1. Privilege escalation

In the world of computer systems, they are designed to be used from multiple users and each user can have different abilities. These abilities are called privilege. A privilege can be defined as a special right, advantage, or immunity granted or available only to a particular person or group of people (google dictionary). Examples of privilege can be view and edit files, modify system files, delete and/or create users, etc. Depending on the users, they are granted different functionalities that they can do within the system and, in the other hand, depending on the account, the person are restrict to do just specific functions on the system. When a commoner user have more than usual privileges on the system, it can be problematic since it can disrupt or modified unauthorized files, which can be a huge threaten for the system and occur data loss and stealing. Also, malicious users such as hackers, can be menace for the system because they try to get into others accounts so they can have access to the system with higher privileges that can do mischievous actions to the system. This situation is called privilege escalation, that is, the act of gaining access to resources which were intended to be protected by authorization mechanisms built into the targeted system (ppt). When the hacker successfully escalates the system privilege, he can use this preeminence to install virus, view private information about the user, and delete important files on the system. Most of the time, the privilege escalation occurs when a system has bug that allows security to be bypassed or, alternatively, has flawed design assumptions about how it will be used (wikipedia). In operating system, the highest privilege access is the kernel, which it’s a computer program that is the core of a computer’s operating system, with complete control over everything in the system (Wikipedia, kernel).

When it comes to privilege escalation in an operating system, it can be divided into two families. They are vertical privilege escalation and horizontal privilege escalation.

* 1. Vertical privilege escalation

As a basic concept, vertical privilege escalation is the use of existing access (whether granted or illicit) to gain resource access beyond what the current user or role is supposed to have access to. In many cases, the act being described is elevating from "normal user" to "administrator" or "root" privileges on a system (ppt).

In an operating system, when a user has the privilege of a kernel, there is nothing that the user can’t do it, since it’s the core of the operating system. Some examples about vertical privilege escalation in Operating systems, such as Windows and Linux, consist:

* Some [Windows services](https://en.wikipedia.org/wiki/Windows_service) are configured to run under the Local System user account. A vulnerability such as a [buffer overflow](https://en.wikipedia.org/wiki/Buffer_overflow) (an [anomaly](https://en.wikipedia.org/wiki/Anomaly_in_software) where a [program](https://en.wikipedia.org/wiki/Computer_program), while writing [data](https://en.wikipedia.org/wiki/Data_(computing)) to a [buffer](https://en.wikipedia.org/wiki/Buffer_(computer_science)), overruns the buffer's boundary and overwrites adjacent [memory](https://en.wikipedia.org/wiki/Main_memory" \o "Main memory)locations) may be used to execute arbitrary code with privilege elevated to Local System. Alternatively, a system service that is impersonating a lesser user can elevate that user's privileges if errors are not handled correctly while the user is being impersonated (e.g. if the user has introduced a malicious [error handler](https://en.wikipedia.org/wiki/Exception_handling))(Wikipedia).
* Under some legacy versions of the [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) operating system, the All Users [screensaver](https://en.wikipedia.org/wiki/Screensaver) runs under the Local System account – any account that can replace the current screensaver [binary](https://en.wikipedia.org/wiki/Executable) in the file system or [Registry](https://en.wikipedia.org/wiki/Windows_Registry) can therefore elevate privileges(Wikipedia).
* In certain versions of the [Linux kernel](https://en.wikipedia.org/wiki/Linux_kernel) it was possible to write a program that would set its current directory to /etc/cron.d, request that a [core dump](https://en.wikipedia.org/wiki/Core_dump) be performed in case it crashes and then have itself [killed](https://en.wikipedia.org/wiki/Kill_(Unix)) by another process. The core dump file would have been placed at the program's current directory, that is, /etc/cron.d, and [cron](https://en.wikipedia.org/wiki/Cron" \o "Cron) would have treated it as a text file instructing it to run programs on schedule. Because the contents of the file would be under attacker’s control, the attacker would be able to execute any program with [root](https://en.wikipedia.org/wiki/Superuser) privileges(Wikipedia).

Also, in the IOS operating system, there is a tool called Jailbreaking, that performs the act of breaking out of the chroot (a Linux operating system operation) or bypassing digital rights management (DRM). This allows the user to run arbitrarily defined code on devices with DRM as well as break out chroot-like restrictions (Wikipedia).

* 1. Horizontal privilege escalation

The definition of horizontal privilege escalation consists on a normal user accesses functions or content reserved for other normal users (paper1). Normally, this escalation happens when users give without consent their credential to the fraudulent or hacker, sometimes called phishing. This doesn’t necessarily have to elevate privilege. Also, this doesn’t necessarily attack the kernel, but it can modify the application level of the user, installing malware under the user level. If the victim user is given out higher privilege than a normal user has, it can have worse consequences on the operating system. For example, in an operating system, an user can only have to the permission to read. If for some reason, the user gets the credential of a higher privileged user, with writing authorization, this can lead the fraudulent to install(write) malware on their operating system.

<https://en.wikipedia.org/wiki/Privilege_escalation> (wikipedia)

<https://en.wikipedia.org/wiki/Kernel_(operating_system)>

(ppt) <https://pdfs.semanticscholar.org/presentation/2759/6cb3993d568ad6ecc34588123fdf6faea263.pdf>

<https://bryanavery.co.uk/vertical-and-horizontal-privilege-escalation/> (paper1)