코드큐어 5월 8일 기초 해킹팀- 리버싱

정보보안공학과 202321316 이승훈

리버싱의 뜻은 reversing, 역공학이라는 뜻을 가지고 있고, 일반적으로 완성품이나 시스템, 기계장치의 구조, 동작을 분석해서 취약점을 찾아서 보완한다(?) 라는 개념을 가지고 있는데, 우리가 배울 그 리버싱 은 응용 프로그램을 뜯어서 구조, 원리를 알아보는 그런 용어다.

디스어셈블 은 원래 프로그램은 코드로 이루고, 그 안에 어셈블리, 그 안에 바이너리 언어가 있는데, 바이너리 언어에서 어셈블리 언어로 해석하는 것이다.

리버싱 에서의 분석은 총 두가지로 나누어지는데,

정적분석: 디스어셈블링 프로그램을 이용해서 그 내부 코드를 눈으로 확인하는 것, 즉 실행하는 것이고, 환경 제약이 없으며, 분석하는 도구만 갖춘다면 충분히 시도 가능, 실행하지 않기 때문에 바이러스나 악성 프로그램의 공격으로부터 안전하다.

단점은 난독화가 진행되면 분석이 어렵고, 실행하지 않기 때문에 어느 특정 시점에 어떤 변수가 있을지는 모른다.

동적 분석은 프로그램을 실행시키면서 분석하는 방법입고, 자세히 보지 않아도 개략적인 동작을 파악할 수 있다.

장점: 출력을 빠르게 확인가능, 동작을 추론해볼 수 있다.

단점: 분석 환경을 구축하는데 어려움을 겪는다,(프로그램 실행 X = 동적 분석 X )

어셈블리 언어

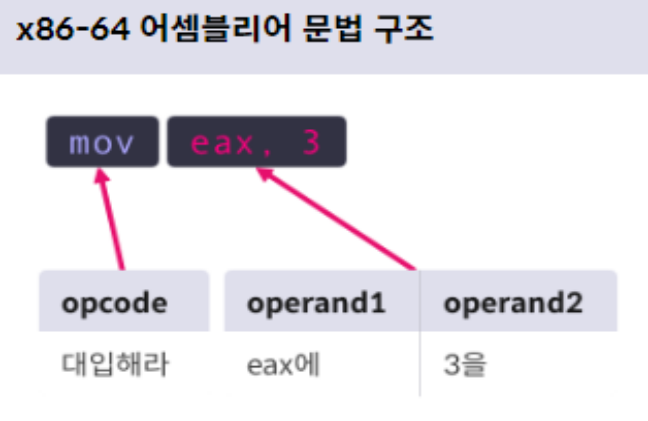
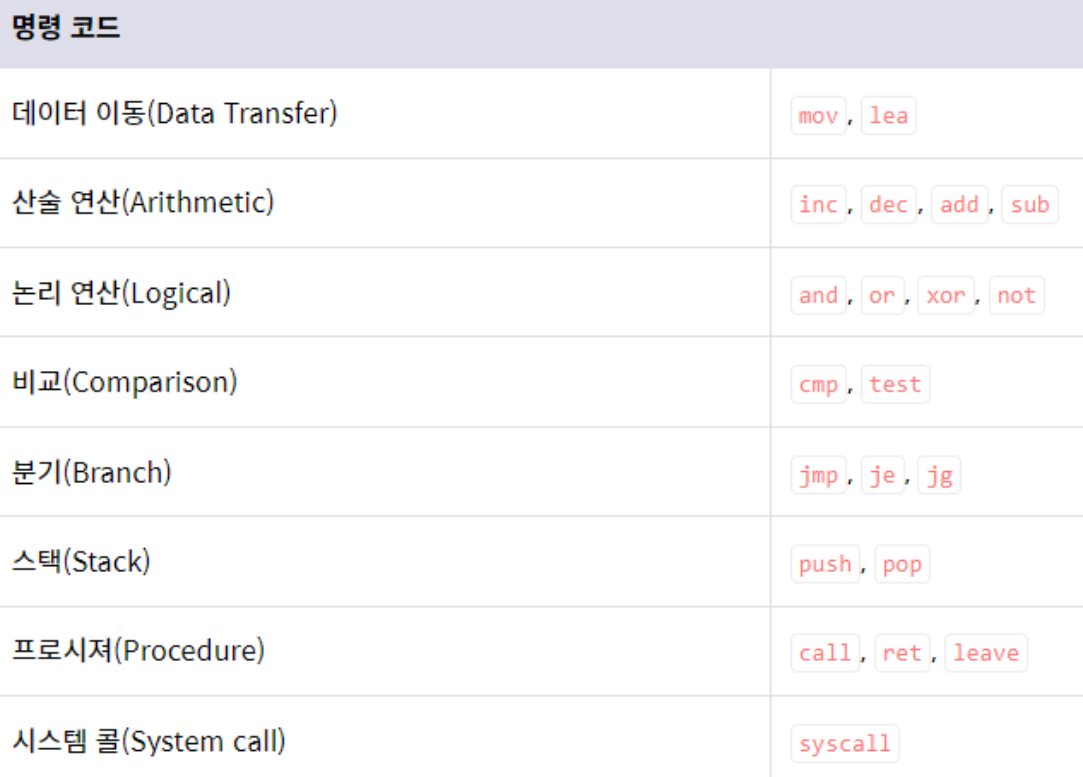
컴퓨터의 기계어와 치환되는 언어이다.

사진에 보이는 것처럼 문법구조는 opcode는 동사에 해당하는 명령어,

그 옆에 oprand1, oprand2는 목적어에 해당하는 피연산자이다.

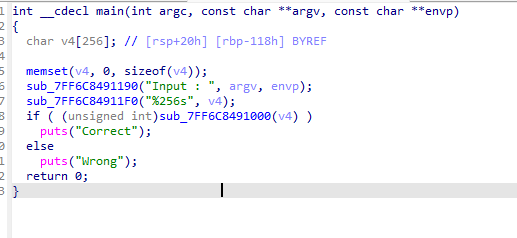
기계어의 종류가 여러가지라서 많은 어셈블리어가 존재한다.

사진에 나온 mov 말고도 더 많은 명령어가 있다.



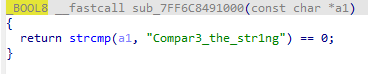
1. Chall0.exe

이 exe 파일을 그냥 실행시키면 결과값이 안나와서 개발자 환경을 통해서 실행시켜봤는데, 어느값을 입력하든 incorrect 라는 결과값만 나온다.



이 사진에 보는 것 처럼 exe 파일의 main 을 디컴파일링 해서 나온 화면인데, if 문 하고 그 뒤에 무언가 많이 있는데, 여기서 결과값이 갈리는 것 같고, sub\_7FF6C8491000 이면 correct 라는 값을

뱉고, 이를 확인해보고 싶어서 또 , sub\_7FF6C84910 라는 값을 또 디컴파일링 해서 들어가보니.



아니 이게 뭐야? Compar3\_the\_str1ng 이라는 값이 나왔다. dreamhack에서 이런 값이 나올 때는 DH{ Compar3\_the\_str1ng }이 정답이라고 했다.

결론: DH{ Compar3\_the\_str1ng }

이게 정답.

1. Patch.exe

내 기준에서는 어려운 건 아니고 조금 열 받는 문제였다. (지금 생각해도 너무 열 받는 문제)

사실 여기서 winmain을 찾고 들어가서 봤는데, 모르겠어서 sub\_1400032F0 이라는 그냥 익숙한 형태의 문자를 보고 들어가고, 또 익숙한 형태로 sub\_140002C40를 들어가니 여기서 이해는 안되지만 Getpaint 라는 영어문자가 있었다. 다시 짚어보니



이런 화면이 나오고, 50번부터 75번까지 동일한 sub가 있는데, 그걸 가지고 차례대로 프로그램을 실행해본, 결과로 검은색 선이 그어지면서 flag가 가려지는 모습을 볼수 있다.

그래서 sub\_140002B80 함수의 역할을 알았고, 패치를 해야 그 선이 안보이게 된다.

근데 Pseudocode에서 패치를 할려면 어셈블리코드를 패치해야 하는데 안뜬다.

IDA view-1 에서 패치를 해야한다고 하넹…

그 창에서 g를 누르고 해당 함수로 이동해서 edit을 한다.

브레이킹 인트를 51번을 걸고 실행시켜봤는데 페인트가 그려지면서 flagfmf 가린다.

거기서 해당 함수로 이동후, ret를 피채한후 저장하면



이런 값이 나온다.

따라서 flag는

DH{UPATCHED} 이다.