# Remote Code Execution Walkthrough

Requirements:

Nmap

Metasploit

Difficulty:

Medium

Walkthrough:

1. Build and host the docker server.
   * docker build -t <NAME> .
   * docker run -p 8080:8080 <NAME>
2. Run NMAP to find the open port.

Text

Description automatically generated

1. Inspect the website found on port 8080.

Graphical user interface, text, application

Description automatically generated

1. Website hints at Log4J. Using Metasploit to test if the site is vulnerable.

Graphical user interface

Description automatically generated

Setting the correct options and executing the script finds the site vulnerable.

Text

Description automatically generated

The exploit returns a low-privilege shell.

Text

Description automatically generated

1. The “joe” user can list its superuser privileges without a password.

Text

Description automatically generated

1. The “joe” user can run the “/usr/bin/time” program as root. This program can be used to elevate privileges according to “GTFO bins”.

A picture containing text

Description automatically generated

1. Elevating privileges allows the retrieval of the flag.

