BOOL OpenProcessToken(

\_\_in   HANDLE ProcessHandle, //要修改访问权限的进程句柄

\_\_in   DWORD DesiredAccess, //指定你要进行的操作类型

\_\_out PHANDLE TokenHandle //返回的访问令牌指针

)； //通过这个函数我们就可以得到当前进程的访问令牌的句柄

第一参数是要修改访问权限的进程句柄；（指定函数的第一个参数GetCurrentProcess()就可以了）。

第二个参数指定你要进行的操作类型，如要修改访问令牌的特权，我们要指定第二个参数为TOKEN\_ADJUST\_PRIVILEGES（其它一些参数可参考Platform SDK）。通过这个函数我们就可以得到当前进程的访问令牌的句柄

|  |  |
| --- | --- |
| **值** | **含义** |
| TOKEN\_ADJUST\_DEFAULT | 需要更改访问令牌的默认所有者，主组或DACL。 |
| TOKEN\_ADJUST\_GROUPS | 需要调整访问令牌中的组的属性。 |
| TOKEN\_ADJUST\_PRIVILEGES | 需要启用或禁用访问令牌中的权限。 |
| TOKEN\_ADJUST\_SESSIONID | 需要调整访问令牌的会话ID。必须提供SE\_TCB\_NAME权限。 |
| TOKEN\_ASSIGN\_PRIMARY | 需要一个附加[主令牌](https://msdn.microsoft.com/en-us/library/ms721603(v=vs.85).aspx" \l "_security_primary_token_gly)一个[过程](https://msdn.microsoft.com/en-us/library/ms721603(v=vs.85).aspx" \l "_security_process_gly)。完成此任务也需​​要SE\_ASSIGNPRIMARYTOKEN\_NAME特权。 |
| TOKEN\_DUPLICATE | 需要复制访问令牌。 |
| TOKEN\_EXECUTE | 组合STANDARD\_RIGHTS\_EXECUTE和TOKEN\_IMPERSONATE。 |
| TOKEN\_IMPERSONATE | 必须将模拟访问令牌附加到进程。 |
| TOKEN\_QUERY | 查询访问令牌时需要。 |
| TOKEN\_QUERY\_SOURCE | 需要查询访问令牌的源。 |
| TOKEN\_READ | 组合STANDARD\_RIGHTS\_READ和TOKEN\_QUERY。 |
| TOKEN\_WRITE | 组合STANDARD\_RIGHTS\_WRITE，TOKEN\_ADJUST\_PRIVILEGES，TOKEN\_ADJUST\_GROUPS和TOKEN\_ADJUST\_DEFAULT。 |
| TOKEN\_ALL\_ACCESS | 组合令牌的所有可能的访问权限。 |

第三个参数就是返回的访问令牌指针；