Steganography Walkthrough

Requirements:

Nmap

Difficulty:

Easy

Walkthrough:

1. Build and host the docker server.
   * docker build -t <NAME> .
   * docker run -p 80:80 <NAME>
2. Run NMAP to find the open port.

A screenshot of a computer

Description automatically generated with medium confidence

1. Navigate to the webpage on port 80.

Graphical user interface, website

Description automatically generated

1. The website hints towards the images present on the webpage. Opening the webpage source reveals the images can be found within the “static” directory with one being named “Steg.jpg”.

Text

Description automatically generated

1. The name of the image file hints towards information being hidden using steganography. The file within this photo can be extracted without a password using many tools or websites. In this example, <https://futureboy.us/stegano/decinput.html> was used.

Graphical user interface, text

Description automatically generated

The output from this website reveals the flag.

Graphical user interface, text, application

Description automatically generated