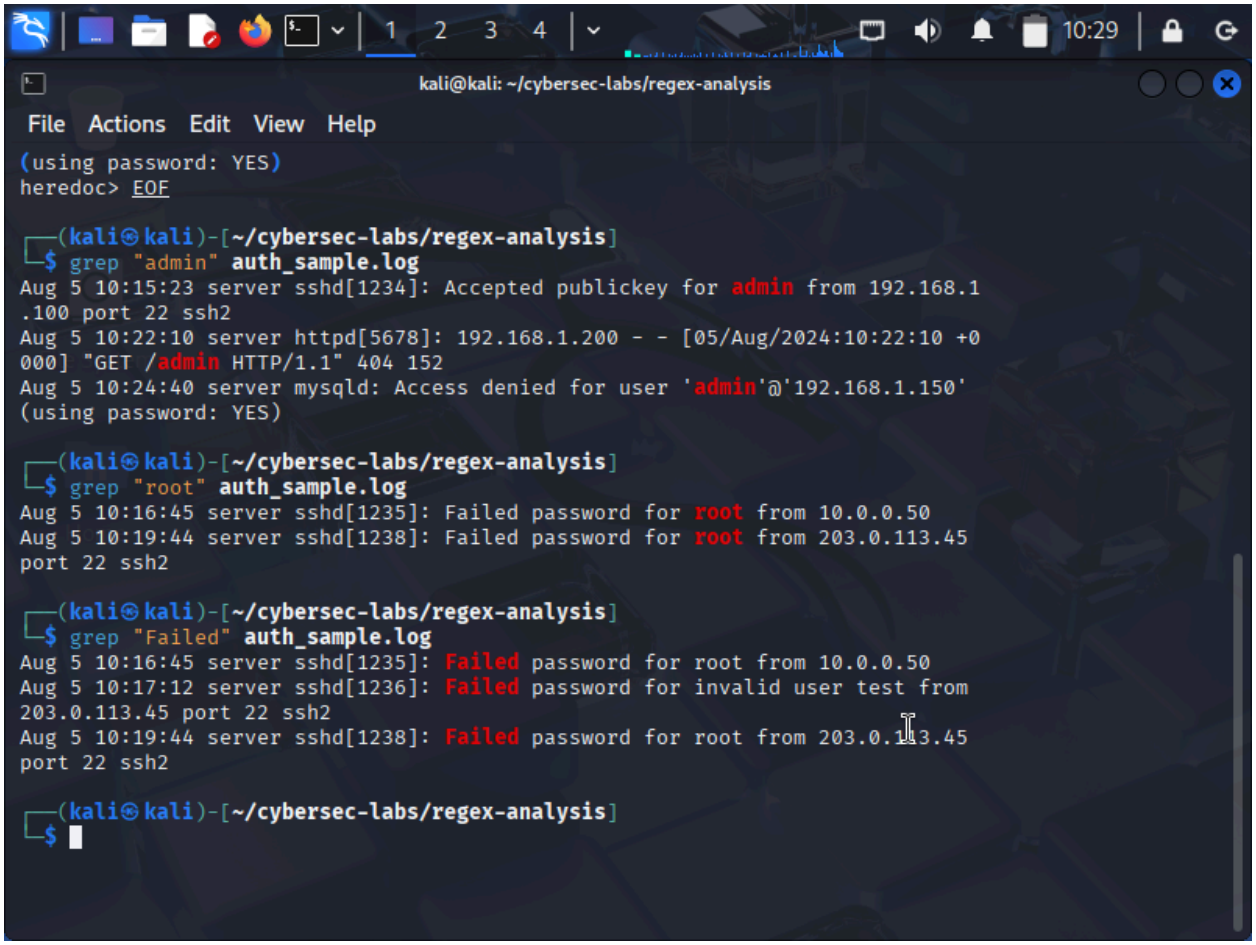
Lab 3: Linux Basics Part 3 - Regular Expressions and Log Analysis

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

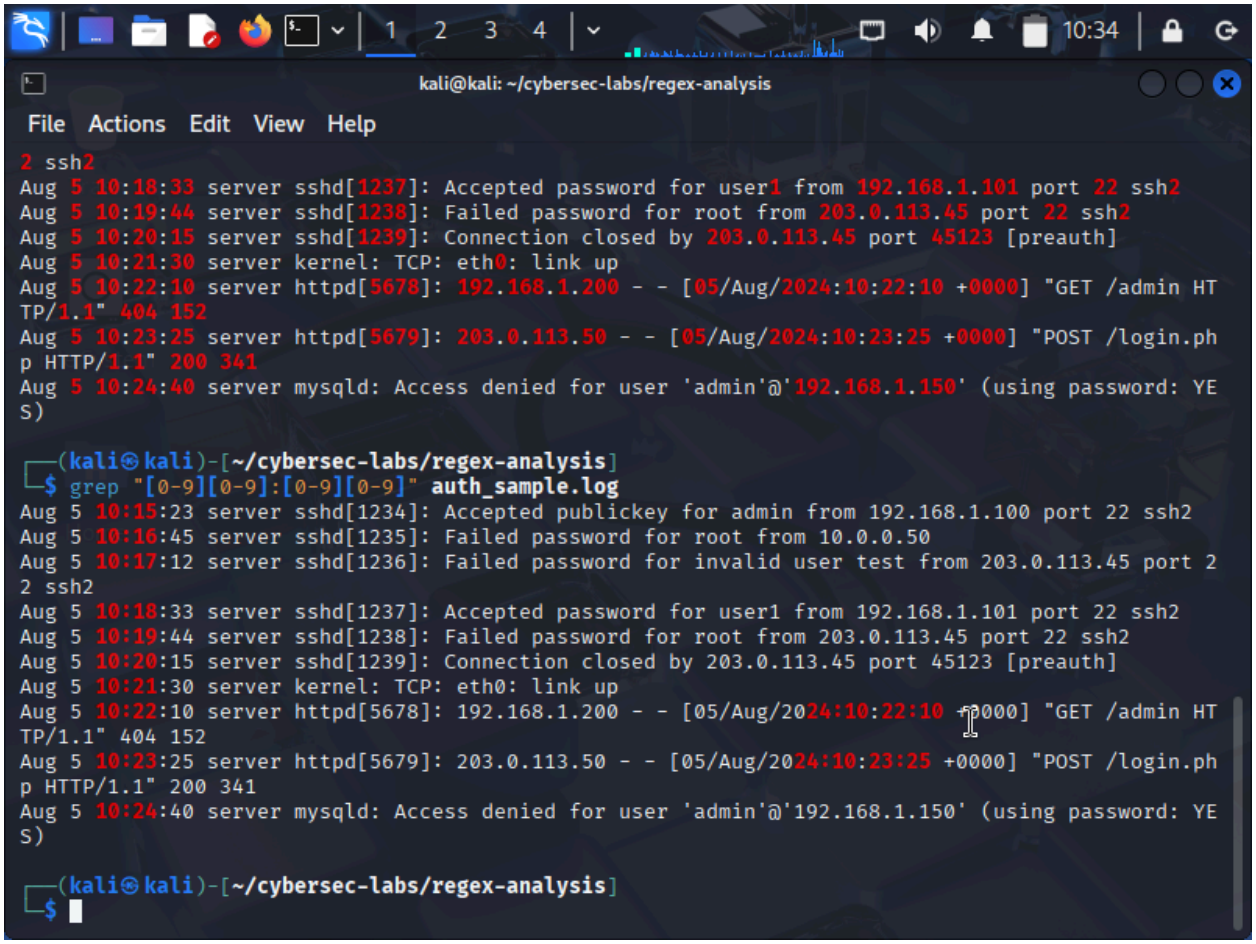
Introduction:

This lab focuses on practical regex applications, emphasizing real-world log analysis scenarios you'll encounter during incident response activities. In this lab, I will be able to understand and construct, and apply regex with grep for advanced log analysis and threat detection. I will be able to identify security-relevant patterns in log files and system outputs.

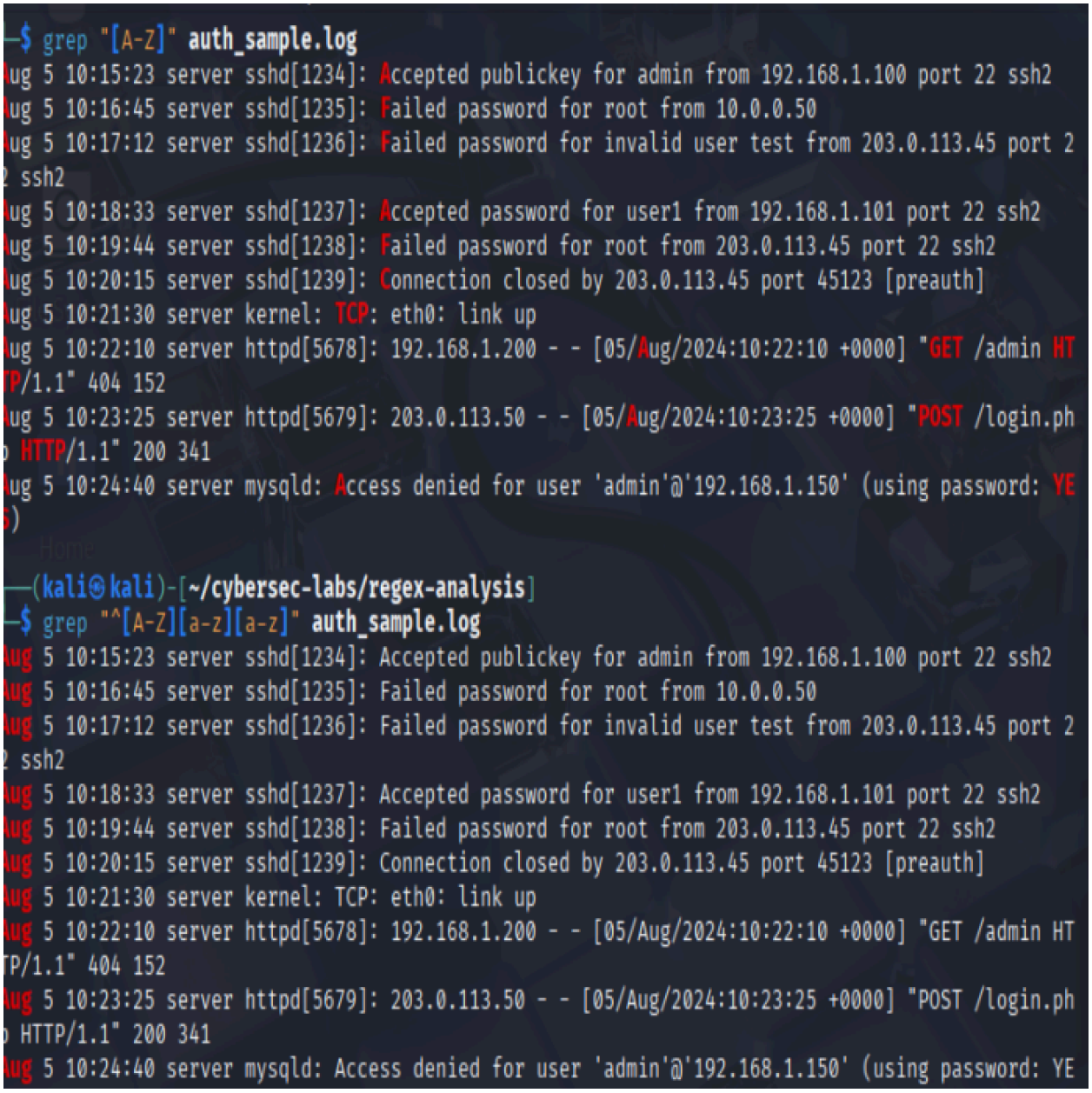
Body:



Here I was able to create a sample log file. What you are currently seeing is just some basic character matching.

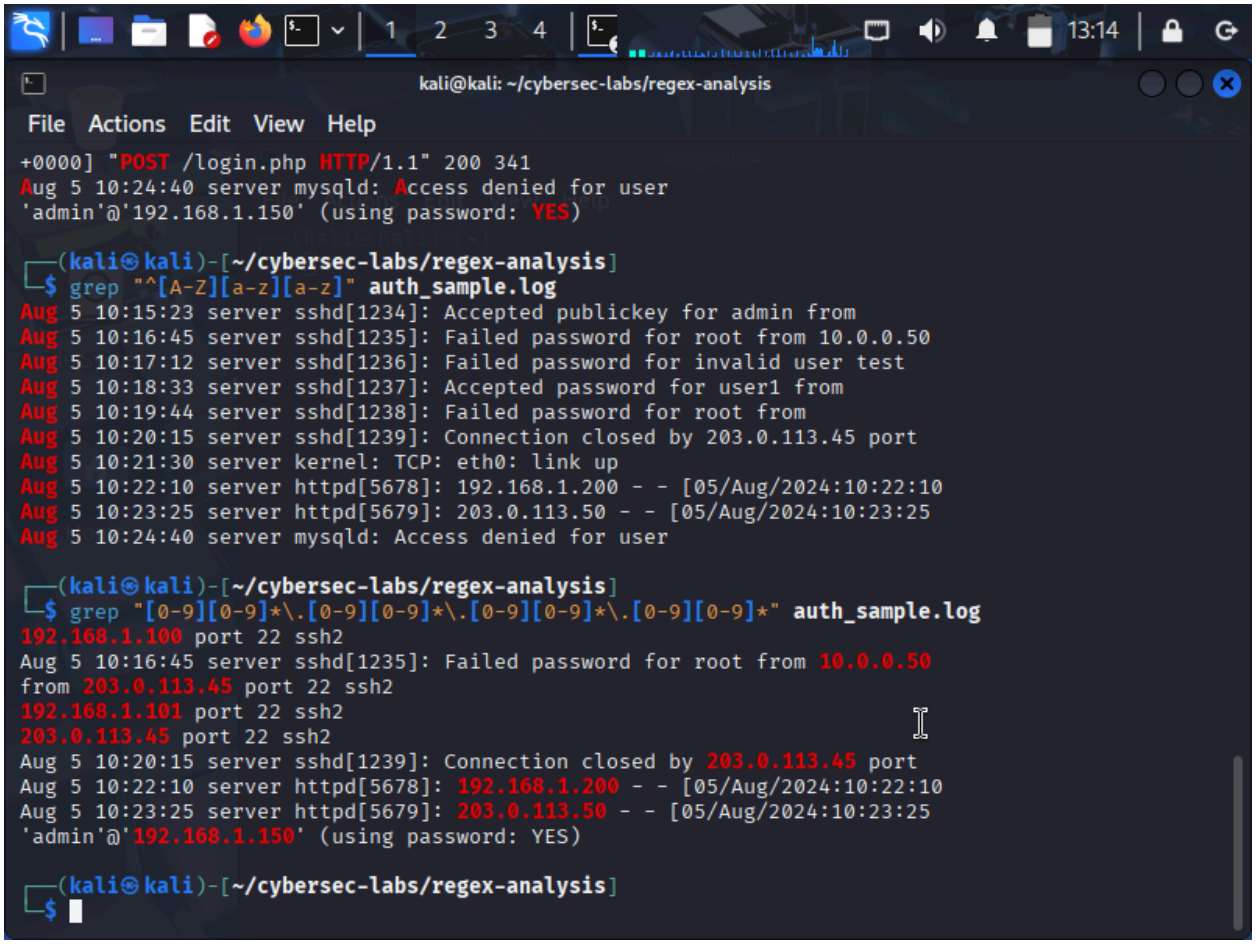


In this image, you can see a few examples of case-insensitive matching and digit matching.

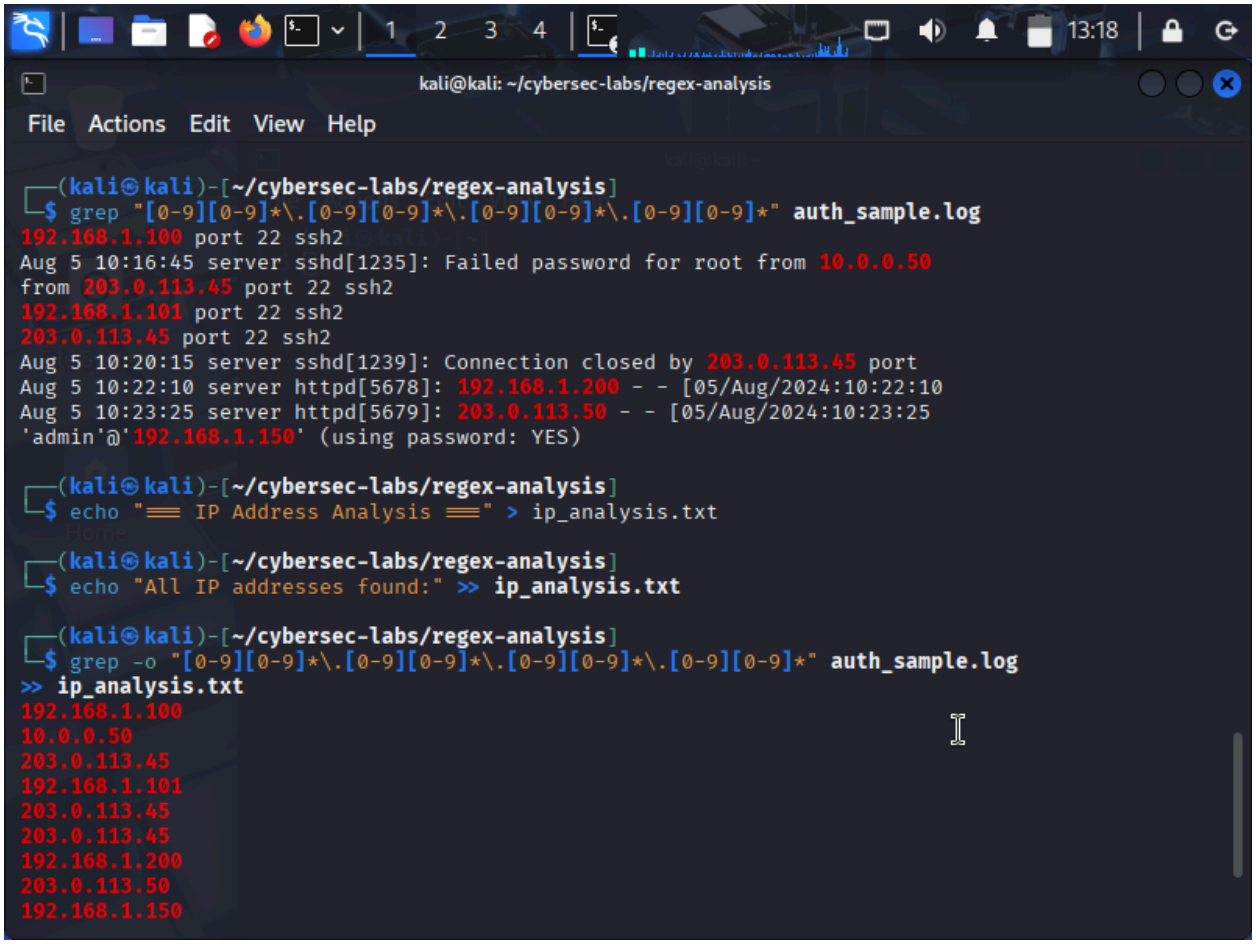


In this image, I tried a different method of taking a screenshot, just to see if it's any better than what I have previously done. But within this image, I used a letter range command that matches lines starting with three-letter month abbreviations.

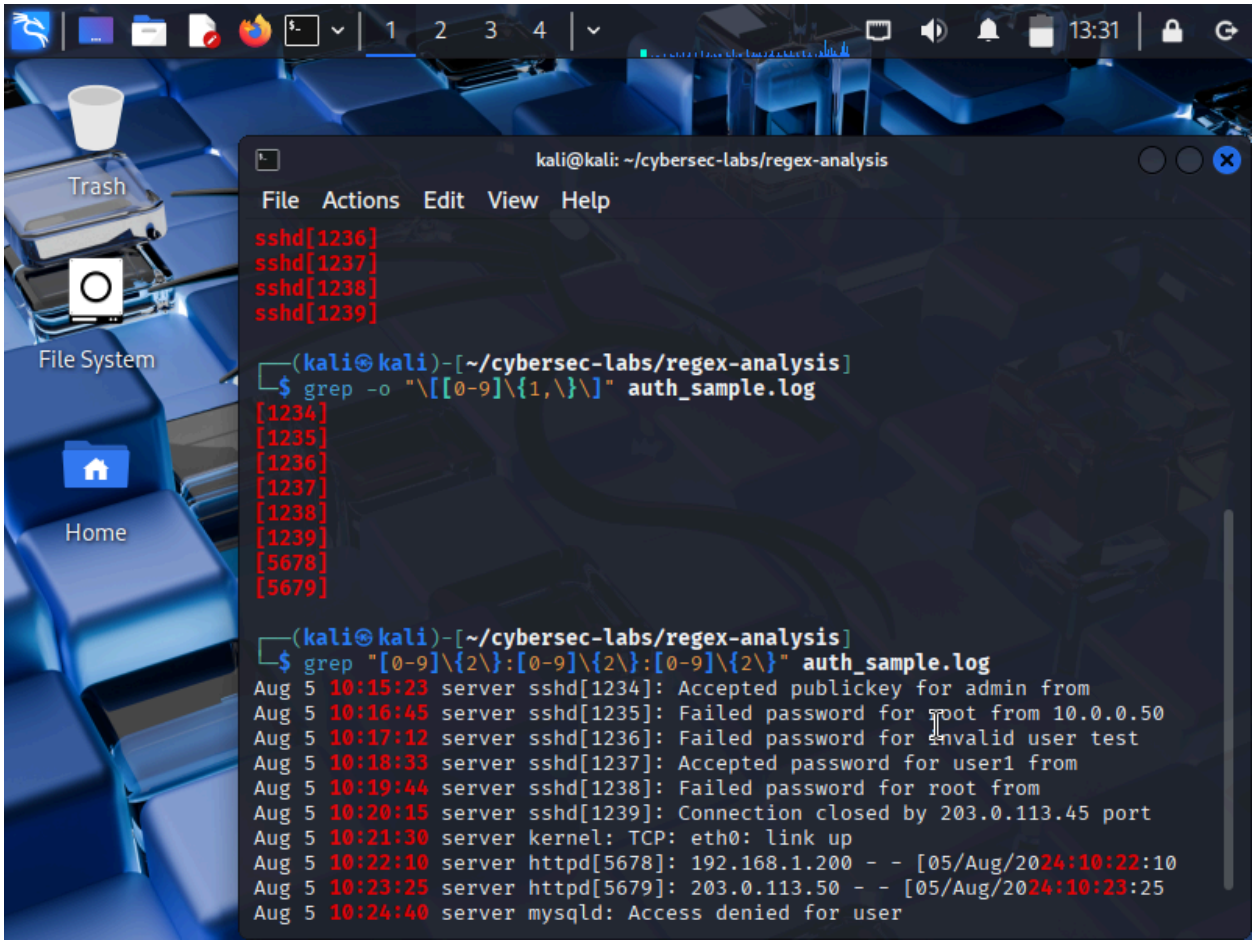
I have no clue what I did wrong here. I will try again once I can get my Kali Linux to not crash.



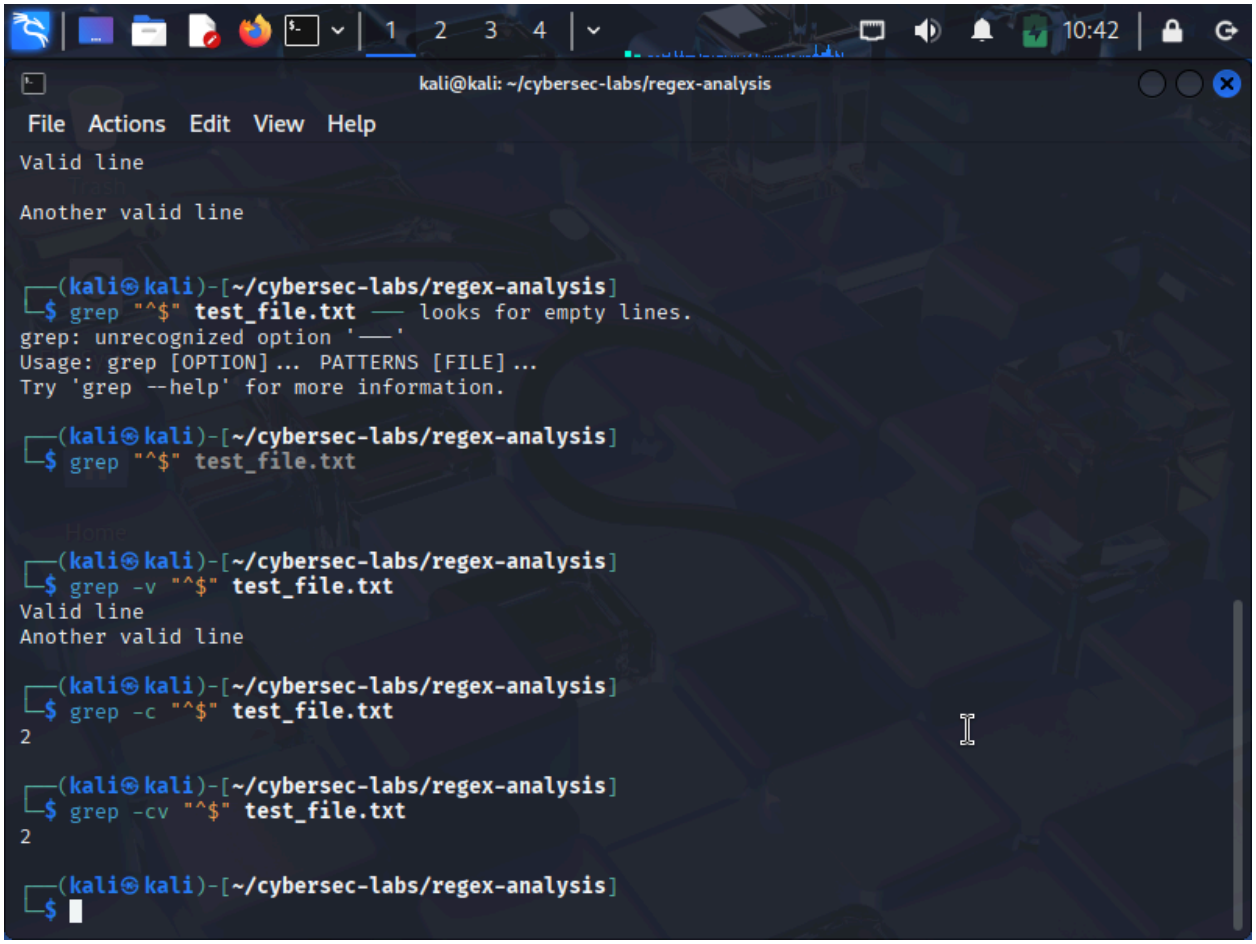
Following the previous image, I finally got it to work. I'd assume I might have missed a line within the sample log files. Or maybe it was an indentation error. But here is a successful IP address pattern matching example.



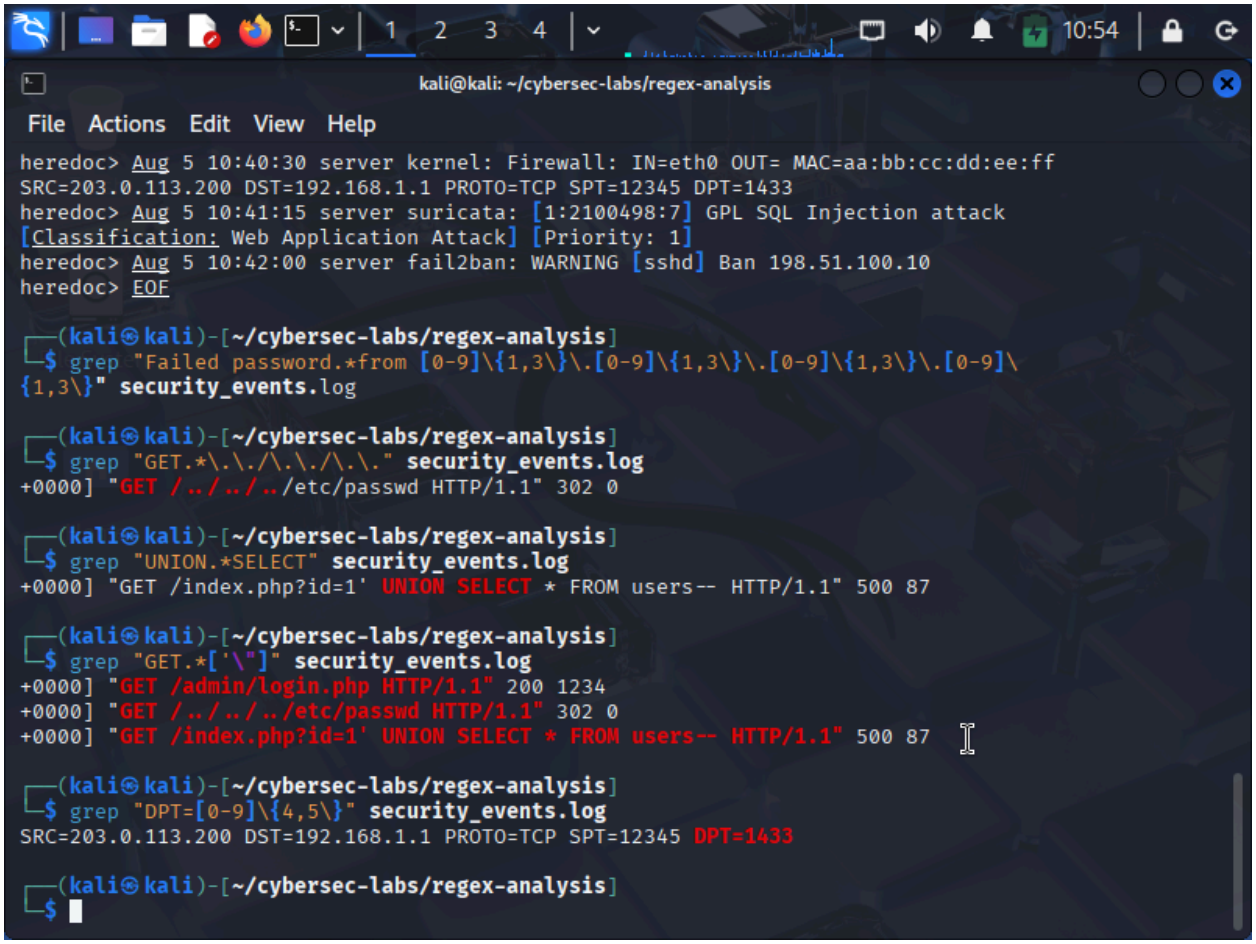
Here, I created an IP address. Now I can continue onto Exercise 3.



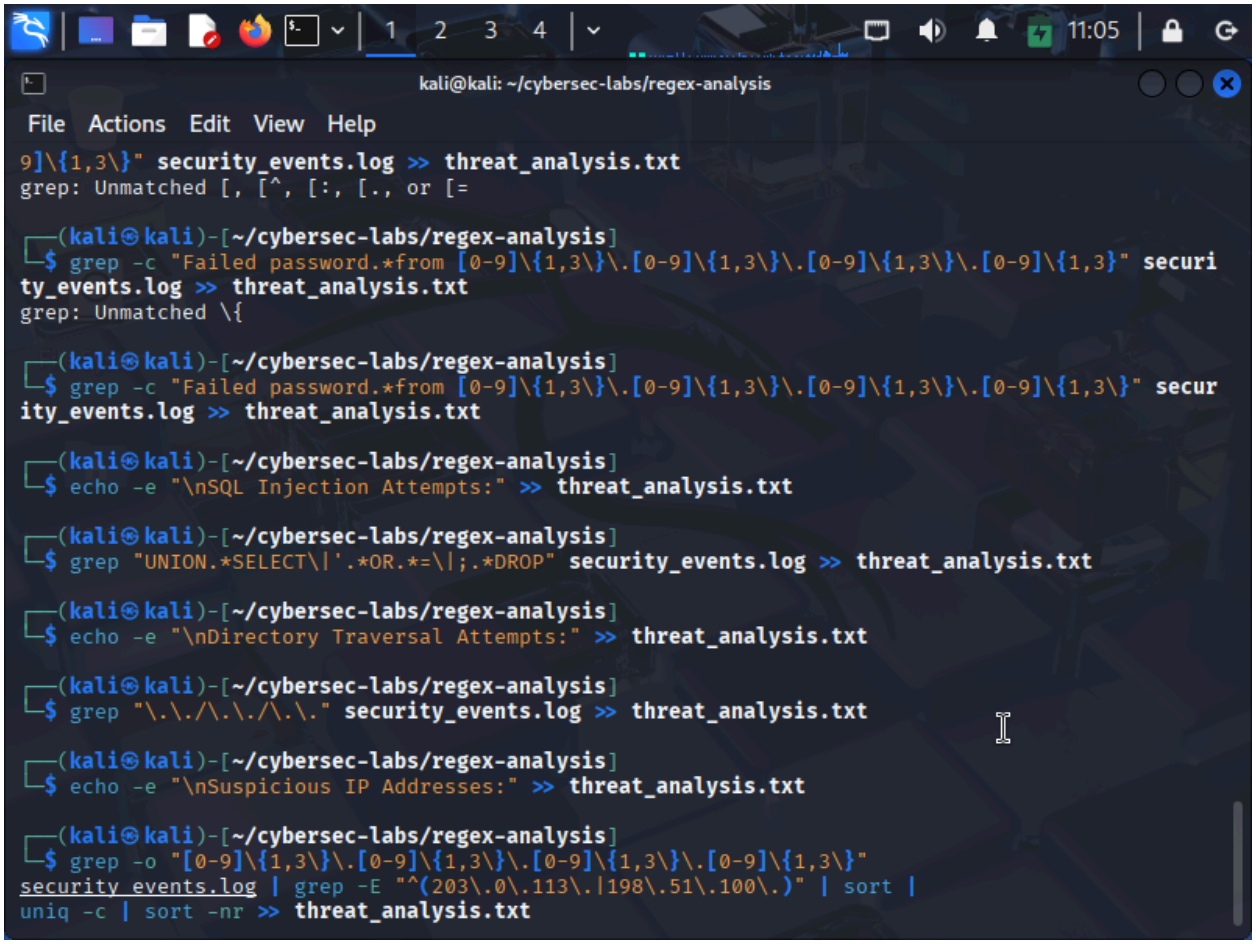
With the conclusion of Exercise 3, I was able to demonstrate basic qualifiers, process ID extraction, and time patterning successfully. I had some issues with successfully executing an improved IP address matching command. I seemed to get stuck in my terminal. But I was able to close it out and move on.



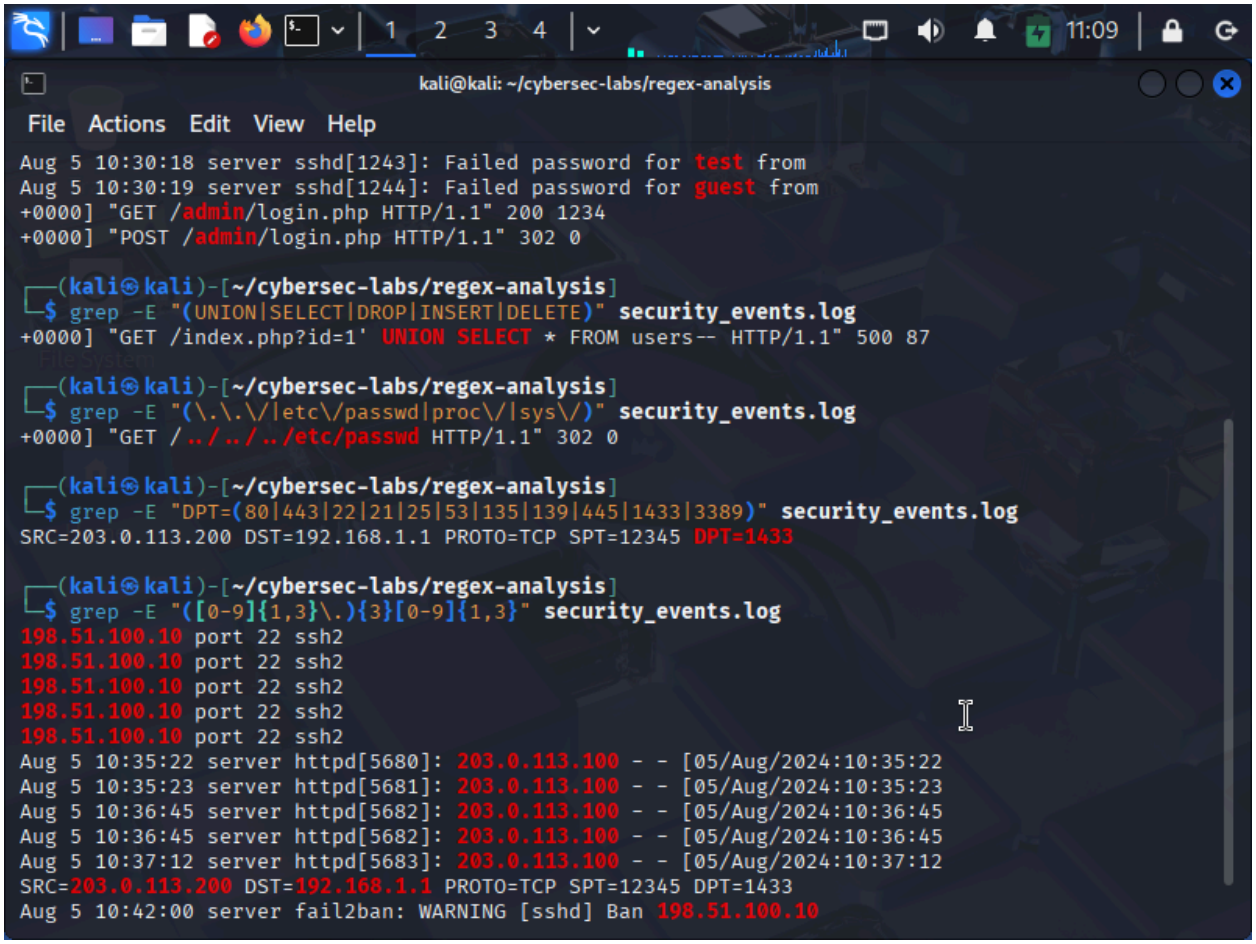
In this assessment, I was able to grab the beginning and end lines. As I went to find specific lines, I entered the command, cat test_file.txt, which then froze my Kali Linux. I think it was just a goof. I was able to eventually close out Kali and reboot it. As you can see, I got it just fine the second time around.



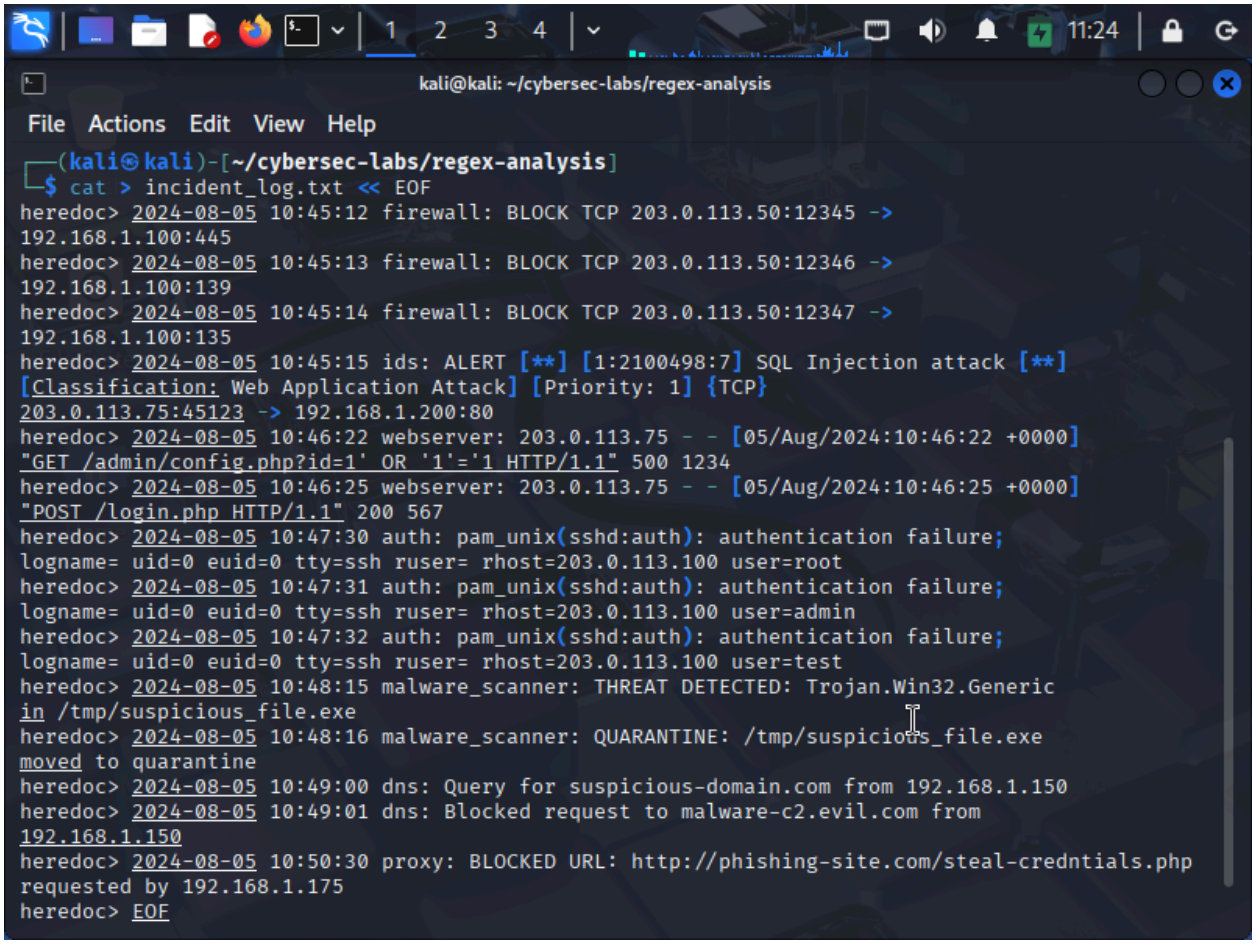
I created a comprehensive security log successfully. Didn't seem to have any goofs this time. I got all of the correct outputs when running various detections and scans.



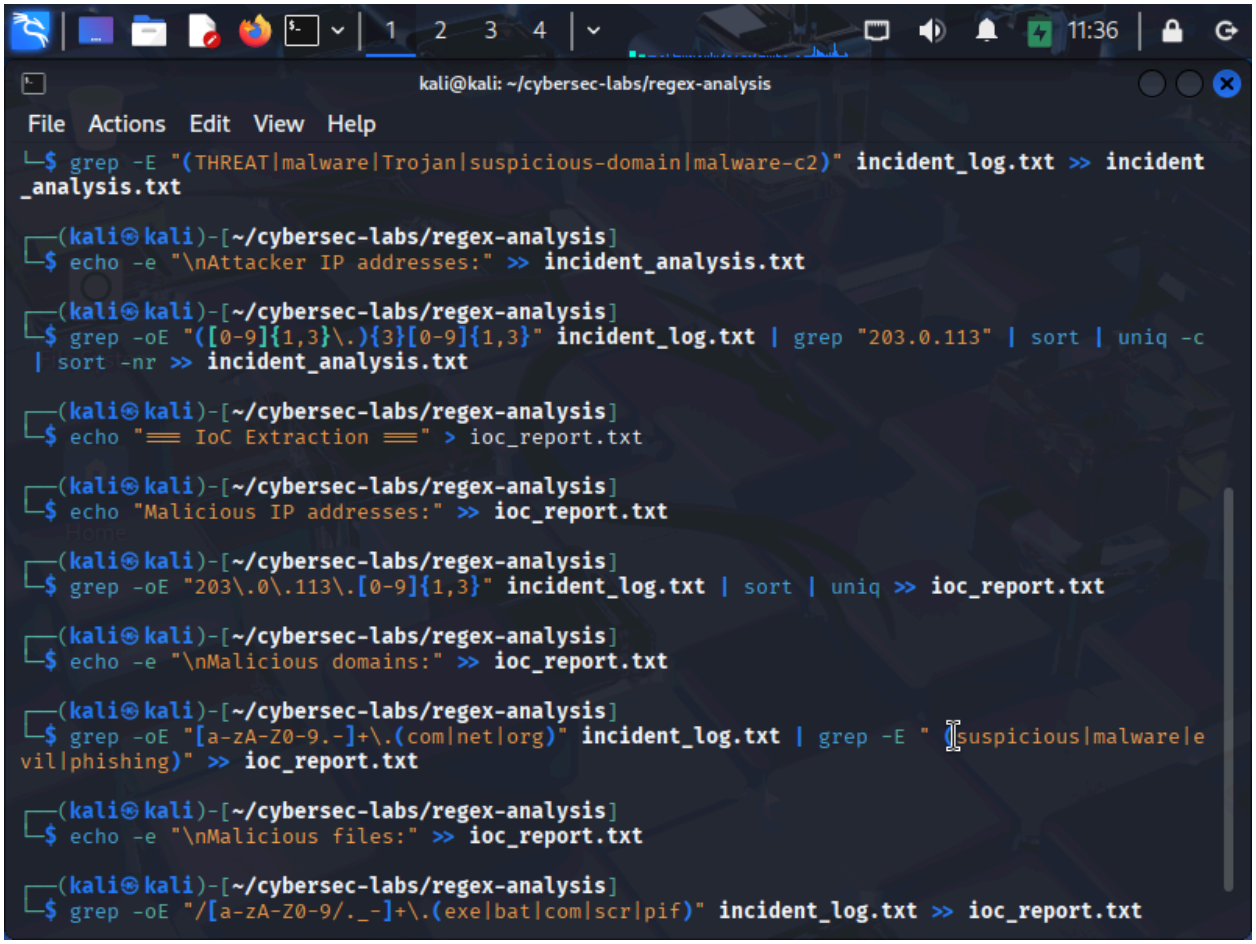
Above, I created a comprehensive threat analysis. I had a couple of spelling issues with the failed password command, but eventually figured it out.



In this screenshot, I can present a few matching commands. I ran an alternative, multiple-stack pattern detection, port range, and complex IP pattern matching commands. These were the steps before creating an advanced log parsing and an incident response log.



Here is my very extensive incident response log. Now it is time to see if I executed this correctly.



I have successfully created the incident analysis and IOC extraction. Therefore, my incident response log was successful. I had no issues. With the conclusion of that exercise, I have completed the lab.

Knowledge Assessment:
Question 1: Which regex pattern would match IP addresses in log files?
b) [0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}

Question 2: True or False: The regex anchor ^ matches the beginning of a line.
True

Question 3: Which grep command would find all lines containing either "Failed" or "Denied"?
b) grep -E "(Failed|Denied)" file.log

Question 4: What does the regex quantifier {2,5} specify?
d) Both b and c are correct

Question 5: Which regex pattern would detect potential SQL injection attempts in web logs?
d) All of the above

Conclusion:

With the completion of Lab 3, I have greatly developed my regex skills. I am now very familiar with running scans and detections such as incident response, threat hunting, and security operations. I now have more interest in specific jobs such as Incident Response Investigator, Digital Forensic Investigator, and Penetration Tester. These skills from this assessment will greatly impact my job search and desire to expand my interests.