**Best of Best 11**

**Window 10 권한 상승 실습 과제**

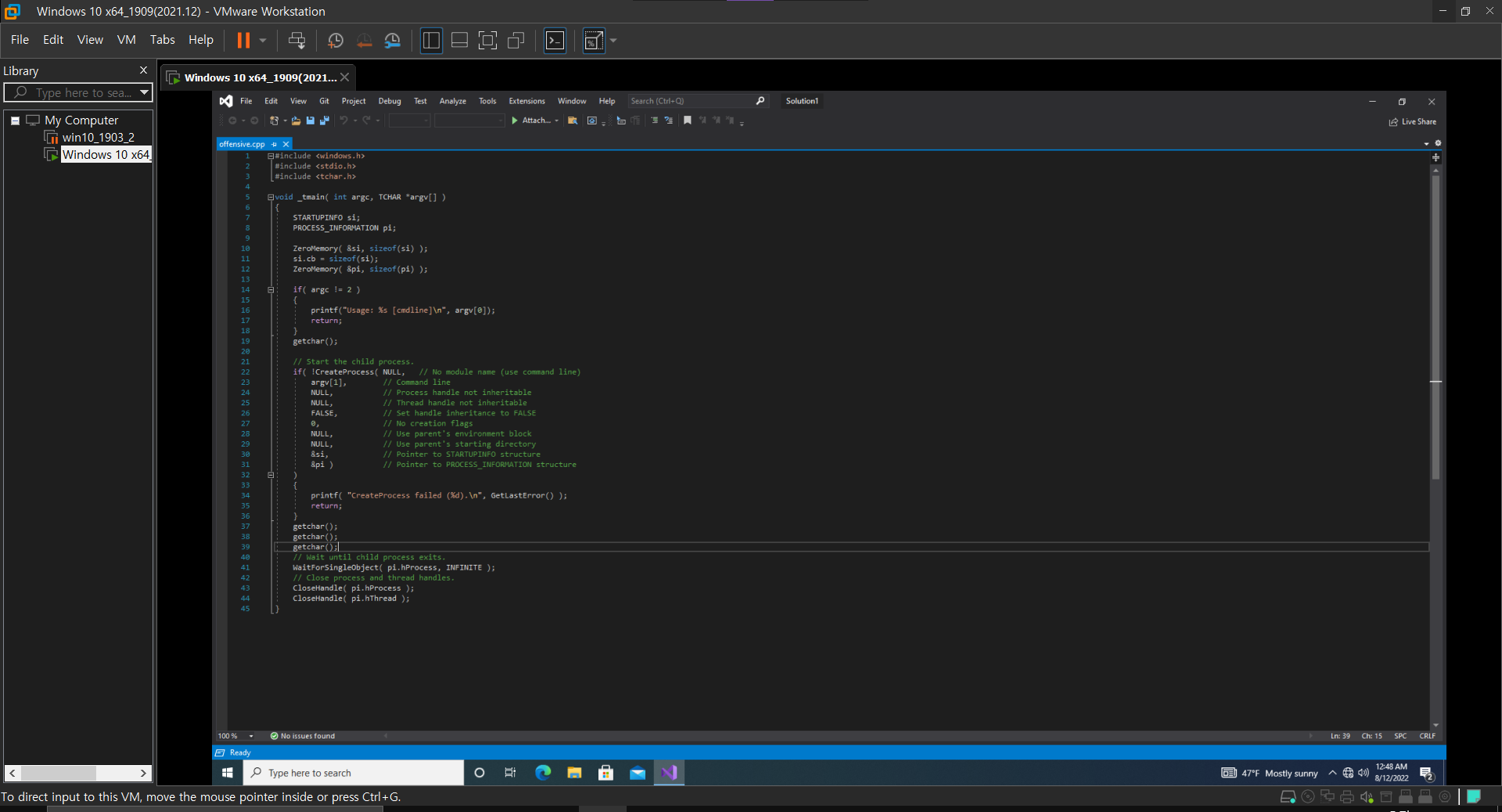
**남성엽 멘토님 과제 #1 번**

**Best of Best 11기**

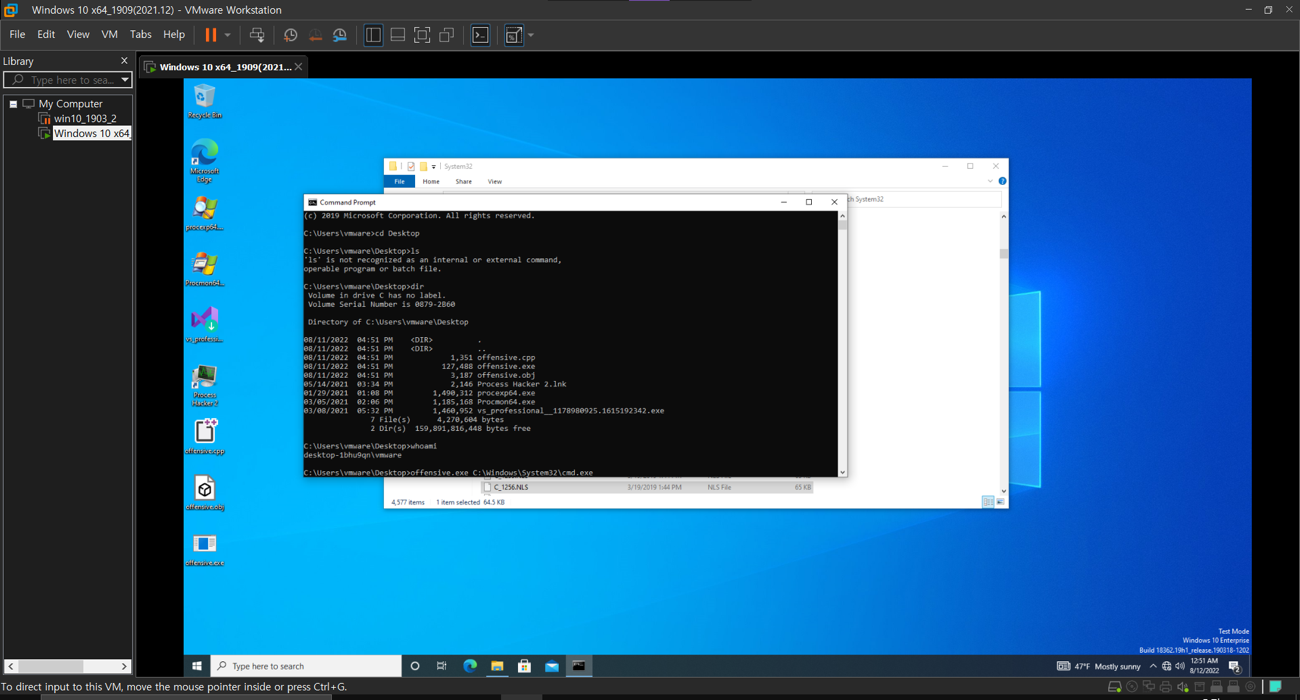
**보안제품 개발 희망 정경재**

**제출날짜:2022-07-07**

기본적인 방법은 윈도우에서 새로운 자식 프로세스를 생성할 때 디버깅모드를 통해 본 프로그램의 권한을 올리는 방법의 방식으로 토큰을 탈취했습니다.



해당 사진은 기본적인 코드에 getchar()를 넣어 자식 프로세스가 생기기 전에 임시로 멈추고 아래와 같이 디버깅 모드에 들어갔습니다.



해당 사진은 아직 프로그램의 권한이 상승되기전입니다.

Graphical user interface, text, application, email

Description automatically generated

먼저 CID가 4번인 system의 기본적인 프로세스 정보입니다.

해당 정보에서 system의 토큰값을 알아냈습니다.

다음은 아까 코드로 만든 offensive의 프로그램입니다.

Graphical user interface, text, application, email

Description automatically generated

해당 프로세스의 정보를 통해 위와 같은 토큰 값을 얻었습니다.

이후 프로세스 구조에서 토큰의 위치를 찾기위해 다음과 같은 명령어를 사용했습니다.

Dt nt!\_EPROCESS (아무 프로세스)

Graphical user interface, text, application, Word

Description automatically generated

해당 명령어를 통해 다음과 같이 토큰의 위치를 찾았고 다음의 명령어를 통해 토큰의 값을 변경했습니다.

Graphical user interface, application, Word

Description automatically generated

이후 권한 상승이 성공한 이후의 모습입니다.

A screenshot of a computer

Description automatically generated with medium confidence

Cmd창의 whoami가 wmware에서 system으로 변경되었습니다.

Text

Description automatically generated

해당 텍스트 파일은 권한상승을 위해 적었던 텍스트 입니다.