

Binaries: This term refers to files that can be executed, similar to executables in Windows. Binaries generally reside in the `/usr/bin` or `usr/sbin` directory and include utilities such as `ps`, `cat`, `ls`, and `cd` as well as applications such as the wireless hacking tool `aircrack-ng` and the intrusion detection system (IDS) `Snort`.

Case sensitivity: Unlike Windows, Linux is case sensitive. This means that `Desktop` is different from `desktop`, which is different from `DeskTop`. Each of these would represent a different file or directory name. Many people coming from a Windows environment can find this frustrating. If you get the error message “file or directory not found” and you are sure the file or directory exists, you probably need to check your case.

Directory: This is the same as a folder in Windows. A directory provides a way of organizing files, usually in a hierarchical manner.

Home: Each user has their own `/home` directory, and this is generally where files you create will be saved by default.

Kali: Kali Linux is a distribution of Linux specifically designed for penetration testing. It has hundreds of tools preinstalled, saving you the hours it would take to download and install them yourself.

root: Like nearly every operating system, Linux has an administrator or superuser account, designed for use by a trusted person who can do nearly anything on the system. This would include such things as reconfiguring the system, adding users, and changing passwords. In Linux, that account is called `root`. As a hacker or pentester, you will often use the `root` account to give yourself control over the system. In fact, many hacker tools require that you use the `root` account.

Script: This is a series of commands run in an interpretive environment that converts each line to source code. Many hacking tools are simply scripts. Scripts can be run with the `bash` interpreter or any of the other scripting language interpreters, such as `Python`, `Perl`, or `Ruby`. `Python` is currently the most popular interpreter among hackers.

Shell: This is an environment and interpreter for running commands in Linux. The most widely used shell is `bash`, which stands for Bourne-again shell, but other popular shells include the `C shell` and `Z shell`.

Terminal: This is a command line interface (CLI).