CASE SCENARIO:

As a new Forensics Investigator, you have been contacted by relevant authorities and tasked to extract and analyze a rookie hacker’s workstation.

The relevant authorities were tipped off in an anonymous phone call that a man Terry Lee has been stealing money from people's bank accounts and his residence. Upon contacting several bank companies, one bank company, TBS, said that the suspect was found with suspicious internet activity on their new payment website, with multiple transfers from different users to his bank account.

The hacker is suspected of stealing vulnerable account credentials and wiring money to himself. When the authorities raided Terry Lee's fdddhouse, they managed to retrieve his laptop in a faulty state

The desired goal is to figure out whether the transfers were legitimate, and if not, to retrieve the compromised accounts suspected to be stolen by the hacker, and to notify the victims of this breach of privacy, in the event that their account details were circulated to other hackers or sold on the dark web.

SUGGESTED DEMO:

VOL

1. find website to download a keylogger? (smth that can steal passwords) smth like (spyware.com)

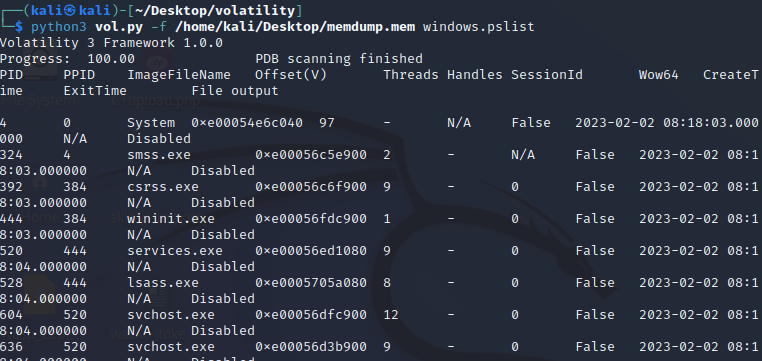
2. find active process of what he downloaded

3. extract zip file from memory (use password: W0wz1pp4ssw0rd) -> zip file contains compromised user credentials

"how can i set up a test environment to map a file into the memory such that i can extract files from the memory using volatility? provide the commands needed to set this up in kali linux"

Graphical user interface, text

Description automatically generated



Text

Description automatically generated

Graphical user interface, text

Description automatically generated