

운영체제

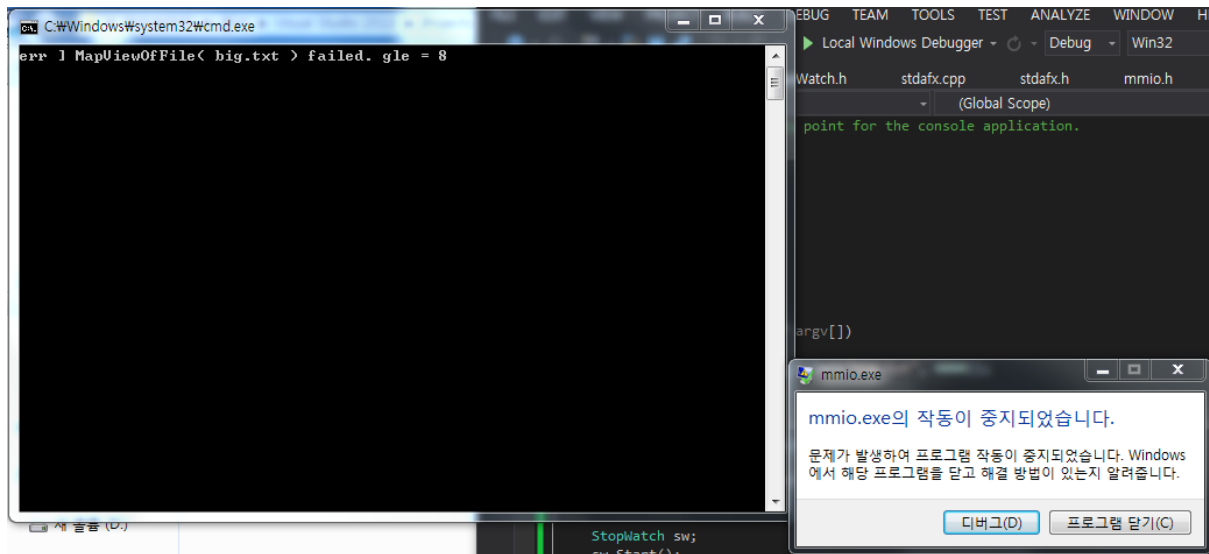
과제3

취약점 분석

이정민

4GB 이상 복사가 안되는 이유

:



getlasterror()함수의 리턴이 의미하는 에러 코드를 찾아보면 저장공간이 부족해서 명령을 수행할 수 없다는 걸 알 수 있다. 에러가 나는 부분은 open_map_context 함수에서 파일의 크기를 고려하여 파일 매핑 커널 오브젝트를 생성하는 CreateFileMapping 부분이다. 4GB 이상의 파일을 복사하기 위해 FileIoHelperClass를 사용할 수 있다.

해결 방법

: FileIoHelperClass.cpp와 헤더파일을 추가 한 후 main함수에서 간단한 코드만 추가하면 4GB 이상의 파일을 복사할 수 있다.

```
_ASSERT(create_very_big_file(L"big.txt",5000));

FileIoHelper fih;
LARGE_INTEGER size;
LARGE_INTEGER offset;
PUCHAR buf = (PUCHAR)malloc(4096);
StopWatch sw2;

size.QuadPart = (LONGLONG)4096;
offset.QuadPart = (LONGLONG)0;
sw2.Start();

fih.FIOpenForRead(L"big.txt");
fih.FIReadFromFile(offset, 4096, buf);
fih.FIOCreateFile(L"big2.txt", size);

fih.FIWriteToFile(offset, 4096, buf);

sw2.Stop();
print("info] time elapsed = %f", sw2.GetDurationSecond());
```

이 코드의 내용은 FIOpenForRead 함수를 통해 big.txt파일을 열고 createfilemapping을 통해 파일 매핑 커널 오브젝트를 생성한다. FIOCreateFile 함수를 통해 big2.txt 파일을 만들고 역시 createfilemapping을 실행한다. FIReadFromFile을 통해 받은 시작주소값과 사이즈를 FIReference 에 넘겨주고 FIOpenForRead에서 createfilemapping을 통해 받은 mFilemap을 Mapviewoffile의 첫번째 인자로 쓰고 주소 공간에 파일 매핑 오브젝트를 매핑시킨다. 결과는 mmio를 이용한 복사가 훨씬 빠르다.

```
info] time elapsed = 0.005159
info] time elapsed = 3.457978
계속하려면 아무 키나 누르십시오 . . .
```

