Learn All About Linux File Systems

In this blog explain Linux File System Architecture, File system Hierarchy atandard (FHS), Extended File System (EXT), Second Extended File System (EXT2), Second **Extended File System** (EXT2) (Cont'd), Second Extended File System (EXT2) (Cont'd) etc…

Linux OS uses different file systems to store the data. As the investigators may encounter the attack source or victim systems to be running on Linux, they should have comprehensive knowledge regarding the storage methods it employs. The following section will provide you a deep insight about the various Linux file systems *and* their storage mechanisms.

Linux File System Architecture

The Linux file system architecture consists of two parts namely:

- **User Space:** The protected memory area where the user processes run and this area contains the available memory.

- **Kernel Space:** The memory space where the system supplies all kernel services through kernel processes. The users can access this space through the system call only. A user process turns into kernel process only when it executes a system call.

Related Product : Computer Hacking Forensic Investigator | CHFI

The GNUC Library (glibc) sits between the User Space and Kernel Space and provides the system call interface that connects the kernel to the user-space applications.
The Virtual file system (VFS) is an abstract layer, residing on top of a complete file system. It allows client applications to access various file systems. Its internal architecture consists of a dispatching layer which provides file system abstraction and numerous caches to enhance the file system operations performance.
The main objects managed dynamically in the VES are the dentry and inode objects in cached manner to enhance file system access speed. Once a user opens a file, the dentry cache fills with entries that represent the directory levels which in turn represent the path. The system also creates an inode for the object which represents the file. The system develops a dentry cache using a hash table and allocates the dentry cache entries from the dentry_cache slab allocator. The system uses a least-recently-used (LRU) algorithm to prune the entries when the memory is scarce.
The inode cache acts as two lists and a hash table for quick look up. The first list defines the used inodes and the unused ones are positioned in the second list. The hash table also stores the used inodes.
Device drivers are pieces of code, linked with every physical or virtual device and help the OS in managing the device hardware. Functions of the device drivers include setting up hardware, getting the related devices in and out of services, getting data from hardware and giving it to the kernel, transferring data from the kernel to the device, and identifying and handling device errors.

Filesystem Hierarchy atandard (FHS)

Linux is a single hierarchical tree structure, representing the file system as one single entity. It supports many different file systems. It implements a basic set of common concepts, developed for UNIX. Some of the Linux file system types are minix, Filesystem Hierarchy Standard (FHS), ext, ext2, ext3, xia, msdos, umsdos, vfat, /proc, nfs, iso 9660, hpfs, sysv, smb, and ncpfs. Minix was Linux's first file system.

The following are some of the most popular file systems:

Filesystem Hierarchy Standard (FHS)

The File system Hierarchy Standard (FHS) defines the directory structure and its contents in Linux and Unix-like operating systems. In the FHS, all files and directories are present under the root directory (represented by /).

Extended File System (EXT)

The Ext file system, released in April 1992, is the first file system developed for Linux. It came as an extension of the Minix file system and to overcome some of its limitations such as 64 MB partition size and short file names. The Ext file system provides a maximum partition size of 2 GB and a maximum file name size of 255 characters. The major limitation of this file system was that it did not offer support for separate access, inode modification, and data modification timestamps. It kept an unsorted list of free blocks and inodes, and fragmented the file system.

This has a metadata structure inspired by Unix File System (UFS). Other drawbacks of this file system include only one timestamp and linked lists for free space, which resulted in fragmentation and poor performance. The second extended file system (Ext2) replaced it.

Second Extended File System (EXT2)

Remy Card developed the second extended file system (ext2) as an extensible and powerful file system for Linux. Being the most successful file system so far in the Linux community, Ext2 is the basis for all of the currently shipping Linux distributions.

Read More : https://info-savvy.com/learn-all-about-linux-file-systems/

This Blog Article is posted by

Infosavvy, 2nd Floor, Sai Niketan, Chandavalkar Road Opp. Gora Gandhi Hotel, Above Jumbo King, beside Speakwell Institute, Borivali West, Mumbai, Maharashtra 400092

Contact us – www.info-savvy.com