Write Up for Medium 1

!! Warning !!

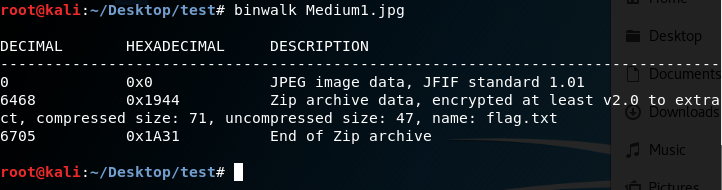
Here be spoilers, this is your final warning

Note

The intention of these write ups is to provide an insight into the intended strategy for solving the challenge. If you used a differing method to solve the challenge, feel free to message @1cysw0rdk0 or @Simon on slack. Write ups may not be provided or complete for all challenges, and may or may not include scripts used to create or solve the challenge.

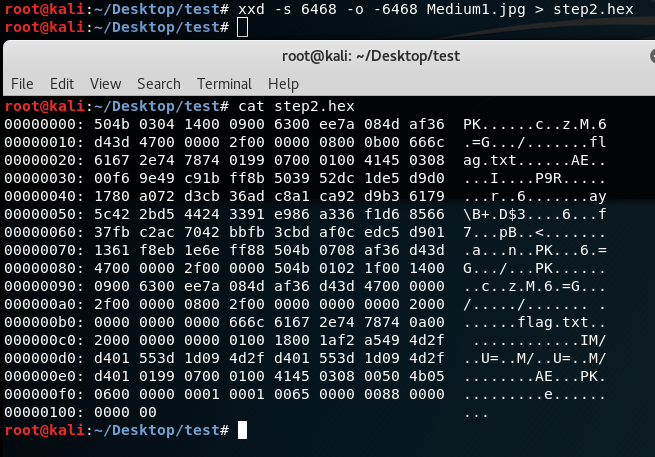
Step 1:

With no obvious signs of hidden or encoded data in the image itself, we look for hidden files or data inside the file data itself, using binwalk.



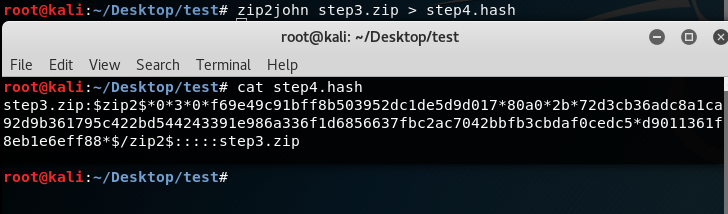
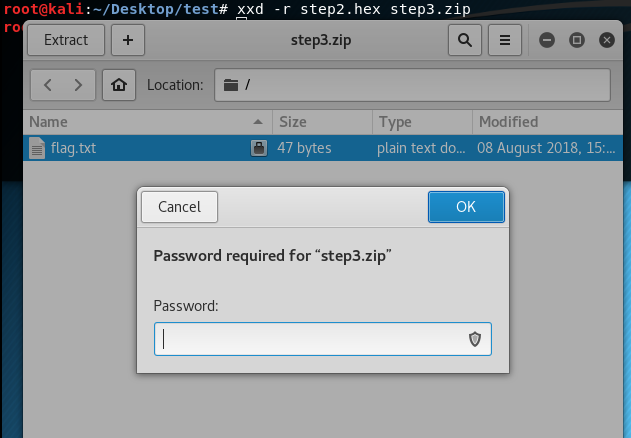
Step 2:

Noting the second file header inside the image data, it appears there is a zip file appended to the image. Using the offset for the file header, we can use xxd to split the file at that offset. The –s flag starts reading the file at the given offset, and the –o flag modifies the offset so that the new file can be generated.



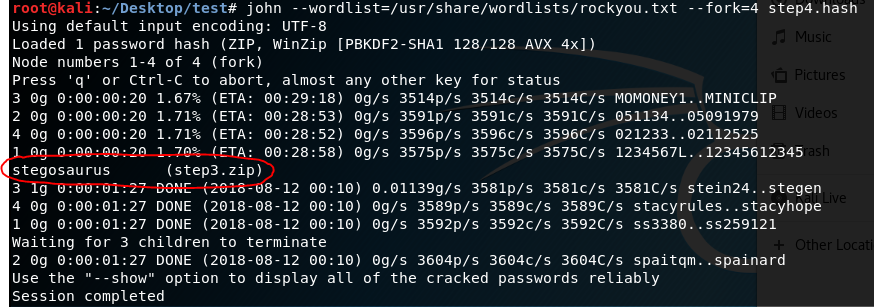
Step 3:

However the file is clearly encrypted, which is preventing us from reading the file. Hopefully whoever made this zip file used a weak password. The next step would be to crack that password. I chose to use John the Ripper, and in order to extract the hash to crack it, I need to run zip2john, which creates a hash file. There are other options to crack the zip file, which I will not cover here.



Step 4:

Next we run john the ripper against the hash file created. I used multiple forks here to decrease my wait time, and am using a wordlist attack using rockyou.txt.



Step 5:

Finally, we extract the zip file using the password we cracked, and the password is just in the text file.

