PiHole Puzzle Walkthrough

Requirements:

Nmap

Netcat

Difficulty:

Easy - Medium

Walkthrough:

1. Build and host the docker server.
   * docker build -t <NAME> .
   * docker run --restart=unless-stopped -p 80:80 --dns=8.8.8.8 <NAME>
2. Run NMAP to find the open port.

Graphical user interface, text

Description automatically generated

1. Navigating to the webpage on port 80 reveals a version 4.4 PiHole server.

Graphical user interface, table

Description automatically generated

1. Googling for a PiHole 4.4 vulnerability reveals an authenticated remote code execution vulnerability.

Text

Description automatically generated

1. To exploit this vulnerability the password is required. The password can either be found using brute forcing tools or trying common passwords as the password is “password”.
2. Downloading the exploit script found: <https://www.exploit-db.com/exploits/48519> and executing the download script results in a reverse shell. The exploit script can be edited to automatically offer the correct detail or entered manually.

Text

Description automatically generated

Capturing the reverse shell with a Netcat listener provides root access.

Text

Description automatically generated

1. Root access allows retrieval of the flag.

Text

Description automatically generated