Forensics 1 Walkthrough

Requirements:

Nmap

Web browser

SSH

Difficulty:

Medium – Longer length

Walkthrough:

1. Build and host the docker server.
   * docker build -t <NAME> .
   * docker run -p 22:22 -p 80:80 <NAME>
2. Run NMAP to find the open ports.

Text

Description automatically generated

1. Navigate to the website hosted on port 80 which hosts a single file.

Graphical user interface, text, application

Description automatically generated

1. Downloading and opening the file’s EXIF data reveals a username and password.

Text

Description automatically generated

1. Connecting to the SSH service on port 22 using the found credentials grants user access.

Text

Description automatically generated

1. The word document found within the user’s home directory contains the root password hidden within.

Text

Description automatically generated

1. The found credential can be used to switch to the root user and retrieve the flag.

Text

Description automatically generated