Tiny File Manager Walkthrough

Requirements:

Nmap

Python, Netcat, and OpenSSL (Used in this walkthrough but are optional)

Difficulty:

Medium-High (Multiple steps)

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 webserver on port 80 reveals a Tiny File Manager login portal.

Graphical user interface, application, website

Description automatically generated

1. Researching Tiny File Manager reveals numerous vulnerabilities. ExploitDB has one for version 2.4.6 the most recent vulnerable version currently.

A screenshot of a computer

Description automatically generated

1. Downloading and executing the exploit script using the suggested credentials results in a web shell.

Text

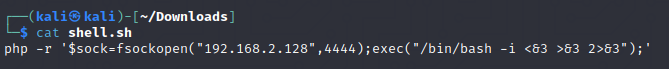
Description automatically generated

Text

Description automatically generated

1. Upgrading to a semi-interactive shell can be done using an uploaded PHP reverse shell. The reverse shell one-liner was found at <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#php>.

The one-liner is then placed within a bash script and uploaded to the victim machine using a python webserver.



Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

The shell script can then be executed and captured using a Netcat listener.



Text

Description automatically generated

1. Scanning the victim machine with an automatic script or manually checking common misconfigurations reveals that “/etc/passwd” is writable. Adding a new user to this file allows for privilege escalation.

Text

Description automatically generated

Creating a password using OpenSSL.

Text

Description automatically generated

Adding the new user and password to “/etc/passwd”.



Switching to the new “admin” user with the password “password” grants access to the root account.

Text

Description automatically generated

1. Retrieve the flag from “/root/Flag.txt”.

Text

Description automatically generated with medium confidence