Федеральное государственное бюджетное образовательное учреждение высшего

образования

«Чувашский государственный университет им. И.Н. Ульянова»

Кафедра вычислительной техники

Лабораторная работа №1

**Контейнер для проверки SUID/SGID.**

Выполнил: Иванов В.С.

студент группы ИВТ-41-22

Проверил: Харитонов С. М.

Чебоксары, 2025

1. **Принцип работы**

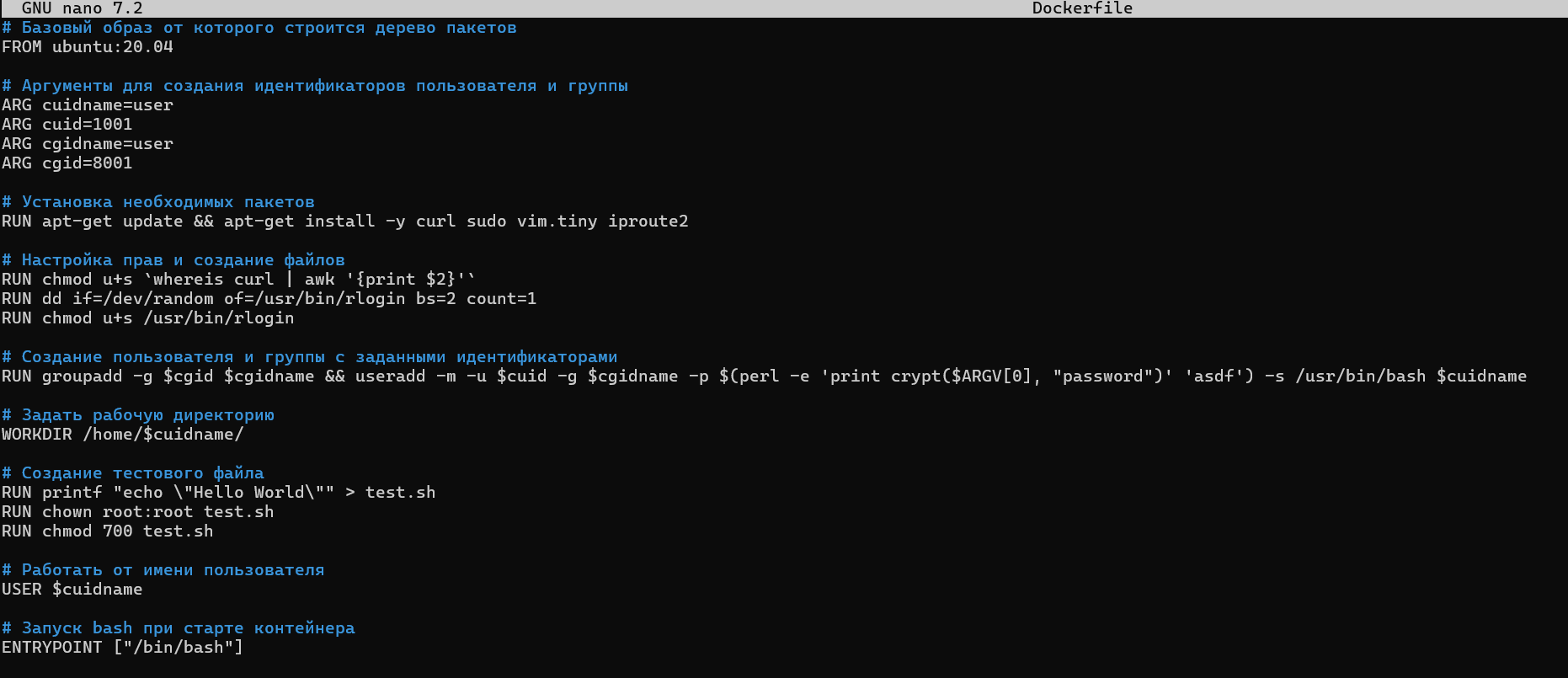
Флаги SUID/SGID являются расширением дискретной модели прав доступа, которые разрешают пользователям запускать исполняемые файлы с правами владельца или группы исполняемого файла. Соответственно, когда установлен флаг SUID, любой пользователь может запускать любую программу, как владелец программы.

Некорректное присваивание данных флагов может привести к атаке «повышение привилегий». Классическим примером некорректного присвоения флага SUID/SGID, является назначение данной привилегии для исполняемого файла, функционал которого позволяет осуществлять взаимодействие с командной строкой или файловой системой.

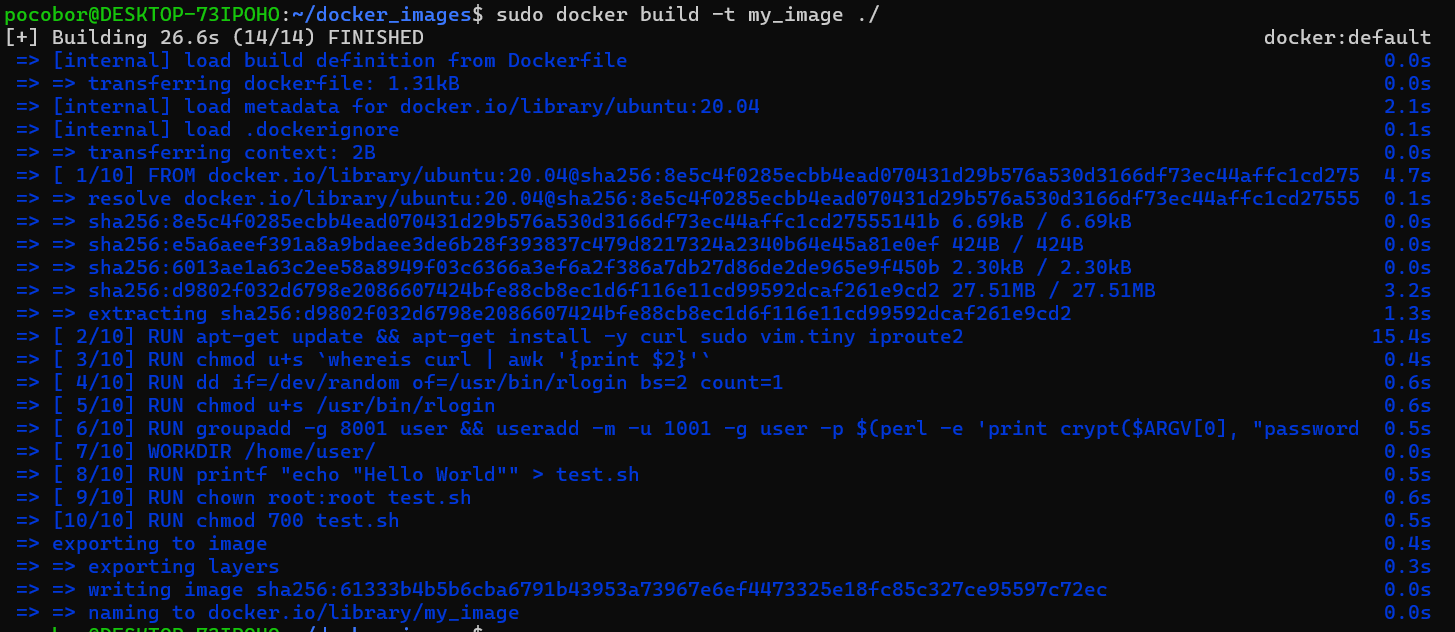
Все проверки проходят от имени пользователя «user» с паролем «asdf».

1. **Описание контейнера.**

Для проведения проверки необходим контейнер с установленными пакетами curl, vim.tiny, sudo и настроенным сетевым интерфейсом.



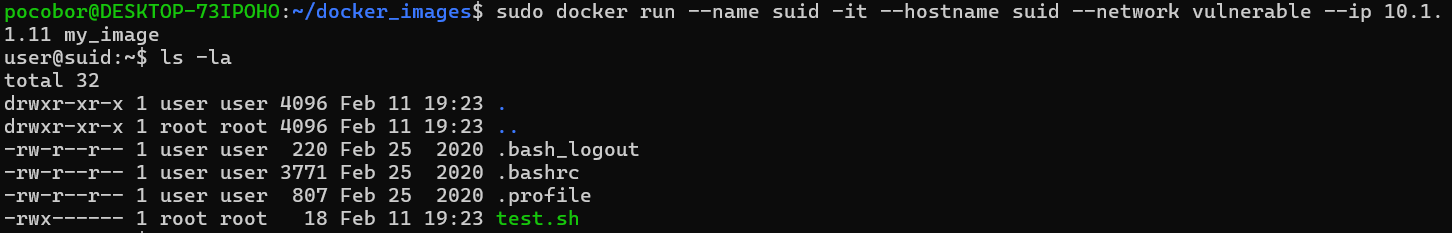
1. **Контрольный пример.**
2. Осуществить сборку образа контейнера из заданного Dockerfile:



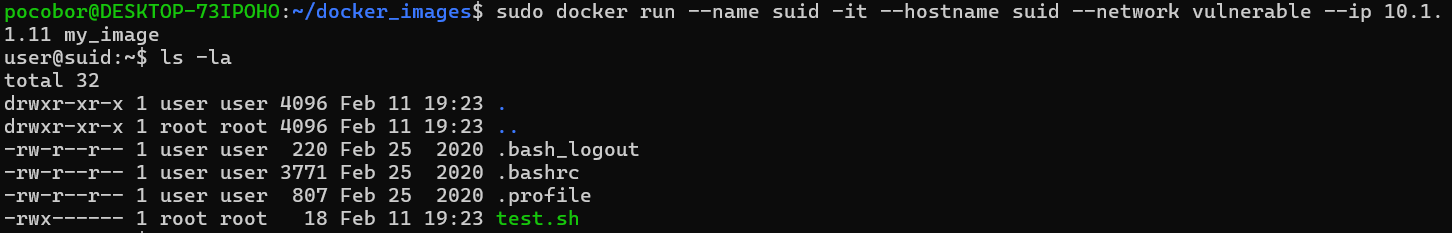
1. Создать сеть Docker:



1. Запустить контейнер:



1. Запросить перечень файлов и папок, размещённых в домашней директории:



* -rwx------ — права доступа к файлу.
* 1 — количество жёстких ссылок на файл.
* root root — владелец и группа файла.
* 18 — размер файла в байтах.

Проанализировав вывод команды, можно заметить что исполняемому файлу

«test.sh» присвоены привилегии 700, что позволяет осуществить запуск только от имени

владельцем файла, которым является пользователь root.

1. Выполнить файл средствам интерпретатора «bash»



Появившееся сообщение говорит о том, что пользователю недостаточно

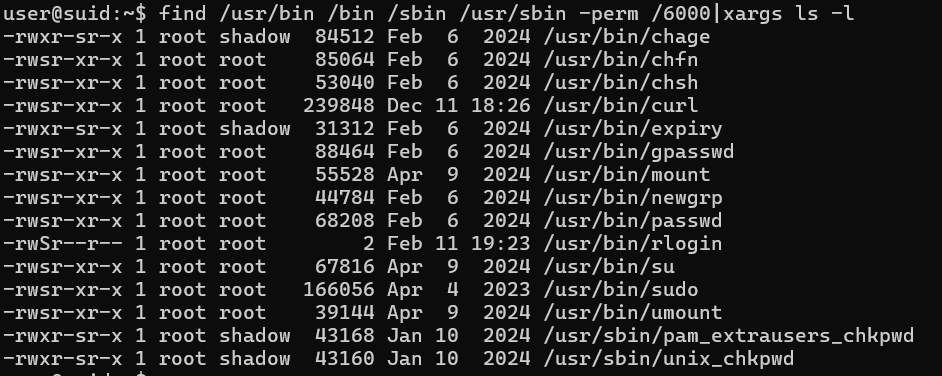
привилегий для выполнения данного файла.

1. Осуществить поиск файлов для которых установлены флаги SUID/SGID:

При анализе вывода команды поиска можно обнаружить что администратор

установил SUID бит для приложения curl, что позволяет осуществить атаку повышения

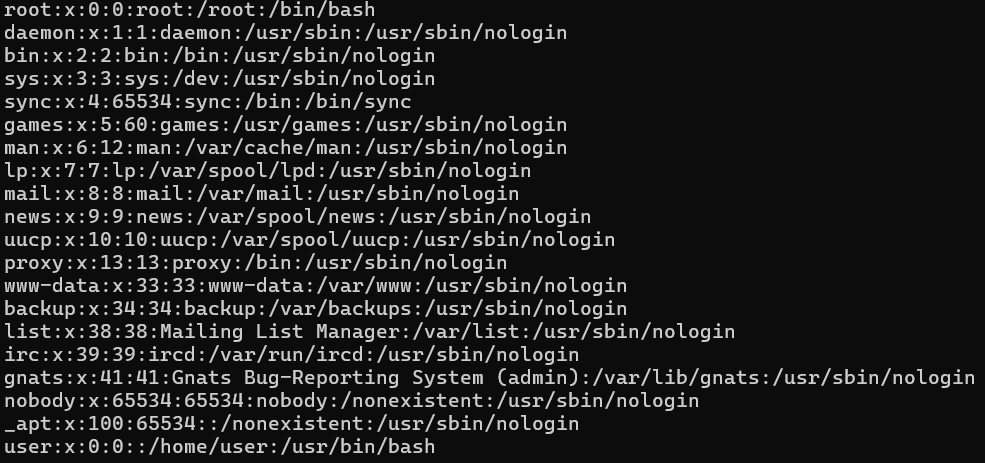
привилегий, т.к владельцем данного файла является пользователь «root»:



1. Скопировать файл /etc/passwd в домашнюю директорию:



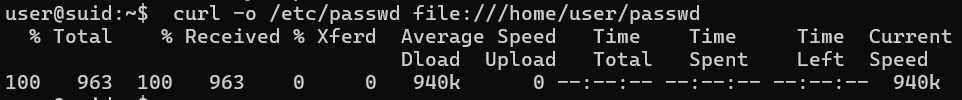
1. Отредактировать файл приведя запись пользователя «user» к следующему виду:



1. Сохранить изменения в файле:

:wq

1. Воспользовавшись некорректным назначением прав доступа, подменить конфигурационный файл /etc/passwd:



1. Выполнить команду id:



Появившееся сообщение говорит о том, что работа осуществляется от имени

непривилегированного пользователя с идентификатором «1001».

1. Воспользовавшись механизмами команды «su» выполнить повторный вход.
2. Выполнить команду id:



Появившееся сообщение говорит о том, что работа осуществляется от имени привилегированного «root» пользователя с идентификатором «0».

1. Выполнить файл средствам интерпретатора «bash»



Появившееся сообщение говорит о том, что файл был успешно выполнен интерпретатором.

1. **Вывод**

Использование флагов SUID/SGID позволяет процессам осуществлять действия от имени владельца файла или от имени группы. Избыточный набор прав предоставленных для конкретного процесса, потенциально может привести к   нарушению работы как подсистемы защиты информации, так и других функций выполняемых в информационной системе.