Al crear contenedores LXC podemos definir si serán contenedores con o sin privilegios. Pero ¿cuál es la diferencia entre ambos?

Pues que los contenedores sin privilegios usan la característica «user namespaces» del kernel de Linux de forma que los identificadores de usuarios y grupos del contenedor (uid y gid, respectivamente) se mapean en el host con un rango numérico diferente al de los usuarios del propio host. Por ejemplo root, que en el host es uid 0, cuando se use en el contenedor, para el host será 100000; 1 del container será 100001 para el host, y asi sucesivamente. Esto lo que hace es que, en el caso extremo de que alguien tome control del contenedor como root, no pueda hacer nada en el host dado que operaría en el mismo siendo el usuario 100000, que para el host es un usuario inexistente y sin privilegios.