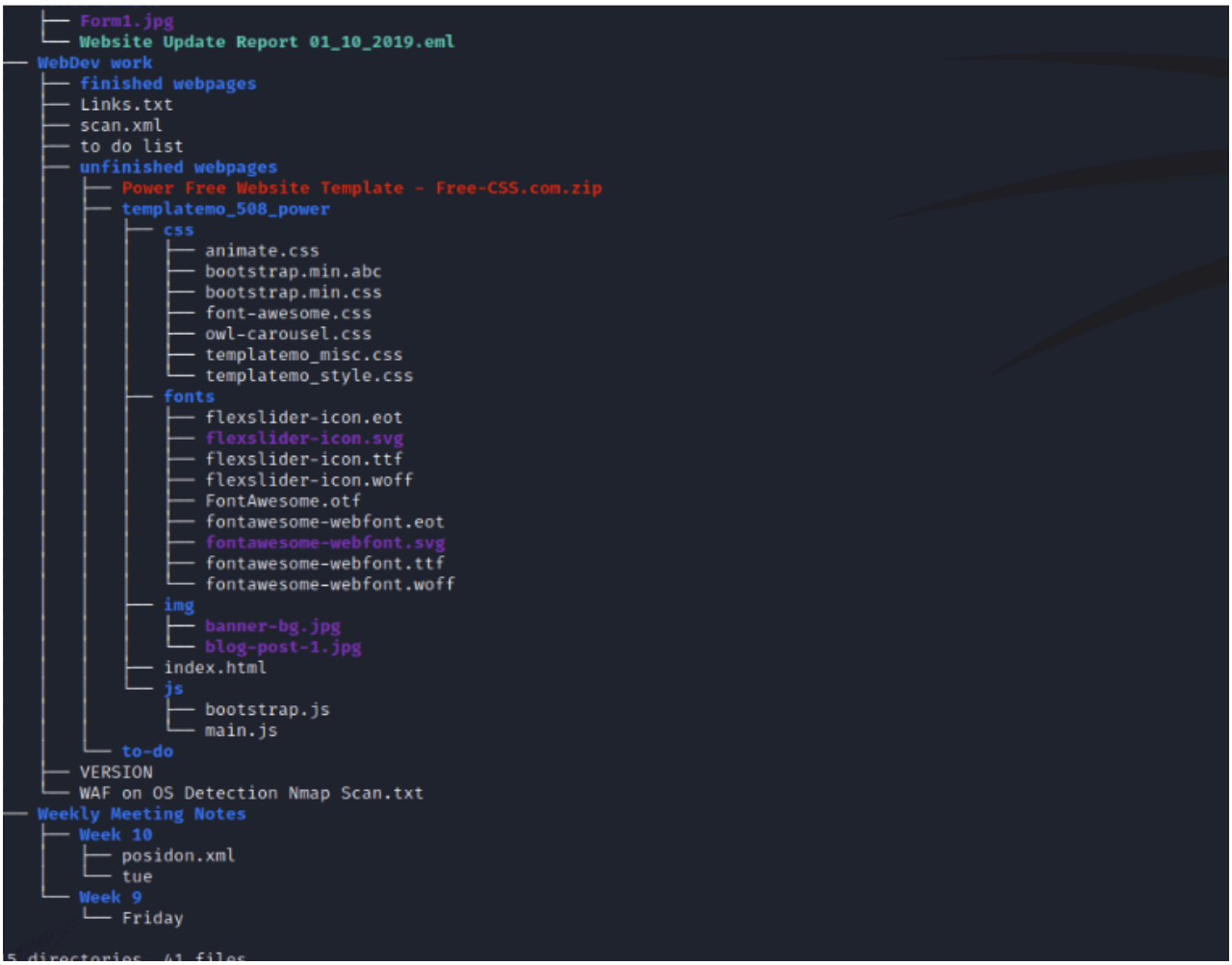
Digital Forensics

- The SOC has received an anonymous report that a user is potentially exfiltrating data from the company. An image of the user's hard drive has been taken, and you are responsible for analyzing the contents of a perfect copy to find any evidence of malicious activity. You have been told that the most recent file on the hard-drive was an email file with an attachment in the "Saved Emails" directory. It is suggested you start there.

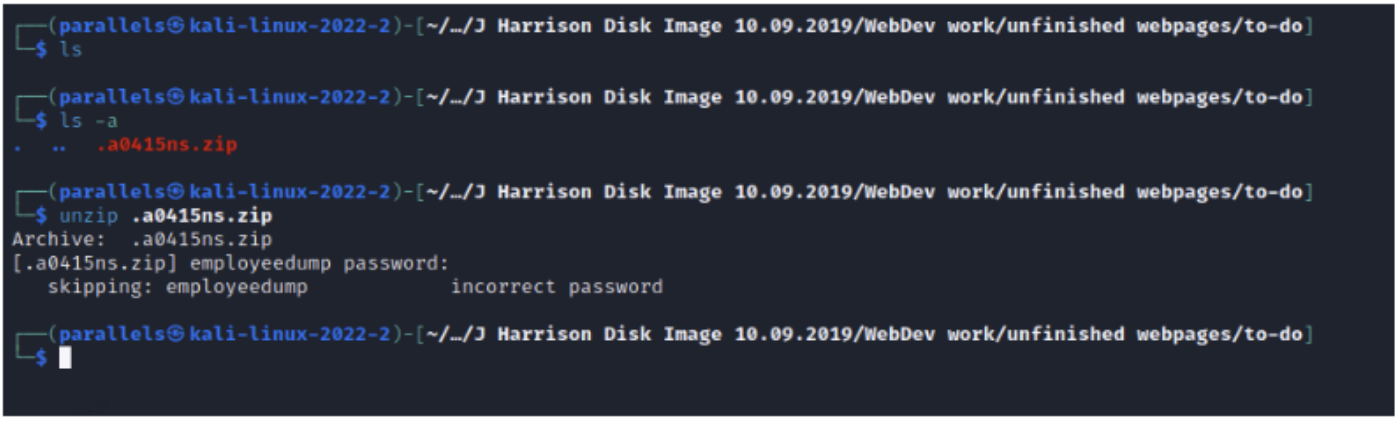
1. Initial File System Analysis for Evidence Location

To begin locating evidence, I started by examining the entire file system of the folder using the tree command. This command helps me see all files and folders, giving me a clearer idea of where important information might be hidden.



2. Discovery of a Hidden, Password-Protected Archive

After carefully going through the "Disk Drive" for a long time, I noticed an empty folder named to-do. At first glance, it seemed to have nothing inside. However, by running the ls -a command (which shows all files, including hidden ones), I discovered a hidden zip file within it. I tried to open this zip file, but it was protected by a password.



3. Accessing Sensitive Data: The Employee Dump File

To open the password-protected zip file, I used a tool called fcrackzip. This tool helped me bypass the password protection. Once the zip file was open, I found a text file inside named employee dump. This file contained personal information belonging to employees, which is highly sensitive and should not have been stored on this user's device.