DC608

August 2022 CTF

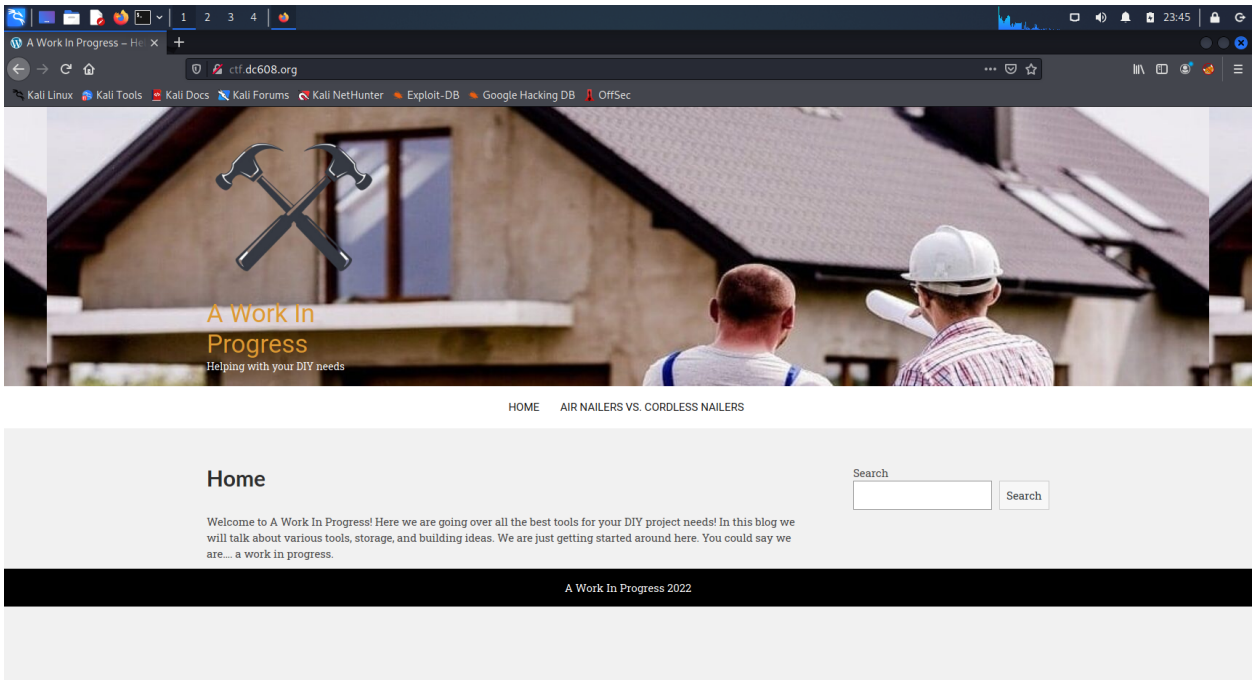
AzureAD - Trent Miller

Overview

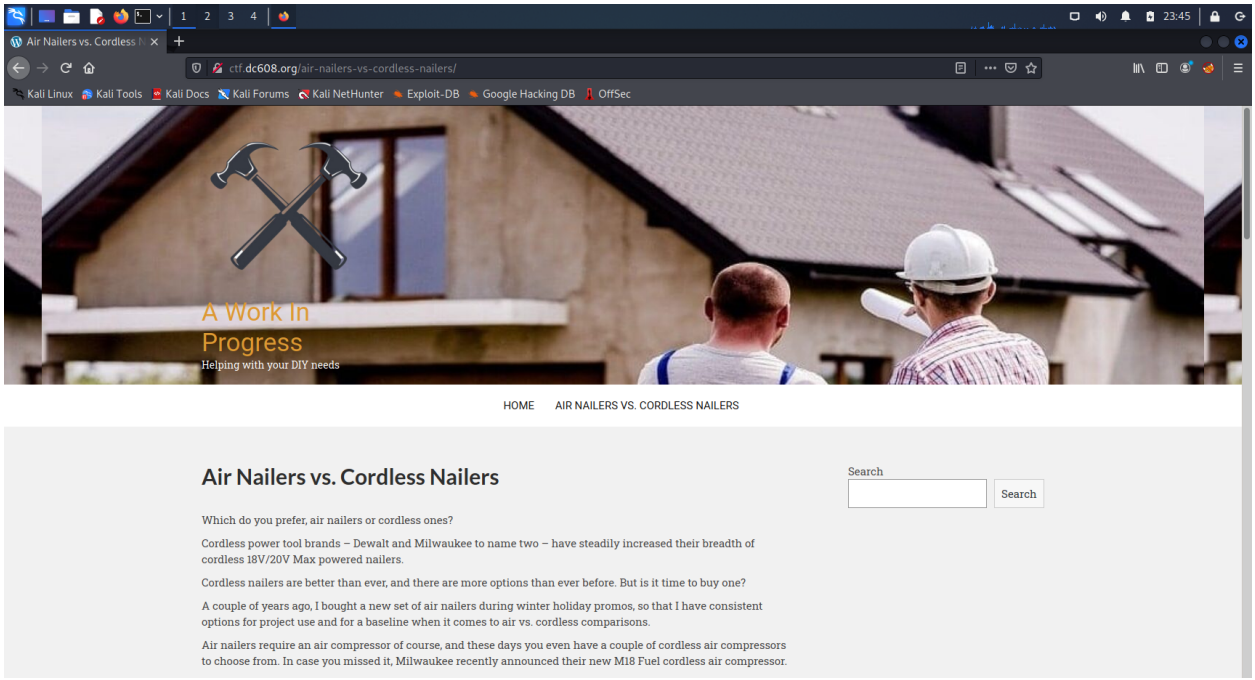
This CTF challenge was a medium level forensics challenge. The goal of this CTF was to assess the current website and locate the hidden flag without bruteforce tools. This challenge utilized reverse image searching, forensic file analysis, and extracting hidden files.

Assessing the website

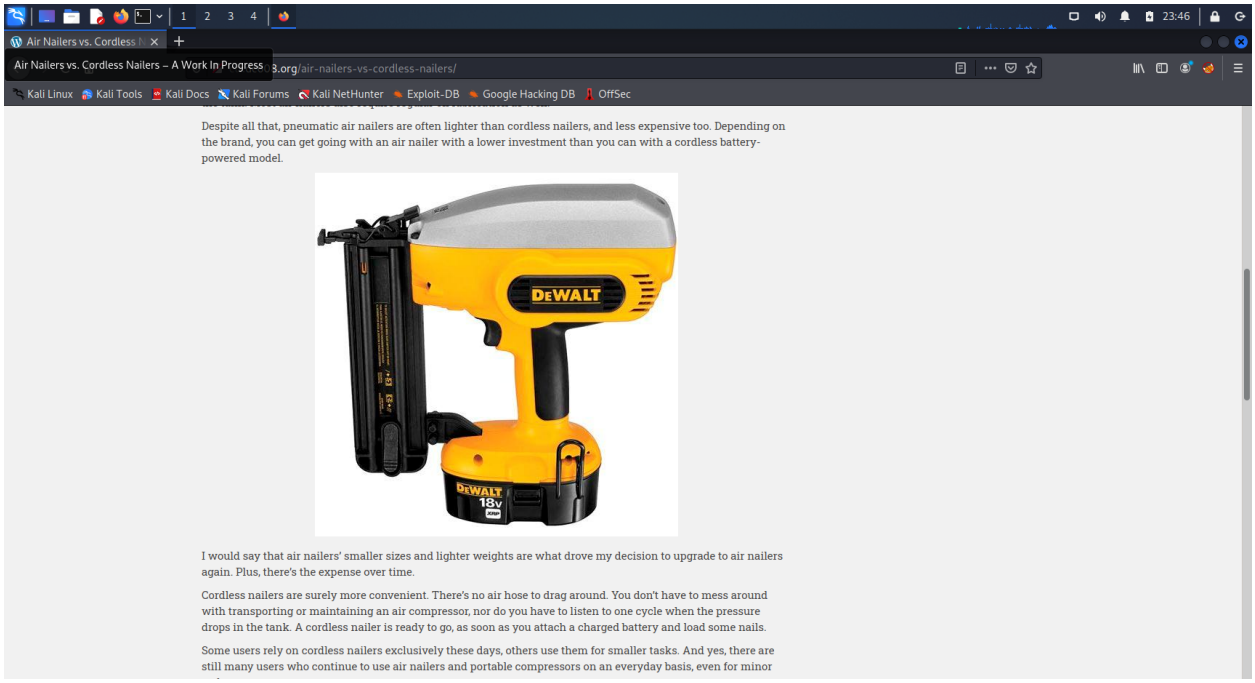
Upon first loading up the website it appears to be a basic DIY and tool information website that is just beginning. It has only a few pages and appears to be pretty basic.



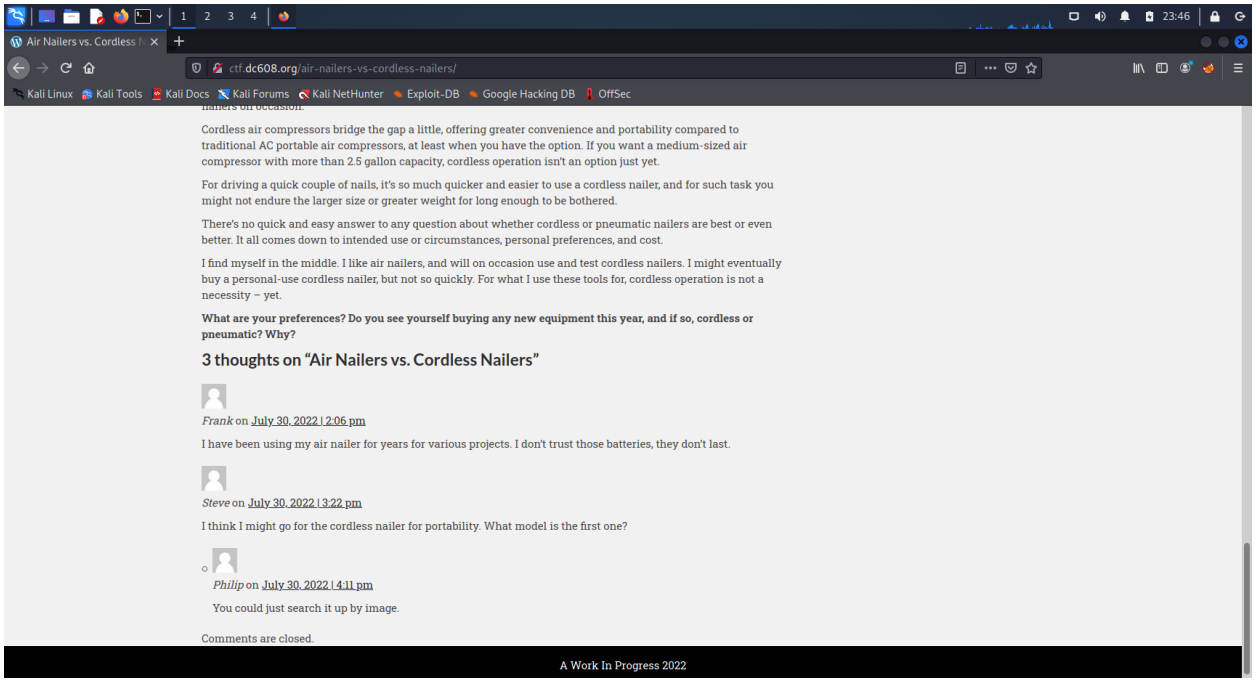
The home page does not have much information to provide to us.



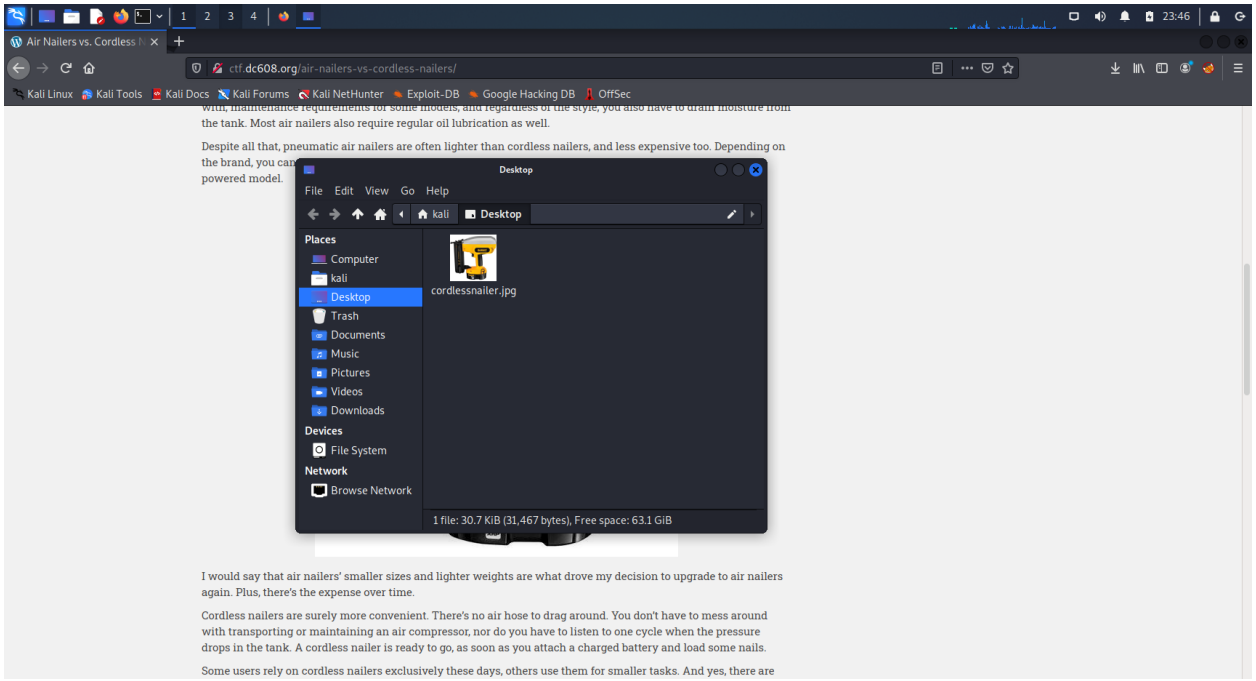
The only article on the page appears to be a comparison about two very close tools and the benefits of one or the other.



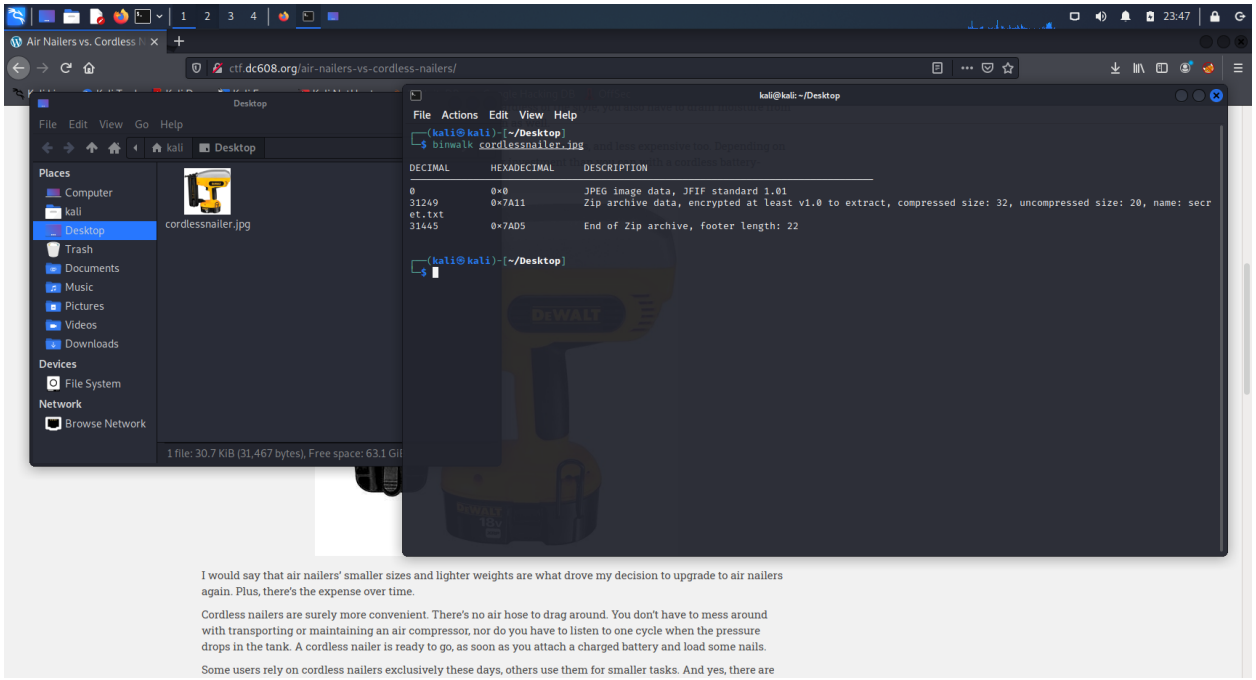
The first image appears to be a product placement image. On this page is one other image that appears to be a real photo. The images don't match so checking them out might be a good idea.



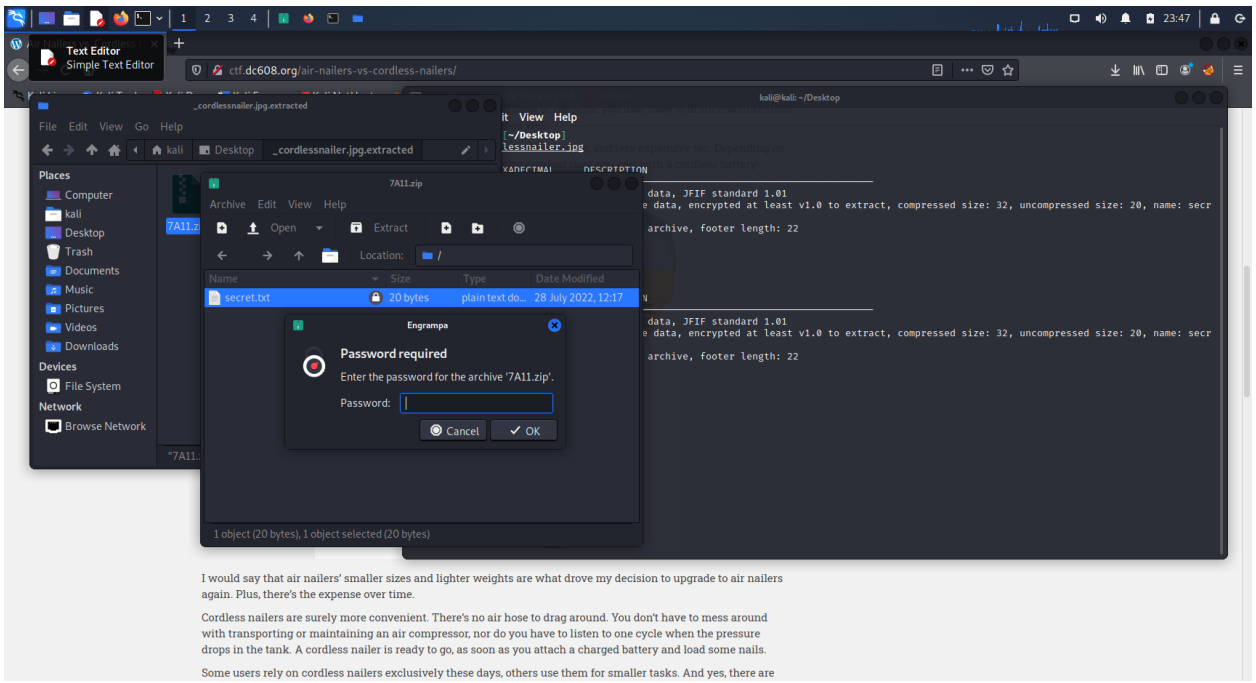
The comments appear to point towards searching the first image for possible clues.



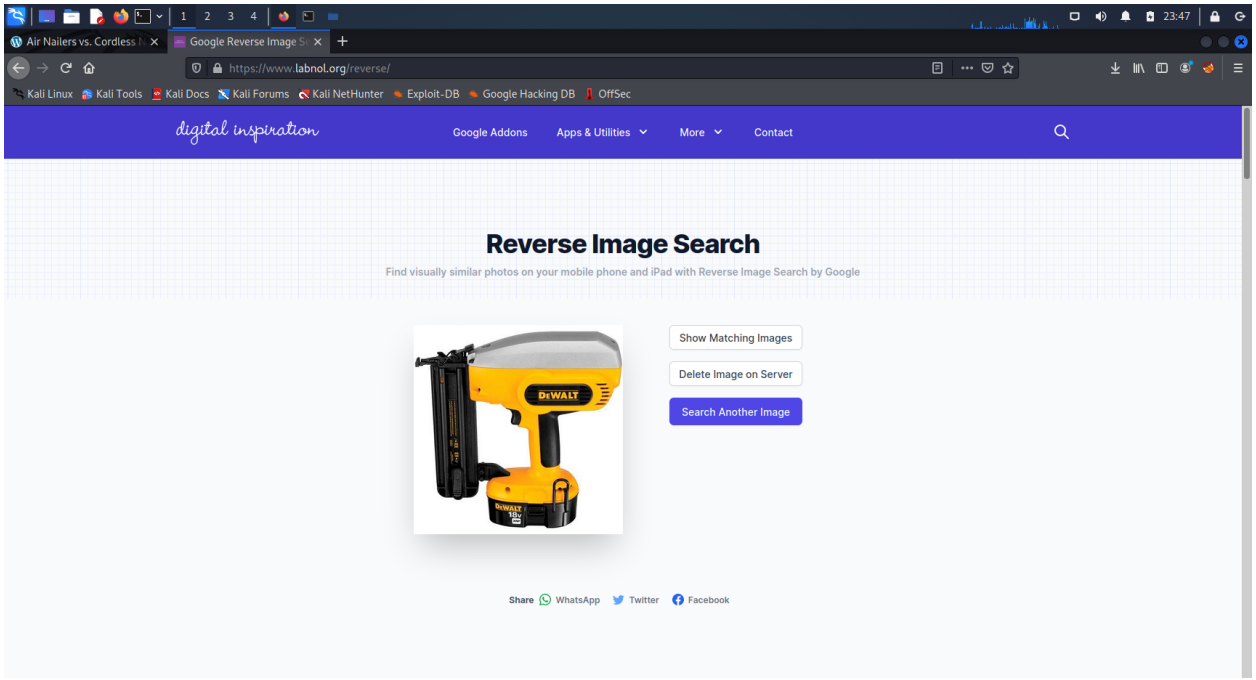
Downloading the file from the website to test it for possible hidden files.

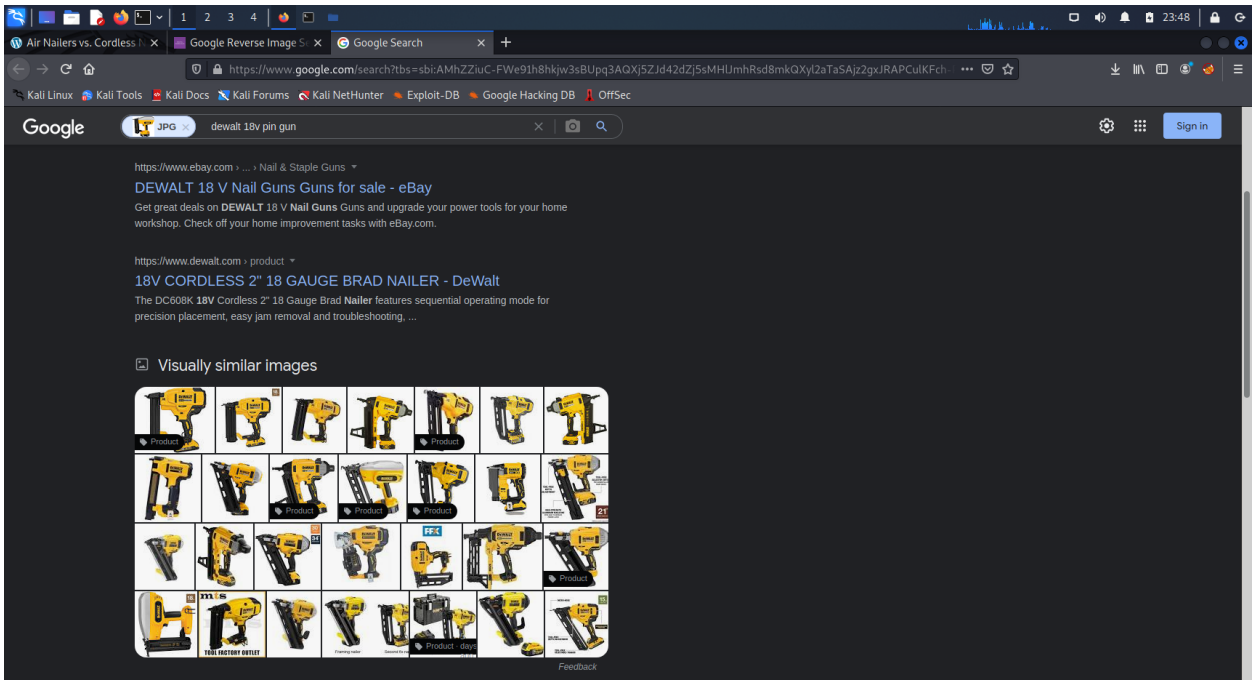


Binwalk informed me that there was a hidden Zip file that contained a secret.txt file. This could be what we are looking for. Utilizing Binwalk -e extracts the files into a folder.

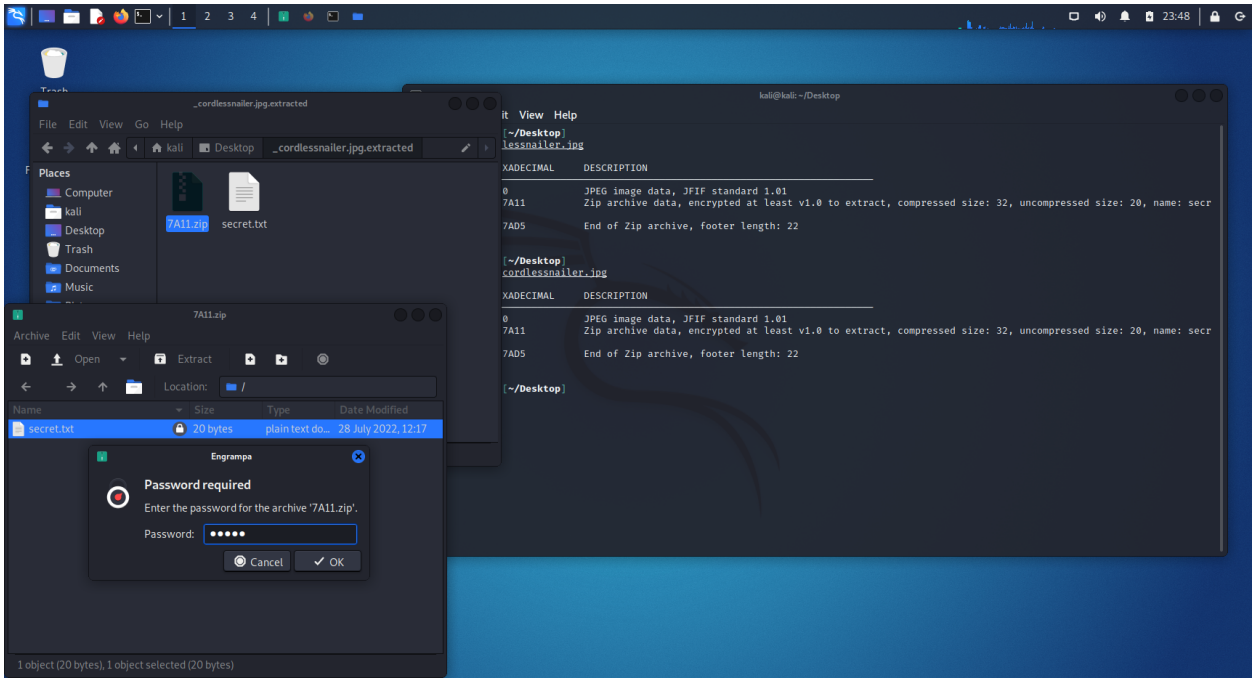


Browsing to the file and running extract presents us with a password. The hint before mentioned the specific model number. A quick reverse image search should give us the answer.

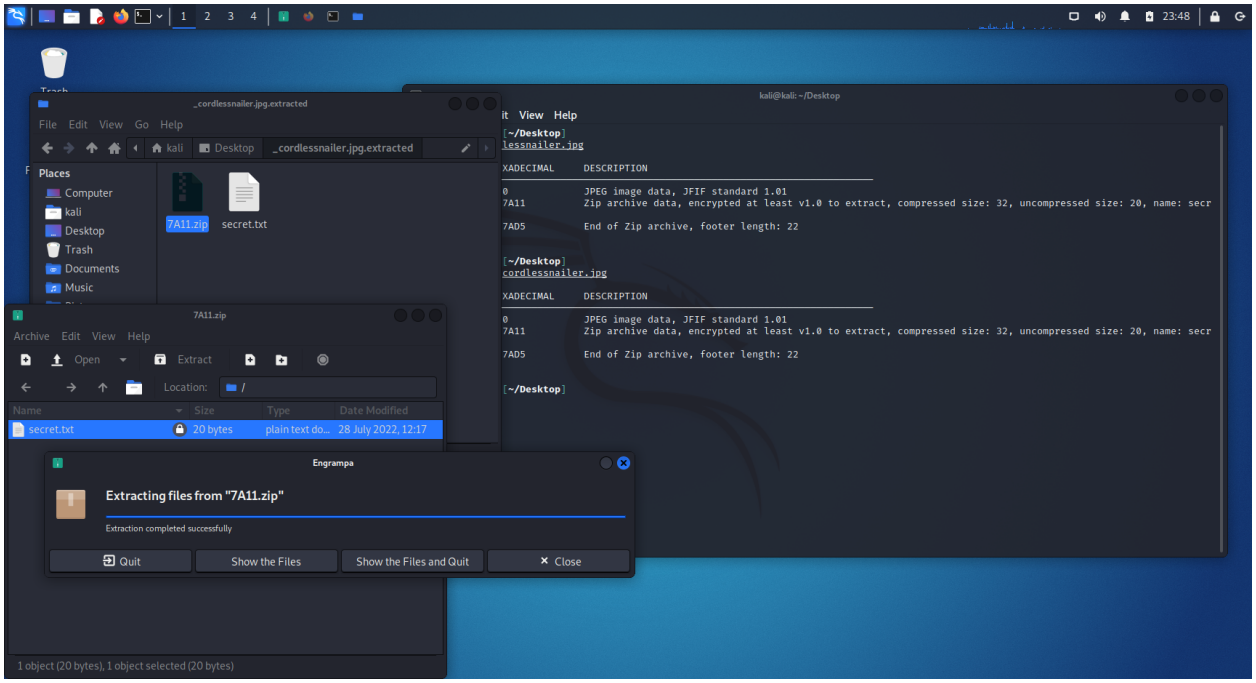


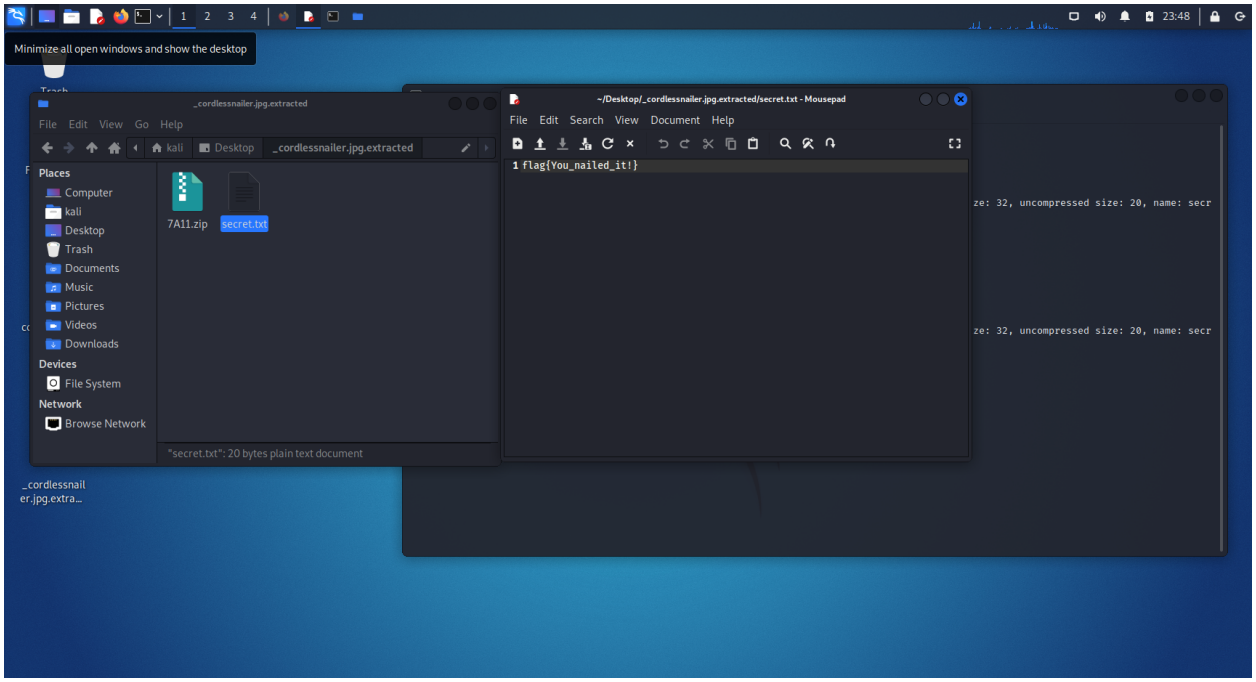


The model number appears to vary but seems to be variations of DC608.



Using the password DC608 works and unlocks the zip file.





The flag is revealed as flag{You_nailed_it!}.

Closing

Thank you to everyone who assisted me in testing and providing feedback for my very first CTF challenge. Please feel free to reach out to @azuread#0001 on Discord with any questions or comments you had about this CTF.