CHALLENGE DESCRIPTION

Luxx, leader of The Phreaks, immerses himself in the depths of his computer, tirelessly pursuing the secrets of a file he obtained accessing an opposing faction member's workstation. With unwavering determination, he scours through data, putting together fragments of information trying to take some advantage on other factions. To get the flag, you need to answer the questions from the docker instance.

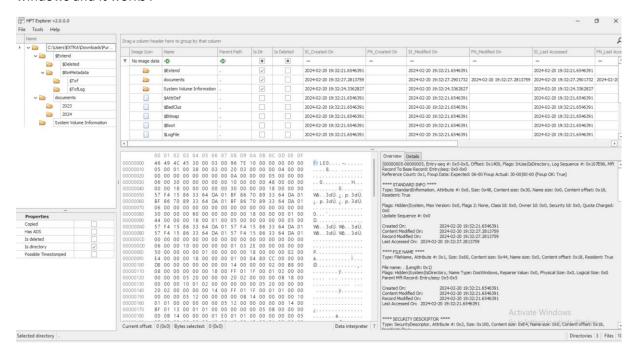
The extracted file from the .zip is : "z.mft", so its an mft(Master file table).

MFT is the master file table in the NTFS file system used by windows OS.

MFT stores information about all the files in the NTFS file system such as filename, size....

Let's goo:

Literally, I tried all the tools that I know on kali linux to extract some information about the .mft file but all of the failed . after some google searching i found this tool "MFT explorer" I install it and I run it on windows and it works .



So lets answer the question:

First question: Files are related to two years, which are those? (for example: 1993,1995):

2023,2024

Next question: There are some documents, which is the name of the first file written? (for example: randomname.pdf):

Just look at the creation date and chose the oldest one .

Final_Annual_Report.xlsx

Next question: Which file was deleted? (for example: randomname.pdf):



Marketing_plan.xlsx

| credentials, bxt .\documents | 2024-02-20 19:32:27.2901732

Next question: How many of them have been set in Hidden mode? (for example: 43):



2024-02-20 19:32:27.2901732

There is one file that contains the word hidden in the Overview (flags)

1

Next question: Which is the filename of the important TXT file that was created? (for example: randomname.txt):

The hidden file: credentials.txt

Next question: A file was also copied, which is the new filename?

	FN_Modified On	SI_Last Accessed	FN_Last Accessed	SI_Record Changed	FN_Record Changed	Timestomped	Copied
	=	=	=	=	=		
872119	2024-02-20 19:32:27.2862572	2024-02-20 19:32:27.2872119	2024-02-20 19:32:27.2862572	2024-02-20 19:32:27.2872119	2024-02-20 19:32:27.2862572		
881770		2024-02-20 19:32:27.2881770		2024-02-20 19:32:27.2881770			
891865	2024-02-20 19:32:27.2901732	2024-02-20 19:32:27.2911603	2024-02-20 19:32:27.2901732	2024-02-20 19:32:27.2891865	2024-02-20 19:32:27.2901732		✓
881770		2024-02-20 19:32:27.2881770		2024-02-20 19:32:27.2881770			
881770	2024-02-20 19:32:27.2872119	2024-02-20 19:32:27.2881770	2024-02-20 19:32:27.2872119	2024-02-20 19:32:27.2881770	2024-02-20 19:32:27.2872119		
004361	2024-02-20 19:32:27.2872119	2024-02-20 19:33:30.3004361	2024-02-20 19:32:27.2872119	2024-02-20 19:33:30.3004361	2024-02-20 19:32:27.2872119		

Financial Statement draft.xlsx

Next question: Which file was modified after creation?

Project_Proposal.pdf

Next question: What is the name of the file located at record number 45? (for example: randomname.pdf):

45=0x2D



its Annual_Report.xlsx

Next question: What is the size of the file located at record number 40? (for example: 1337)

40=0x28

The file name is Final_Project_Proposal.pdf

Non Resident Data

Starting Virtual Cluster #: 0x0, Ending Virtual Cluster #: 0xD, Allocated Size: 0xE000, Actual Size: 0xE000, Initialized Size 0x0

Non resident data: this means the file's content is not stored directly in the MFT entry but in clusters on the disk.

The file size is :0xE000 == 57344

And you get the flag.