Практическое задание 6

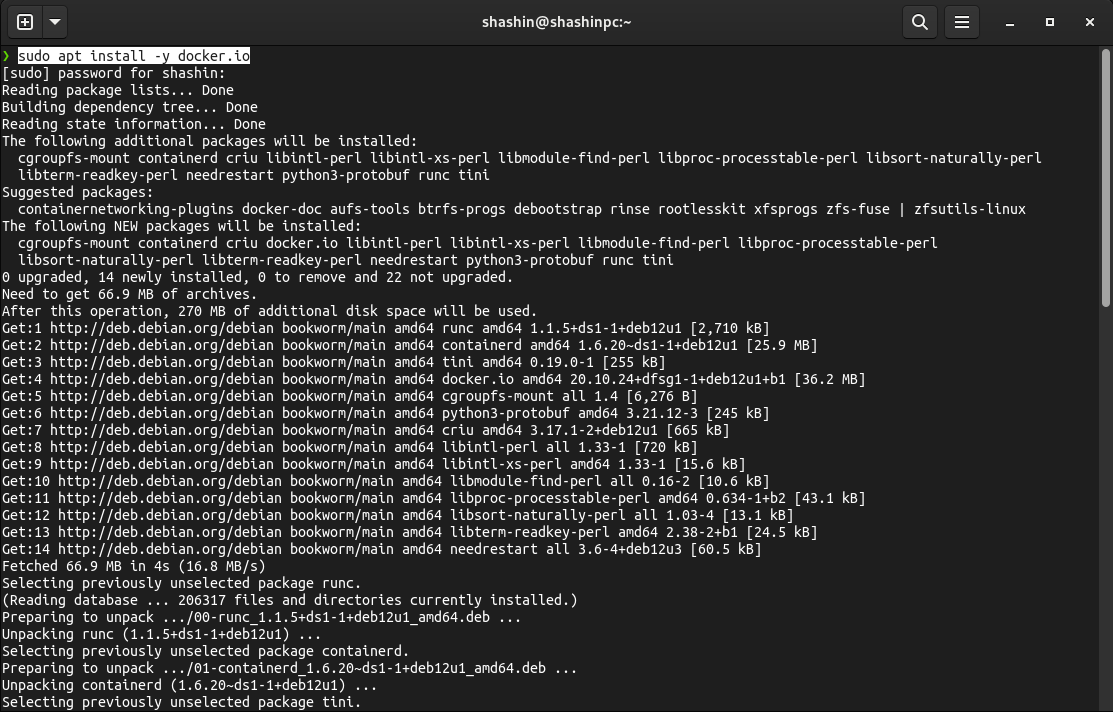
Фаззинг-тестирование приложения

Задачи:

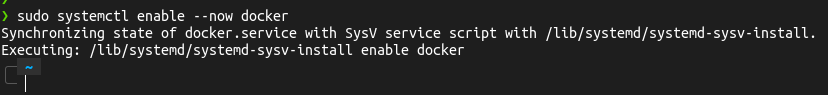
1. Подготовить ВМ с OC Linux.
2. Запустить в ВМ Docker
3. Выполнить команду `docker pull aflplusplus/aflplusplus`
4. Выбрать фаззинг-цель для тестирования (простое приложение на ‘C’) и запустить фаззинг-тестирование исследуемой программы.
5. Подготовить отчет со скриншотами.

Фаззинг — это метод тестирования программного обеспечения, который используется для обнаружения уязвимостей и ошибок в приложениях. Этот подход включает в себя автоматическую генерацию и отправку случайных или некорректных данных (входных данных) в программу с целью выявления сбоев, исключений или других нежелательных реакций.

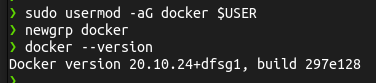
1. Устанавливаем Docker



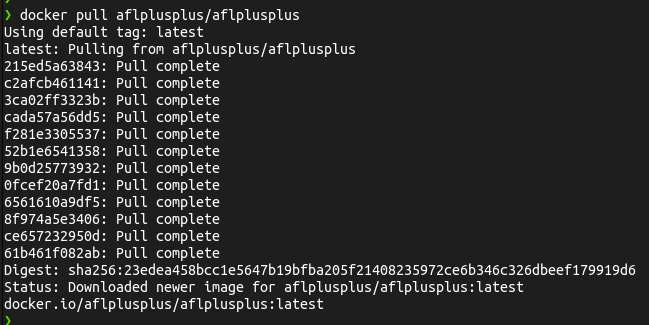
1. Запускаем Docker



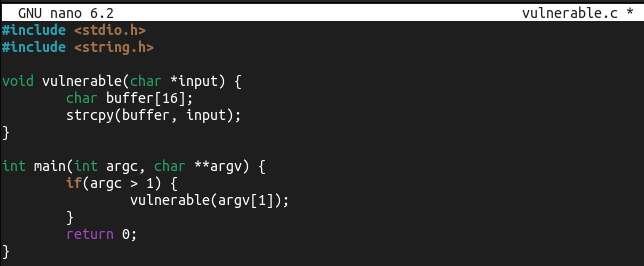
1. Добавляем пользователя в группу docker



1. Загрузка docker образа с инструментарием для фаззинга

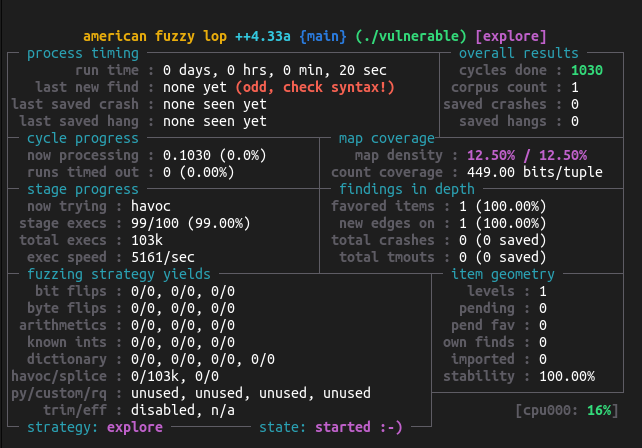


1. Запуск контейнера 
2. Пишем скрипт на С для запуска фаззинга

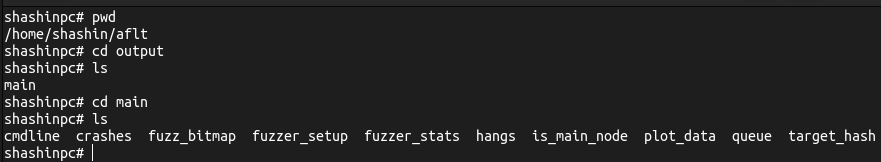


1. Запуск





В случае краша, система напишет об этом (“saved crashes:”, “total crashes” справа)



Описание компонентов фаззер.

1. queue — место где хранятся входные данные, используемые фаззером для создания новых текстовых вариантов
2. crashes — каталог, в котором хранятся файлы, вызывающие сбои программы во время тестирования
3. hangs — папка, где хранятся тестовые файлы, которые привели к зависанию программы, то есть к длительному выполнению без завершения
4. fuzzer\_stats — файлы, содержащие статистические данные о работе фаззера, такие как количество выполненных циклов и покрытие кода
5. plot\_data — информация, используемая для построения графиков, например, зависимость покрытия кода от времени
6. target\_hash — данные о хэшировании целевых файлов, которые помогают отслеживать уникальность входных данных
7. cmdline — запись команд, используемых для запуска фаззера, включая аргументы командной строки
8. fuzz\_bitmap — данные, которые отслеживают покрытие кода, включая битмапы, используемые для определения новых ветвей выполнения
9. fuzzer\_setup — конфигурационные файлы или параметры, определяющие настройки работы фаззера

Фаззинг является мощным методом тестирования. Его автоматизация и способность находить ошибки делают его незаменимым инструментов в современном процессе разработки программного обеспечения.