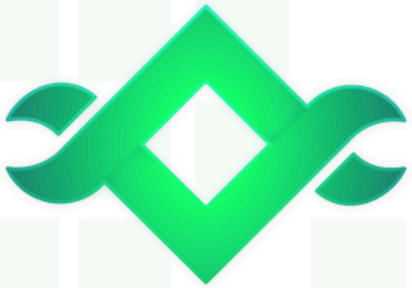


TDX ARENA

Certification Report

Araseli Serrano
Final Assessment Report Submission

Case: Imperial Memory

12.18.2024

Executive Summary

During a gathering, a cyber researcher hinted they would give me his “Secrets of Success” on my desktop. After opening the desktop I discovered some files including a password protected file. Included was a memory dump file which seemed to have some cryptic clues that would later help me get access to the archive file.

The challenge was to analyze the dump file and extract data to search for clues that would later unlock a series of files including the cyber researcher’s “secrets to success”

Findings and Analysis

Finding	Finding Details	Description
User	Jules	The name of the end user is Jules.
Strings	strings Emperor.vmem | grep -E 'password|gift|7z' > output.txt	This command was customized to extract any readable text in the dump file to reveal any clues containing keywords.
File	/home/derrek/Desktop/gift.7z	This is the path to the archive file that was password protected.
TCPdump file	Emperor.vmem	This dump file contained many cryptic contexts and clues that later led to the finding of the password for suspicious.docx.
Previous Host	\Users\Aaron\Desktop\gift.7z	It seems that the archive file was originally on the desktop of a previous user named Aaron.

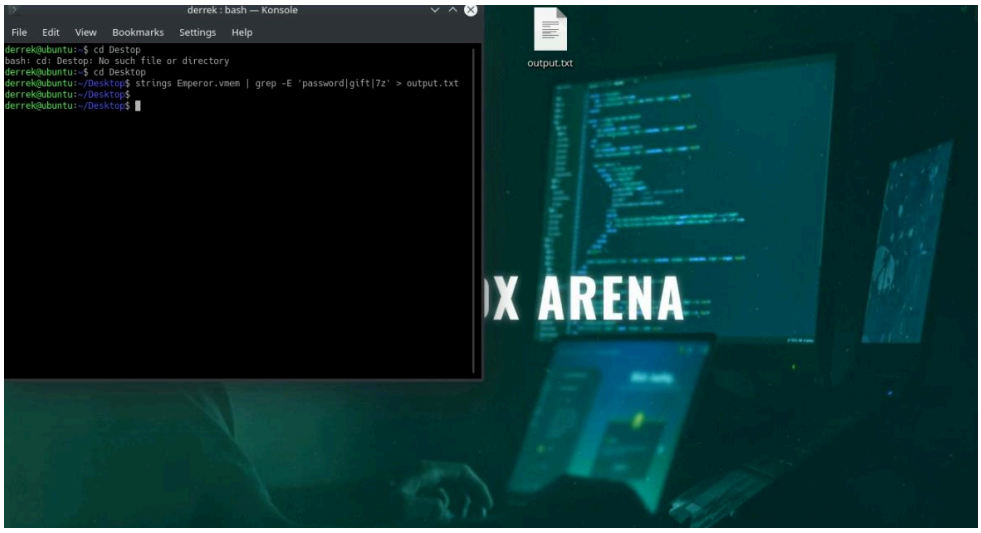
Methodology

Tools and Technologies Used

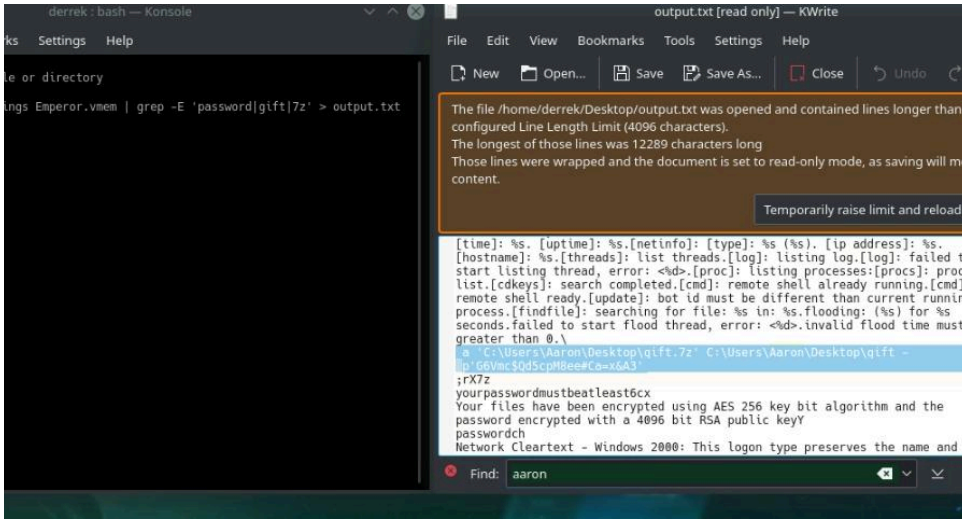
- **strings**: strings command is to scan specific sequences of printable characters.
- **grep:** grep helps filter out specific strings by customization.

Investigation Process

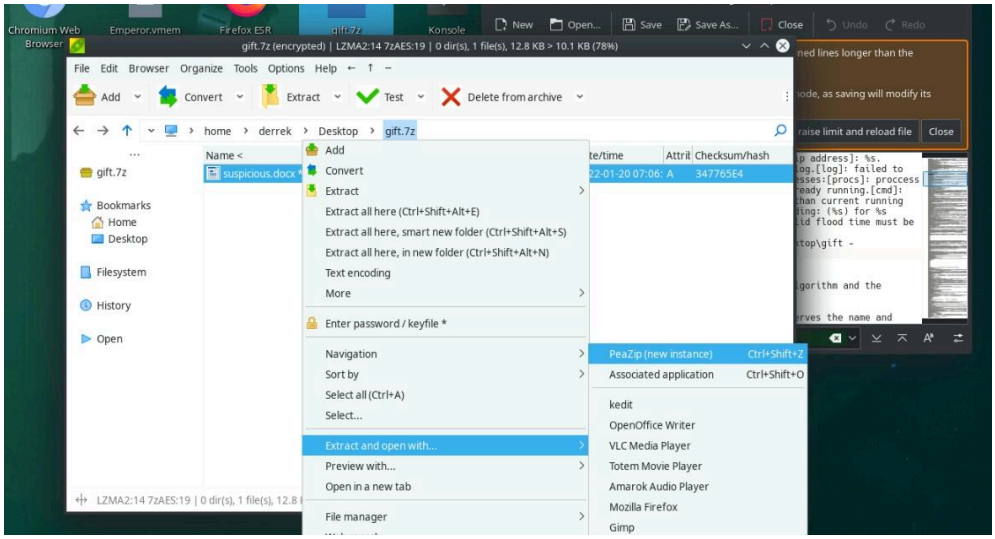
1. I started by extracting all readable text in the dump file that contained keywords i.e. password,gift, and 7z.



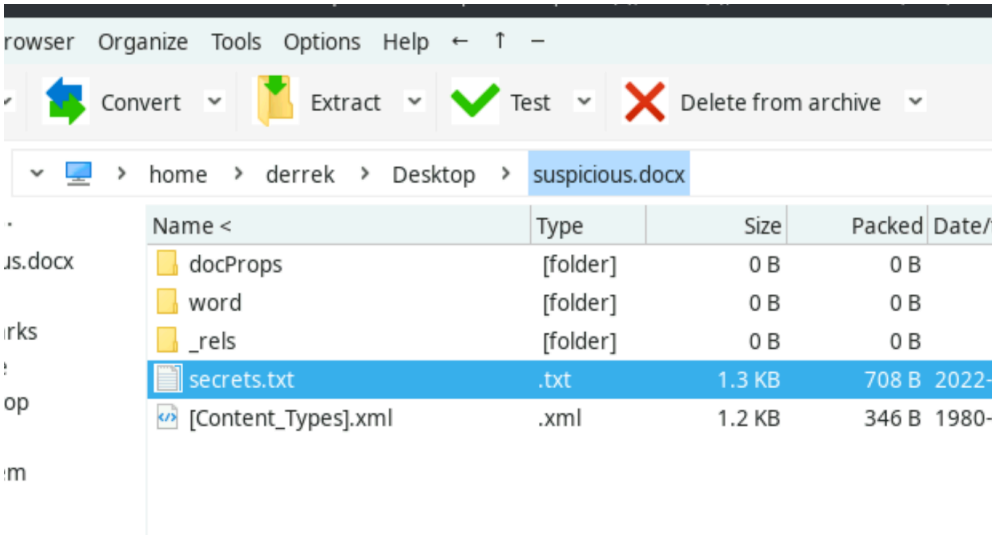
2. After looking inside the extracted text I searched for clues and potential passwords for gift.7z.



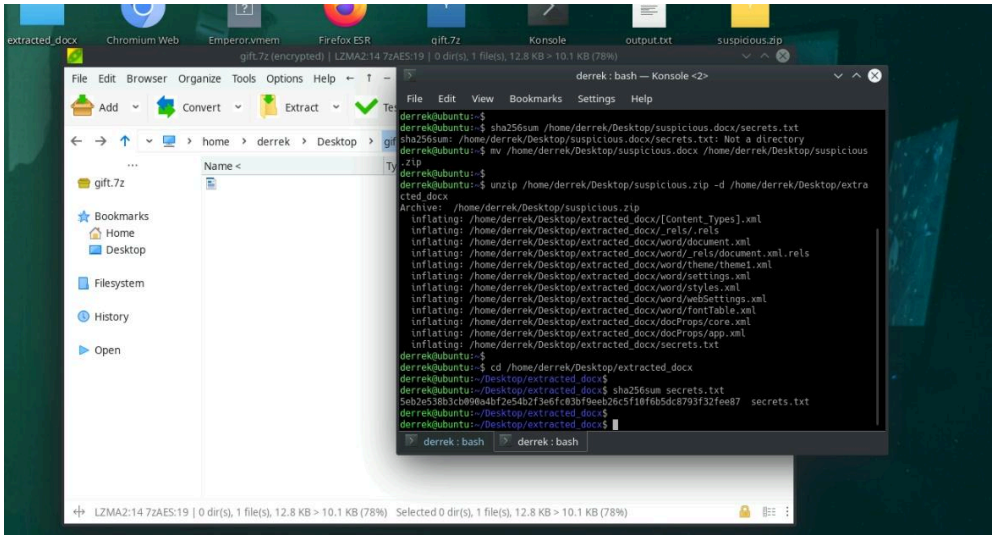
3. I was able to get access but the file was empty, so I extracted and opened it with PeaZip.



4. New files were displayed including secrets.txt which was the file containing the “Secrets of Success”.



5. After the file was found we used sha256sum to retrieve the flag ID.



Recommendations

Based on the findings, it is recommended to:

1. Using the strings command in large files can help filter out what you are looking for along with grep.
2. The use of memory forensic or memory dump analysis can uncover hidden information in systems.
3. Continue doing deeper analysis and more attention should be given to docx or zip files as they might be hiding important information.