LAMP Log Search Workout

Introduction

In this workout, you will learn the basics of using the command line tools *cat* and *gr ep* to analyze logs generated by a LAMP (Linux, Apache, MySQL, PHP) web server.

Begin by logging into your workout with the Enter Workout button on your landing page. Log in using the credentials provided on your landing page.

Tools

For this exercise, you will only need two command line tools: *cat* and *grep*

cat is a simple method of reading text files directly from the command line. For example, if you wished to read a file called example.txt, rather than opening it in a word processor, you could simply type *cat example.txt* in the command line. This will print all the text in the file to the terminal window. An important note is that you must be in the same directory as the file you wish to read. To navigate through the various folders, use the *cd* (change directory) command (`cd /<destination_folder>` to move into a folder, `cd ..` to move back to the parent folder). To show all the files in the current directory, you can use the *ls* (list) command.

grep is a command line tool used to search through text for certain patterns. It is similar to using Ctrl + F (or Command + F for Macs) to search for text in a particular document.

You can use these two commands together to open documents, and quickly find valuable information without having to read through the entire file yourself. To use the tools together, you pipe the output of *cat* into the *grep* command. This is done using the | character (Shift + \). For example, to find the sentence “This is an example” in example.txt, you would enter the following command into the terminal: *cat example.txt | grep “This is an example”* .

Objective

You will be given access to a poorly configured LAMP server. This server has been targeted by several different forms of cyberattack. The attacks include editing server files, executing foreign code, and a slowloris Denial of Service (DoS). Your mission is to find evidence of these attacks by analyzing the logs generated by the server.

After logging in to your workout, open the terminal on the desktop and navigate to the /var/log directory. This is the location that stores the various logs generated by the system. The folders that you are most interested in are /var/log/apache2 and /var/log/mysql (the logs for the Apache server and the MySQL database). As mentioned above, you can use the *cd* command to move between directories. You can also use the *pwd* (print working directory) command to show which directory you are currently in if you get lost.

In the /apache2 folder, there are two main files: access.log.1 and error.log.1. The first maintains a list of all requests made to the server, the latter keeps track of any internal errors the server may encounter. For example, a DoS attack would likely generate many entries in access.log to random URLs on the server. Similarly, in the /mysql server, there are two main files: error.log and mysql.log (they may be under error.log.1 and mysql.log.1, depending on when the server rotated the logs. The files with the most traffic are the ones in question). The former keeps track of any database errors encountered while the server is running, the latter maintains a list of ALL queries made to the database. You may have to unzip the files in the mysql folder (if the files end in .gz). If this is the case, you can simply type `gunzip <file>.gz` to gain access to the files.

You have been given a list of questions on your landing page to inspire your search of the logs. Use the *cat* and *grep* commands to find the relevant information, and submit it on the landing page.