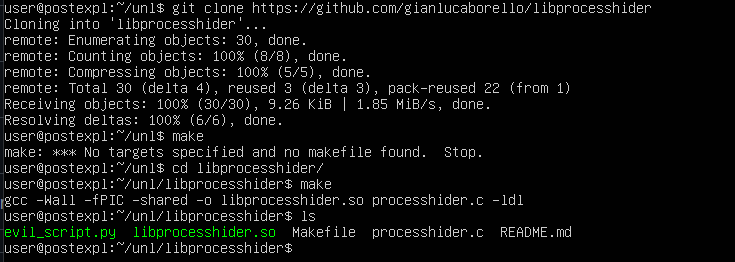
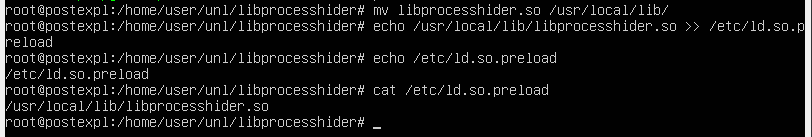
**Обязательная часть 1.**

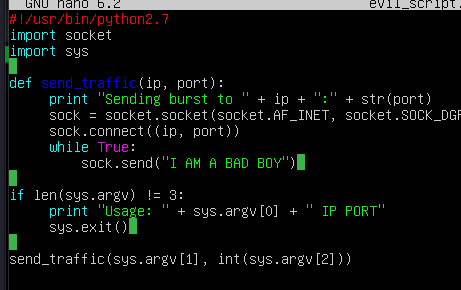
Установим и скомпилируем файл



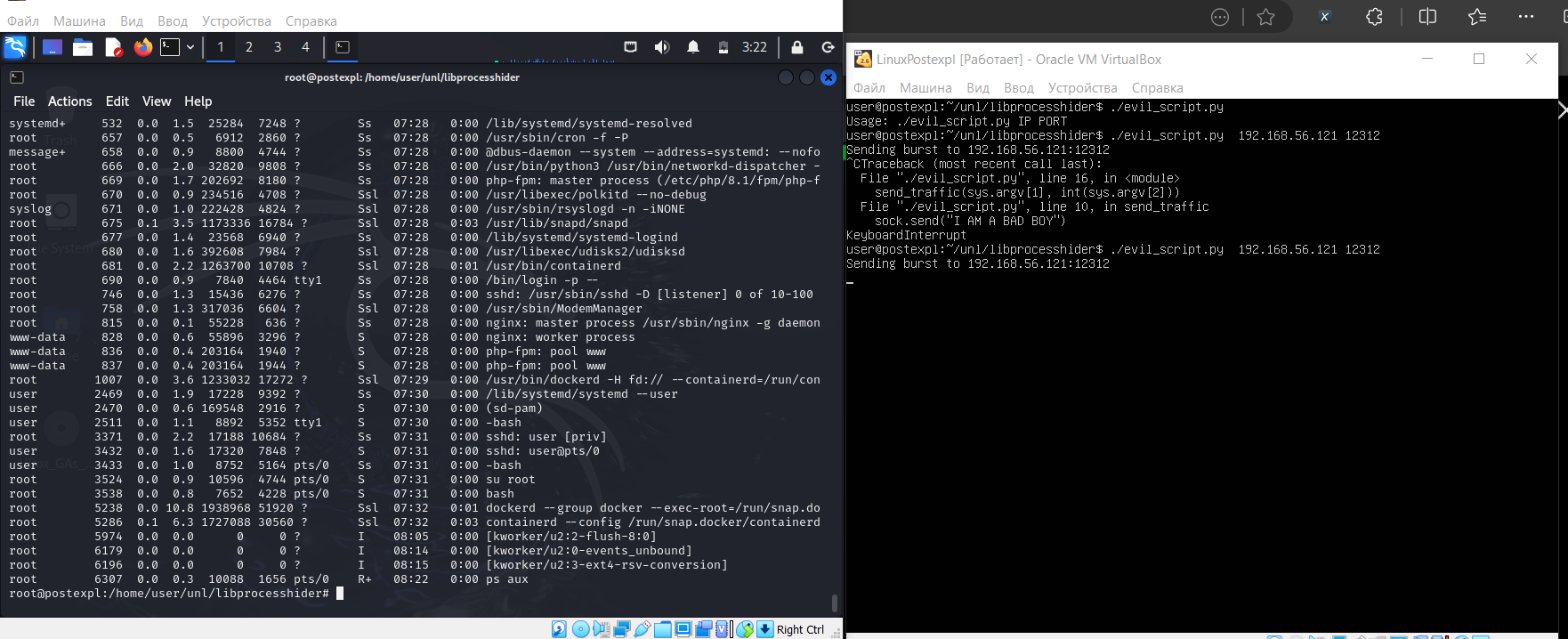
Скопируем файл в /usr/local/lib и запишем его в preload



Исправим запуск (версию python) evil\_script.py



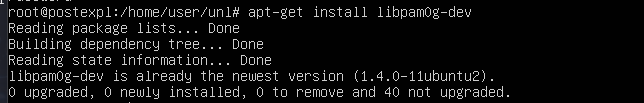
Запустим evil\_script.py указав случайны адрес и порт и проверим процессы от root



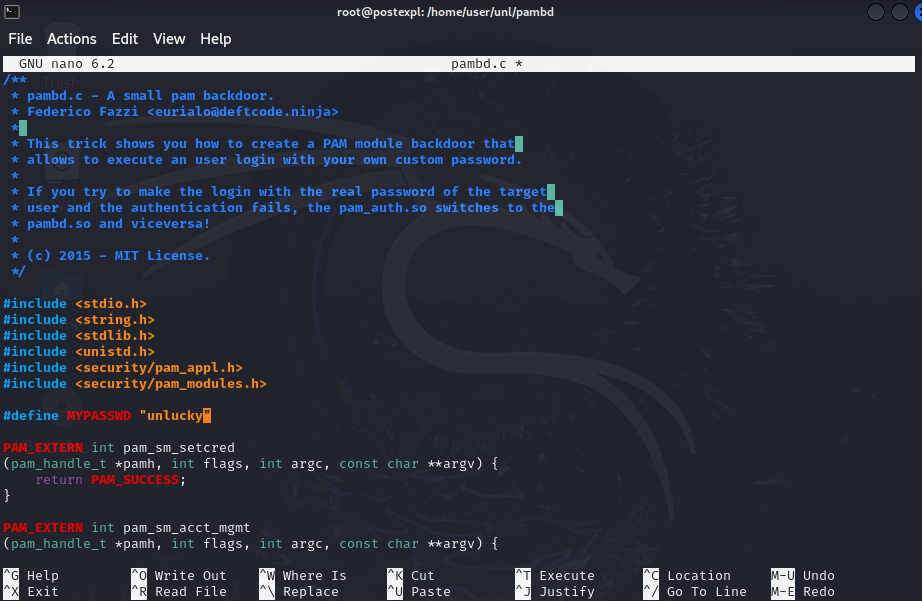
**Обязательная часть 2.**

Установим pambd с помощью git clone <https://github.com/ociredefz/pambd.git>

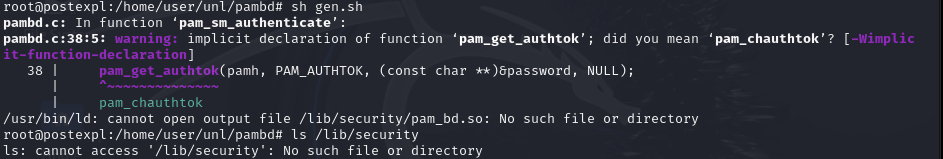
Установим дополнительный пакет libpam0g-dev (либо libpam-dev)



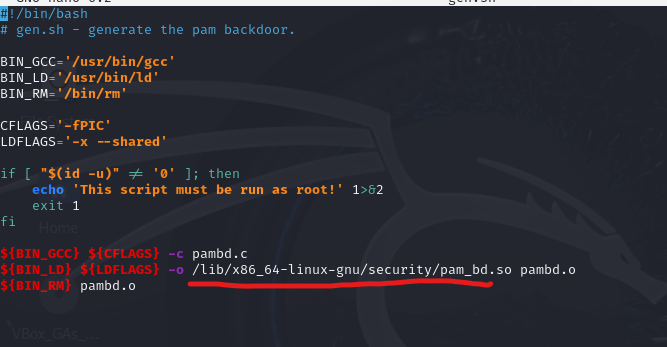
Изменим MYPASSWD на unlucky



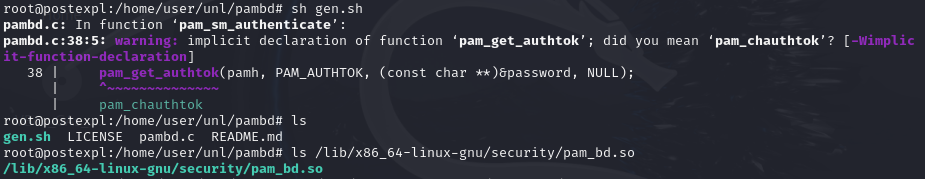
Попробуем запустить скрипт и получим ошибку тк папка находится в другом месте



Изменим скрипт

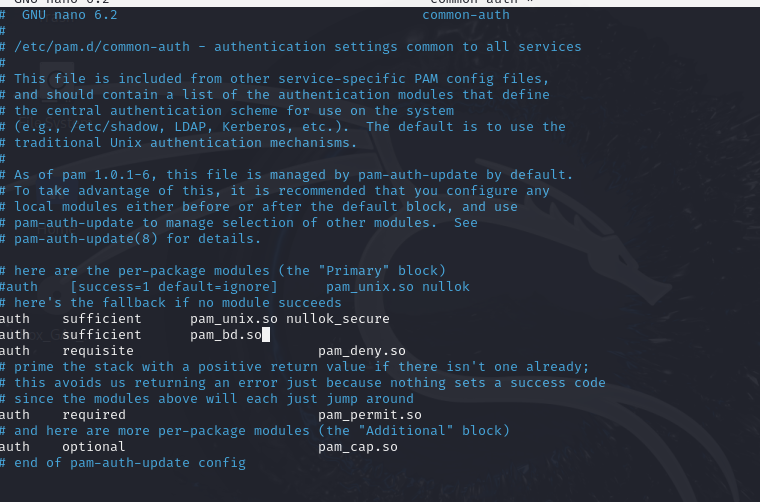


Запустим еще раз

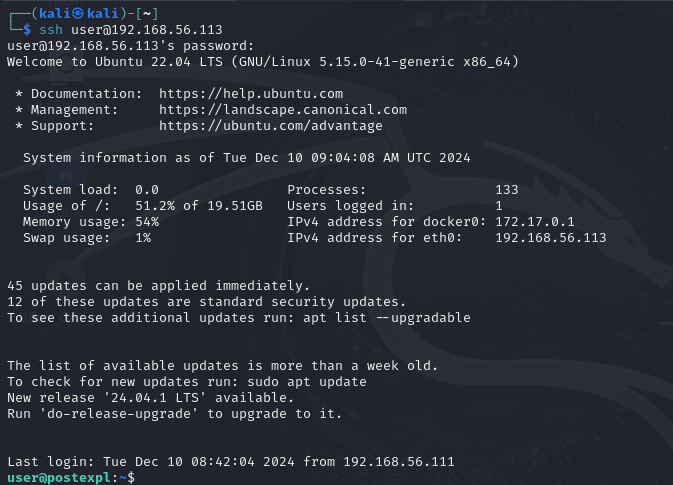


Скрипт выполнился и скомпилировался файл по пути /lib/x86\_64-linux-gnu/security/pam\_bd.so

Теперь изменим файл /etc/pam.d/common-auth и добавим туда строки для аутентификации по MYPASSWD указанному в созданной библиотеке pam\_bd.so

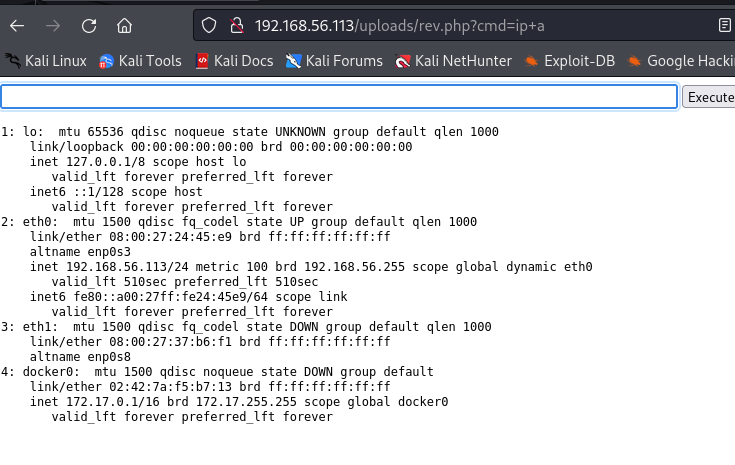


Попробуем подключиться с паролем unlucky и получим доступ



**Дополнительная часть 1**

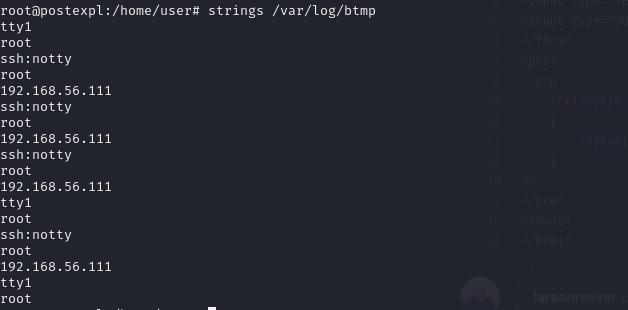
Загрузим web-shell на сайт (взятый шелл <https://gist.github.com/joswr1ght/22f40787de19d80d110b37fb79ac3985>) и проверим его работу



Скопируем репозиторий для сокрытия следов работы с сайтом и входа ssh

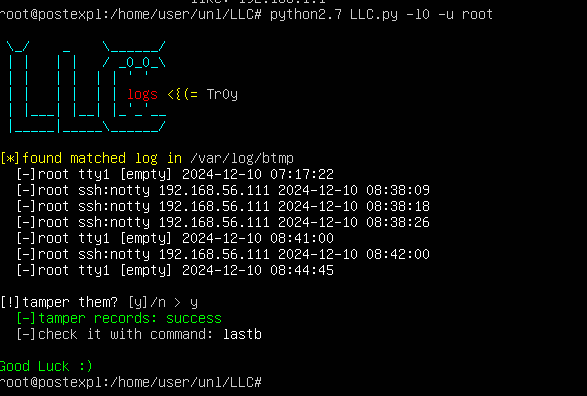


Проверим наличие логов

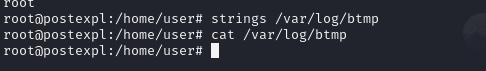




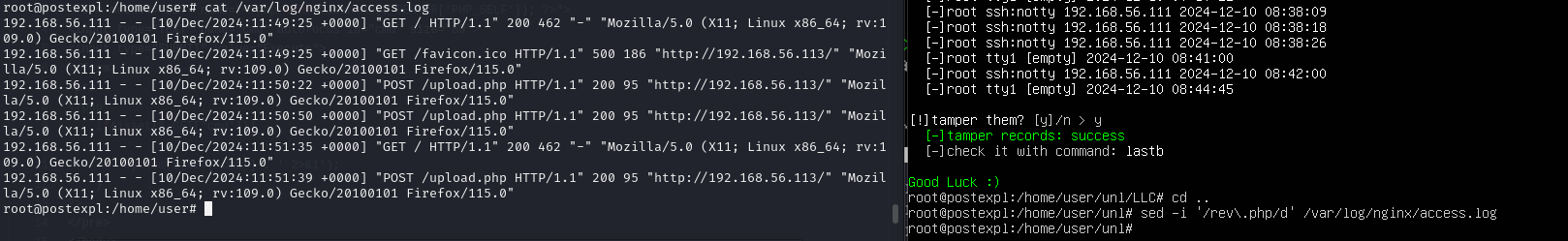
Запусти LLC с помощью python2.7 с параметрами –l0 (лог 0 = btmp) и пользователь –u root



Убедимся что логи очищены



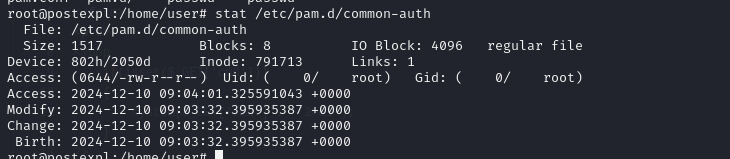
С помощью sed удалим логи nginx, в которых есть упоминание web-shell (rev.php) и убедимся что они пропали

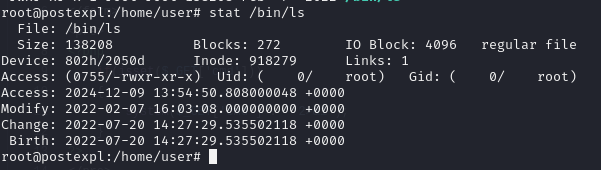


**Дополнительная часть 2**

Для примера возьмем файл /etc/pam.d/common-auth, который создавали в обязательной части 2

Проверим подробную информацию нашего файла и /bin/ls





С помощью touch изменим время последнего чтения и изменения файла

touch -m --date="2022-02-07 16:03:08.000000000 +0000" /etc/pam.d/common-auth

touch -a --date="2024-12-09 13:54:50.808000048 +0000" /etc/pam.d/common-auth

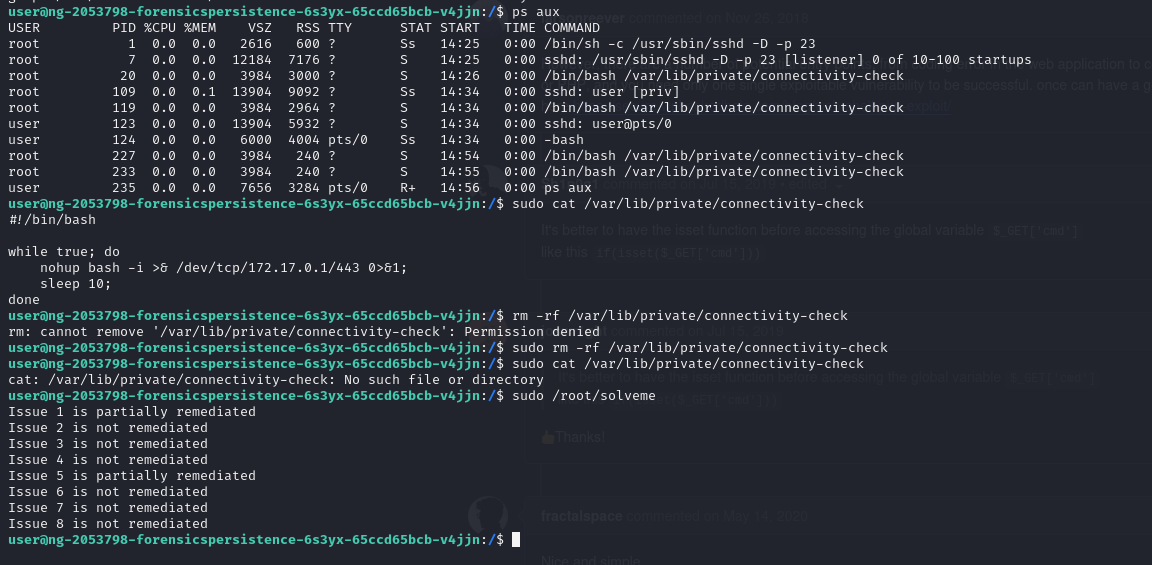
Проверим файл и сравним с /bin/ls



**Повышенная сложность 2**

Проверим запущенные процессы

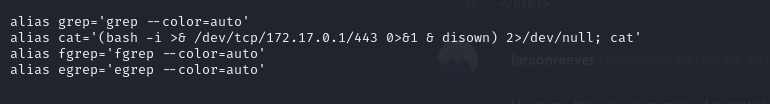
Видим странный процесс /var/lib/private/connectivity-check. Изучив его можно смело заявить что он вредоносный и можно его удалить



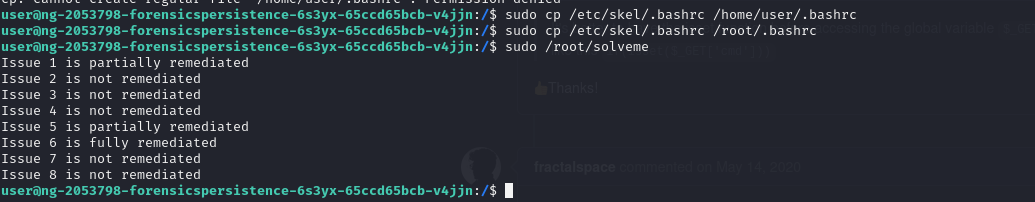
Также убьем все процессы связанные с этим скриптом



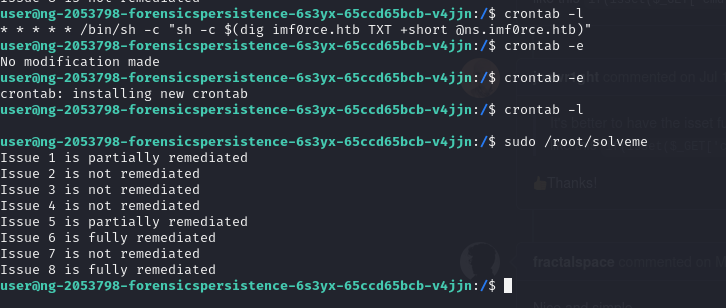
Проверим home/user/.bashrc и видим команду на соединение



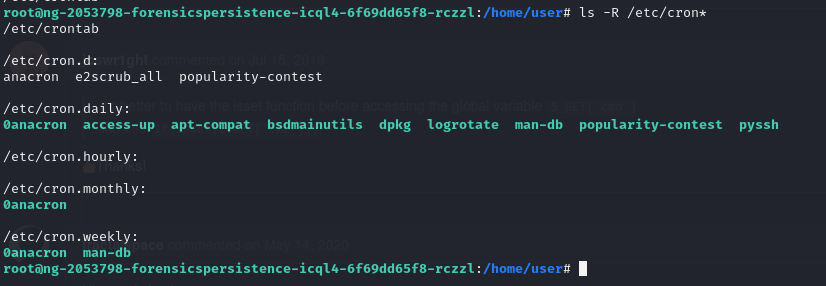
Директория /etc/skel содержит копии различных установочных и других файлов. Замени .bashrc у пользователя и рута( на всякий случай)



Проверим инструкции (?) crontab и увидим явно что-то плохое. Открыв crontab с помощью crontab –e удалим содержимое и сохраним файл

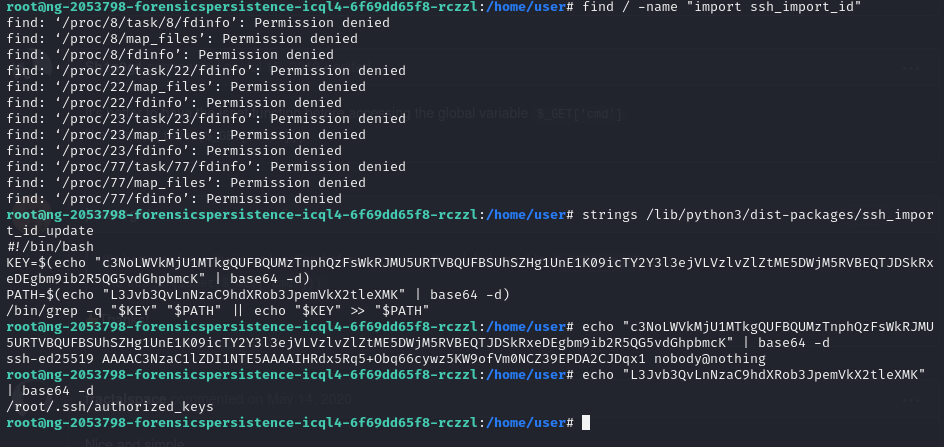


Проверим планировщик задач и сами задачи



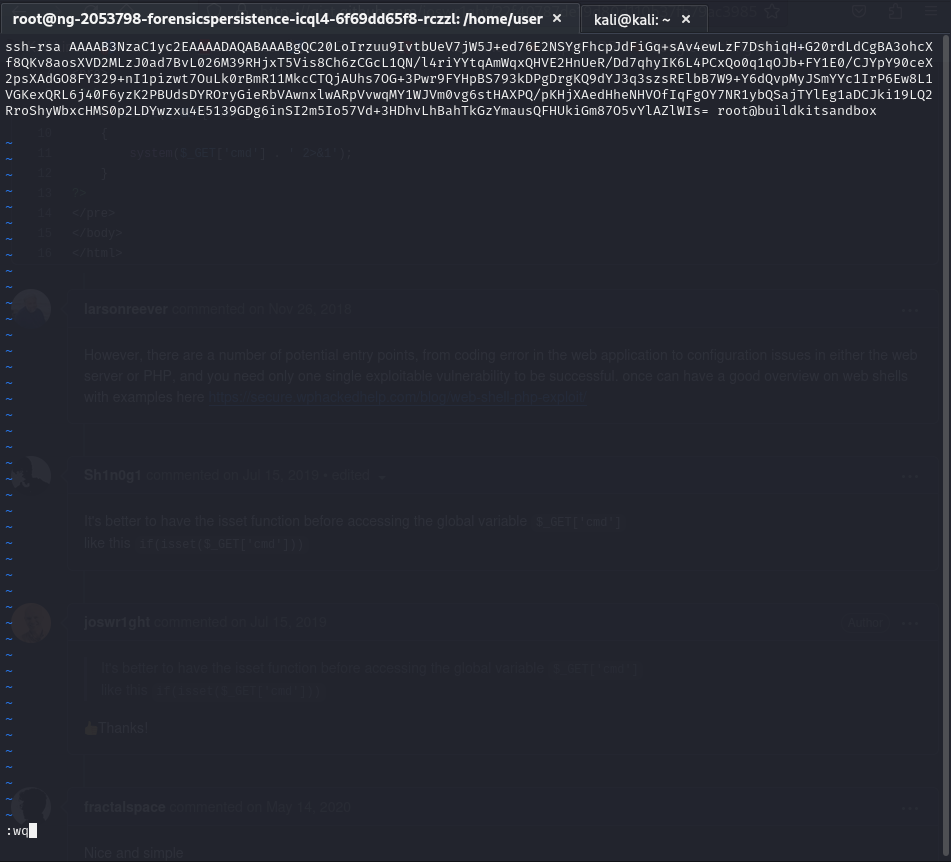


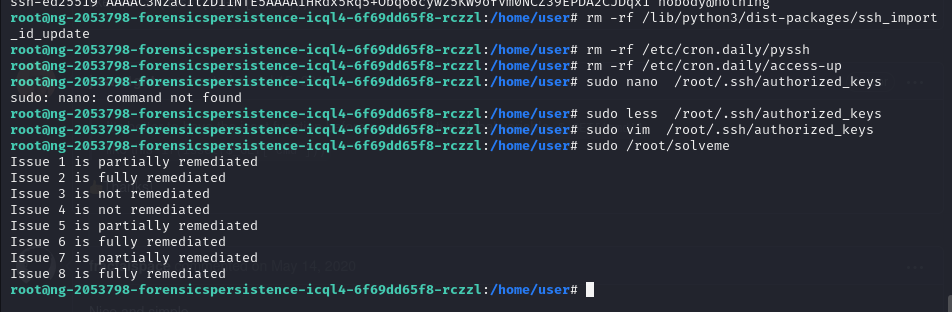
Две ежедневные задачи выглядят подозрительно, проверим что они делают



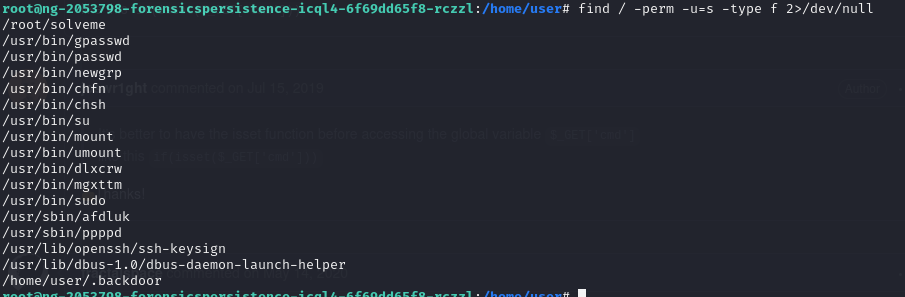


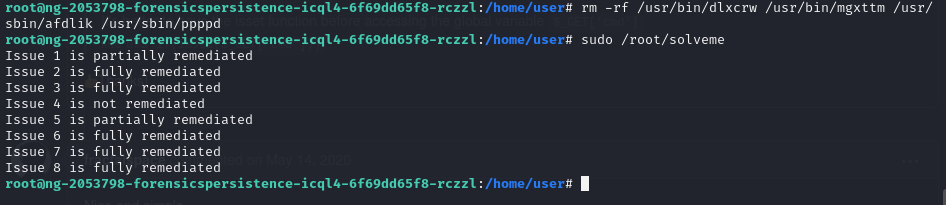
Задачи записывают авторизированный ключ ssh и мы можем смело их удалять,а также очистим сохраненные ключи



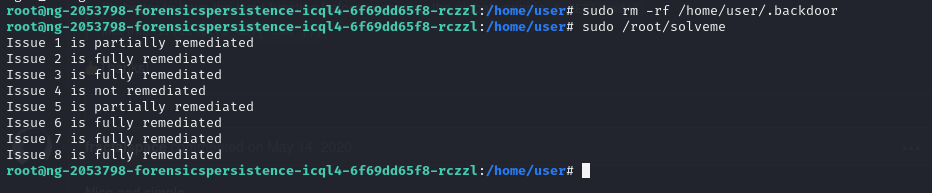


Проверим SUID файлы и увидим несколько странных названий. Они связаны с ежедневными задачами (access-up) - удаляем





В домашней директории видим файл .backdoor и удалим его навсякий случай





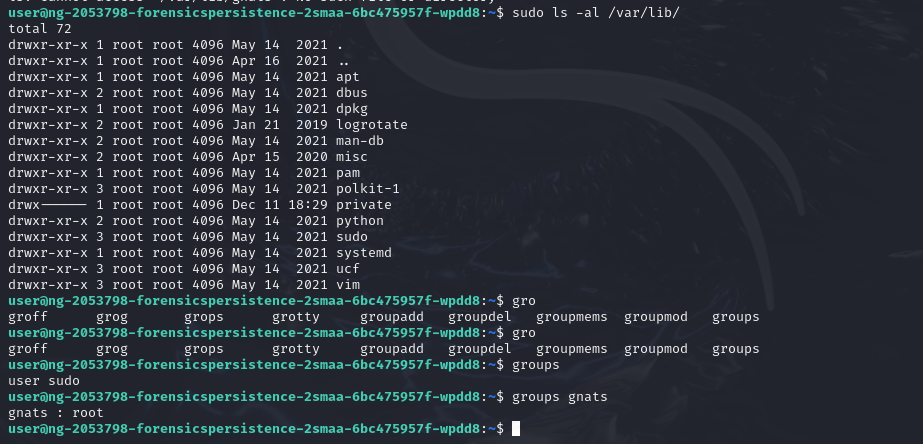
Проверим файлы с именем passwd и уберем ошибки из выдачи



В стандартном файле увидим системного пользователь(?) с измененным паролем, записанным в shadow

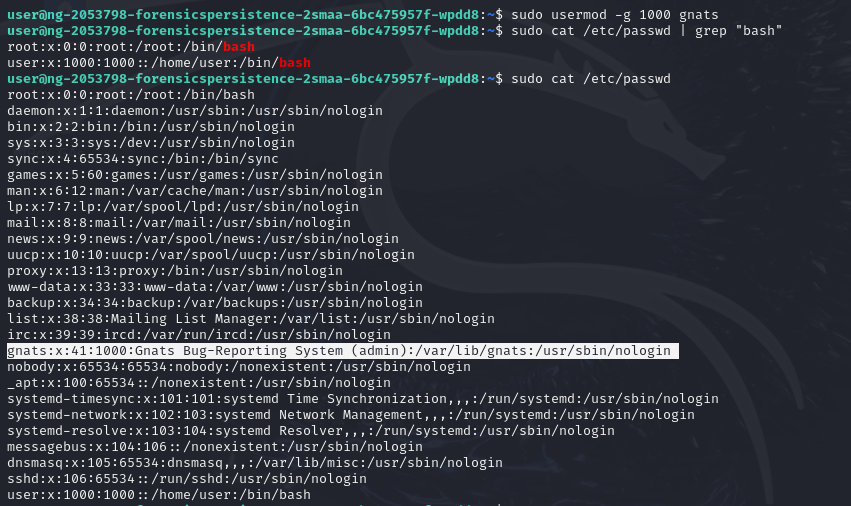


Его директории не существует, а также у него включен вход и стоит группа root (for what??????) – такого не должно быть

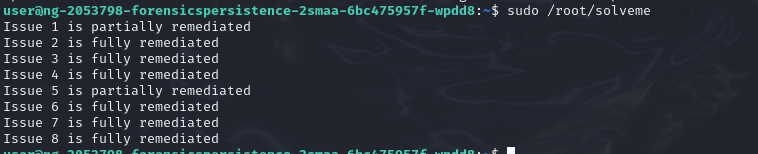


Уберем вход и изменим ему группу (например обычный пользователь (правильнее было бы указать группу 41))



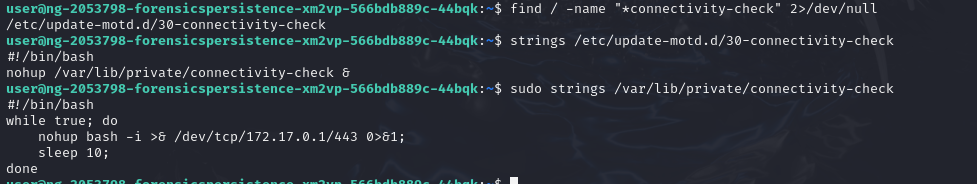


Спустя много времени и ошибок не получалось закрыть 2 задачи – попробуем заново, но более тщательно изучить систему

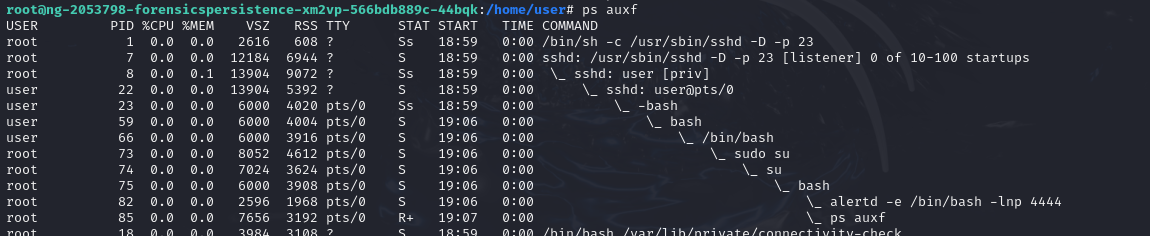


**Работа над ошибками**

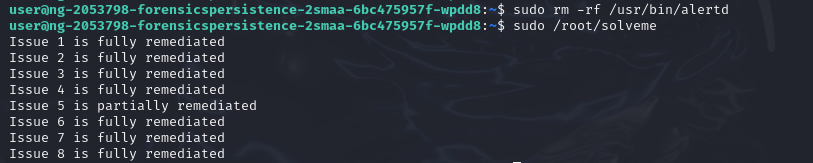
Если выполнить поиск по имени процесса, который создавал подключение то увидим место где хранится корень проблемы и удалим его

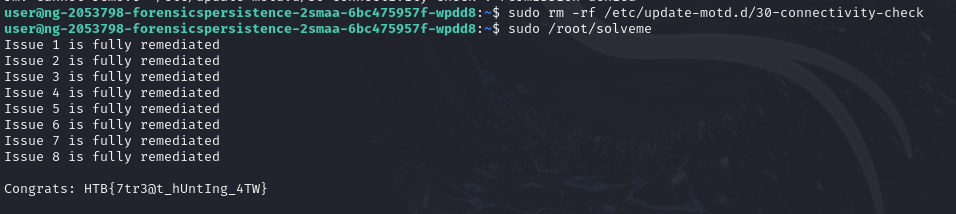


Если зайти под root (sudo su) и проверить процессы, то увидим новый процесс, который начинает слушать порт 4444



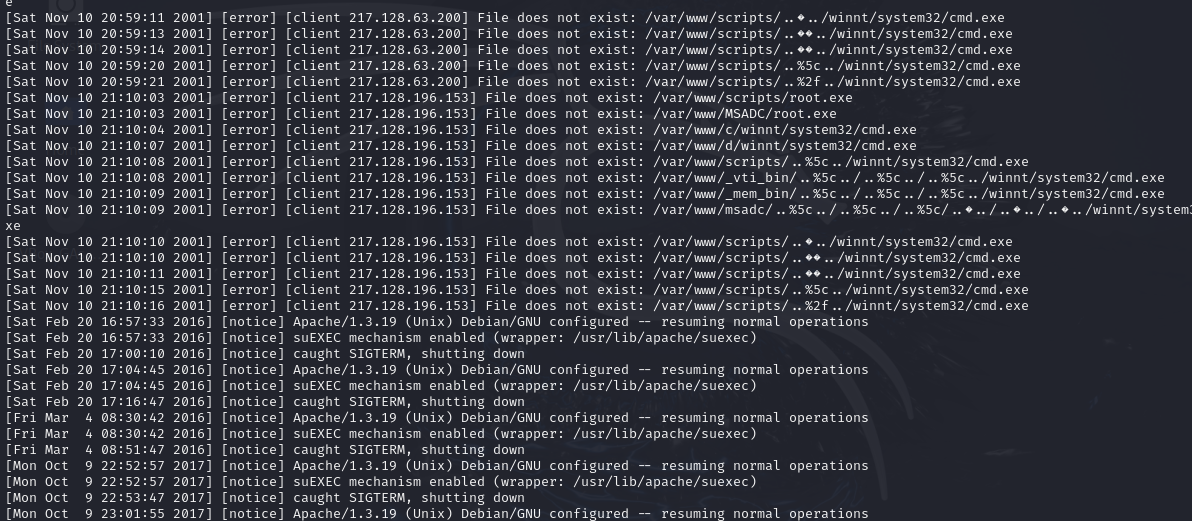
Отыскав его по имени ( find / -name “alertd” ) удаляем его и можем получить флаг

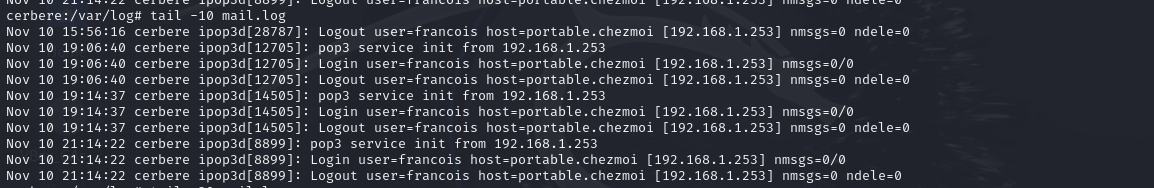


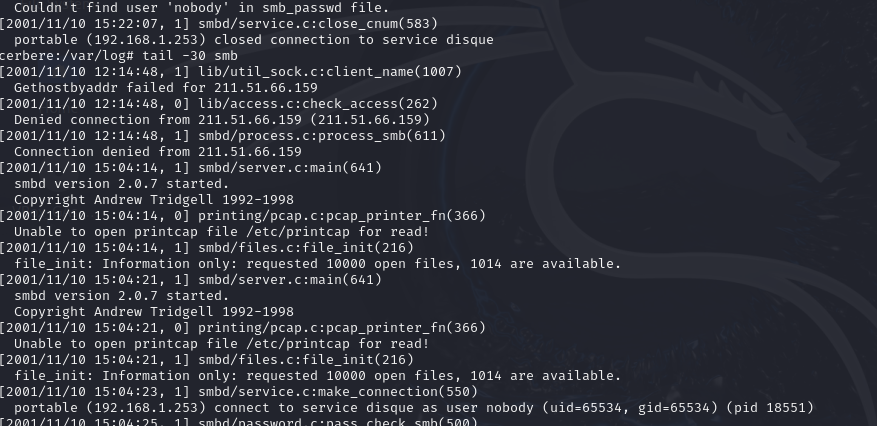


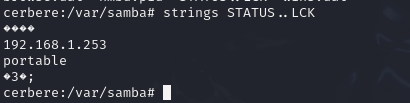
**Повышенная сложность 1 НАБРОСКИ (можно не смотреть, сохранил для себя)**

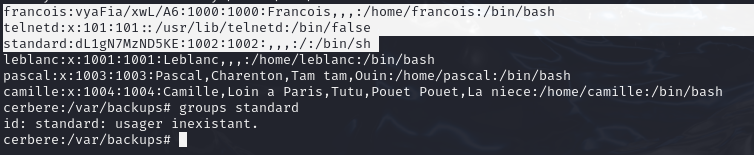
**НЕ РЕШЕНО,TRY HARDER**







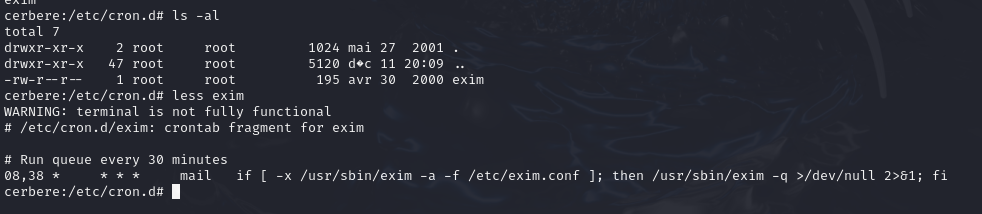


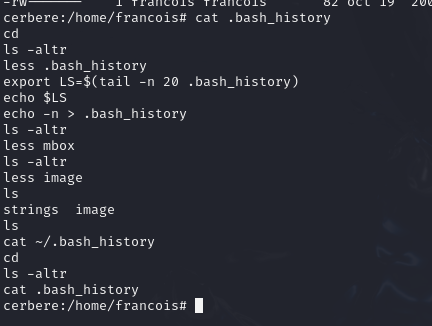


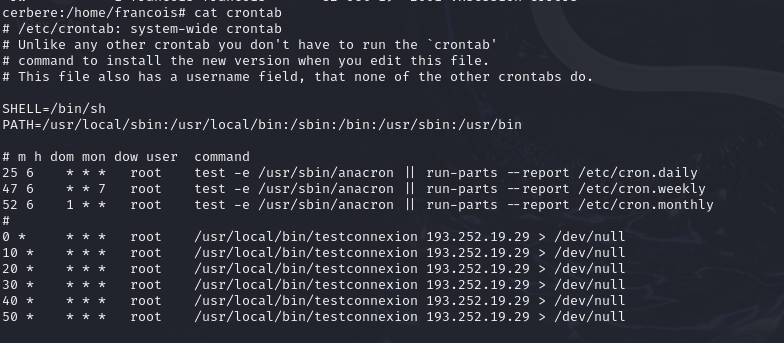


vyaFia/xwL/A6

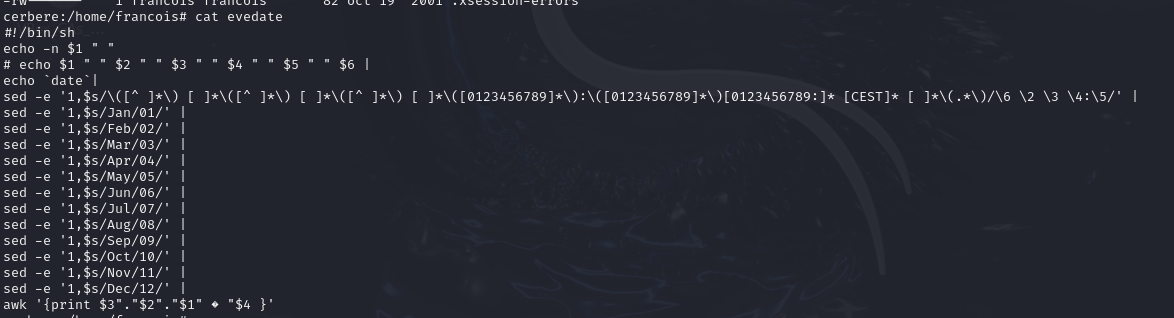
dL1gN7MzND5KE

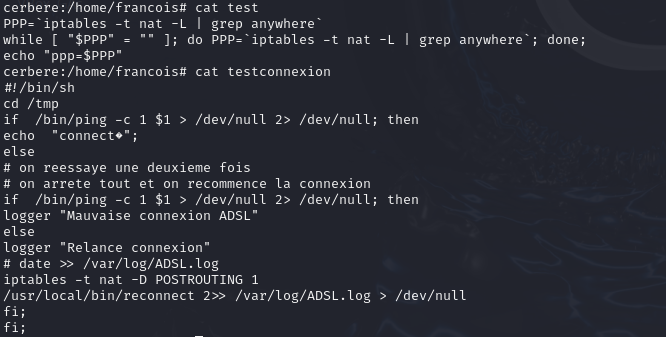


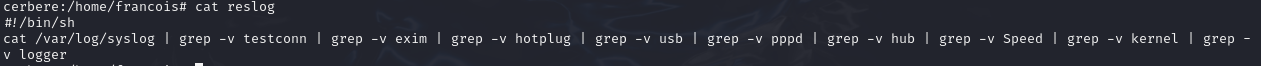


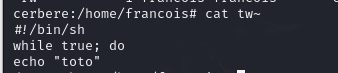


193.252.19.29

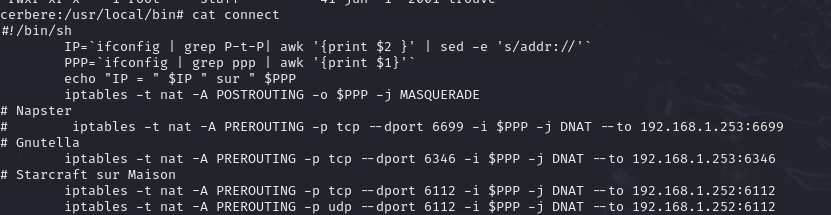


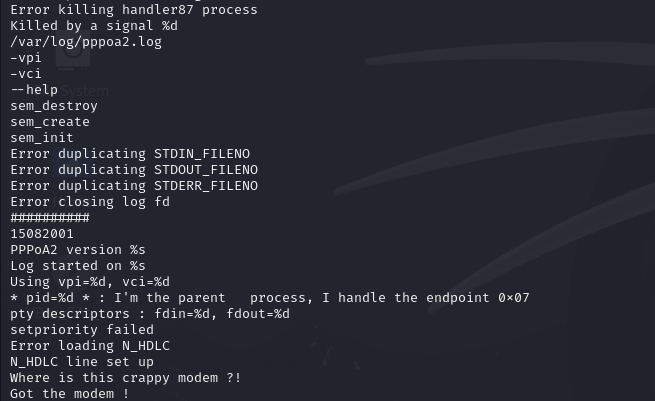












Cat /passwd

63f9b439d6afe71591da7637df2fc4ff ---- 441511066