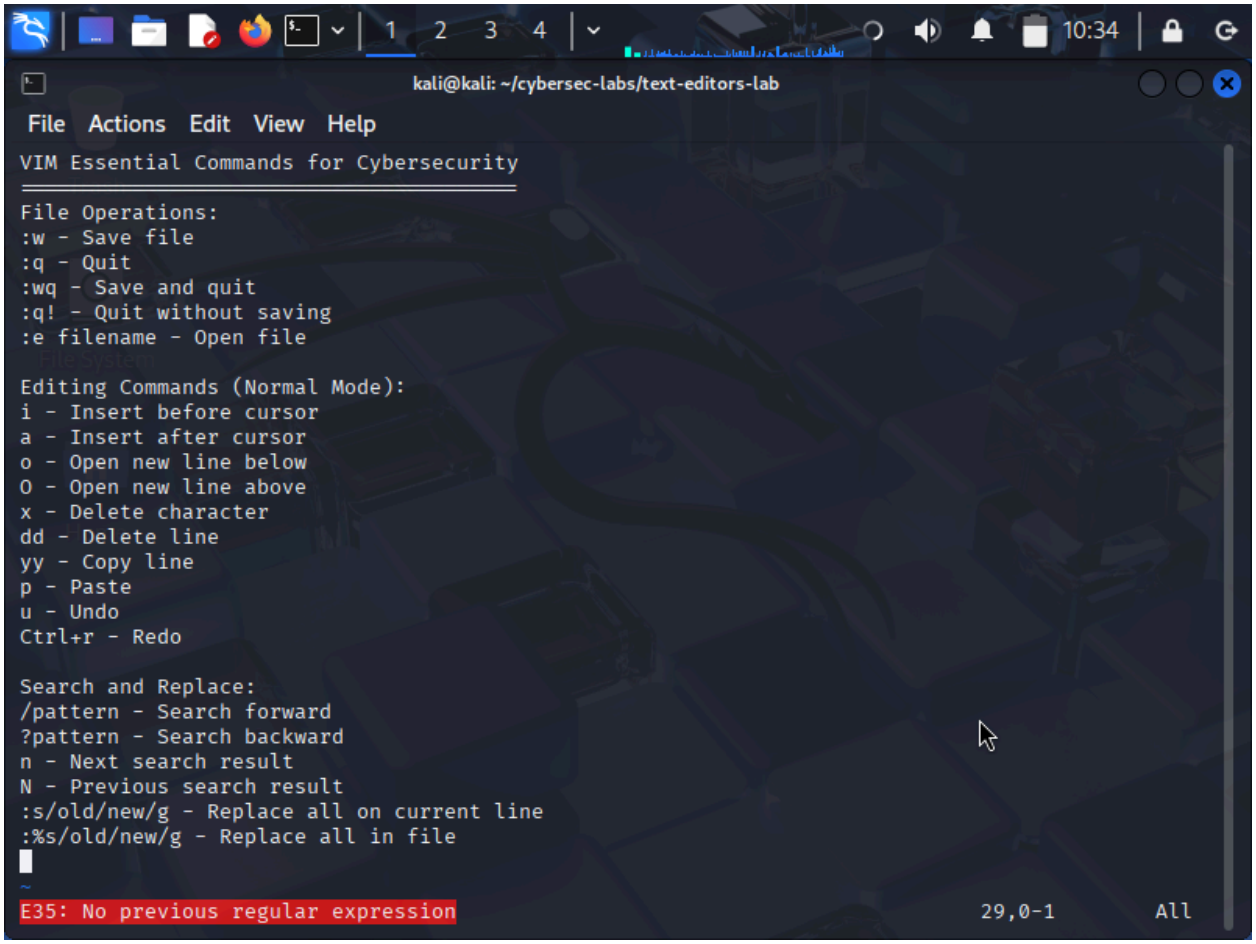
Introduction:

In this lab, I will be showing my learning process using VIM and nano. I will be able to use text editing skills for common cybersecurity tasks. Whether modifying configuration files, creating custom scripts, analyzing log files, or editing exploit code, proficiency with command-line text editors is essential. This lab focuses on practical applications of nano and VIM in cybersecurity contexts, emphasizing real-world scenarios you'll encounter in penetration testing, incident response, and security administration.

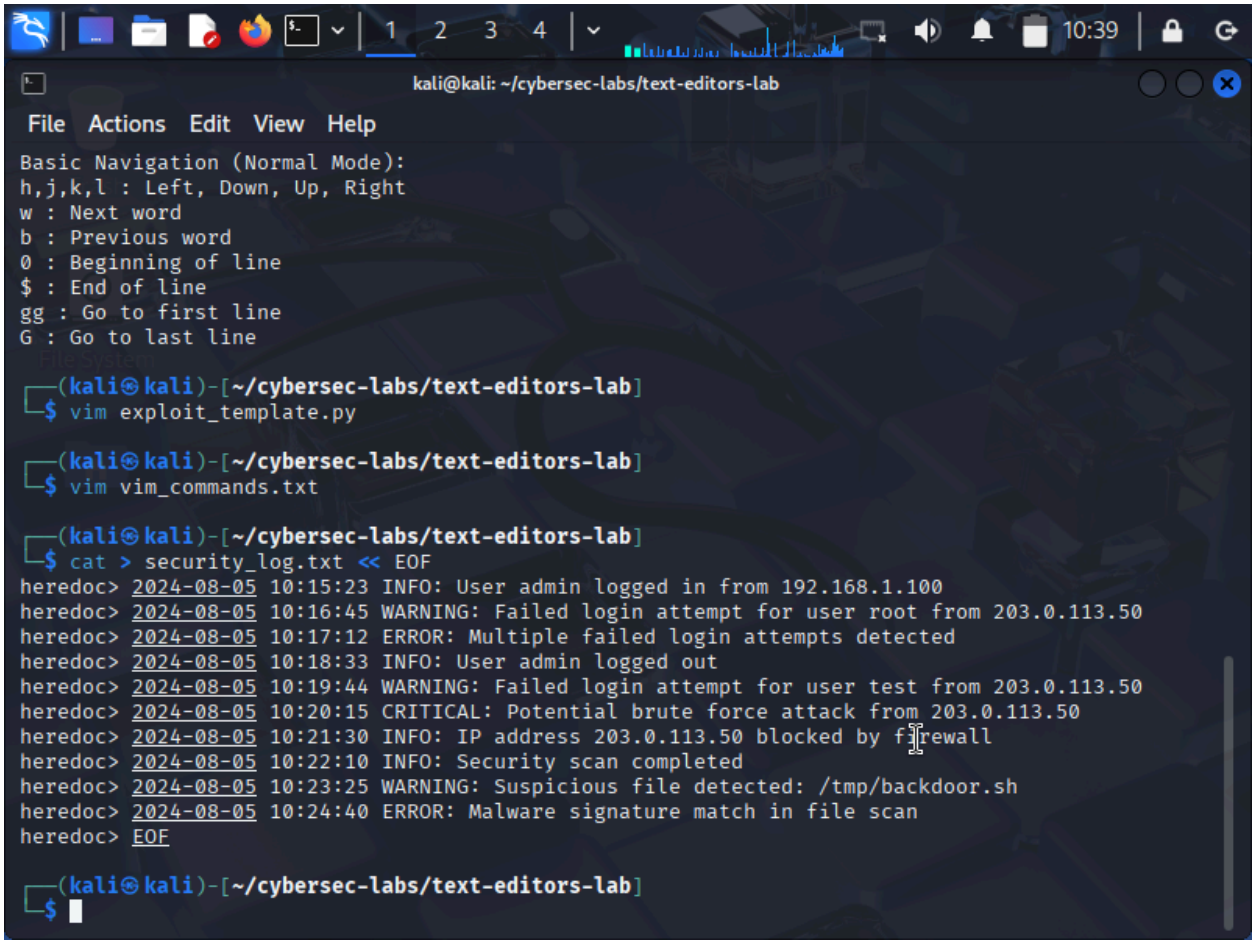
Body:



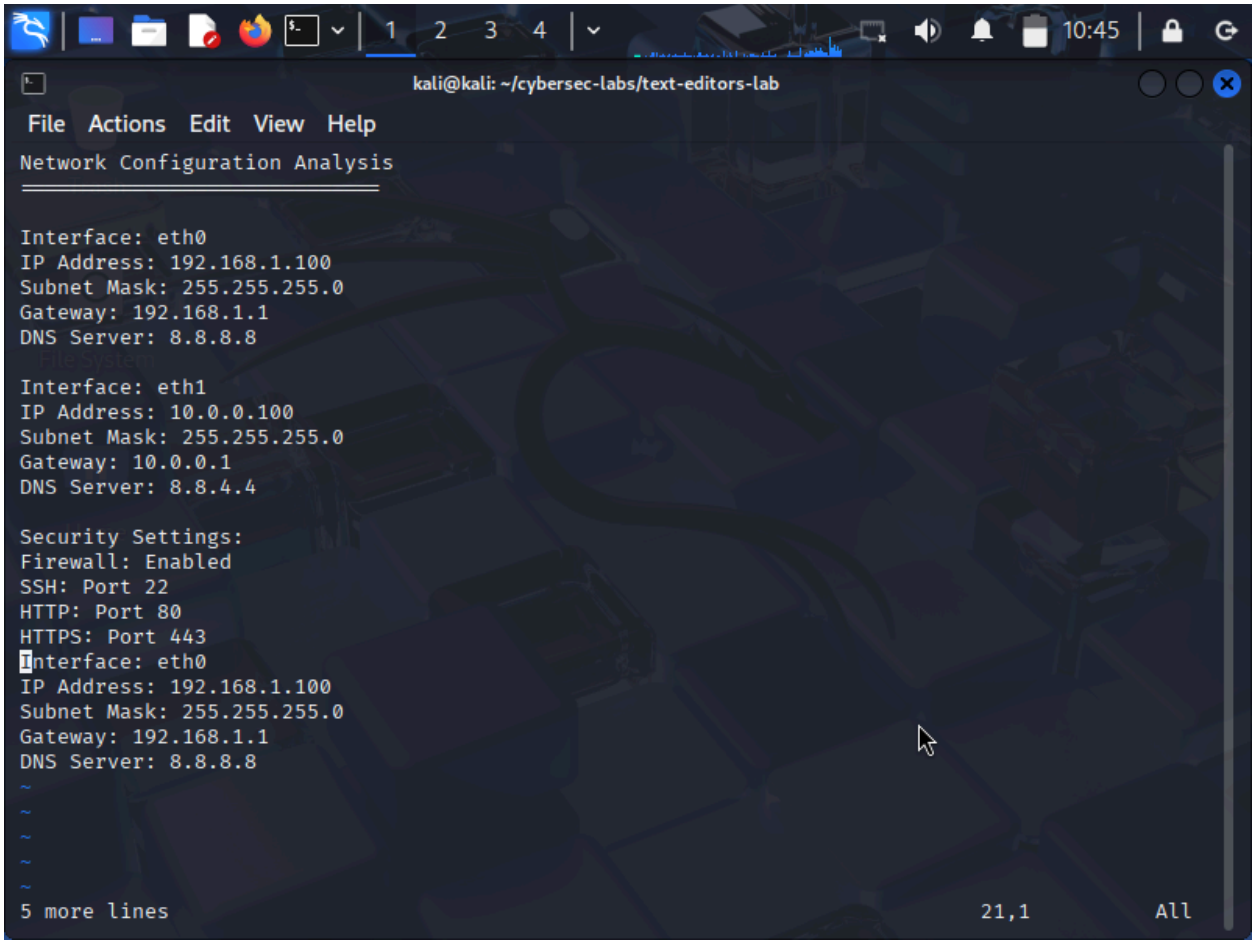
This is the first file that I have created with nano.



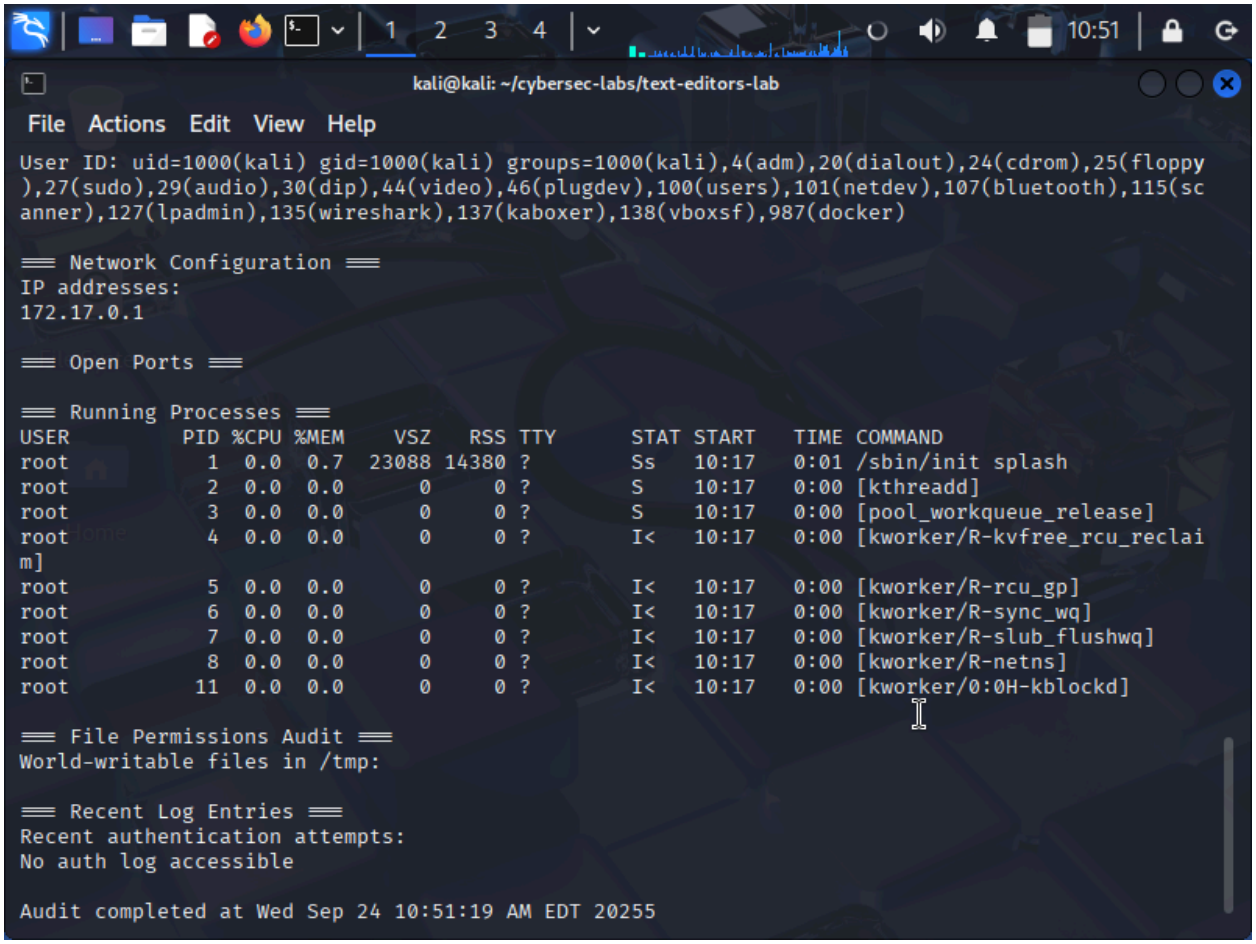
Here, I am just getting very comfortable with VIM commands. I also just completed using some VIM navigation tools.



This shows that I created a VIM for log analysis. I'm proceeding with using a few other VIM navigation tools. Then I will proceed with a few more advanced features.



This is an example of text manipulation using the VIM commands. I was able to yank five lines, copy and paste them at the bottom.



I created a security audit script in VIM. Then I made it executable. I then tested it, and everything seems to go accordingly.

Following this process, I didn't take screenshots of the following exercises. But everything went smoothly without any troubles. A list of things I completed without documenting includes creating incident response notes, creating an IOC tracking file with VIM, updating IOC's with VIM, creating a SSH hardening configuration, and creating firewall rule configurations.

Knowledge Assessment:

Question 1: True or False: In VIM, you must be in Insert mode to save a file using ":w".
False

Question 2: Which nano shortcut saves the current file?
Ctrl+O

Question 3: True or False: VIM has three main modes: Normal, Insert, and Command mode.
False

Question 4: In VIM, which command would replace all occurrences of "password" with "credential" in the entire file?
b) :%s/password/credential/g

Question 5: Which editor would be better for a quick configuration file edit on a remote server with limited terminal capabilities?
b) Nano, because it's more user-friendly and shows shortcuts on screen

Conclusion:

With the completion of this lab, I have gained a good understanding of using nano and VIM. As well as learning tools such as text editing and creating, and modifying scripts. This lab had a concentration on some real job executions, such as Configuration Management: Editing security tool configurations, firewall rules, and system settings. Incident Response: Quickly documenting incidents, tracking IOCs, and creating response playbooks. Log Analysis: Searching through large log files, extracting relevant information, and correlating events.