Linux Incident Response - using the find command

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-11-10

Introduction to the Find Command

The find command in Linux is a powerful utility for searching and locating files and directories within the filesystem hierarchy based on a wide range of criteria such as names, sizes, modification dates, and permissions. It traverses the directory tree, starting from a given path, and evaluating each file and directory against the specified criteria. The true power of find lies in its flexibility and the vast array of options that can be combined to refine the search.

Basic Usage of Find

The general structure of the find command is: **find [starting point] [expression]**.

The indicates where should start searching. If no starting point is specified, uses the current directory by default. The part of the command can include tests (like or), actions (like or), and options (like or), which can affect the tests and actions.

Here are a few components of the :

- **Tests**: These are used to specify criteria that determine which files or directories match (e.g., , ,).
- **Actions**: These define what to do with the matching files (e.g., , ,).
- **Options**: These modify the behaviour of the command itself (e.g., to limit the search depth of directories).

Examples and use-cases

To begin with a simple example: finding files by name is straightforward with find. The following command searches for files named access.log starting from the current directory and descending into all subdirectories:

This command will output the path to any file named access.log within the current directory tree.

Finding Files by Modification Date

When investigating a security incident, it's often necessary to identify files modified within a specific time frame. The find command can locate binary files that have been modified between two dates using the -newermt and ! -newermt options:

This command searches the entire filesystem for executable files modified between 1 January 2023 and 4 January 2023.

Identifying Files with SUID Bit Set

Files with the SUID bit set can pose a security risk, especially if they are not properly managed. To find all files with the SUID bit set, use:

This search is critical in DFIR (Digital Forensics and Incident Response) to ensure that SUID executables have not been tampered with or maliciously introduced.

Searching for PHP Files Containing Specific Strings

A common task in incident response is to search for signs of webshells or other malicious code. To find PHP files and then search within them for a particular string, such as a common webshell keyword, you can combine find with grep:

This command will list PHP files under the /var/www directory that contain the string **eval($_POST**, which is frequently used in webshells.

Advanced Use of Exec

The exec directive within find allows for the execution of external commands on the found files. For instance, to change the permissions of all .txt files to 644, one would use:

Each file found is represented by {}, and the command terminates with \;.

DFIR-Specific Applications

In DFIR, the find command's ability to identify files based on permissions, timestamps, and other attributes is invaluable. For example, to locate files that were accessed or modified within a recent time window, which might indicate unauthorized access, the following command can be used:

This finds files accessed within the last 60 minutes.

Archiving Found Files

During an incident response, you might need to archive files of interest. With find and tar, you can archive all .conf files modified in the last two days:

This archives recently modified configuration files, which may contain changes made by an intruder.

Conclusion

The find command is an essential tool for systems administrators and forensic investigators alike. It provides a comprehensive search capability that can be tailored to very specific file conditions and can be combined with other commands to perform a wide range of actions on the found items. Mastery of find and its options enables professionals to efficiently locate potential evidence of system compromise or to simply manage files systematically. With its scalability and flexibility, find is indispensable in the realm of Linux DFIR.

Further study

If you want to learn more about Linux Incident Response, have a look at the SANS Institute course FOR577 "Linux Incident Response and Threat Hunting" - https://sans.org/for577

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858