Forensics 2 Walkthrough

The zip file can be found (Due to space constraints): <https://1drv.ms/u/s!At4xJBcDqBvWhckXtnafvaDeHLH9ig?e=qaeP0O>

Requirements:

Nmap

Web browser

AccessData FTK Imager

OpenSSL

Difficulty:

Medium

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 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. Download and extract the “Disk.img” file.

Graphical user interface, text

Description automatically generated

1. Open FTK Imager, adding the extracted image file as evidence.

Graphical user interface, text, application

Description automatically generated

A picture containing table

Description automatically generated

1. Within the “/root” directory an encrypted flag file can be found.

Graphical user interface, text, application

Description automatically generated

1. The encryption key can be found in the “/root/.bash\_history” file.

Graphical user interface, text, application

Description automatically generated

1. The flag file can then be exported using FTK Imager and decrypted using OpenSSL to retrieve the flag.

Graphical user interface, text, application

Description automatically generated

Text

Description automatically generated