LinkedIn: Kelvin Kimotho

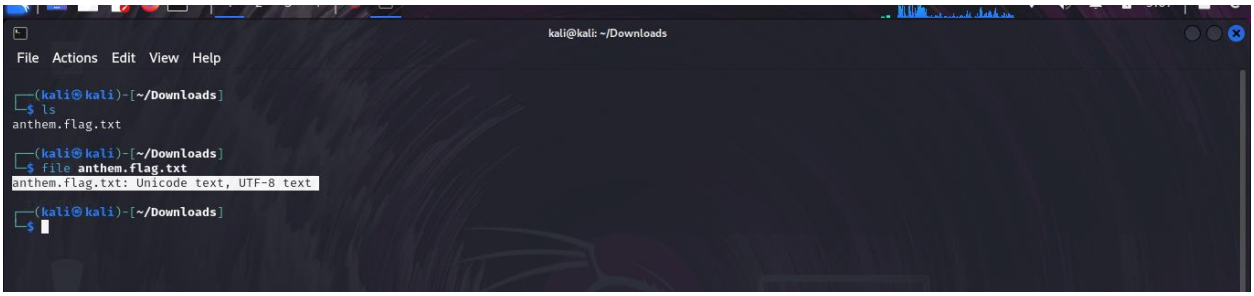
Description

The challenge provided a file titled anthem.flag.txt, with a hint: *"Download the file and search for the flag based on the known prefix."* This suggests that there might be a hidden flag within the file, and the flag is likely in a specific format commonly used in Capture The Flag (CTF) challenges in this case, the flag likely begins with the prefix picoCTF{.

The task was to extract the flag from the large dataset hidden within the file. Here's a detailed explanation of the steps I took to solve the challenge

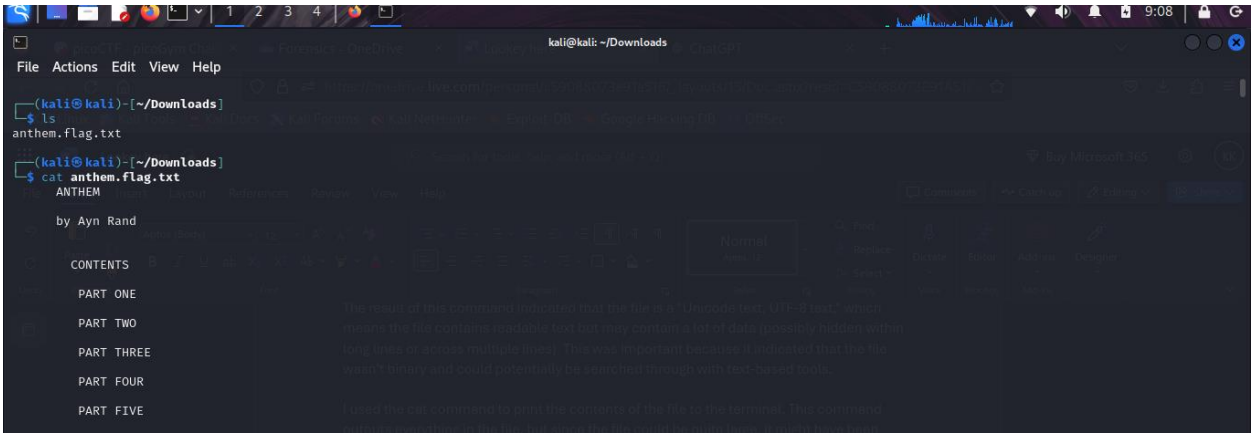
Solution

After downloading the file (anthem.flag.txt), I first checked its properties using the file command to understand its format:



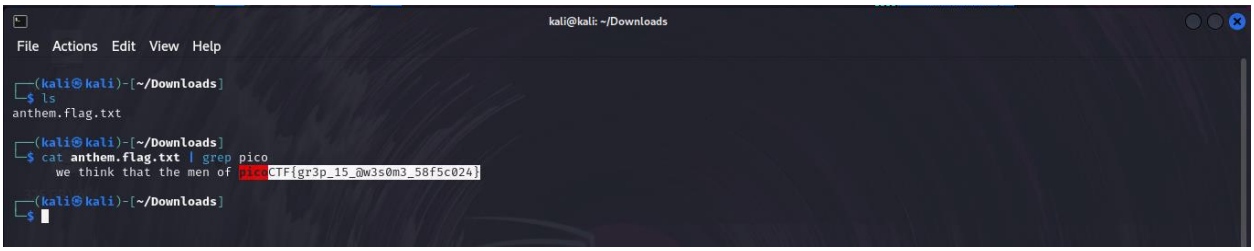
The result of this command indicated that the file is a "Unicode text, UTF-8 text," which means the file contains readable text but may contain a lot of data (possibly hidden within long lines or across multiple lines). This was important because it indicated that the file wasn't binary and could potentially be searched through with text-based tools.

I used the cat command to print the contents of the file to the terminal. This command outputs everything in the file, but since the file could be quite large, it might have been inefficient for thorough examination.



I used the grep command to search for any occurrence of the prefix "pico" within the file. grep is a powerful command-line tool that searches for patterns in files.

This command searched the entire file for the string pico. The output returned the following:



I now had the full flag, and this was the solution to the challenge.

Conclusion

This challenge tested the ability to search through a potentially large file for a hidden flag based on a known prefix. By utilizing basic Linux commands such as cat and grep, I was able to locate the flag efficiently.