Reverse Shell Walkthrough

Requirements:

Nmap

Netcat

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.

Text

Description automatically generated

1. Navigating to the webpage on port 80 reveals a PHP web shell.

A screenshot of a computer

Description automatically generated

1. The web shell can be used to open a reverse shell.



The reverse shell one-liner can be found: <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#php>

The reverse shell is caught using Netcat.

Text

Description automatically generated

1. The config file found within the website directory reveals a set of credentials.

Graphical user interface, text

Description automatically generated

1. Using the found credentials to switch users.

Graphical user interface, text

Description automatically generated

1. Within the user’s home directory there is a script that has SUID permissions and is executable by the user.

Text

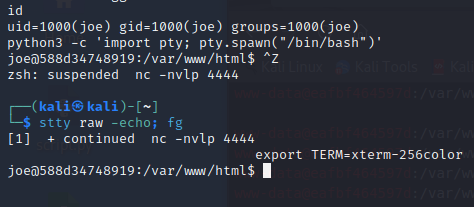
Description automatically generated

1. Following the instructions and entering “Ctrl+C” when the program is executing exits the reverse shell.

Text

Description automatically generated

1. To be able to enter “Ctrl+C” without exiting the reverse shell requires upgrading the shell to be fully interactive. The following series of commands can be used to elevate the shell.
   * python3 -c 'import pty; pty.spawn("/bin/bash")'
   * CTRL + Z
   * stty raw -echo; fg
   * export TERM=xterm-256color



1. The fully interactive shell allows the script to detect the “Ctrl+C” and output the flag.

Text

Description automatically generated