Byron Laferriere

IT-365

Professor Hardikar

Milestone One: Linux

**File Structure**

The Linux kernel will be the focus of this final project this semester. This system uses the standard Unix file-system model (Silberschatz et al, 2009). This means that a file or object does not have to be stored on a disk or retrieved from a server, instead the file can be anything capable of handling input or output from data (Silberschatz et al, 2009). Through this design, the Linux kernel uses a Virtual Filing System (VFS) that is designed around object-oriented principles and has four main object types. They are as follows: an inode object, a file object, a superblock object, and a dentry object. The file structure on the Linux system follows the Filesystem Hierarchy Structure (FHS) file system that most Unix systems use (Hoffman, 2016). Everything is located under the /root directory for the system. Beneath this design, there are folders like /etc, /boot, /bin, and /dev that contain key system functionality for the kernel (Hoffman, 2016). All of these folders interact with /root in order to help the system function correctly.

**File Type**

According to Linux.com there are only seven types of files that can be specified for the Linux kernel operating system. The Linux kernel views just about anything as a file, therefore makes storage of these objects simple to identify. The file types used are regular files, directory files, and special files. Now within this spectrum, special files actually contains five types of files, which is why there are considered to be seven types of files used by the Linux system (Anne, 2016). These special file types are:

* Block file(b)
* Character device file(c)
* Named pipe file or just a pipe file(p)
* Symbolic link file(l)
* Socket file(s)

There is another type of file that can be found in the Sun Solaris systems called file(D), which could actually bring the total of Unix/Linux file system types to eight (Anne, 2016). The regular file type is used to store items like readable files, binary files, image files, compressed files, etc… (Anne, 2016). The directory file type is used to store files, folders, or special files in containers on a physical device (Anne, 2016). Combining these simple, yet powerful file combinations is just one reason why this FHS system is superior in file management strategies.

**File Access Mechanisms**

The Linux system uses a security model that is closely tied to the mechanisms provided through the UNIX OS (Silberschatz et al, 2009). By combining authentication and access control, these systems offer a very secure system for any user. Authentication is used to ensure that nobody can access the system without first proving that they have the proper entry rights. Access control is the mechanism used for checking whether a user has the right to access a certain object and prevent access to those same objects as necessary (Silberschatz et al, 2009). Using what is referred to as the ‘salt value’, the system stores the encrypted authentication password in a file and recombines the password entry with the ‘salt’ to see if it is a match (Silberschatz et al, 2009). Access control is another essential piece of the machine’s security. Through unique user identifiers (UID) and group identifiers (GID), the system is able to manage and control access rights across the server. Every file in the system can be controlled by this mechanism which adds an extra level of security for users. The only thing that can override the privileges attached to each file is the root user of the system (Silberschatz et al, 2009). Because of the design of the file system, it is commonly accepted that UNIX and Linux do not need antiviral or malware protection.

**Operating System Protection**

Much like UNIX systems, Linux is thought to need no extra security software like anti-virus software. However, with the way that cybersecurity is progressing it is more important than ever to ensure the safety of your information that is stored on the machines we use. With this in mind, anti-virus software and malware protection are always available through third parties online for any platform. Linux does have certain distributions that emphasize security more than others. The security offered through different features available for Linux users is beginning to outshine the MacOS these days. Features like file transfers securely via SFTP, secure connections with SSH available, and access to remote desktop clients are forerunners in the argument (Moth & Hyde, 2020). The most secure Linux distro’s available to the public and used by many famous hackers and whistleblowers like Ed Snowden are Qubes OS, Tails Linux, and Kali Linux. I have heard of Kali Linux’s popularity among the cybersecurity world before, mainly for its free courses on ethical hacking and bundled pen-testing (penetration testing) tools that it comes with. The Qubes OS platform is very intriguing due to its compartmentalization of each application upon launching them into virtual machines (Moth & Hyde, 2020). Through innovations like this, Linux is able to surpass mainstream operating systems in safety offered and the price paid for that safety.

References:

Anne, S. (2016, February 10). File types in Linux/Unix explained in detail. Retrieved March 14, 2021, from <https://www.linux.com/training-tutorials/file-types-linuxunix-explained-detail/>

Hoffman, C. (2016, September 22). The Linux directory Structure, Explained. Retrieved March 14, 2021, from <https://www.howtogeek.com/117435/htg-explains-the-linux-directory-structure-explained/#:~:text=%20The%20Linux%20Directory%20Structure,%20Explained%20%201,the%20files%20needed%20to%20boot%20the...%20More>

Moth, J., & Hyde, T. (2020, July 21). Top 10 most SECURE distros for complete protection & privacy in 2020. Retrieved March 14, 2021, from <https://www.blackdown.org/most-secure-linux-distros/>

Silberschatz, A., Galvin, P. B., & Gagne, G. (2009). *Operating System Concepts with Java* (8th ed.). John Wiley & Sons.