Bandit Level 12 - Level 13

Password is contained in a data.txt file. However this time to file has been repeatedly compressed.

First thing to do is make a temporary directory and copy the file across.

```
bandit12@bandit:~$ mktemp -d
/tmp/tmp.FGconEJlp1
```

The above command creates a temporary directory with a unique name.

Lets copy the data.txt file over to this temp directory.

```
bandit12@bandit:~$ cp data.txt /tmp/tmp.FGconEJlp1
```

Change directory to the temp directory and list the contents to make sure the file is there.

```
bandit12@bandit:~$ cd /tmp/tmp.FGconEJlp1
bandit12@bandit:/tmp/tmp.FGconEJlp1$ ls
data.txt
```

The data.txt is a hexdump file that needs to be converted back to binary. We can use the xxd command which converts binary to hex dump and can also reverse it.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ xxd -r data.txt databinary.bin
bandit12@bandit:/tmp/tmp.FGconEJlp1$ ls
databinary.bin  data.txt
```

Use the xxd command with the -r flag to reverse it back to binary and output it to a new file called 'databinary.bin'.

'databinary.bin' has been compressed multiple times, but we do not know which compression method has been used, e.g. is it tar? gzip? bzip? zip? We can use the file command to get more information of the file.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ file databinary.bin
databinary.bin: gzip compressed data, was "data2.bin", last modified: Thu
```

```
Sep 19 07:08:15 2024, max compression, from Unix, original size modulo 2^32
574
```

We can derive from above that the file has been compressed with gzip. Lets change the extension to gz to represent the file compression that was used.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ mv databinary.bin databinary.gz
bandit12@bandit:/tmp/tmp.FGconEJlp1$ ls
databinary.gz  data.txt
```

Then we can uncompress it.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ gunzip databinary.gz
bandit12@bandit:/tmp/tmp.FGconEJlp1$ ls
databinary  data.txt
```

Once again we can use file, to see what file type it is.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ file databinary
databinary: bzip2 compressed data, block size = 900k
```

The file is now a bzip2 file. Lets rename the file to end in bz2, uncompress it and see what file type it is. I have added ls after every operation to ensure the files have be renamed or created.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ mv databinary databinary.bz2
bandit12@bandit:/tmp/tmp.FGconEJlp1$ ls
databinary.bz2  data.txt
bandit12@bandit:/tmp/tmp.FGconEJlp1$ bunzip2 databinary.bz2
bandit12@bandit:/tmp/tmp.FGconEJlp1$ ls
databinary  data.txt
bandit12@bandit:/tmp/tmp.FGconEJlp1$ file databinary
databinary: gzip compressed data, was "data4.bin", last modified: Thu Sep 19
07:08:15 2024, max compression, from Unix, original size modulo 2^32 20480
```

The file is now compressed using gzip. Lets rename, uncompress and check the file type.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ mv databinary databinary.gz
bandit12@bandit:/tmp/tmp.FGconEJlp1$ ls
databinary.gz  data.txt
```

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ gunzip databinary.gz
bandit12@bandit:/tmp/tmp.FGconEJlp1$ ls
databinary  data.txt
bandit12@bandit:/tmp/tmp.FGconEJlp1$ file databinary
databinary: POSIX tar archive (GNU)
```

Now the file is compressed in a tar archive! Same thing again and hopefully this is the last time and we get a text file with the password.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ mv databinary databinary.tar
```

We can use tar followed by flags to uncompress the file. the -x flag is to uncompress, the -v is for verbose mode, which shows the progress in the terminal (probably not needed since the file is small), the -f flag is to specify the filename of the output.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ tar -xvf databinary.tar
data5.bin
```

Lets find out what file type is is.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ file data5.bin
data5.bin: POSIX tar archive (GNU)
```

Argh! Another compression!

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ mv data5.bin data5.tar
bandit12@bandit:/tmp/tmp.FGconEJlp1$ tar -xvf data5.tar
data6.bin
```

Check file type, rename, uncompress.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ mv data6.bin data6.bz2
bandit12@bandit:/tmp/tmp.FGconEJlp1$ bunzip2 data6.bz2
```

A file data6 was produced. Lets uncompress it again.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ mv data6 data6.tar
bandit12@bandit:/tmp/tmp.FGconEJlp1$ tar -xvf data6.tar
```

```
data8.bin
bandit12@bandit:/tmp/tmp.FGconEJlp1$ file data8.bin
data8.bin: gzip compressed data, was "data9.bin", last modified: Thu Sep 19
07:08:15 2024, max compression, from Unix, original size modulo 2^32 49
```

A file data8.bin was produced, rename and uncompress.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ mv data8.bin data8.gz
bandit12@bandit:/tmp/tmp.FGconEJlp1$ gunzip data8.gz
```

Check its file type.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ file data8
data8: ASCII text
```

Finally!!! Lets cat the contents out and then pass out.

```
bandit12@bandit:/tmp/tmp.FGconEJlp1$ cat data8
The password is FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```