

TDX ARENA

Certification Report

Brett Reich

Final Assessment Report Submission

Case: Imperial Memory

8/12/24

Executive Summary

A cyber researcher that had just left our company put a file on my computer that was related to a question I had asked him about the secret to his success. The file was embedded in a folder that was left on my desktop that was password protected in a memory dump file.

The .vmem file was output into a .txt file which could then be used to search for the password to the file that needed to be extracted. Once extracted, the .docx file seemed to have nothing in it besides the words: "I am empty!" After reading the .docx file through the cat command on the terminal it seemed there was also a hidden file somehow also trapped. Once the .docx file was turned into a .7z extension, it could be extracted to show the researcher's secrets of success .txt file. The .txt file could then be turned into a MD5 hash to complete the flag for the challenge.

Findings and Analysis

Finding	Finding Details	Description
Extraction Password	G6Vmc\$Qd5cpM8 ee#Ca=x&A3	The password to unlock the gift.7z extraction that was found after converting the .vmem file into .txt and searching through it.

Once found the password could be used to extract the suspicious.docx file from the gift.7z folder.

Finding	Finding Details	Description
File to be extracted	suspicious.docx	File that contained secrets.txt embedded in it once it was extracted.

Once this file was unlocked it could be converted into a .7z file to extract the hidden files from it.

Finding	Finding Details	Description
Hidden file	secrets.txt	File that contained the researcher's hidden secrets of success quotes and is the MD5 hash that completed the challenge.

Once the suspicious.docx was turned into .7z and extracted then the secrets.txt file could be read and converted to MD5 hash.

Finding	Finding Details	Description
MD5 Hash Flag	0f235385d25ade312a2d151a2cc43865	Challenge flag that was derived from the secrets.txt hidden file.

Methodology

Tools and Technologies Used

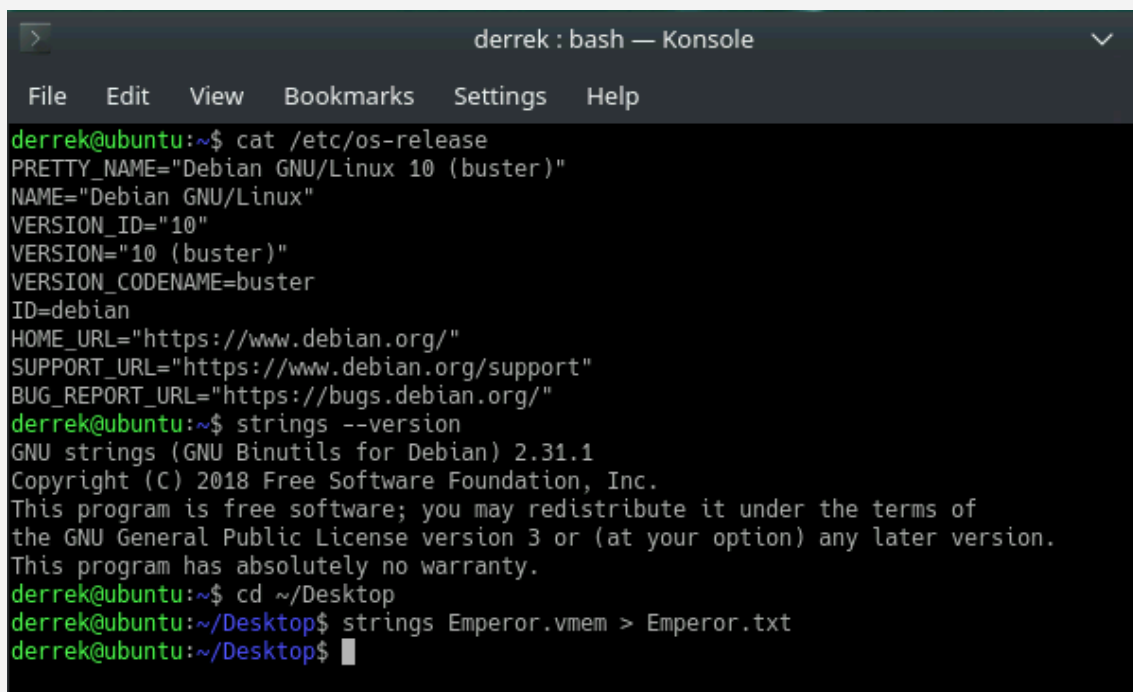
List and describe the tools and technologies employed in the investigation, including a brief explanation of why they were used.

Example:

- **Strings:** Strings is a command-line tool that can be used to convert files into readable language. I used strings to change the .vmem file into a .txt file that could be searched through easier for the password to the encrypted folder.
- **Cat:** Cat is a command in the CLI that can be used to concatenate and display the contents of files. This was used to help display the hidden text for the .docx file in the encrypted folder.
- **MD5sum:** MD5sum is a command in the CLI that is used to calculate and verify MD5 (Message Digest Algorithm 5) checksums. I used this to find the MD5 hash from the secrets.txt file.

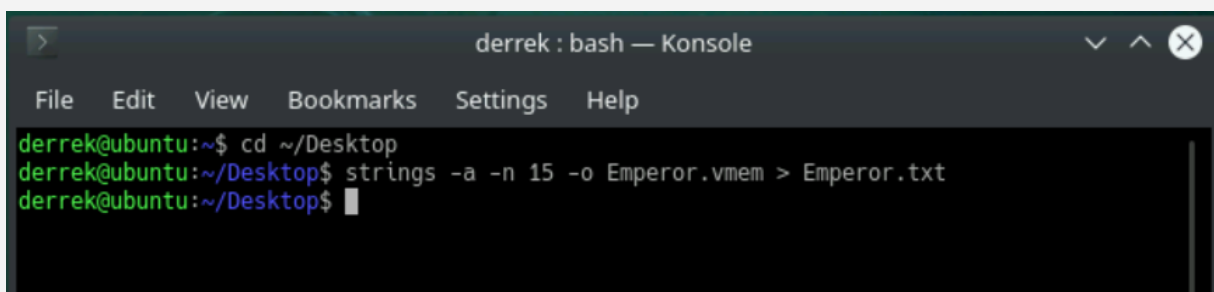
Investigation Process

1. I started by determining the OS version and then used strings to convert the Emperor.vmem file into the Emperor.txt file.

A terminal window titled 'derrek : bash — Konsole' with a menu bar (File, Edit, View, Bookmarks, Settings, Help). The user runs 'cat /etc/os-release' showing Debian GNU/Linux 10 (buster) information. Then they run 'strings --version' showing GNU strings 2.31.1. Finally, they run 'cd ~/Desktop' and 'strings Emperor.vmem > Emperor.txt' to convert the file.

```
derrek@ubuntu:~$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
VERSION_ID="10"
VERSION="10 (buster)"
VERSION_CODENAME=buster
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
derrek@ubuntu:~$ strings --version
GNU strings (GNU Binutils for Debian) 2.31.1
Copyright (C) 2018 Free Software Foundation, Inc.
This program is free software; you may redistribute it under the terms of
the GNU General Public License version 3 or (at your option) any later version.
This program has absolutely no warranty.
derrek@ubuntu:~$ cd ~/Desktop
derrek@ubuntu:~/Desktop$ strings Emperor.vmem > Emperor.txt
derrek@ubuntu:~/Desktop$
```

2. Next, I made a better conversion from the .vmem to .txt file to simplify the output and made it easier to search through.

A terminal window titled 'derrek : bash — Konsole' with a menu bar (File, Edit, View, Bookmarks, Settings, Help). The user runs 'cd ~/Desktop' and then 'strings -a -n 15 -o Emperor.vmem > Emperor.txt' to create a more readable text file.

```
derrek@ubuntu:~$ cd ~/Desktop
derrek@ubuntu:~/Desktop$ strings -a -n 15 -o Emperor.vmem > Emperor.txt
derrek@ubuntu:~/Desktop$
```

3. I then searched through the Emperor.txt file for gift.7z. The code G6Vmc\$Qd5cpM8ee#Ca=x&A3 was associated with the gift.7z file and allowed access to extract the file.

Emperor.txt — KWrite

File Edit View Bookmarks Tools Settings Help

New Open... Save Save As... Close Undo Redo

The file '/home/derrek/Desktop/Emperor.txt' was modified by another program. View Difference Reload Ign

```
1055540774 3:42:35
1055541120 2022-01-P
1055541234 3:42:35
1055541274 3:42:35
1055541320 Aaron
1055541420 sharedFoldersLock
1055541774 trolProcin
1055542120 2022-01-P
1055542160 2022-01-p
1055542474 TextDomain
1055542534 3:42:35
1055542720 2022-01-
1055543320 DnDPlugI
1055543733 13:42:35
1055506661 A_A^A]A\_^[
105550727 t$ WH
105551227 t$ WH
105551523 WAWAWH
105551745 A_A^_
105553572 VWAVH
105554605 A^_^
105555683 UAVAWH
105556202 H9|$XH
105556547 H9|$Pt
105557632 A_A^]
105557725 UVWATAUAVAWH
1055566300 copypaste.transport
1055566425 a 'C:\Users\Aaron\Desktop\gift.7z' C:\Users\Aaron\Desktop\gift -p'G6Vmc$Qd5cpM8ee#Ca=x&A3'|
105570070 418A073AA3BC1475
105570354 geJ>I1D
105570464 oeJ>I1D
```

gift.7z | Archive seems password protected

Password

G6Vmc\$Qd5cpM8ee#Ca=x&A3

Keyfile

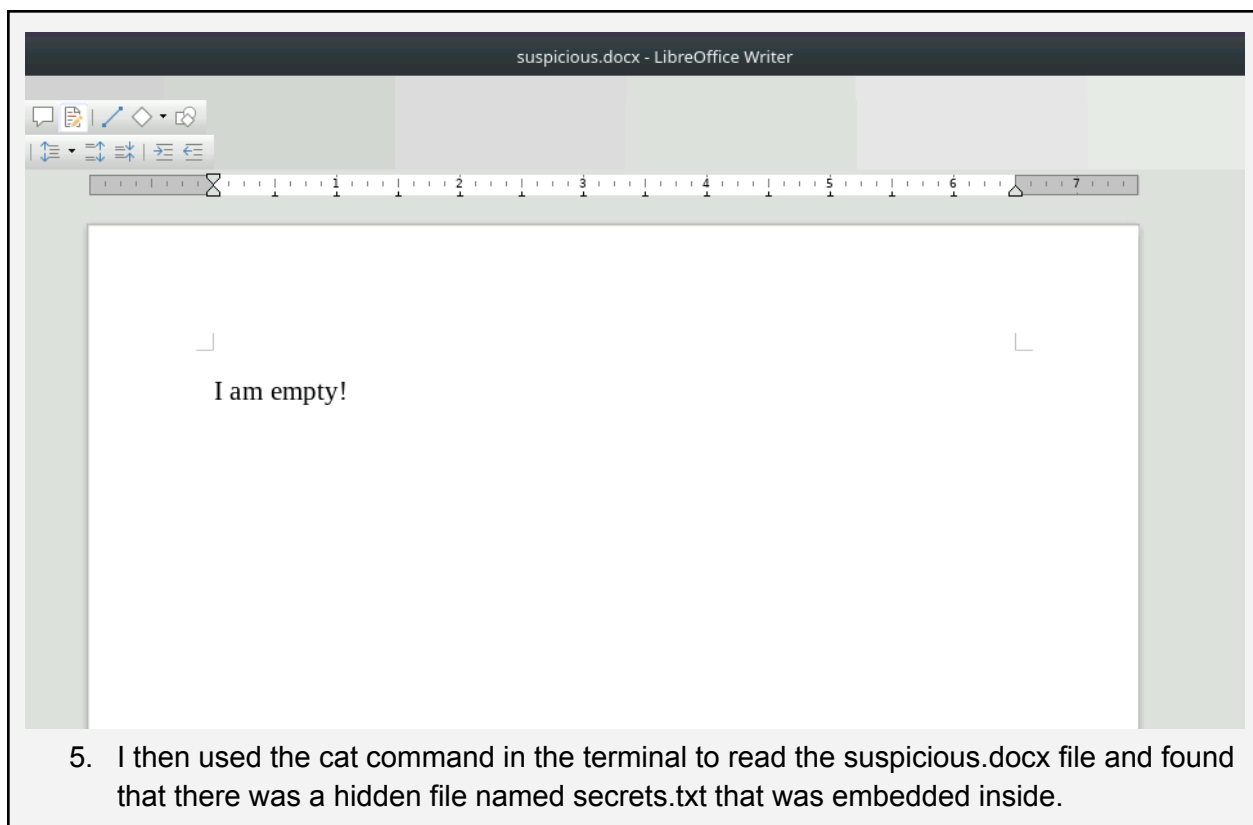
☐ Keep password/keyfile for current session

☐ Show password field content

Cancel

OK

- Once the suspicious.docx file was extracted and opened, nothing could be found on it besides the words: “I am empty!”



5. I then used the cat command in the terminal to read the suspicious.docx file and found that there was a hidden file named secrets.txt that was embedded inside.

```

derrek : bash — Konsole
File Edit View Bookmarks Settings Help

`063B100000J
00"!`0z/,m0"0000000=000e000U^00,00TG"00000Gz0`y00-0 a000類eA細3G00y00P0H4TV0000m
ts.txtmT,00
00?0C/Y0B0]t0z(00-01[=\0J00/){0是8Er83000>000000}000w0.TV00wr3V@h06)<6!00B000
00<pL0+3000p00000
0/0K0L00T00I090\0000
9+00C"0=0DQ00#00A000sG!c0P000
0Qu0Z[A000n&h004b00000000E/00b)0B00B00X000007000j"T0000G0C0.\q00L000&00
nhZ000E0*0d`0j000000x07c00i0qzy;*P0@f0m0z.000E0
U00l000J@00000B\L\8000005Y060=Z"L00000}000Urs600v400000a0se00P#00000>0l0000G0U09000b0x0Z
[$0m000000<000zA00005)0e00vm*001*>0070n0#000`09Zt0gQ00u00^000Vv00B0jj#Mo0(00`006t0D0ttY0
B0D00000I700
0000VaRU00000s0s0X60Q0
0#c00zN00T000,vsvsZ0}w00XX006000/0W000M0T60000"800B0X00C000{ :HT0*7000Z0)h00000N
0_rel
s/.relsPK!0 0-
0word/document.xmlPK!0d0Q010 word/_rels/document.xml.relsPK!00g000 2
w
ord/theme/theme1.xmlPK!0?[0
7word/settings.xmlPK!0UJ0#
0u0word/styles.xmlPK!00}00#word/web
Settings.xmlPK!00<D00%word/fontTable.xmlPK!n00{n00'docProps/core.xmlPK!0M30m00*docProps/
app.xmlP0H4TV0000m
$ C-secrets.txt
000~1~
0PK

00derrek@ubuntu:~/Desktop$

```

6. After scouring information online, I found that you can change .docx files to .7z files like the encrypted one earlier which will allow extraction of the files within.
7. Once extracted the secrets.txt file showed quotes from the researcher that were the promised answers to his secrets of success question.

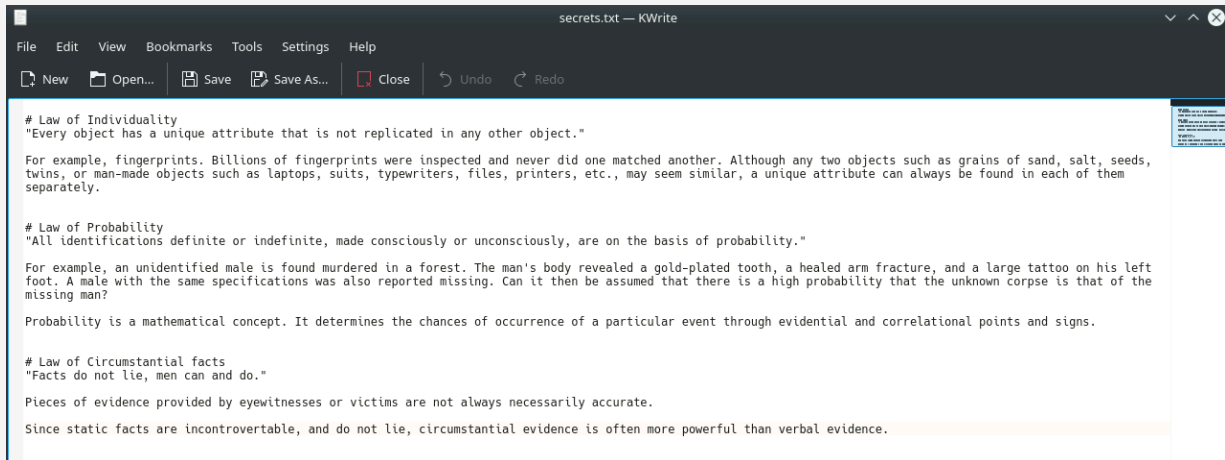
suspicious.7z | Deflate | 5 dir(s), 12 file(s), 52.1 KB > 9.7 KB (18%)

File Edit Browser Organize Tools Options Help

Add Convert Extract Test Delete from archive

home > derrek > Desktop > suspicious.7z

Name <	Type	Size	Packed	Date/time	Attrit	Checksum/hash
suspicious.7z						
docProps	[folder]	0 B	0 B		D	
word	[folder]	0 B	0 B		D	
_rels	[folder]	0 B	0 B		D	
secrets.txt	.txt	1.3 KB	708 B	2022-01-20 07:05: A		C2C6AD56
[Content_Types].xml	.xml	1.2 KB	346 B	1980-01-01 00:00:		secrets.txt Type - .txt Size - 1.3 KB Packed - 708 B Checksum/hash - C2C6AD56 Date/time - 2022-01-20 07



```
# Law of Individuality
"Every object has a unique attribute that is not replicated in any other object."

For example, fingerprints. Billions of fingerprints were inspected and never did one matched another. Although any two objects such as grains of sand, salt, seeds,
twins, or man-made objects such as laptops, suits, typewriters, files, printers, etc., may seem similar, a unique attribute can always be found in each of them
separately.

# Law of Probability
"All identifications definite or indefinite, made consciously or unconsciously, are on the basis of probability."

For example, an unidentified male is found murdered in a forest. The man's body revealed a gold-plated tooth, a healed arm fracture, and a large tattoo on his left
foot. A male with the same specifications was also reported missing. Can it then be assumed that there is a high probability that the unknown corpse is that of the
missing man?

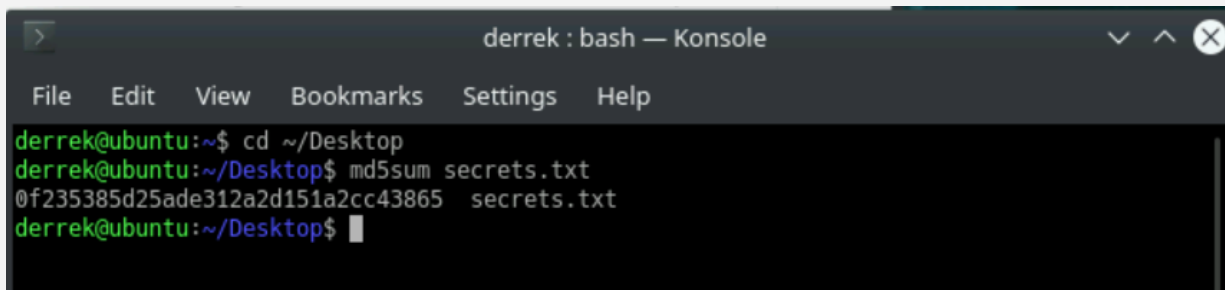
Probability is a mathematical concept. It determines the chances of occurrence of a particular event through evidential and correlational points and signs.

# Law of Circumstantial facts
"Facts do not lie, men can and do."

Pieces of evidence provided by eyewitnesses or victims are not always necessarily accurate.

Since static facts are incontrovertable, and do not lie, circumstantial evidence is often more powerful than verbal evidence.
```

8. However, the challenge flag was not part of the secrets.txt. Running the MD5sum command in the terminal allowed for the hash to show, which was the proper flag to complete the challenge: 0f235385d25ade312a2d151a2cc43865



```
derrek@ubuntu:~$ cd ~/Desktop
derrek@ubuntu:~/Desktop$ md5sum secrets.txt
0f235385d25ade312a2d151a2cc43865 secrets.txt
derrek@ubuntu:~/Desktop$
```

Appendix A

File-related Findings	
~/desktop/Emperor.vmem	File that was left on desktop by researcher which contained memory dump.
~/desktop/gift.7z	Encrypted file that contained suspicious.docx
G6Vmc\$Qd5cpM8ee#Ca=x&A3	Password for gift.7z extraction that was found in Emperor.vmem file
suspicious.docx	File that contained secrets.txt embedded in it once it was extracted.
secrets.txt	File that contained the researcher's secrets of success and was the MD5 hash flag.
0f235385d25ade312a2d151a2cc43865	Challenge flag that was converted from secrets.txt through MD5sum command.