Document

2014313303 홍태하

1번은 그냥 실행하게 되면 system이라는 함수에 의해서 rebooting이 되게 된다. 그래서 rebooting은 되지 않고 그 사실을 프로그램은 알지 못하게 return값을 0으로 해주고 아무 기능도 수행하지 않도록 interpositoning을 해주면 된다.

2번은 그냥 실행하게 되면 unlink라는 함수에 의해서 important 파일을 지우게 된다. 그래서 1번과 마찬가지로 원래 함수의 기능은 사용하지 않게 하면서 return 값만 0으로 해줘서 프로그램은 그 함수가 제대로 작동된 것으로 알도록 한다.

3번은 프로그램이 Tigger라는 것의 password가 horangyi라는 것을 알아채지 못하게 해야 한다. 그래서 strtok라는 함수를 interpositoning하는데 strtok는 문자열을 문자로 자르는 함수이다. 첫번째 인수로 잘라질 string을 입력받고 두번째 인수로 자르기를 위한 문자를 호출한다. strtok가 처음 실행되면 잘라 내기한 문자열의 첫번째 포인터를 반환하며 이후에는 NULL과 자르기를 위한 문자만 인수로 전달하면서 잘라진 문자열들을 반환한다. 프로그램이 Tigger의 password를 알려고 하는데 assembly code를 보면 strtok이 두 번 실행된다. 첫번째는 “Tigger horangyi”라는 문자열을 자르는데 첫번째 포인터를 반환하므로 “Tigger”가 반환된다. 원래대로라면 두번째 실행되었을 때 “ “(공백)에 의해서 잘려진 “horangyi”를 반환할 것이다. 따라서 strtok의 return 값을 “Tigger”라고 하면 프로그램은 비밀번호를 Tigger라고 잘못 생각하게 할 수 있다.

4번은 프로그램이 password파일에 "Pikachoo zwi"라는 문자열을 추가하는데 이것을 막으면 된다. 먼저 fwrite라는 함수는 문자열의 길이를 반환하는데 "Pikachoo zwi"의 길이가 13이므로 return 13을 해주면 된다. 그리고 fgets라는 함수가 있는데 이 함수가 계속 반복되어서 실행된다. 근데 이 함수는 3번에서도 쓰이므로 call이라는 변수를 전역으로 선언해서 call이 그냥 0이면 제대로 작동하도록 해놓고 1증가시킨다. 그리고 만약 call이 0이 아닌 값이면 strcpy(str, "Pikachoo zwi\n"); return 0;을 해서 "Pikachoo zwi\n"가 원래 들어있는 것처럼 착각하게 하여 password파일에 추가 되지 않도록 한다.

5번은 들어가는데 시간이 1초이상 걸리면 time bomb가 되어서 실패하게 된다. main함수에서 보면 phase5에 들어가기 전에 sleep라는 함수가 작동된다. 이 함수는 남은 시간이 반환되므로 return 0만을 반환하도록 interpositioning해주면 phase5에 바로 들어갈 수 있게 되어서 time bomb가 작동하지 않게 된다.