**Component 3**

**Design comparison between Linux and windows**

Linux: Linux is an open-source (freely available), Unix-like operating system kernel. Linux is the core part of an operating system that handles crucial tasks such as managing memory, organizing files, handling basic networking functions, and providing fundamental services to the entire operating system. Linux has a huge support for a broad selection of hardware platforms, making it the main Unix-like system in the current time. (Unix Fundamentals — System Administration for Cyborgs, 2016). Linux is composed of three layers: hardware, encompassing the tangible components of a machine (memory and processor); the kernel, acting as the interface between hardware and software while also managing memory and CPU control; and processes, which are programs in execution on the system under the supervision of the kernel ("https://phoenixnap.com/kb/what-is-linux?", 2023).

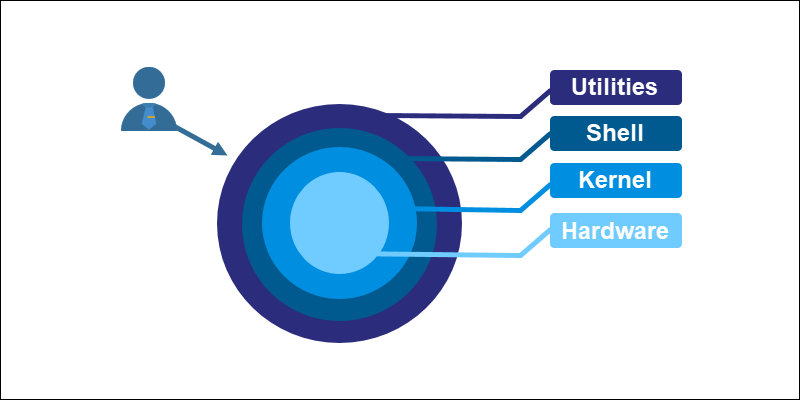


Figure 1: Picture Source: PhoenixNAP (2023) 'What is Linux?' Available at: https://phoenixnap.com/kb/what-is-linux? (Accessed: 19 December 2023)

**The three commands**

Cp: The cp command is a handy tool in Unix-like systems for copying files and folders. It does three main things, each with a specific job. You can use it to copy individual files, copy entire folders along with their contents, and make sure important details like creation dates stay the same in the copies. So, cp is a versatile tool that helps you easily duplicate and manage your files. The cp command in Unix-like operating systems features several useful flags to customize its functionality. The -r or -R flag allows for the recursive copying of directories and their contents, while the -i flag prompts the user for confirmation before overwriting existing files. The -u flag copies only when the source file is newer, and the -a flag preserves the original file's attributes and there is many more.

Cat: The cat command is one of the most widely used commands in Linux. The name of the cat command comes from its functionality to concatenate files. It can read, concatenate, and write file contents to the standard output. If no file is specified or the input file name is specified as a single hyphen (-), it reads from the standard input. The cat command in Unix-like operating systems offers several flags to enhance its functionality, and three notable ones are -n, -E, and -T. The -n flag introduces line numbering, which is especially useful when dealing with large text files, as it provides a quick reference for specific lines. With the -E flag, the command appends a dollar sign ('$') at the end of each line, making it easier to visually identify line breaks and there is many more.

Rm: The rm command in Linux is used to delete files and directories. You can remove a single file with rm filename, delete multiple files with rm file1 file2, or use rm -r directoryname to recursively remove a directory and its contents. The -f option can be added to force removal without confirmation.

|  |  |
| --- | --- |
| Windows | Linux |
| Has different versions and pricing options. | Most distributions are free of charge. |
| Distributed under a license that restricts user’s ability to modify the software. | Open source, publicly available. |
| Extremely simple to use. | Simple to use but there are significant barriers for newcomers. |
| Programs are downloaded from websites or physical storage media. | Programs are supplied from fixed repositories. |
| The stability of windows has improved over the years but still not on Linux’s level. | Extremely stable to run. |
| Frequently threatened by viruses and other malware. | Very rarely attacked. |
| The longer it is used the slower it runs. | Generally, runs very quickly. |

|  |  |  |  |
| --- | --- | --- | --- |
| **System calls triggered** | **cp** | **cat** | **rm** |
| open | Y | Y | Y |
| Fstat64 | Y | Y | Y |
| Brk | Y | Y | Y |
| Access | Y | Y | Y |
| Read | Y | Y | Y |
| Mmap2 | Y | Y | Y |
| Mprotect | Y | Y | Y |
| execve | Y | Y | Y |
| Fadvise64 | N | Y | N |
| close | Y | Y | Y |
| munmap | Y | Y | N |
| write | Y | N | Y |
| lseek | N | N | Y |
| Exit\_group | Y | N | Y |
| uname | Y | N | N |
| getrlimit | Y | N | N |
| ioctl | N | N | Y |

**System call analysis**

The open() system call is used to access the file identified by the given pathname. If the specified file is not present, it can be created as an option when open() includes the flag O\_CREAT. The outcome of open() is a file descriptor, a small, non-negative number serving as an index in the process's list of open file descriptors. The argument flags must include one of the following access modes: O\_RDONLY, O\_WRONLY, or O\_RDWR. These request opening the file read-only, write-only, or read/write, respectively ("https://www.man7.org/linux/man-pages/man2/open.2.html”, n.d.).

The Brk() system call modifies the position of the program break, determining the end of the data segment for a process. If the Brk() call succeeds, it returns 0; otherwise, it returns -1 along with an associated error code stored in the variable ‘errno’. The Brk() function takes a single argument, indicating the new end of the data segment or heap. This argument is a pointer to the desired top position of the heap, leading to the extension or reduction of the heap up to this specified address ("https://stackoverflow.com/questions/6988487/what-does-the-brk-system-call-do”, n.d.).

The mmap() system call establishes a new mapping in the virtual address space of the calling process. It has a length parameter that indicates the size of the mapping, and it must be greater than 0. There is also the ‘prot’ argument which describes the desired memory protection of the mapping, It is either PROT\_NONE or the bitwise OR of one or more of the following flags: PROT\_EXEC, PROT\_READ, PROT\_WRITE and PROT\_NONE. By their names, what they do is allow pages to be executed, read, written on or not be accessed. After the mmap() call has returned, the file descriptor, can be closed immediately without invalidating the mapping (“https://www.man7.org/linux/man-pages/man2/mmap.2.html”, n.d).

write() system call writes from a buffer to a file referred to at the start of the argument. It writes up to a number of bytes which is specified after the destination file in the argument. When the process is successful the number of bytes written is returned, but when its not -1 is returned (“https://www.man7.org/linux/man-pages/man2/write.2.html”, n.d).

lseek() is a system call in Linux that moves the position in a file where the next read or write operation will occur. It adjusts the file offset of the open file description associated with a given file descriptor. The new position is determined by the parameter following the given file parameter. Whereas there is a third argument which specifies how to interpret the offset (“https://www.man7.org/linux/man-pages/man2/lseek.2.html”, n.d).

**What is Strace?**

Strace is a tool in Linux that is used to view the system calls made by a process/command. It allows you to see the interactions made between a program and the kernel.

Here are the results of strace for the 3 commands:

cp (3 screenshots)

**A screen shot of a computer screen

Description automatically generated**

**A screen shot of a computer screen

Description automatically generated**

**A screen shot of a computer screen

Description automatically generated**

**rm (2 screenshots)**

**A computer screen shot of a computer error

Description automatically generated**

**A screen shot of a computer screen

Description automatically generated**

**cat**

**A screen shot of a computer screen

Description automatically generated**

**System calls comparison between Linux and Windows**

|  |  |
| --- | --- |
| Windows | Linux |
| copy | cp |
| del | rm |
| type | cat |

Copy: The copy command is used in windows. It is used to replicate a file or a group of files, storing the other version in a different address of your choice. There are different copying options just like cp in Linux (flags).

Del: The del command is used in windows. It is used to remove a file or a directory.

Type: The type command is used in windows. It is used to display the contents of a file or to concatenate multiple files.

CreateFile() is a system call in windows similar to the open() system call in Linux. It is used to create or open a file and is used in the copy, del and type commands.

Readfile() is a system call in windows similar to the read() system call in Linux. It is used to read the content of files and is used in the copy, del and type commands.

WriteFile() is a system call in windows similar to the write() system call in Linux. It is used to write data to a file and is used in copy and type commands.

CloseHandle() is a system call in windows similar to the close() system call in Linux. It is used to close file handles and is used in copy, del and type commands.

**Other equivalent system calls**

|  |  |
| --- | --- |
| Windows | Linux |
| CreateProcess | execve |
| GetFileAttributes | access |
| VirtualAlloc | Mmap2 |
| HeapFree | Brk(null) |
| SetFilePointer | llseek |

**References**

Cyborg Institute (2016). Unix Fundamentals — System Administration for Cyborgs. *Cyborg Institute*. Available at: <http://cyborginstitute.org/projects/administration/unix-fundamentals/> (Accessed: 19 December 2023).

*PhoenixNAP* (2023). What is Linux? Available at: <https://phoenixnap.com/kb/what-is-linux> (Accessed: 19 December 2023).

Linux Manual Pages. (n.d.). open(2) - Linux manual page. The Linux man-pages Project. <https://www.man7.org/linux/man-pages/man2/open.2.html>

Stack Overflow. (n.d.). What does the brk() system call do? Stack Overflow. <https://stackoverflow.com/questions/6988487/what-does-the-brk-system-call-do>

Linux Manual Pages. (n.d.). mmap(2) - Linux manual page. The Linux man-pages Project. <https://www.man7.org/linux/man-pages/man2/mmap.2.html>

Linux Manual Pages. (n.d.). write(2) - Linux manual page. The Linux man-pages Project. <https://www.man7.org/linux/man-pages/man2/write.2.html>

Linux Manual Pages. (n.d.). lseek(2) - Linux manual page. The Linux man-pages Project. <https://www.man7.org/linux/man-pages/man2/lseek.2.html>