**DLL Injection**

Other name: dll spoofing

We explain the relationship between dll injection and elevation of privilege. This attacked is also called: dll spoofing. (more information about attack can be found in spoofing descriptions)

**Description 1.**

DLL injectioncan be used to run code in the context of another process by causing the other process to load and execute code. Running code in the context of another process provides adversaries many benefits, such as access to the process's memory and permissions. It also allows adversaries to mask their actions under a legitimate process. A more sophisticated kind of DLL injection, reflective DLL injection, loads code without calling the normal Windows API calls, potentially bypassing DLL load monitoring. Numerous methods of DLL injection exist on Windows, including modifying the Registry, creating remote threads, Windows hooking APIs, and DLL preloading [1]

References

[1] https://attack.mitre.org/wiki/Privilege\_Escalation