**PWN-9: Портал в Край**

В задании предоставляется консольное приложение с исходным кодом на языке C, скомпилированное под архитектуру linux amd64. При запуске приложения пользователю выводится меню с несколькими опциями.

**Флаг 1:**

Из исходного кода можно было заключить, что в меню есть скрытая опция, которую можно активировать введя символ - ` (обратный апостроф), после чего пользователю предлагается выполнить арифметическое сложение двух случайных шестнадцатеричных чисел, если введенные пользователем результат окажется верным, на экран выведется первый флаг.

Изображение выглядит как текст, диаграмма, снимок экрана, дизайн

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Флаг 2:**

В опции меню [T] Teleport to coordinates используется не безопасная функция gets для записи пользовательского ввода (sdtin) в буфер расположенный на стеке. Также в бинарном файле была представлена функция win(char \*password), позволяющая запустить интерпретатор sh, если передать строку “password” в аргумент char \*password. Так как при компиляции были выключены защиты PIE (исполняемый модуль с позиционно-независимым кодом) и canary (стековая канарейка), для решения было достаточно переписать только адрес возврата на константный (не меняющийся при перезапусках) адрес функции win, чтобы обойти проверку пароля в этой функции, достаточно взять небольшое смещение от начала функции win, чтобы пропустить инструкции отвечающие за проверку пароля.

Скрипт с решением на языке python с использованием библиотеки pwntools:

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.