REPORT:

x32dbg 사용법 및 CRACKME WRITEUP

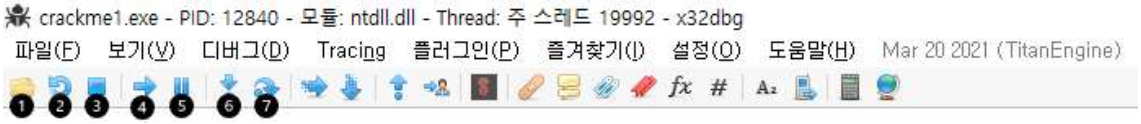
COLONY
1824275 정상지

2021.05.

1. x32dbg 사용법

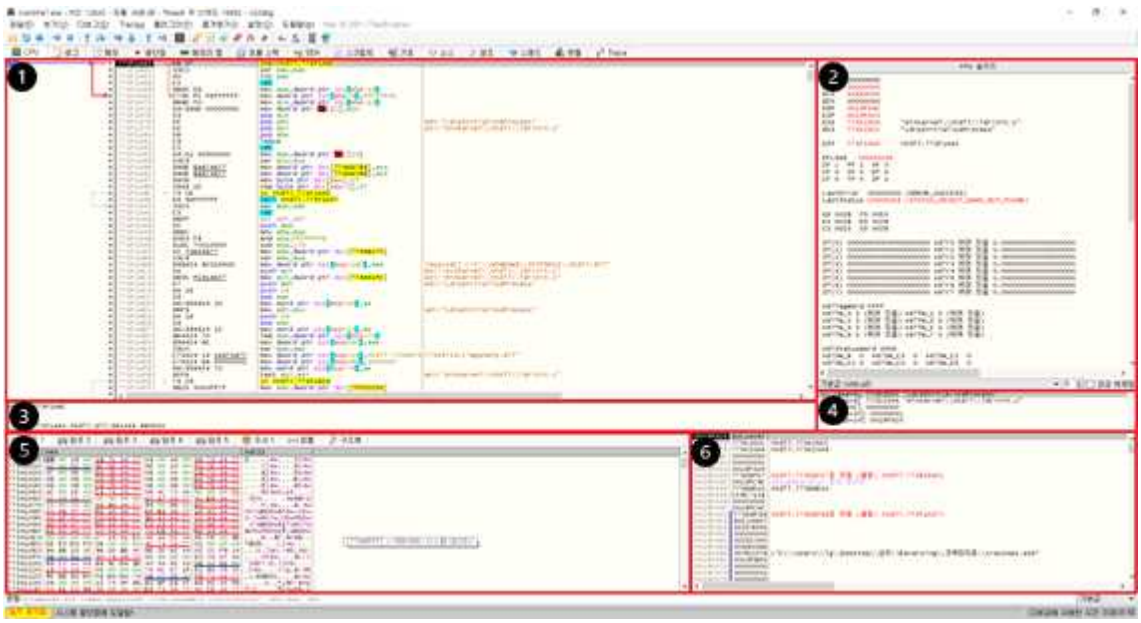
1) x32dbg 기본적인 인터페이스

(1) 상단바 인터페이스 구성



❶ 분석할 프로그램을 열기
❷ 프로그램 재시작
❸ 프로그램 정지
❹ 프로그램 실행/재개
❺ 프로그램 일시정지
❻ 어셈블리어 코드 한 줄 실행 -> call 함수 호출 시 call 함수 내부 진입
❼ 어셈블리어 코드 한 줄 실행 -> call 함수 호출 시 call 함수의 ret 명령어 실행까지 실행

(2) CPU 탭의 인터페이스 구성



❶ 주소 및 어셈블리어 코드, 사용자가 작성한 주석 등이 왼쪽부터 차례대로 표시
- 주소 / 옵 코드 / 기계어 코드 / 주석

❷ 현재 CPU 레지스터 상태가 표시
❸ ❶창에서 선택한 부분에 대한 정보가 표시
❹ 레지스터 중 esp의 값을 표시
❺ 메모리 덤프 창으로, 메모리 데이터를 16진수 바이트로 표시
❻ 스택 메모리 esp의 값과 스택을 보여주며, push가 이루어질 때 esp는 4가 줄어듦

2) 단축키 사용

(1) F2: 소프트웨어 브레이크 포인트를 설정/삭제 시 사용하는 단축키
(2) F7: 어셈블리 코드 한 줄 실행, call 함수 호출 시 call 함수 내부 진입
(3) F8: 어셈블리 코드 한 줄 실행, call 함수 호출 시 ret 명령어 return 까지 실행
(4) F9:- 프로그램 실행 재개
(5) Ctrl + g: 현재 창이 보여주는 주소를 변경
(6) -,+: 이전 또는 다음 주소로 이동, call 이나 jmp 명령어 사용 시 이전 주소로 이동
(7) <Enter>키: call 이나 jcc와 같은 PC를 변경시키는 명령어 선택한 상태에서 누르면 해당하는 주소로 이동
(8) <space>키: 선택한 어셈블리어 수정

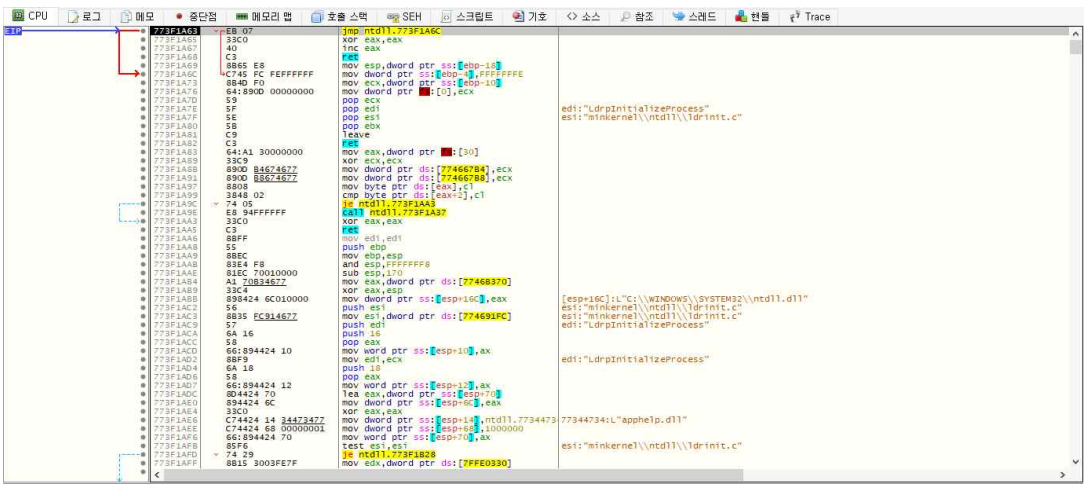
2. abex crackme 1 writeup

1) 프로그램 동작 확인

첫 시작 모습 - "하드디스크를 CD-Rom으로 생각하라"

전 화면에서 [확인]을 누른 후 모습 - "하드디스크가 CD-Rom으로 인식하지 못했다"
[확인]을 누르면 프로그램이 종료

2) 프로그램 리버싱



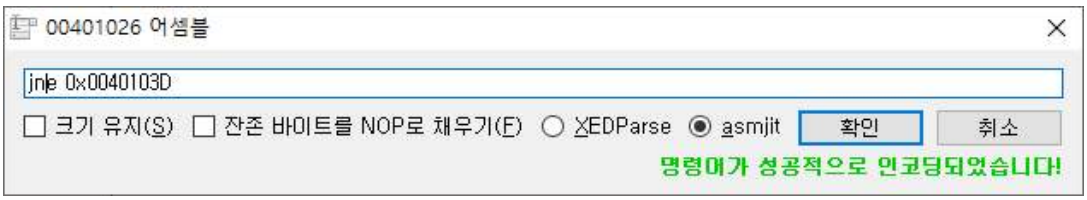
[설정]에서 [시스템 중단점]및 [진입점 중단점]을 설정하고 crackme1파일을 열었을 때 첫 모습

단축키 F9를 통하여 프로그램 재개 시 나타나는 화면

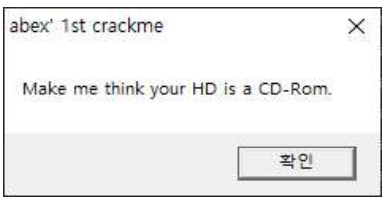
해당 화면서 주석공간에 MessageBox 내용이 존재

이중 주소 00401026의 어셈블리어 코드 je crackme1.40103로 분기점을 통해 해당 프로그램 출력이 다르게 나타남

분기점 코드 je crackme1.40103D를 <space>키를 이용하여 jne crackme1.40103D로 변경



변경 후 프로그램 재개 F9

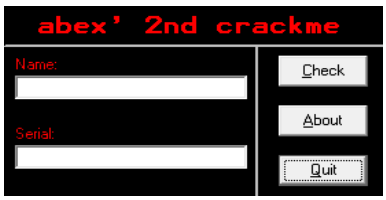


[확인]을 누르면

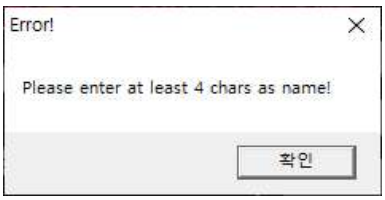
아래와 같이 ”하드디스크가 CD-Rom으로 인식한다“라고 출력

3. abex crackme 2 writeup

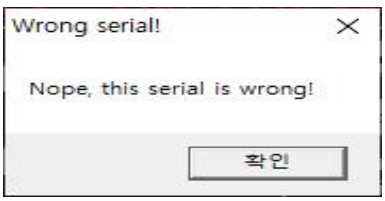
1) 프로그램 동작 확인



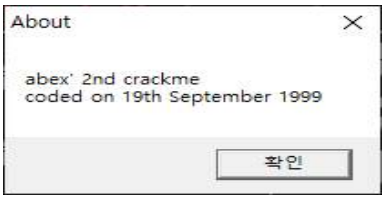
- Name / Serial 입력 공간과 Check 버튼, About 버튼, Quit 버튼이 존재



- Name은 4글자 이상 입력이 필요

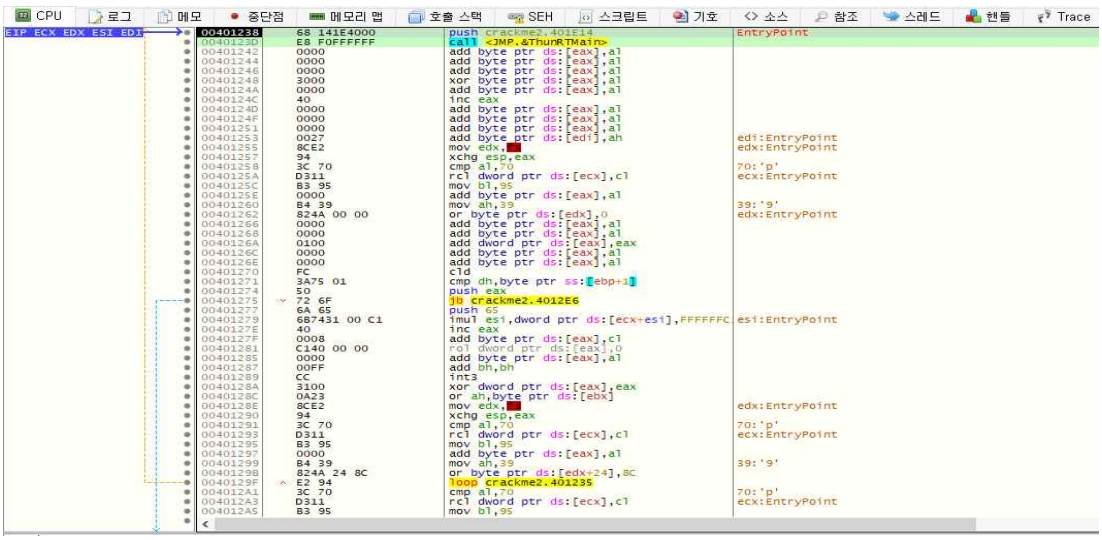


- 4글자 이상의 Name과 무작위 입력의 Serial을 통해 나온 Error

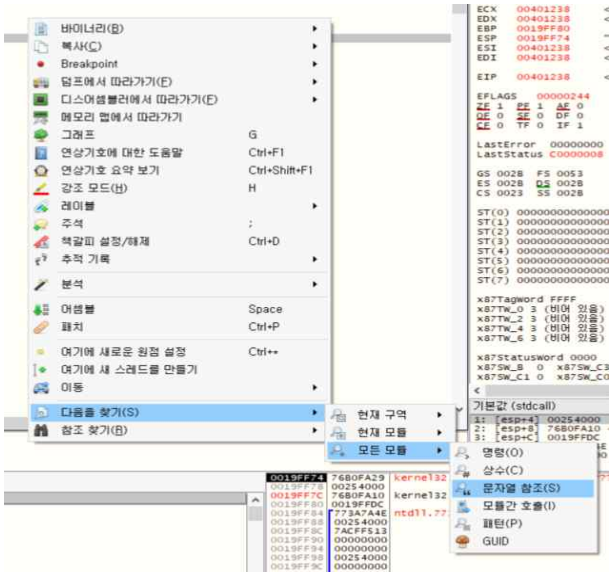


- [About] 버튼을 누르면 출력되는 메시지박스
- [Quit] 버튼 누르면 프로그램 종료

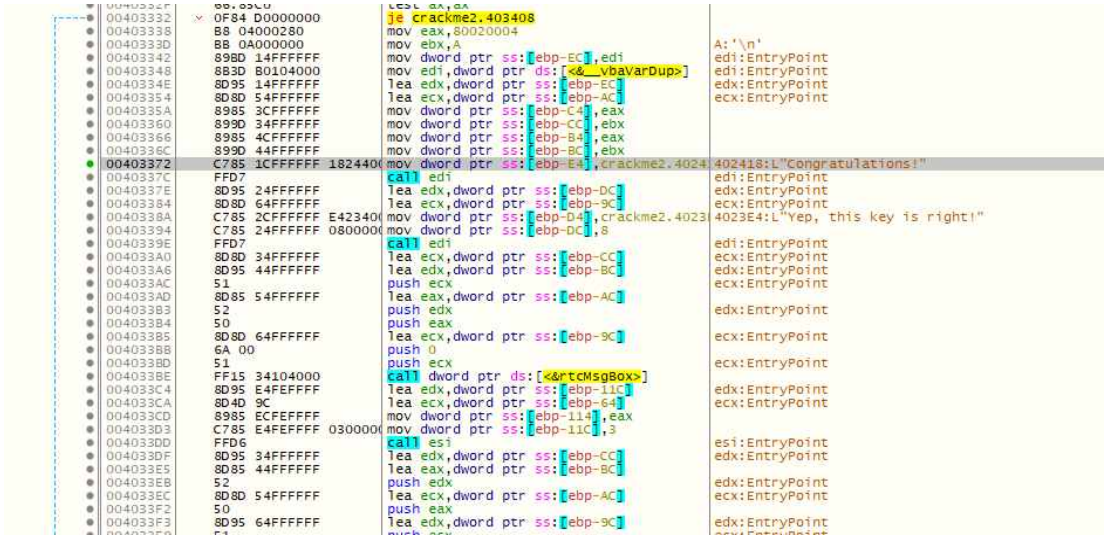
2) 프로그램 리버싱



- x32dbg를 이용하여 [시스템 중단점]에서 F9로 [진입점 중단점]으로 이동

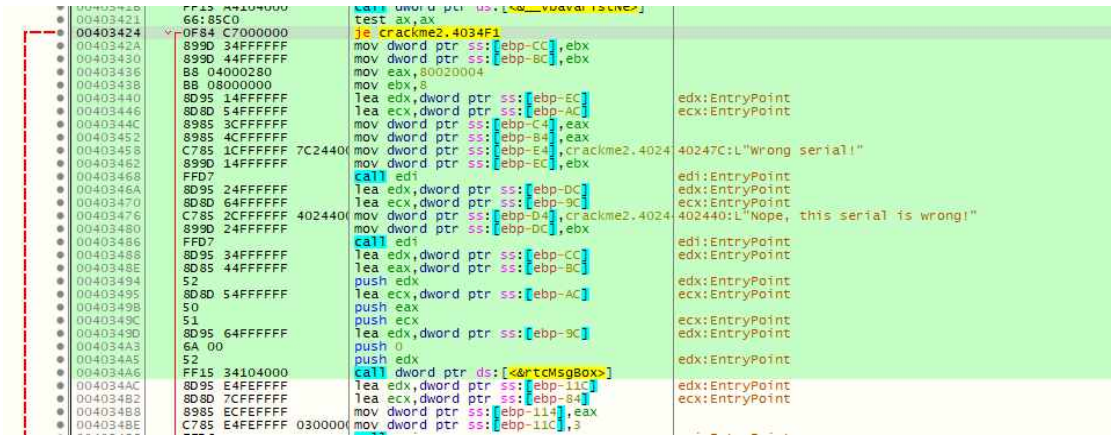


- 문자열 참조를 통해 해당하는 문자 여기서는 프로그램이 동작할 때 발생했던 메시지 박스의 텍스트로 이동

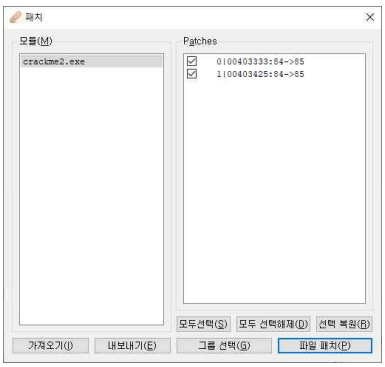


- 회색 줄의 주석을 보면 ”Congratulations!“가 있고 그 위에 분기문을 통해서 Serial값을 확인
- 분기문 자체를 부정하면 밑의 어셈블리어가 실행

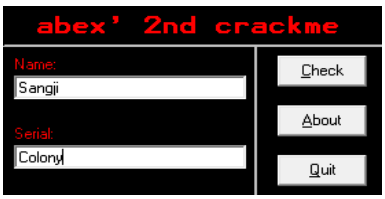
- 그 이후 어셈블리어 코드서 시리얼이 틀린 것을 확인하는 코드가 있으므로 해당 분기점도 수정



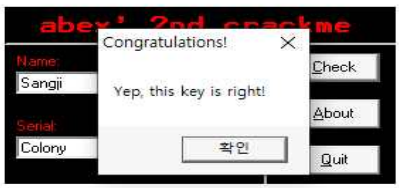
- je 0x004034F1을 jne 0x004034F1으로 설정 후 패치 파일 생성



- 패치 적용 후 해당 프로그램 실행



- Name과 Serial에 무작위 값을 입력하여 [확인]버튼



- 해당 Serial키가 맞다고 메시지박스 출력