TDX ARENA

Lindsay Anson
Final Assessment Report Submission

Final Assessment Report Submission
Case: Imperial Memory
Date: 2024-11-27

Executive Summary

This Capture The Flag (CTF) presents a scenario where a cyber researcher, Jules, leaves a farewell gift on your desktop – a password-protected archive named 'gift.7z' containing a DOCX file. The challenge is to find the password, analyze the DOCX file, and uncover Jules' secrets.

The password is found within a virtual machine's paging file ('Emperor.vmem') using the 'strings' command and searching for specific keywords.

The extracted DOCX file appears empty, but reformatting it to '.7z' and unzipping reveals a hidden text file named 'secrets.txt'. The MD5 hash of this file is the desired flag.

Findings and Analysis

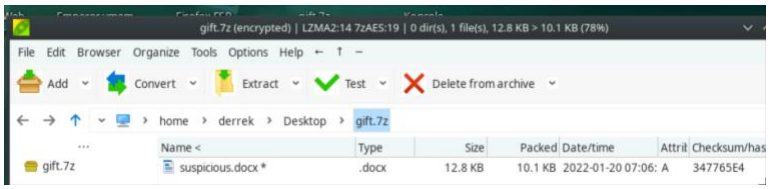
- Strings: A command-line tool used to extract text strings from binary files.
- Volatility: A Python-based forensic tool used for analyzing volatile memory (RAM) dumps**.**

Methodology

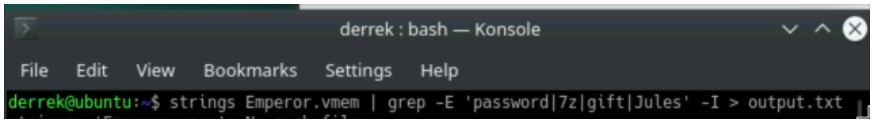
Tools and Technologies Used

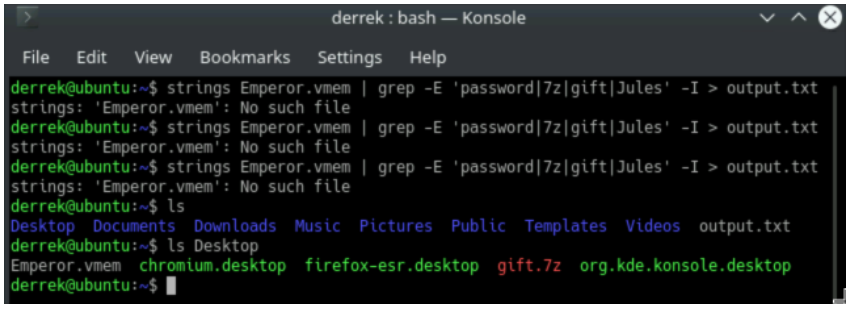
- Strings: A command-line tool for extracting text strings from binary files.
- Volatility: A Python-based framework for analyzing volatile memory (RAM) dumps.
- File.io: A file-sharing service used to transfer the output file.
- md5sum: A command-line tool for calculating the MD5 hash of a file.

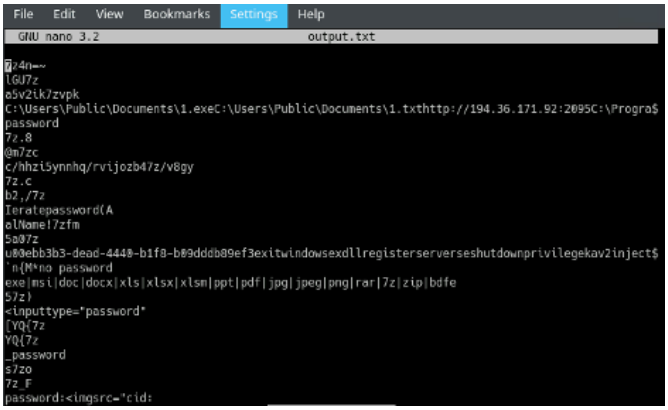
Investigation Process

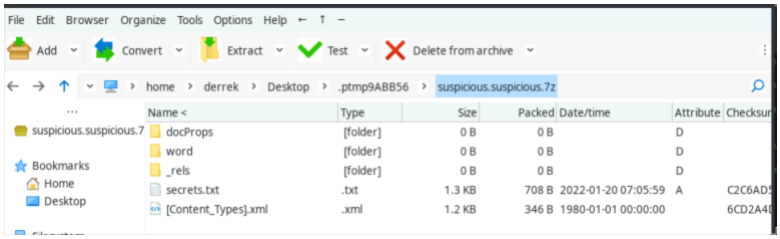
1. **Analyze the 'gift.7z' file:** Determine that it is encrypted and requires a password.
   - 

2. **Analyze the 'Emperor.vmem' file:**

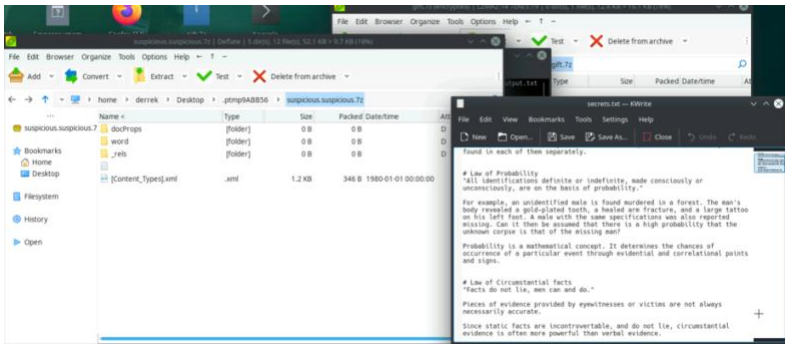
- Use 'strings' to extract text strings and search for keywords related to the password and the encrypted file.
- 

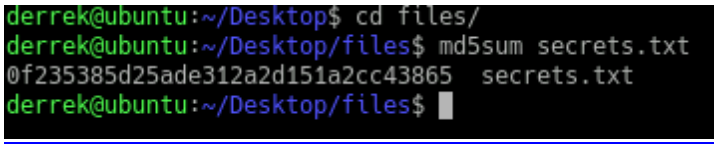
- Locate the password for 'gift.7z' within the output.
- 

3. **Extract the 'suspicious.docx' file:**
   - Use the password to extract the contents of 'gift.7z'.
   - 

   - Observe that the extracted DOCX file appears empty.
4. **Analyze the 'suspicious.docx' file:**
   - Reformat the file extension to '.7z' and unzip its contents.
   - 

   - Find a hidden text file named 'secrets.txt'.

- 

5. **Calculate the MD5 hash of 'secrets.txt' to obtain the flag.**
   - 

Recommendations

- **Password Security:** Avoid storing passwords in plain text within memory or easily accessible files. Use strong, unique passwords and consider a password manager.
- **Data Hiding:** Be aware of techniques used to hide data within seemingly innocuous files, such as embedding files within DOCX documents.
- **File Analysis:** Develop skills in analyzing files and memory dumps using tools like 'strings' and 'volatility' to uncover hidden information.
- **CTF Practice:** Participate in CTF challenges to gain practical experience in cybersecurity concepts and techniques.