Round 1: Log file traversal

A guideline to round 1 of NWC: CTF 2025, hosted by NWC Association.

Introduction

Let's go through the what, and why of logs in a system. Logs are lists of texts that contain the actions done by a user, program or kernel. For example, a log file may contain all the packages installed in a system by a package manager, and there can be many package managers in a system, e.g **apt, yum or nix** are examples of package managers found in linux based distros, **winget** in terms of windows, and **homebrew** in terms of MacOS.

How to view logs in a linux system.

Logs in linux can be viewed by going to the directory **/var/log,** which contains, for example

Var/log/auth.log:
Stores authentication logs, including successful and failed logins

Var/log/syslog:
Tracks errors related to application services and other messages logged during system startup

Var/log/boot.log:
Contains information logged when the system boots

Var/log/daemon.log:
Contains information about running system and application daemons

Var/log/dmesg:
Contains messages from the kernel ring buffer, including information about hardware components, drivers, and kernel initialization.

Var/log/kern.log:
Logs kernel information and events on the system

Var/log/mail.log: Contains information about mail server related details, such as postfix, smtp, MailScanner, and SpamAssassin

Objective

In round 1, you have to download an encrypted file **logs.zip** from the url (https://ctf-docs-gyre.onrender.com/logs) for which you have to find a passphrase using the riddles given in the same webpage to extract the content for further inspection.

The passphrase is of the format “*solution1-solution2-solution3-solution4*”, this is your first flag of the CTF.

What to look for?

The logs presented are from a computer used to create the challenge, along with other processes, there are also tampered segments hiding the further flags. Refer to the workflow below, and imagine the possible file to look for.

Workflow

Downloaded an open-source tool used for image modification, from a well known package manager in linux. → Use the tool to divide the image hiding the flag into several segments → Use a cli tool to encrypt the sequence of images, using a well known encryption algorithm.

Downloading the images.

Once finding all the names of encrypted images, they the can downloaded by visiting the url https://ctf-docs-gyre.onrender.com/download/<image-name>

Flags

You have to submit

a. Passphrase for extracting the **logs.zip**
b. 8 encrypted names of the images.

Points.

You’ll be awarded a grand total of 25 points, if you’re able to find all the flags in this round. If failing to do so, you’ll be awarded an equity split of 25 points for every flag found.

Qualification to round 2:

Only the top 50% of the teams will qualify for the next round.

Where to submit the flags:

A google form will be distributed at the end of each round, where you can submit your flags for evaluation. Submitting irrelevant options will lead to immediate disqualification.