

DC608

August 2022 CTF

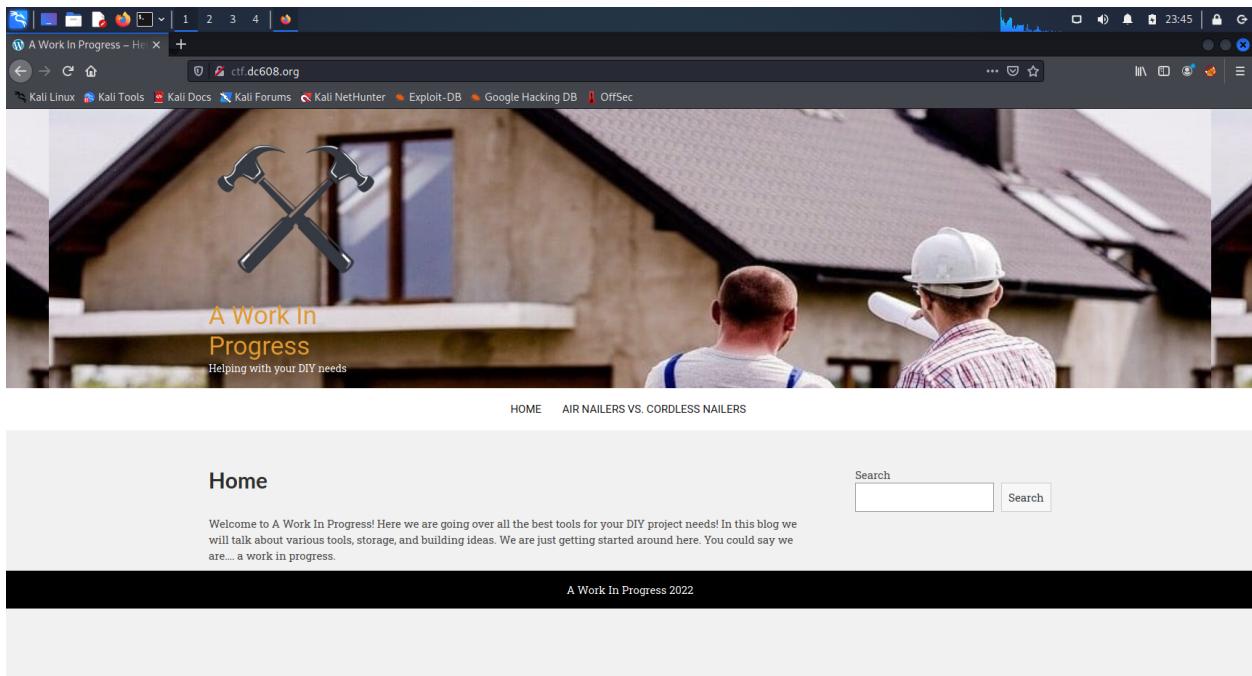
AzureAD - Trent Miller

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.

Air Nailers vs. Cordless Nailers

A Work In Progress
Helping with your DIY needs

HOME AIR NAILERS VS. CORDLESS NAILERS

Search

Air Nailers vs. Cordless Nailers

Which do you prefer, air nailers or cordless ones?

Cordless power tool brands – Dewalt and Milwaukee to name two – have steadily increased their breadth of cordless 18V/20V Max powered nailers.

Cordless nailers are better than ever, and there are more options than ever before. But is it time to buy one?

A couple of years ago, I bought a new set of air nailers during winter holiday promos, so that I have consistent options for project use and for a baseline when it comes to air vs. cordless comparisons.

Air nailers require an air compressor of course, and these days you even have a couple of cordless air compressors to choose from. In case you missed it, Milwaukee recently announced their new M18 Fuel cordless air compressor.

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

Air Nailers vs. Cordless Nailers – A Work In Progress

Despite all that, pneumatic air nailers are often lighter than cordless nailers, and less expensive too. Depending on the brand, you can get going with an air nailer with a lower investment than you can with a cordless battery-powered model.

I would say that air nailers' smaller sizes and lighter weights are what drove my decision to upgrade to air nailers again. Plus, there's the expense over time.

Cordless nailers are surely more convenient. There's no air hose to drag around. You don't have to mess around with transporting or maintaining an air compressor, nor do you have to listen to one cycle when the pressure drops in the tank. A cordless nailer is ready to go, as soon as you attach a charged battery and load some nails.

Some users rely on cordless nailers exclusively these days, others use them for smaller tasks. And yes, there are still many users who continue to use air nailers and portable compressors on an everyday basis, even for minor

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.

A screenshot of a web browser window. The title bar says "Air Nailers vs. Cordless". The address bar shows the URL "ctf.dc608.org/air-nailers-vs-cordless-nailers/". The page content discusses the convenience and portability of cordless air compressors compared to traditional AC portable air compressors. It mentions that if you want a medium-sized air compressor with more than 2.5 gallon capacity, cordless operation isn't an option just yet. The text notes that driving a quick couple of nails is much quicker and easier with a cordless nailer, though it might not endure the larger size or greater weight for long enough. There's a section asking what preferences people have for buying new equipment. Below that, there's a "3 thoughts on 'Air Nailers vs. Cordless Nailers'" section with three comments:

- Frank** on July 30, 2022 | 2:06 pm: I have been using my air nailer for years for various projects. I don't trust those batteries, they don't last.
- Steve** on July 30, 2022 | 3:22 pm: I think I might go for the cordless nailer for portability. What model is the first one?
- Philip** on July 30, 2022 | 4:11 pm: You could just search it up by image.

At the bottom, it says "Comments are closed." and "A Work In Progress 2022".

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

A screenshot of a Kali Linux desktop environment. A file manager window titled "Desktop" is open, showing a single file named "cordlessnailer.jpg" in the "Desktop" folder. The file is represented by a small icon of a nail gun. The file details at the bottom of the window show "1 file: 30.7 KB (31,467 bytes), Free space: 63.1 GB".

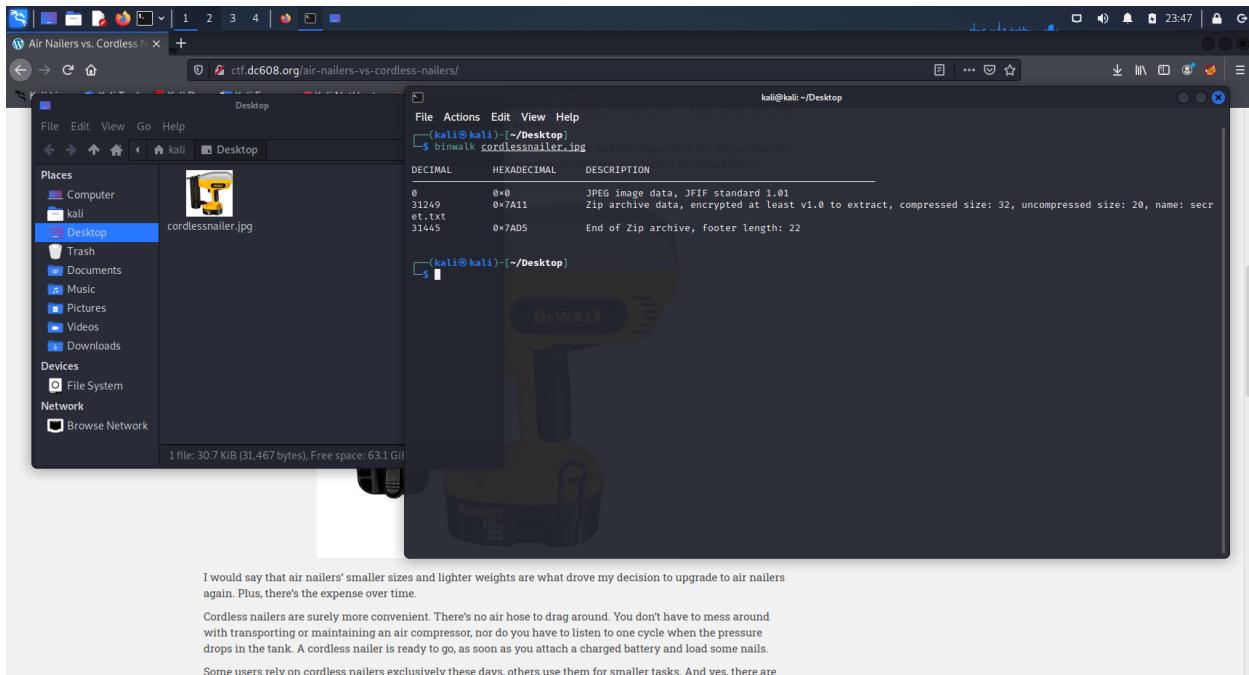
Below the file manager, there is some text from the website:

I would say that air nailers' smaller sizes and lighter weights are what drove my decision to upgrade to air nailers again. Plus, there's the expense over time.

Cordless nailers are surely more convenient. There's no air hose to drag around. You don't have to mess around with transporting or maintaining an air compressor, nor do you have to listen to one cycle when the pressure drops in the tank. A cordless nailer is ready to go, as soon as you attach a charged battery and load some nails.

Some users rely on cordless nailers exclusively these days, others use them for smaller tasks. And yes, there are

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

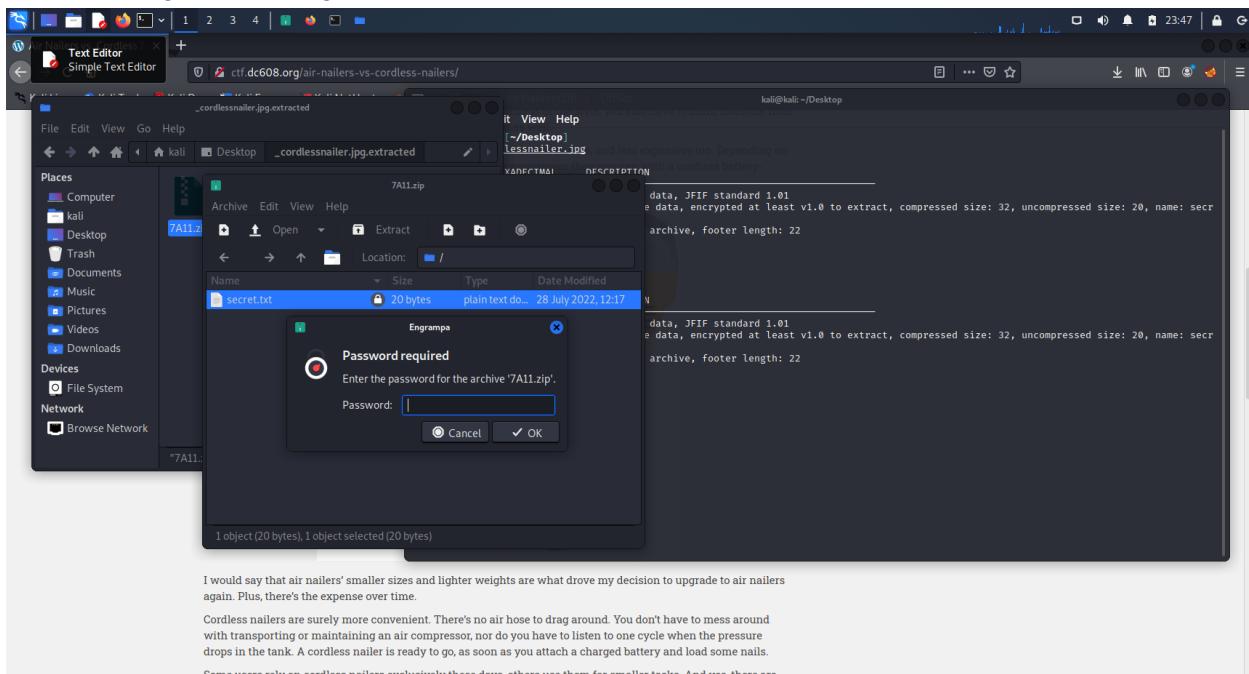


I would say that air nailers' smaller sizes and lighter weights are what drove my decision to upgrade to air nailers again. Plus, there's the expense over time.

Cordless nailers are surely more convenient. There's no air hose to drag around. You don't have to mess around with transporting or maintaining an air compressor, nor do you have to listen to one cycle when the pressure drops in the tank. A cordless nailer is ready to go, as soon as you attach a charged battery and load some nails.

Some users rely on cordless nailers exclusively these days, others use them for smaller tasks. And yes, there are

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.



I would say that air nailers' smaller sizes and lighter weights are what drove my decision to upgrade to air nailers again. Plus, there's the expense over time.

Cordless nailers are surely more convenient. There's no air hose to drag around. You don't have to mess around with transporting or maintaining an air compressor, nor do you have to listen to one cycle when the pressure drops in the tank. A cordless nailer is ready to go, as soon as you attach a charged battery and load some nails.

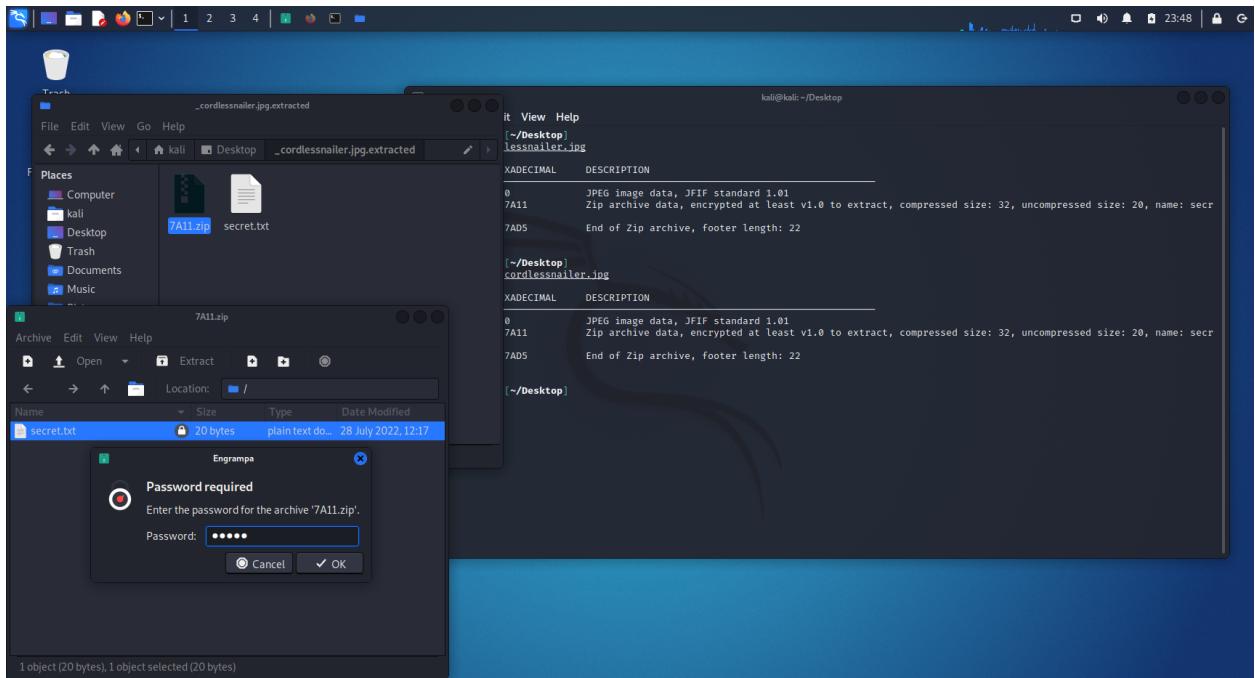
Some users rely on cordless nailers exclusively these days, others use them for smaller tasks. And yes, there are

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.

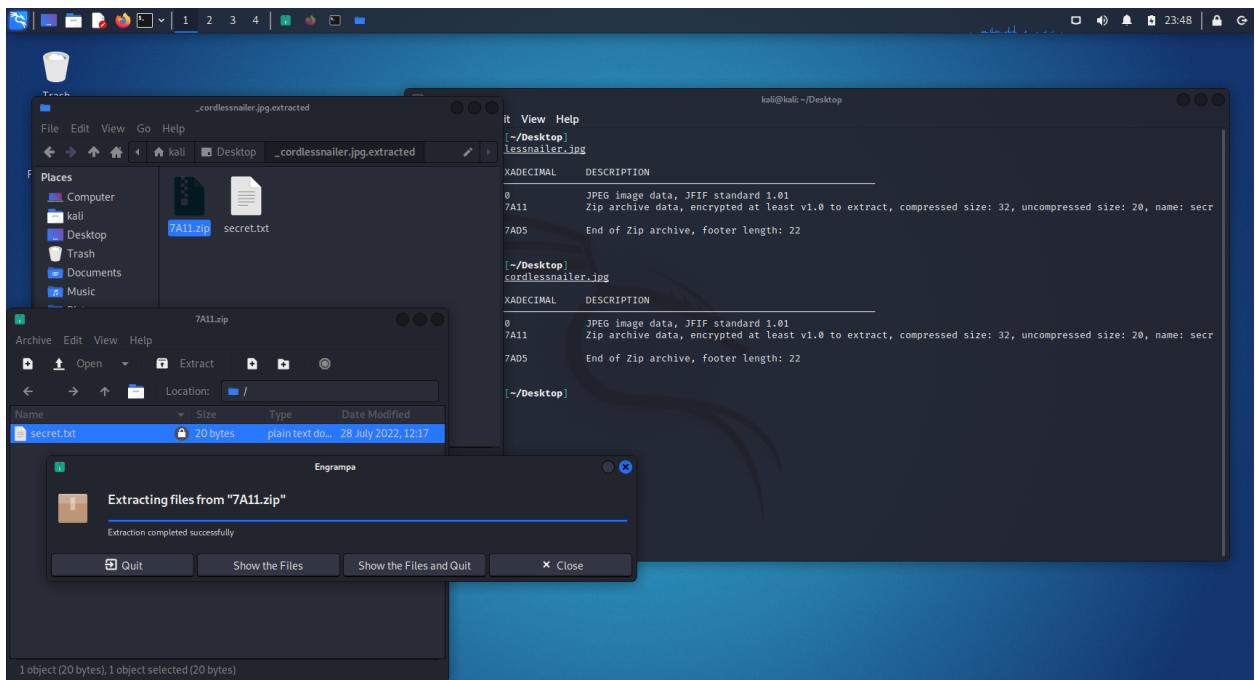
A screenshot of a web browser window showing the [labnol.org](https://www.labnol.org/reverse/) website. The main content is titled "Reverse Image Search" and features a yellow DEWALT cordless nail gun. Below the image are three buttons: "Show Matching Images", "Delete Image on Server", and "Search Another Image". At the bottom of the page, there are sharing options for WhatsApp, Twitter, and Facebook.

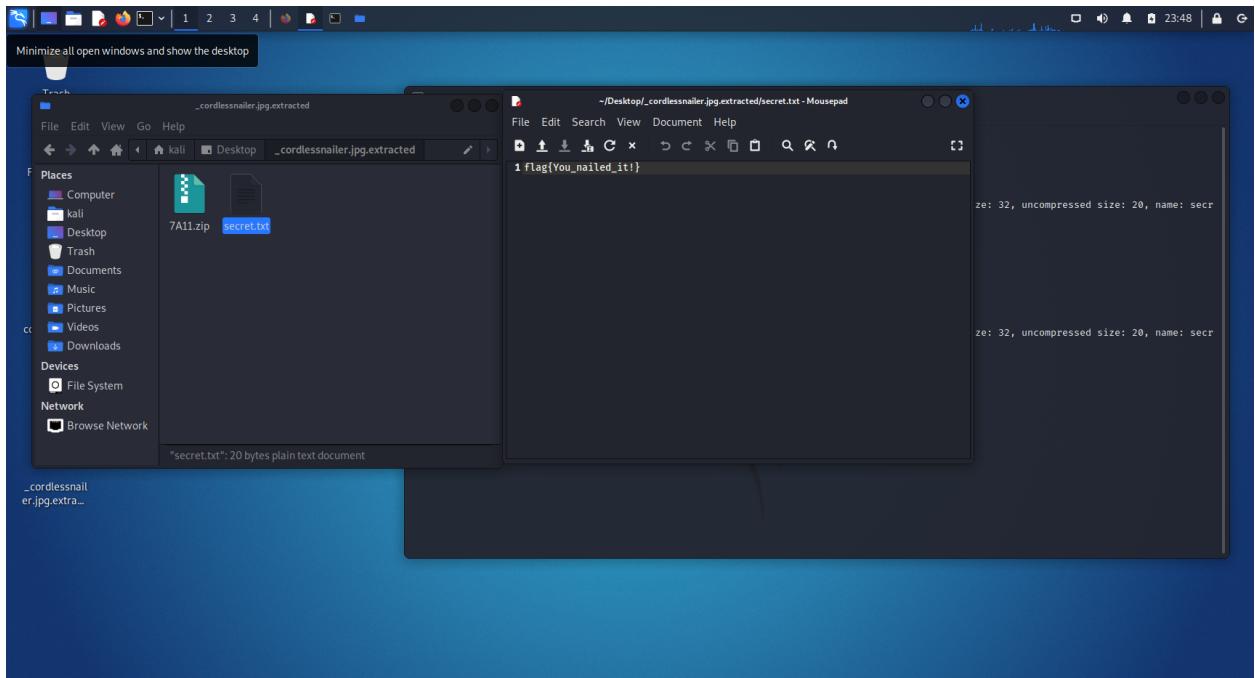
A screenshot of a web browser window showing a Google search results page for the query "dewalt 18v pin gun". The top result is a link to eBay for "DEWALT 18 V Nail Guns Guns for sale - eBay". Below the link, there is a snippet of text about great deals on DEWALT 18V nail guns. Further down the page, there is a section titled "Visually similar images" which displays a grid of various yellow and black DEWALT power tools, likely nail guns, from different angles and perspectives.

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.