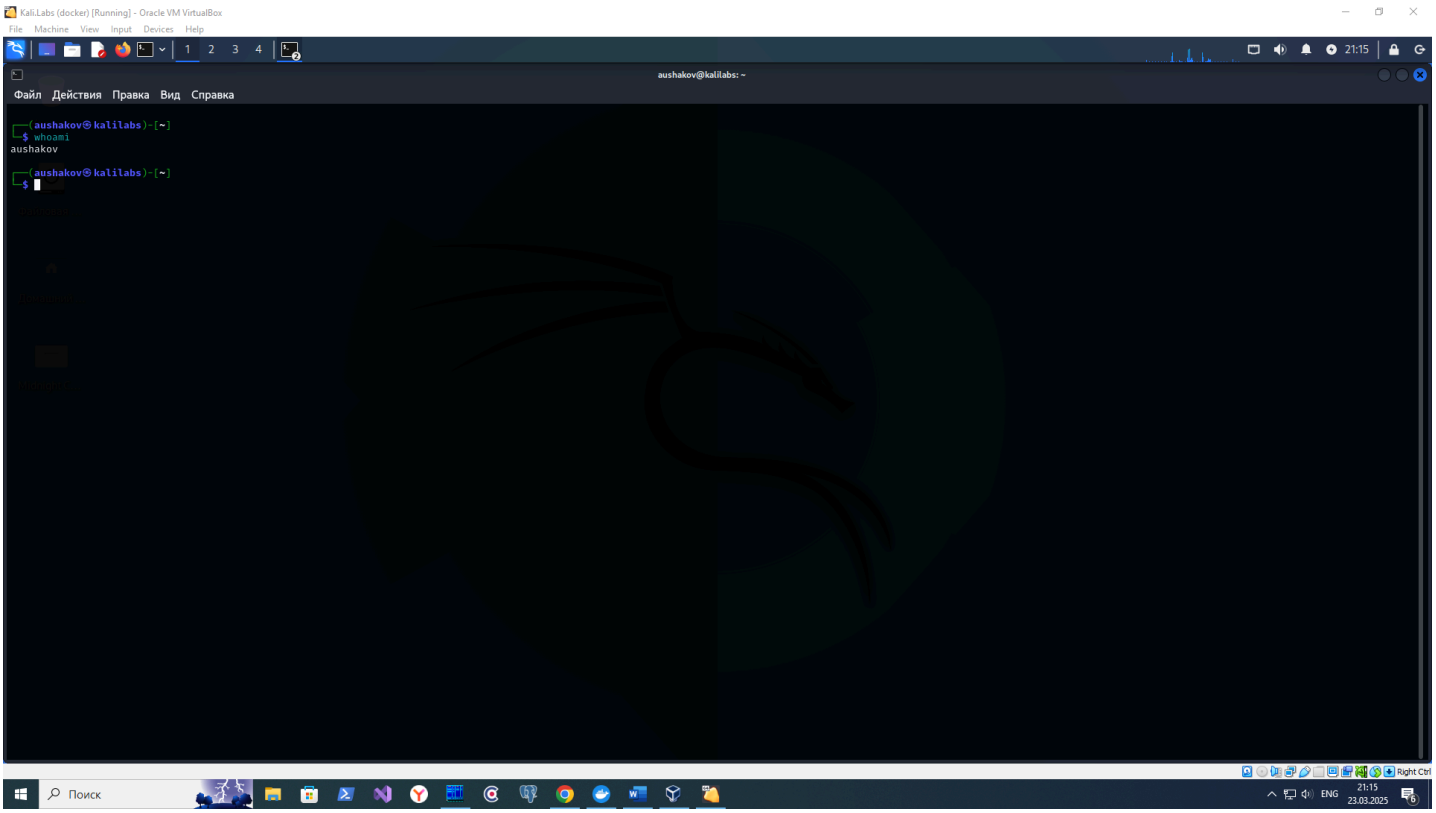
Описание уязвимости

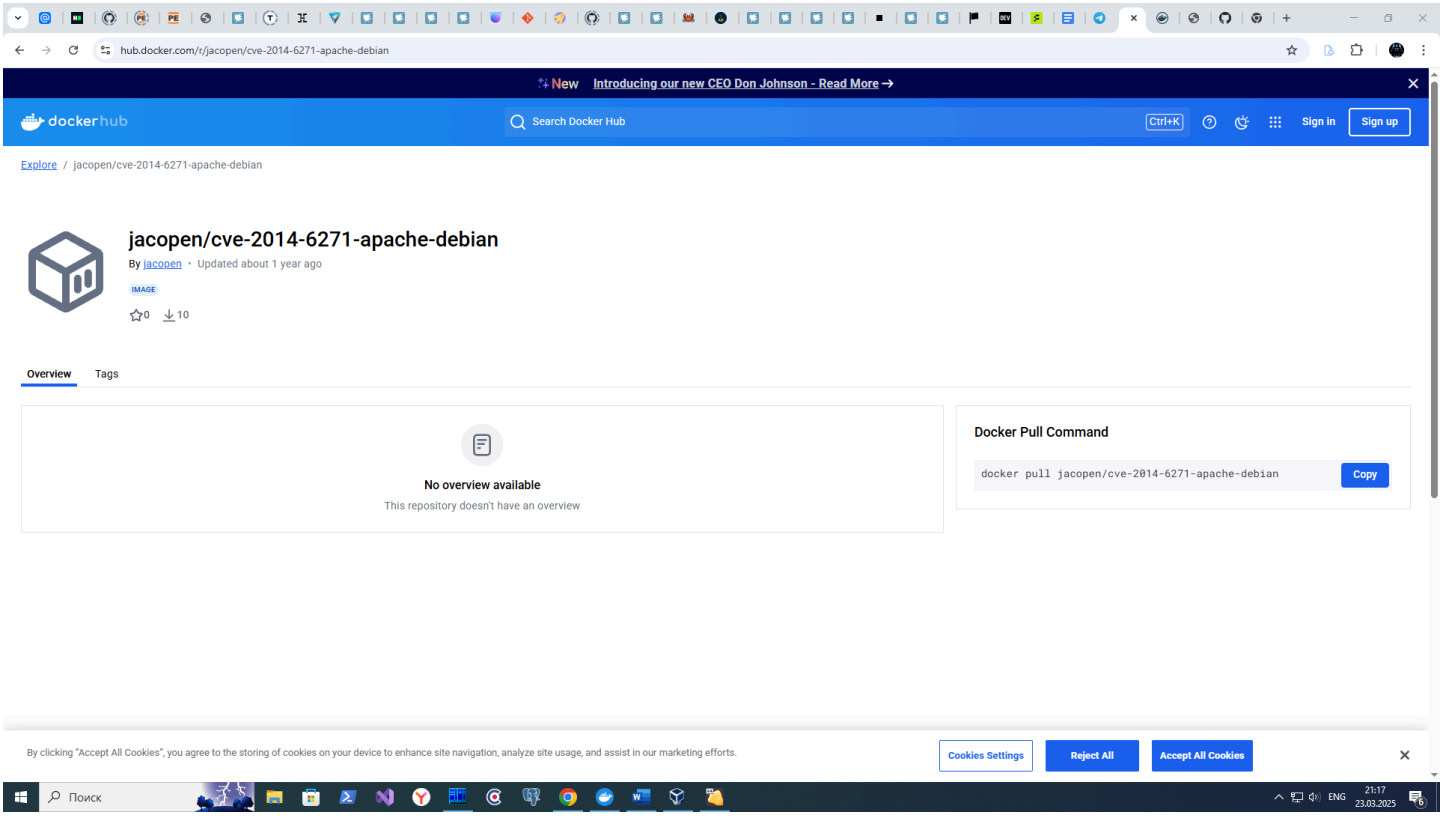
Уязвимость Shellshock (CVE-2014-6271) — это критическая уязвимость в интерпретаторе командной строки Bash, которая позволяет злоумышленникам выполнять произвольный код на уязвимых системах. Уязвимость возникает из-за недостатков в обработке переменных окружения, что позволяет внедрять и выполнять произвольные команды через HTTP-заголовки.

Эта уязвимость может быть использована для удаленного выполнения кода, что делает системы, использующие уязвимые версии Bash, особенно уязвимыми к атакам. Злоумышленники могут использовать ее для выполнения вредоносных команд, получения доступа к данным или даже полного контроля над системой.

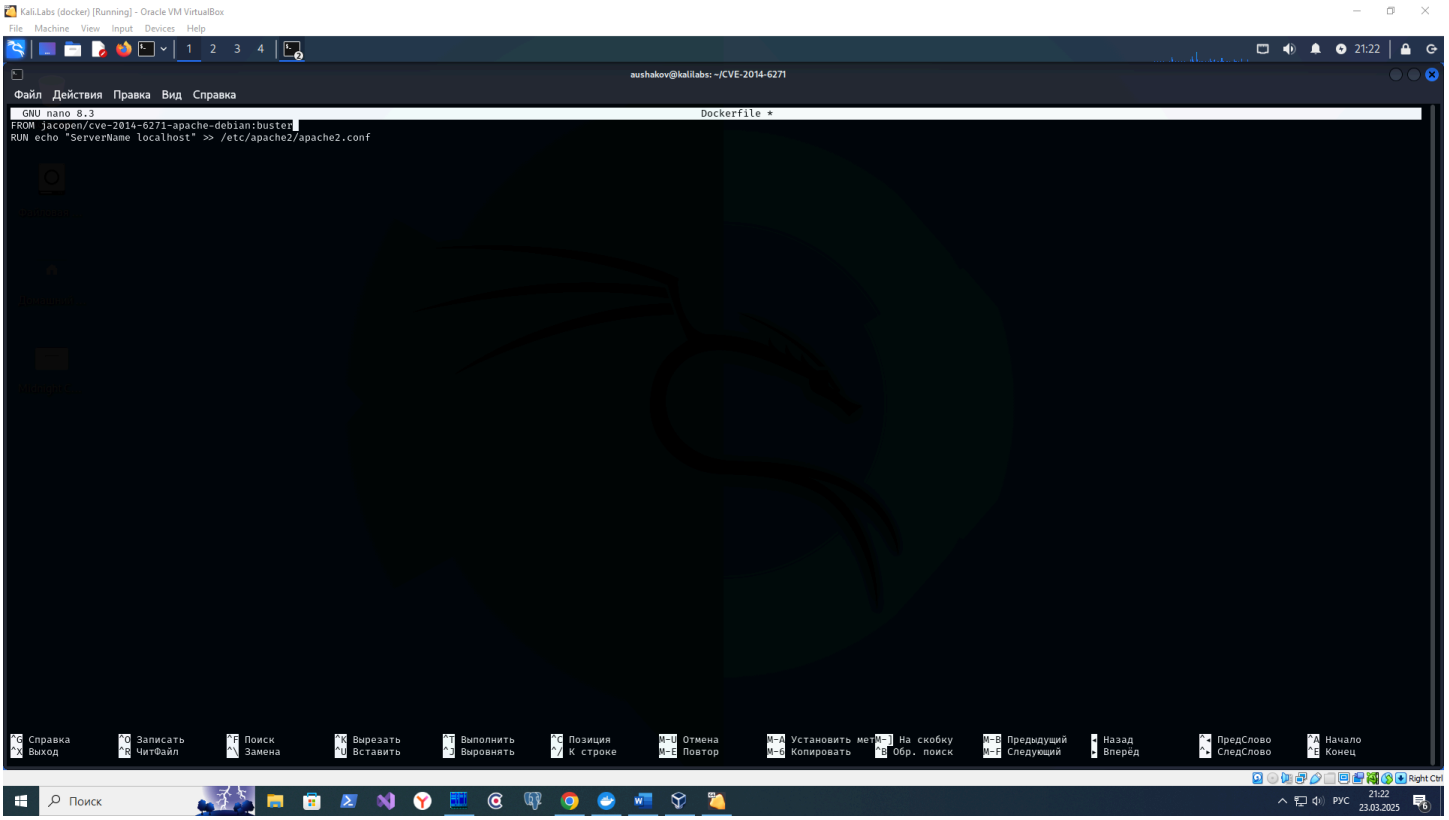
Создаю виртуальную машину на Kali Linux



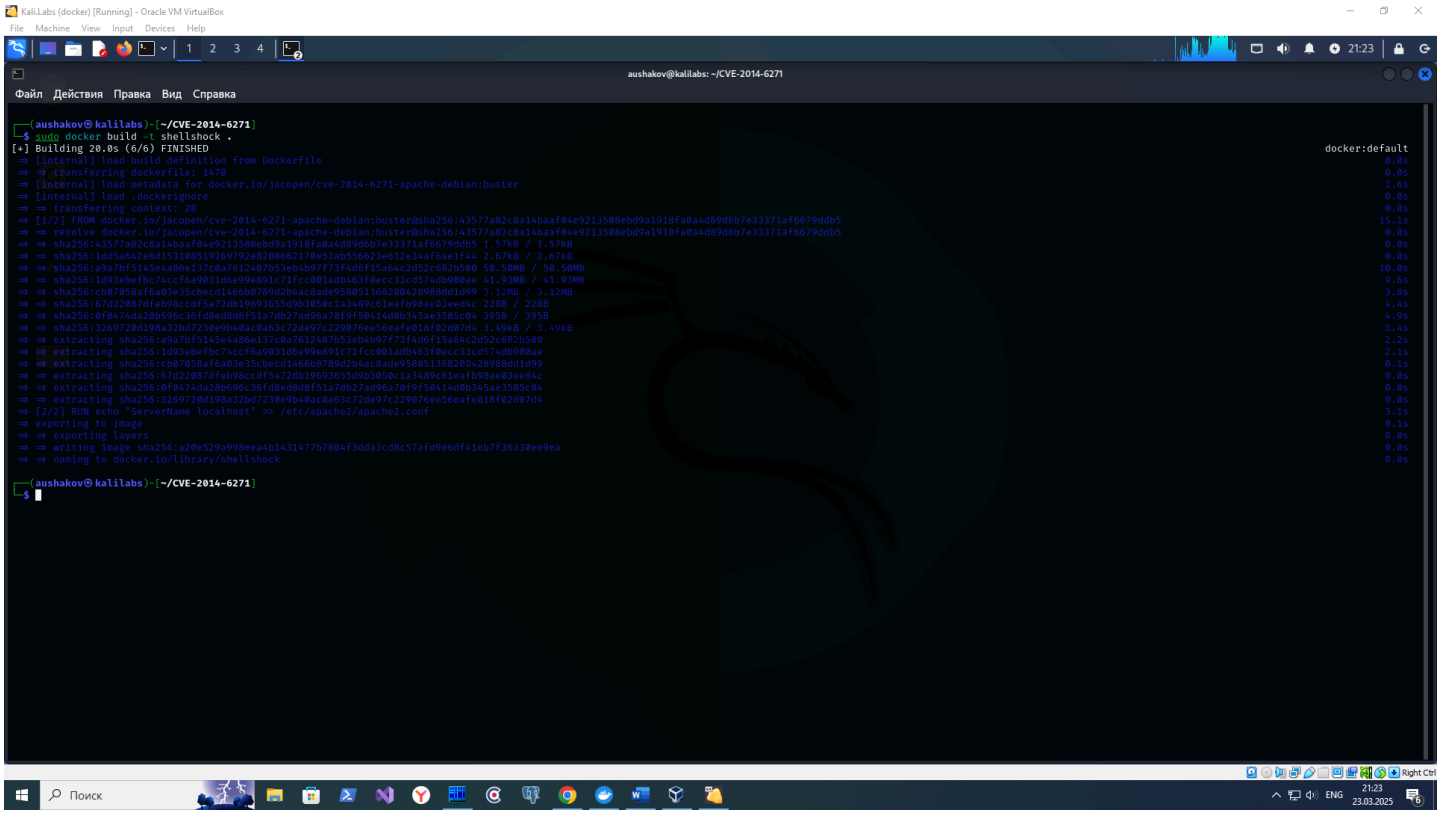
Пробую воспроизвести cve-2014-6271 вручную:
1) Для этого я буду использовать образ jacopen/cve-2014-6271-apache-debian для создания docker контейнера (vulnerables/cve-2014-6271 у меня не заработал)



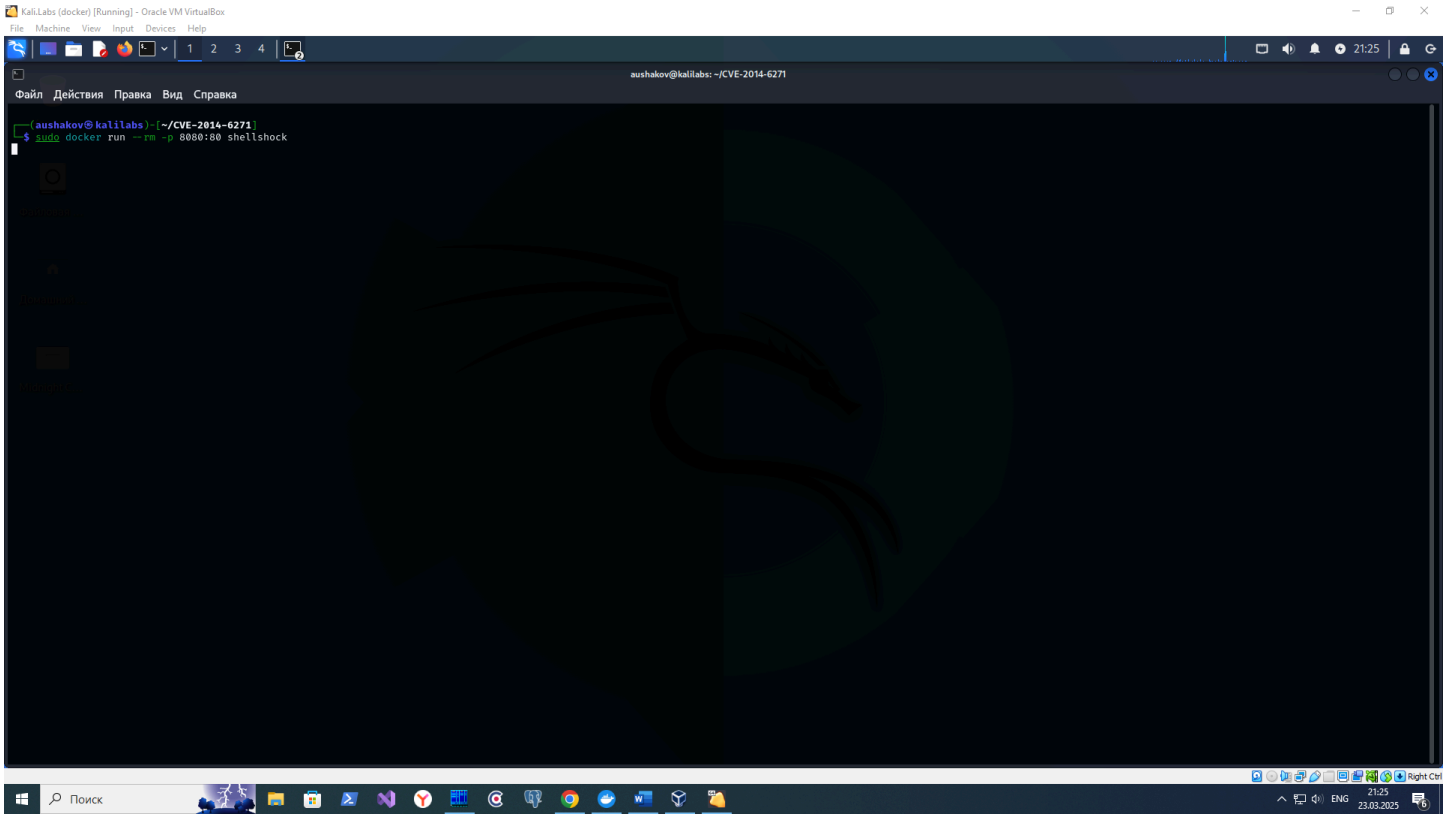
2) Создаю Dockerfile на основе образа jacopen/cve-2014-6271-apache-debian:

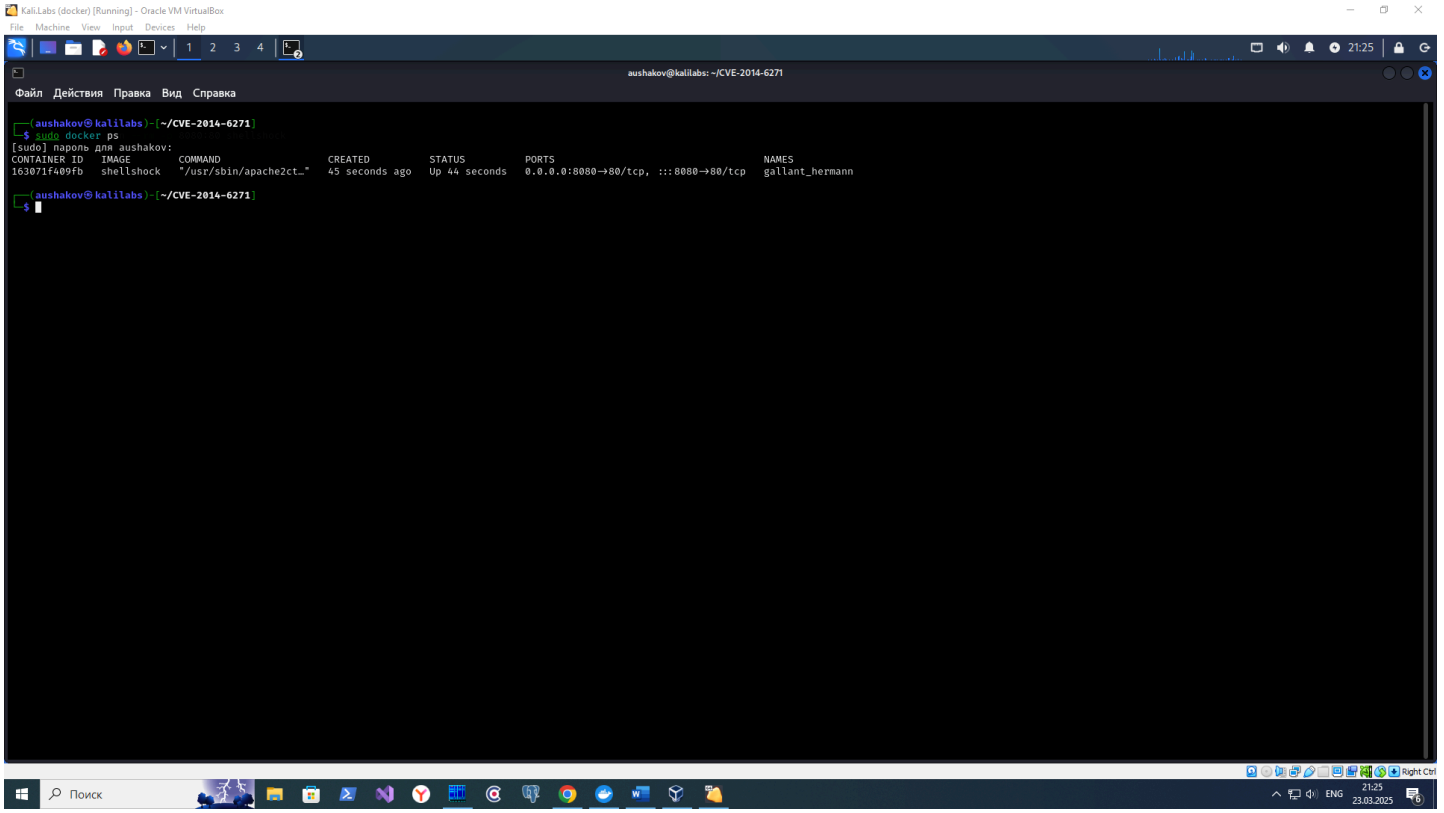


3) Запускаю сборку образа моего контейнера docker

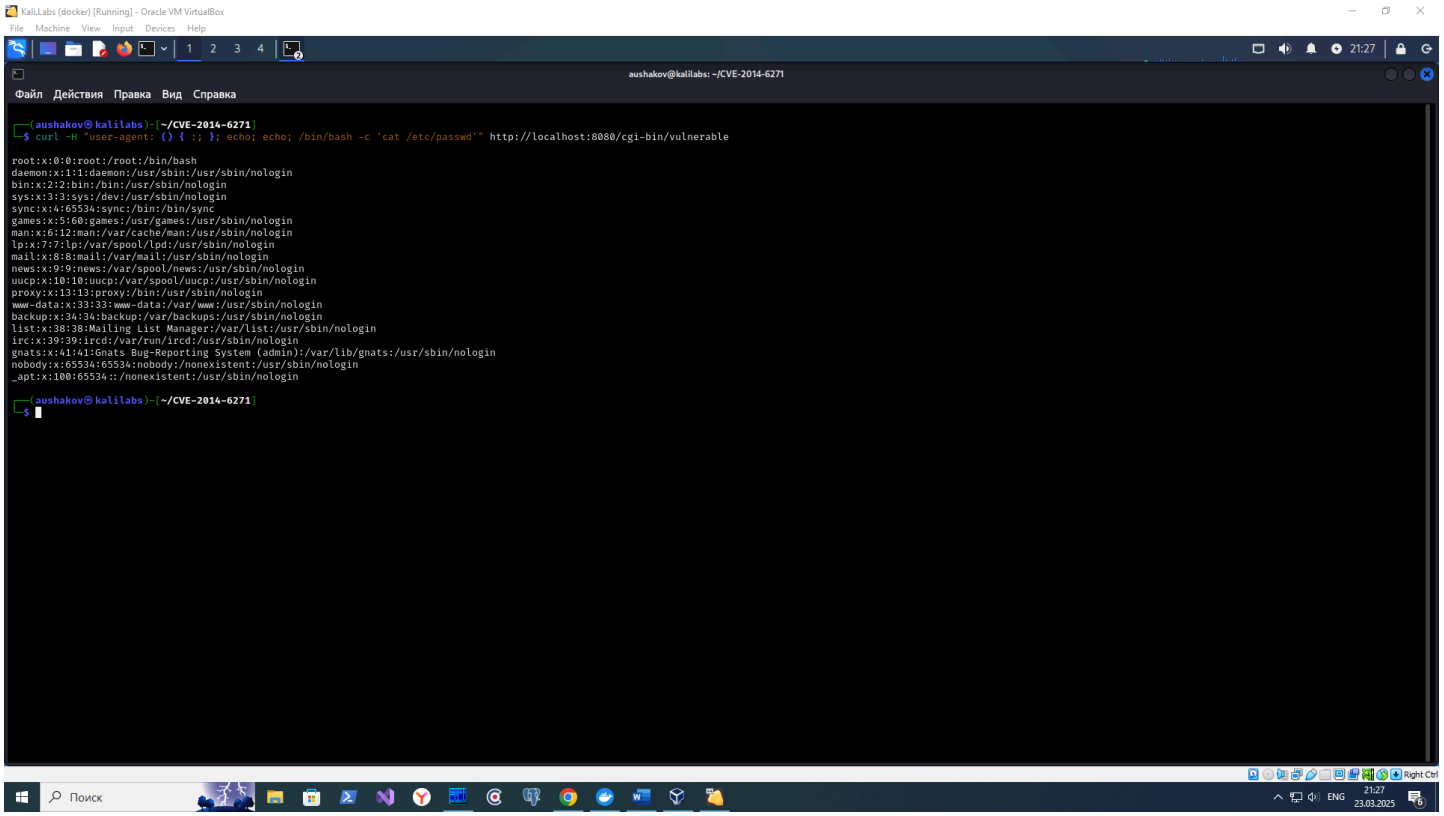


4) Запускаю созданный контейнер docker (с учетом необходимости проброса портов)



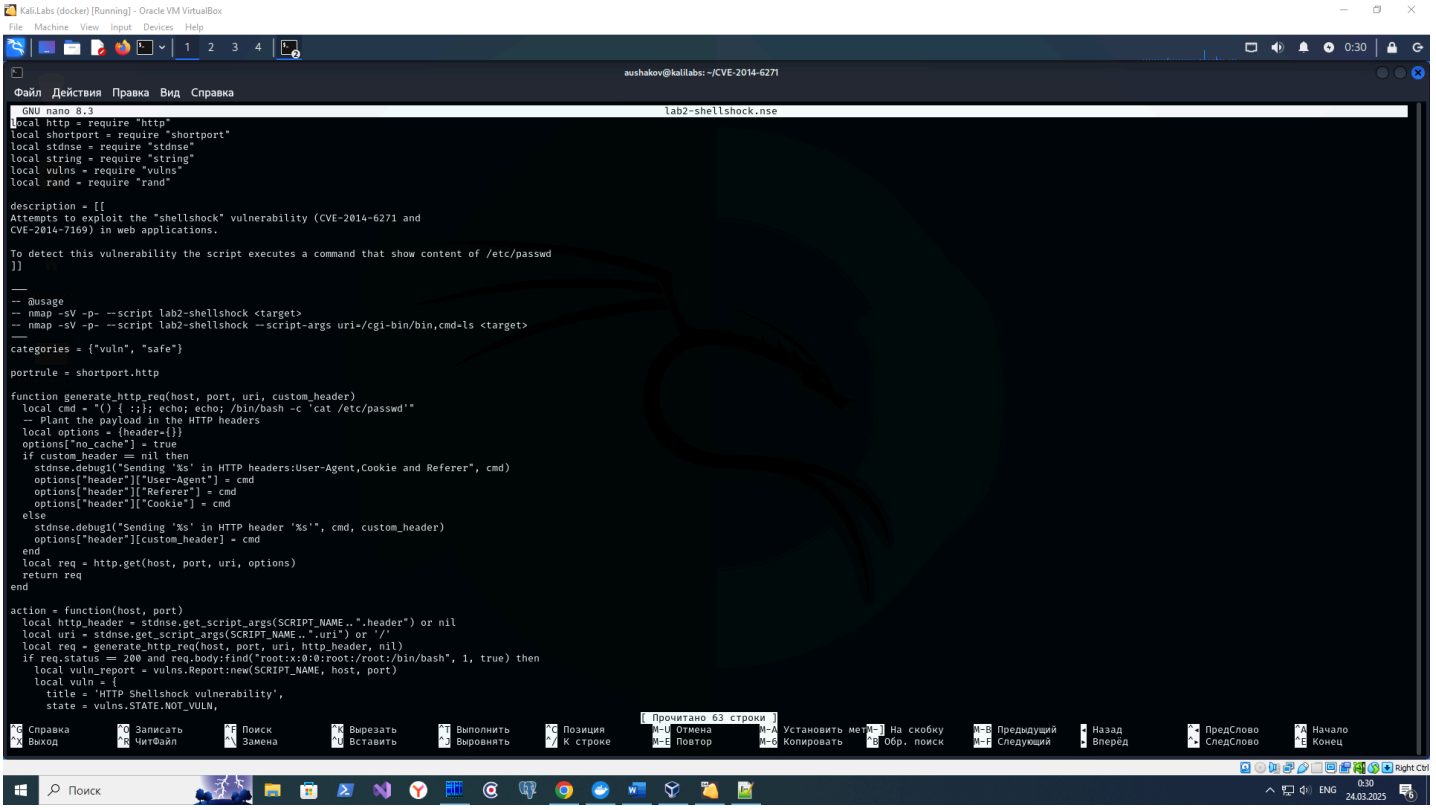


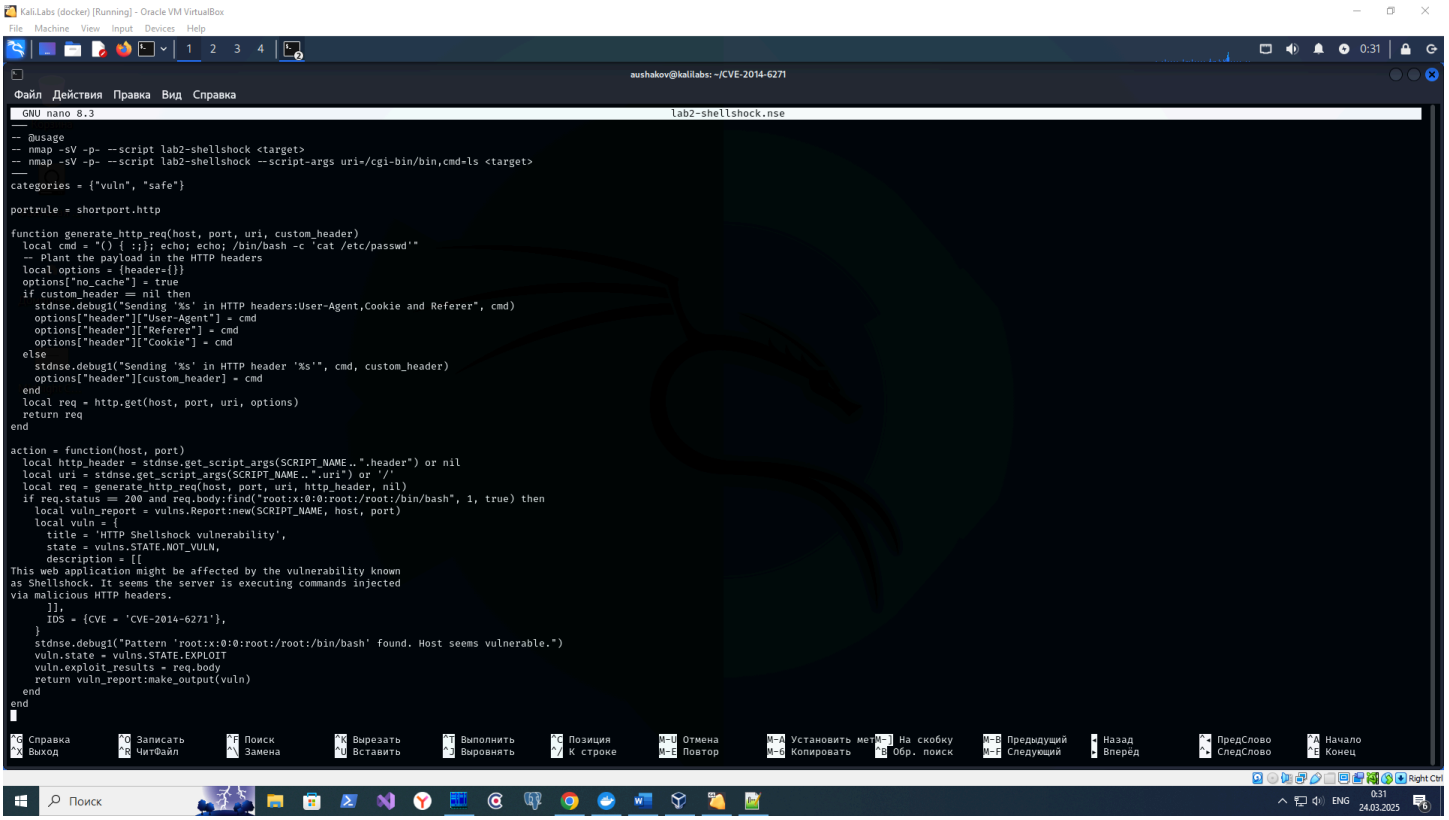
5) Запускаю проверку наличия и воспроизводимости cve-2014-6271



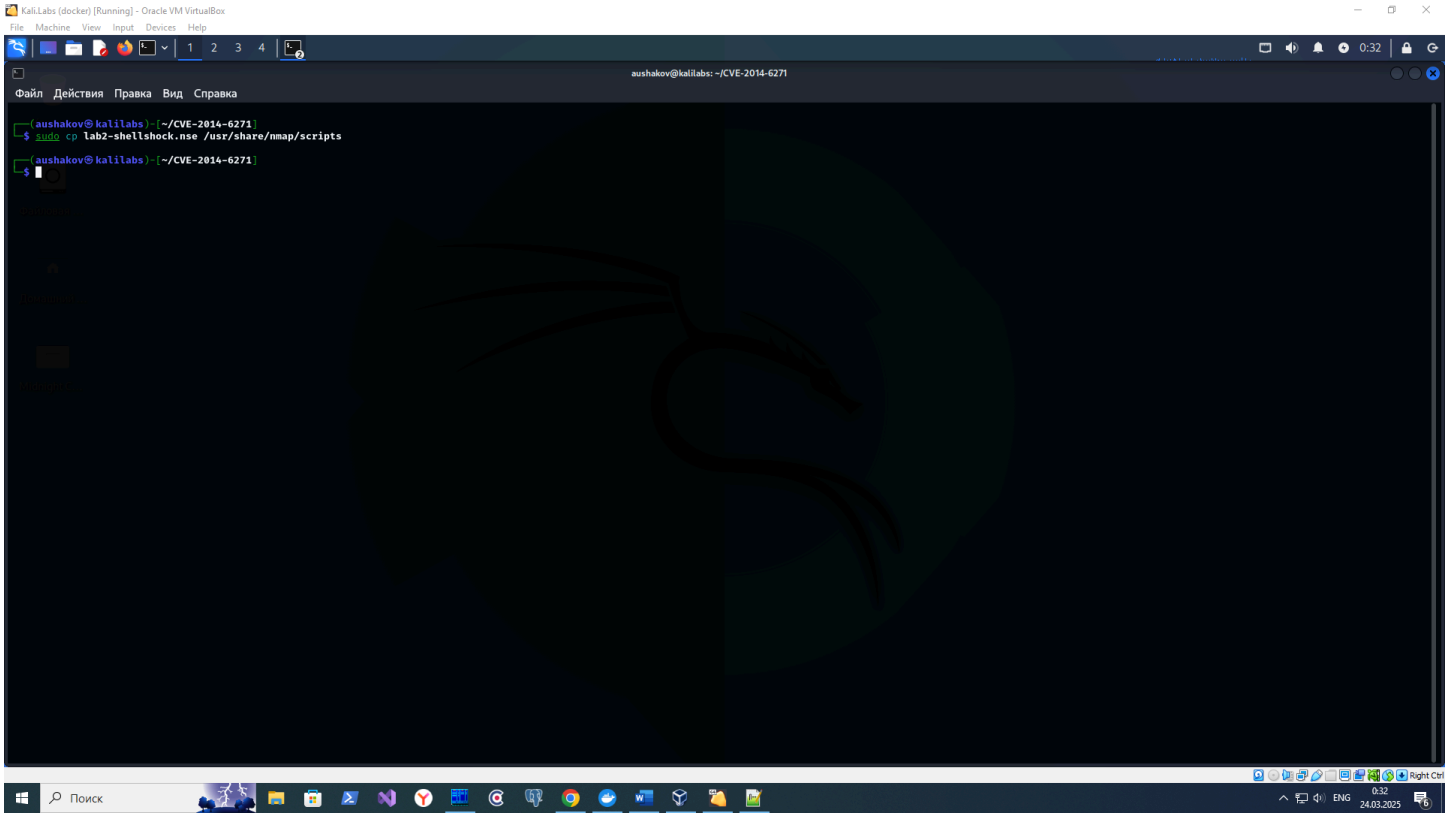
Из результатов запуска видно, что cve-2014-6271 воспроизводится

Создаю nse скрипт с именем lab2-shellshock.nse (сам скрипт находится в отдельном файле)

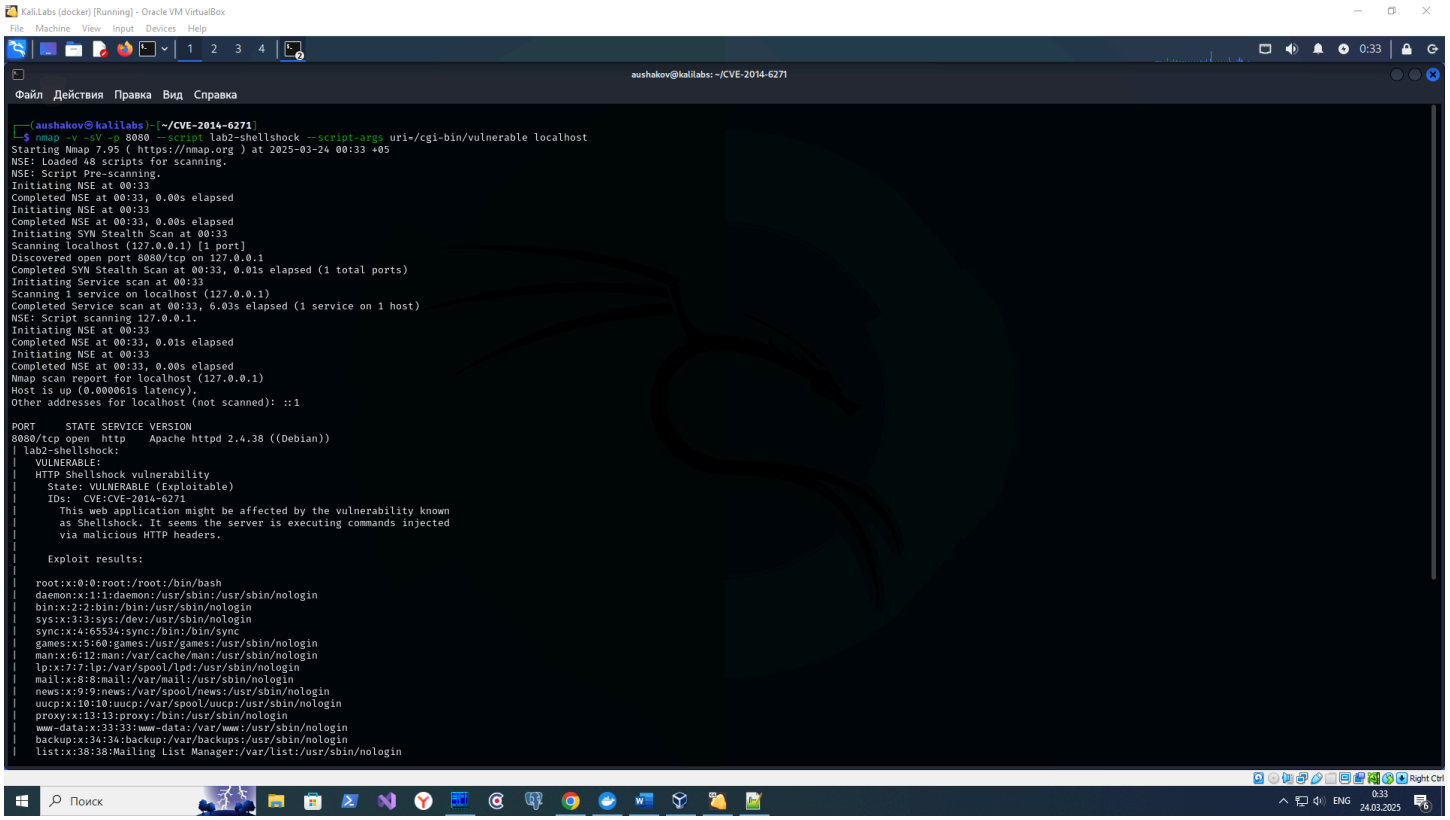


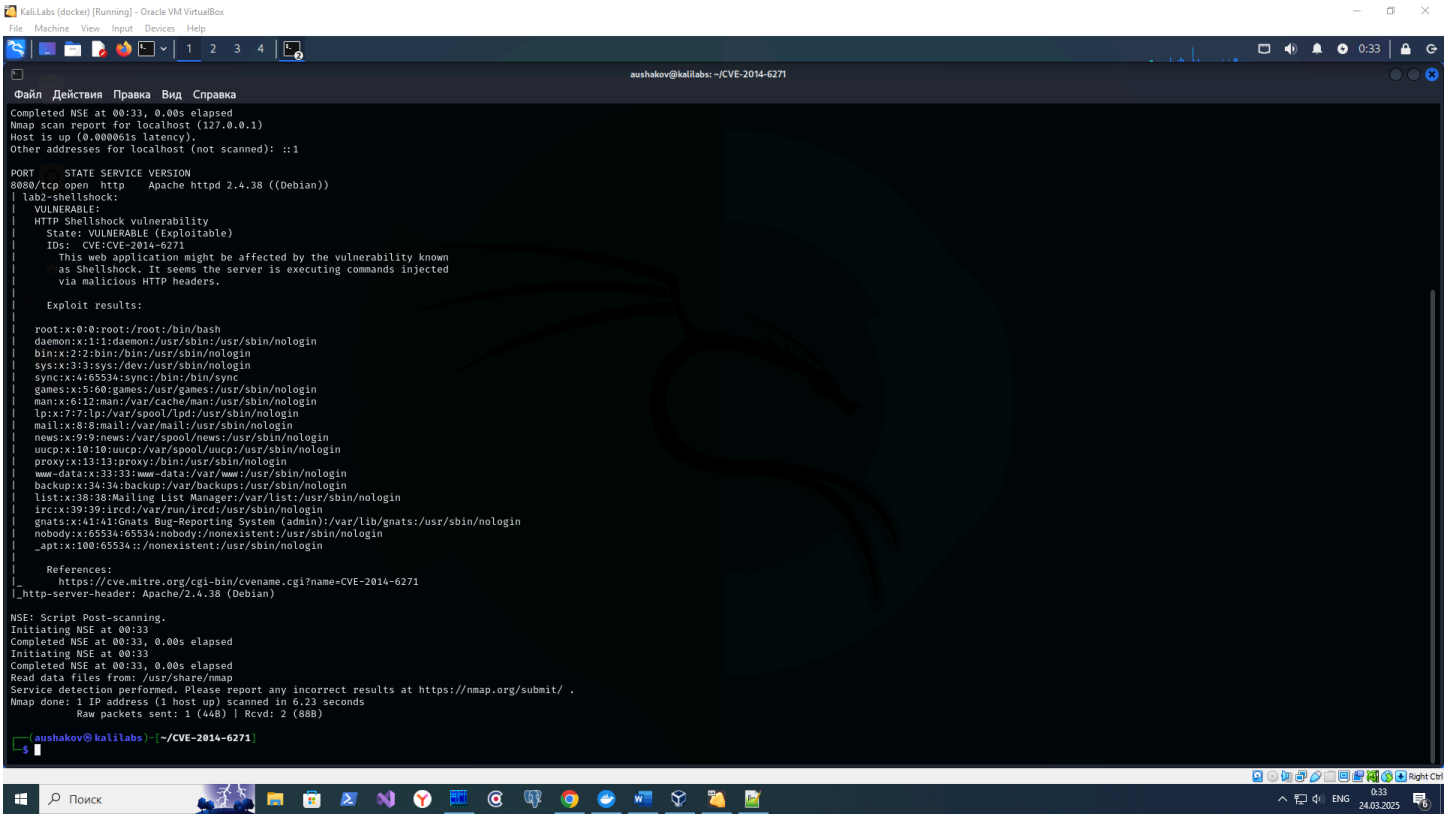


Копирую созданный скрипт в директорию с nse скриптами для nmap (в моем случае - это /usr/share/nmap/scripts)



Запускаю созданный nse скрипт через nmap





Из результатов запуска видно, что nmap находит в сервисе, расположенном в контейнере docker, уязвимость cve-2014-6271. Значит скрипт работает верно.

Уязвимость Shellshock (CVE-2014-6271) — это серьезная уязвимость в интерпретаторе команд Bash, которая позволяет злоумышленникам выполнять произвольные команды на системах, где Bash используется для обработки входящих данных, например, через CGI-скрипты на веб-серверах.

Краткое описание:

- Что: Уязвимость в Bash, позволяющая удаленно выполнять команды.
- Как: Злоумышленник может внедрить вредоносный код в HTTP-заголовки или переменные окружения.
- Где: Веб-серверы и системы, использующие Bash для обработки сценариев.
- Последствия: Возможность полного контроля над системой, утечка данных и другие вредоносные действия.