

LLM 2 Reverse engineering

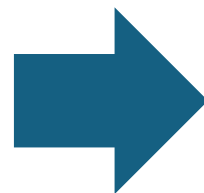
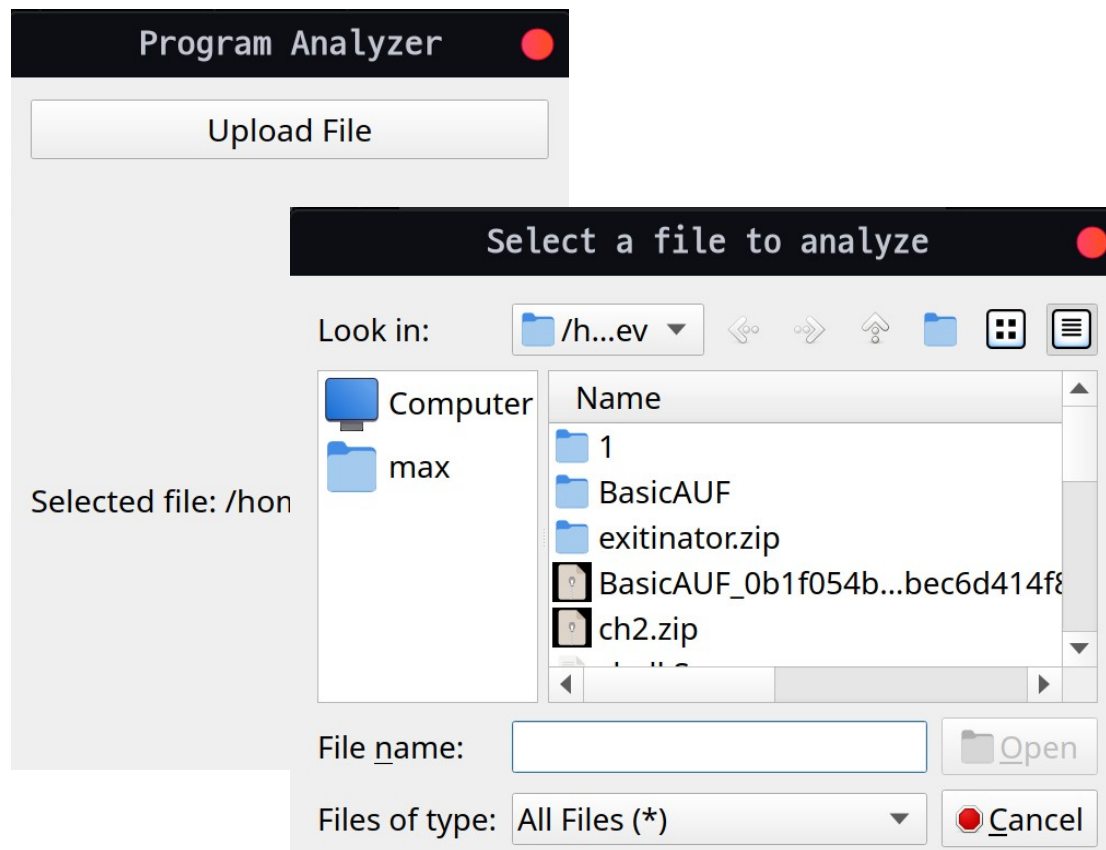
MAXWELL



제안배경

- 유연한 파일 분석의 필요성
 - 리버스 엔지니어링의 진입장벽
-

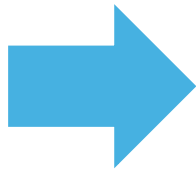
프로그램 동작 방식



radare2

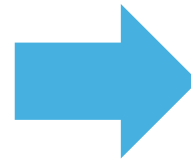
Radare2

- Information
- Functions
- Strings
- Sections



LLM

- 자연어 답변
생성



User

- 채팅 인터페이스를 통해
파일 분석 결과를
자연어로 제공받음.
- 채팅을 통해 추가적인
정보를 요청할 수 있음.

Chat Interface

Analysis: information(실행 가능한 ELF 64비트 파일)
function(main, printf, exit 등 정상적인 함수만 찾음)
strings(정상적인 문자열만 찾음)
section(.text, .data, .rodata 등 정상적인 섹션만 찾음)
위험도: L(정상적인 ELF 실행 파일로 보임)

정보 분석 결과 정상적인 ELF 실행 파일로 보입니다. 의심스러운 함수나 문자열, 비정상적인 섹션이 발견되지 않았기 때문에 악성코드의 가능성은 낮다고 판단합니다. 다만 실행로직과 목적에 대해 정확히 알 수 없기 때문에 중립적인 입장을 취합니다. radare2에서 제공한 정보만으로는 악성코드 여부를 정확히 판단하기 어려우므로 추가 분석이 필요할 것으로 보입니다.

Analysis Result:

Ask a question about the analysis...

Send

Chat Interface

Analysis: information(실행 가능한 ELF 64비트 파일)
function(main, printf, exit 등 정상적인 함수만 찾음)
strings(정상적인 문자열만 찾음)
section(.text, .data, .rodata 등 정상적인 섹션만 찾음)
위험도: L(정상적인 ELF 실행 파일로 보임)

정보 분석 결과 정상적인 ELF 실행 파일로 보입니다. 의심스러운 함수나 문자열, 비정상적인 섹션이 발견되지 않았기 때문에 악성코드의 가능성은 낮다고 판단합니다. 다만 실행로직과 목적에 대해 정확히 알 수 없기 때문에 중립적인 입장을 취합니다. radare2에서 제공한 정보만으로는 악성코드 여부를 정확히 판단하기 어려우므로 추가 분석이 필요할 것으로 보입니다.

User: 사용된 함수에 대해 더 자세히 분석해줄래?

Assistant: 네, 실행 파일에서 사용된 함수들을 더 자세히 분석해보겠습니다.

main 함수가 있고, printf와 exit 함수가 호출되는 것을 확인했습니다.
printf 함수는 문자열을 출력하는 표준 C 함수이고, exit 함수는 프로그램을 종료하는 함수입니다.
두 함수 모두 정상적인 기능을 하는 것으로 보입니다.

그 밖에 사용된 다른 함수들을 살펴보면,
- __libc_start_main: 라이브러리 초기화 함수
- setbuf: 버퍼링 설정 함수
- __isoc99_scanf: 입력 함수
- memset: 메모리 초기화 함수
- strlen: 문자열 길이 계산 함수
등이 사용되었습니다.

이들 함수는 모두 정상적인 C 표준 라이브러리 함수들로, 의심스러운 기능은 발견되지 않습니다.

따라서 실행 파일에서 사용된 함수들만으로 볼 때 악성코드 가능성은 낮다고 판단됩니다. 다만 실행 파일의 정확한 기능과 목적에 대해서는 함수 사용 정보만으로는 정확히 알 수 없습니다. 추가적인 정적/동적 분석이 필요할 것으로 보입니다.

Analysis Result:

Ask a question about the analysis...

Send



향후 계획

- AI 개선
 - 악성 코드 데이터셋을 이용한 모델 개선
 - Radare2와의 상호작용 개선
-

- Product:
- Price: 유 / 무료 혼합 . 구독제 .
- Place: 패키징 후 배포
- Promotion: 악성 코드 탐지 기록 배포

