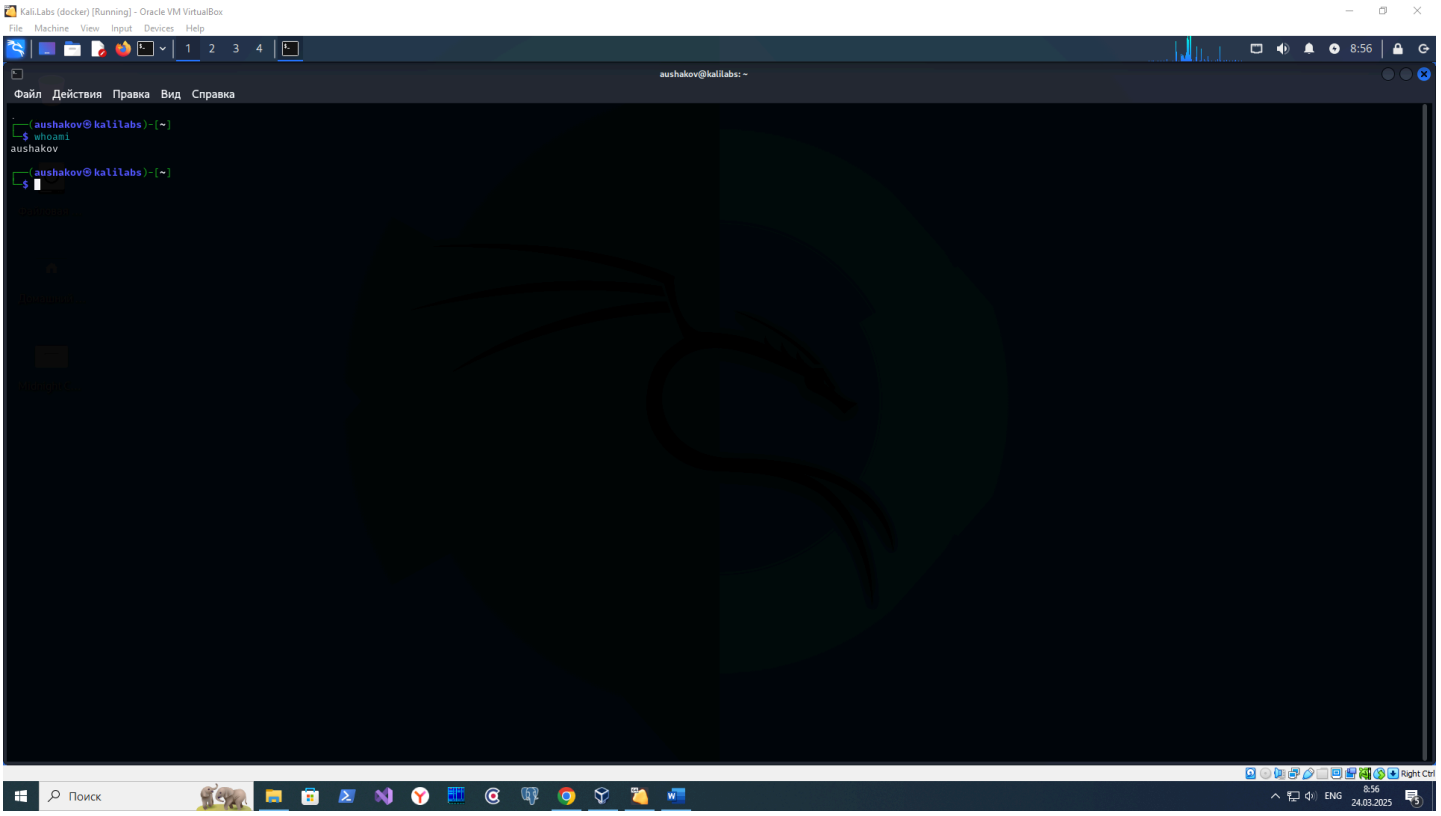
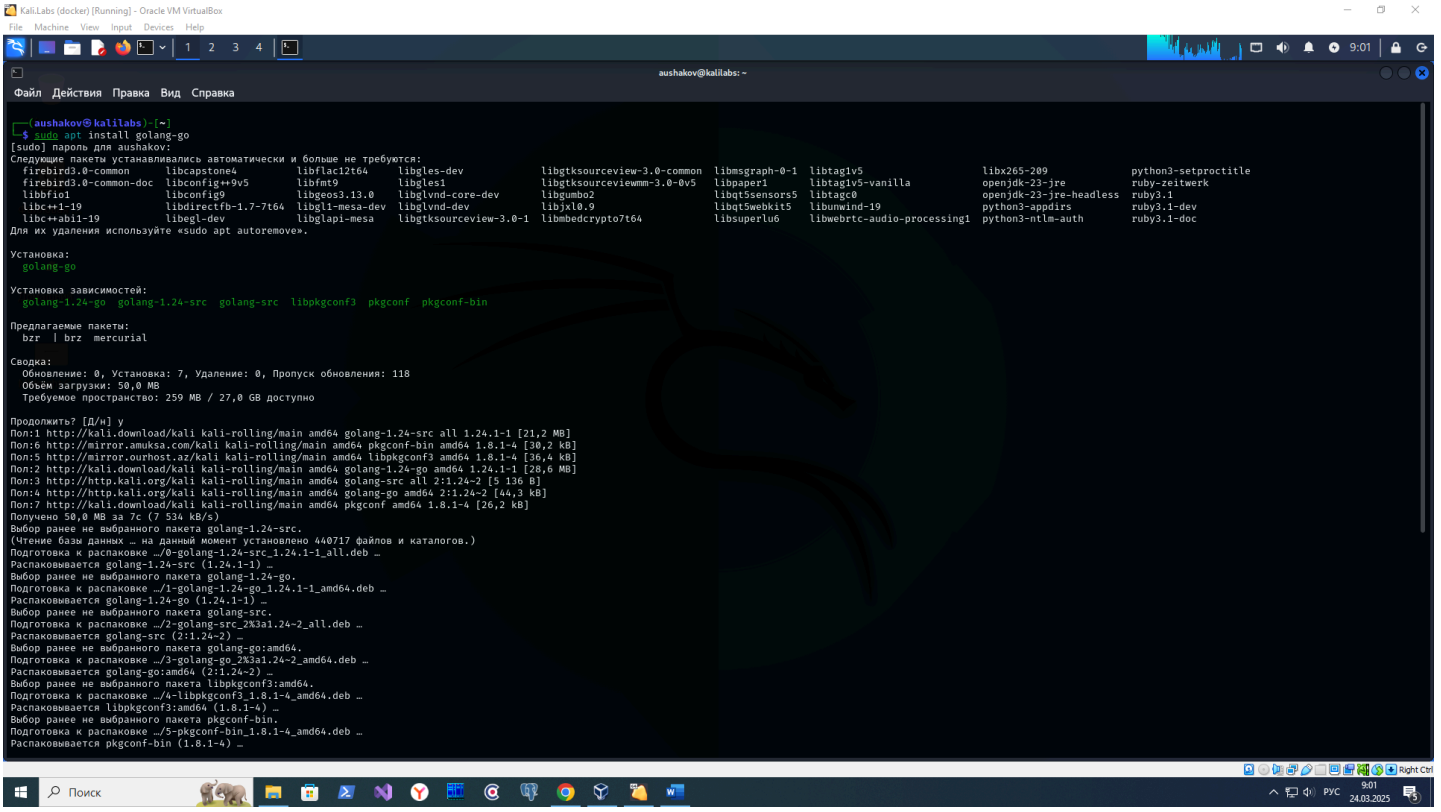
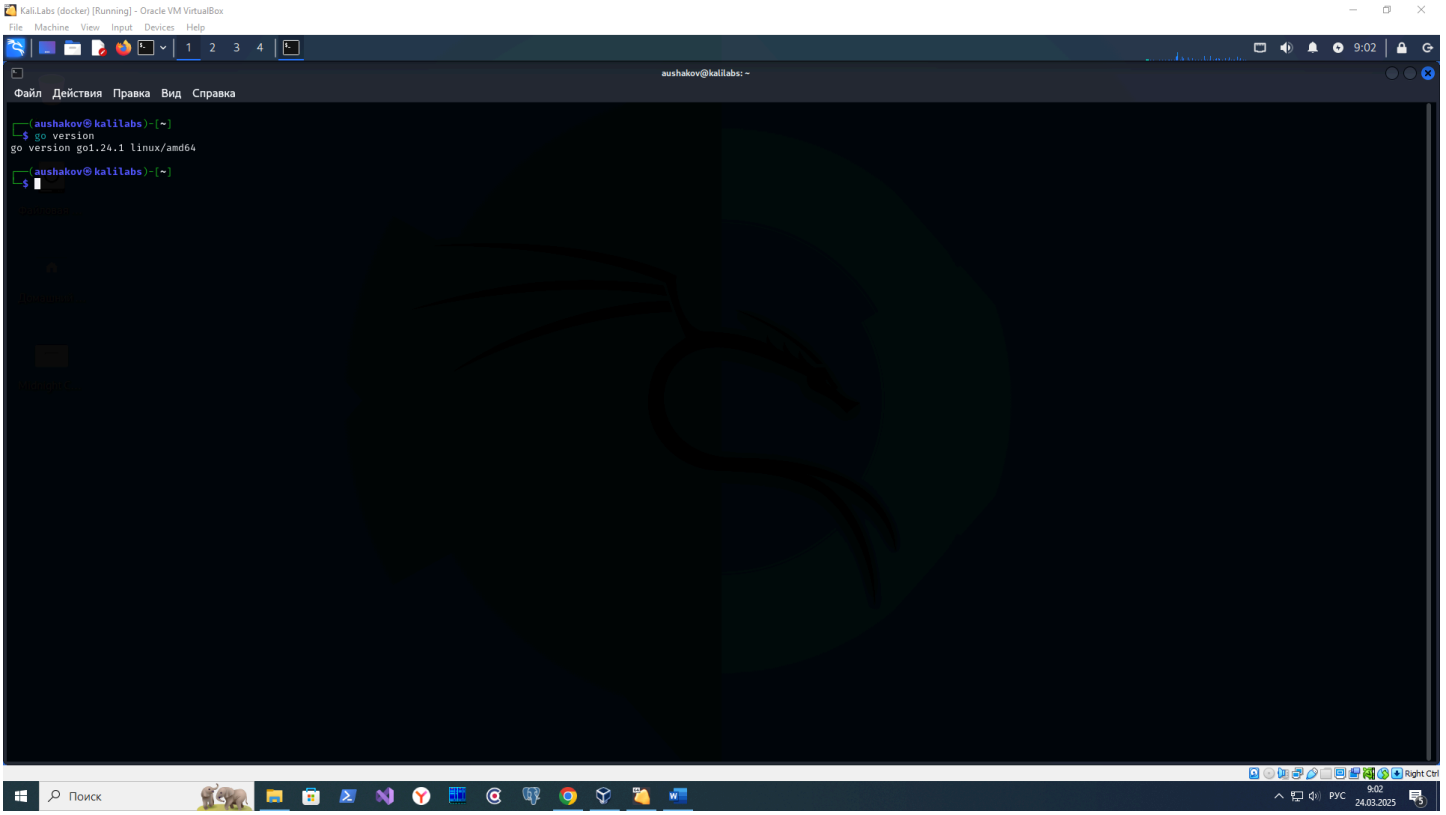
Создаю виртуальную машину на Kali Linux



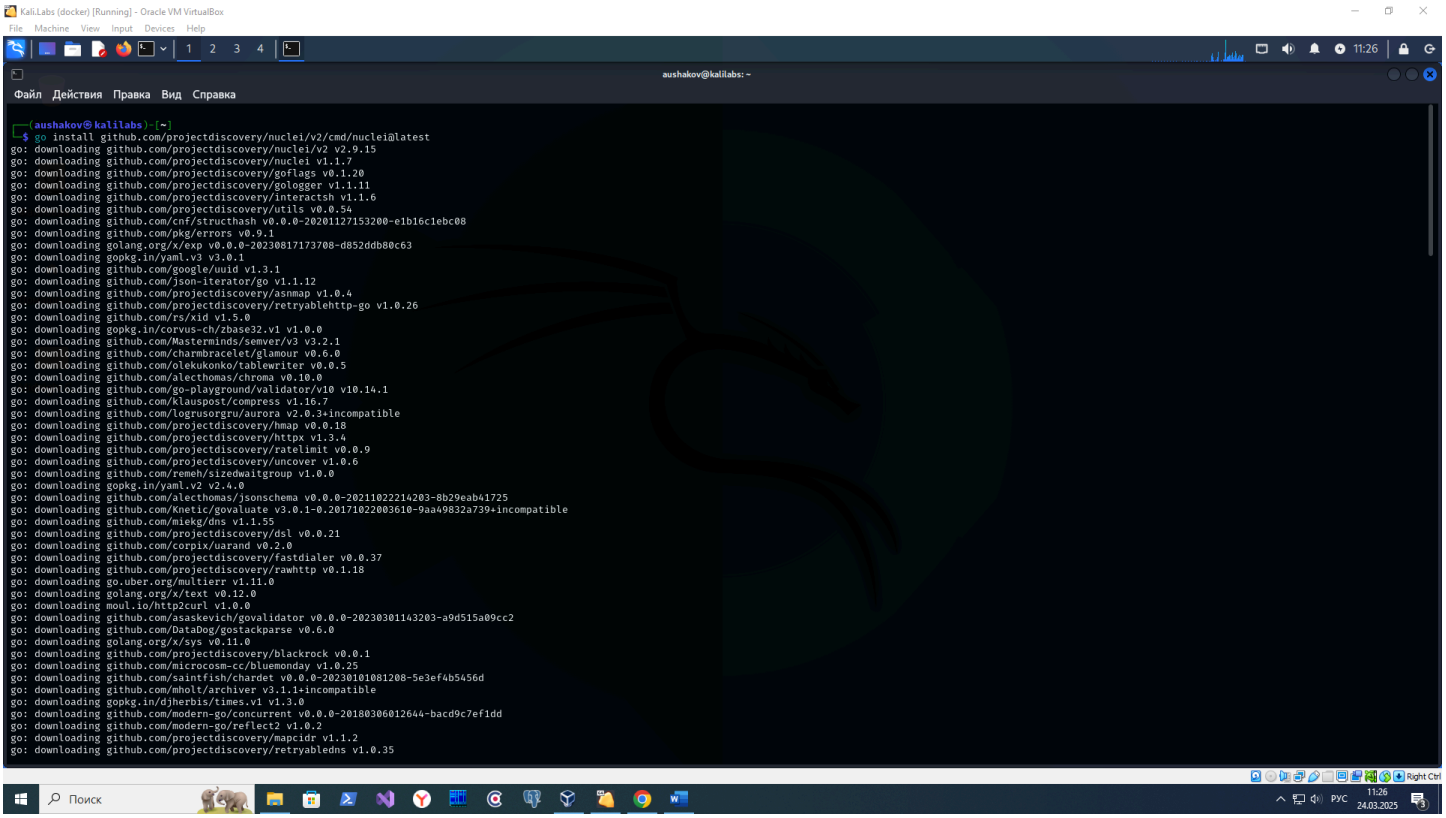
Устанавливаю golang для работы с Nuclei



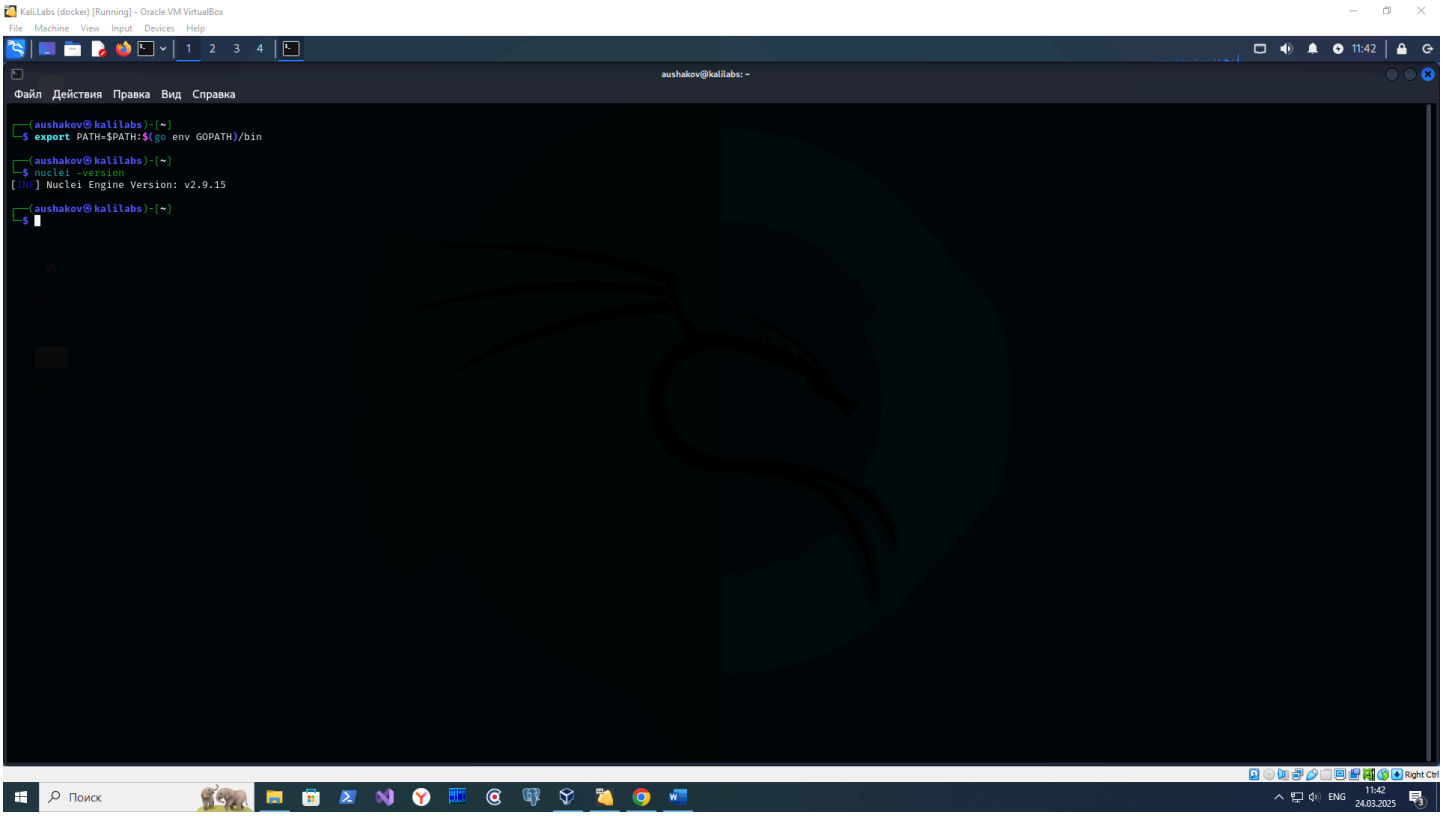
Проверяю версию golang



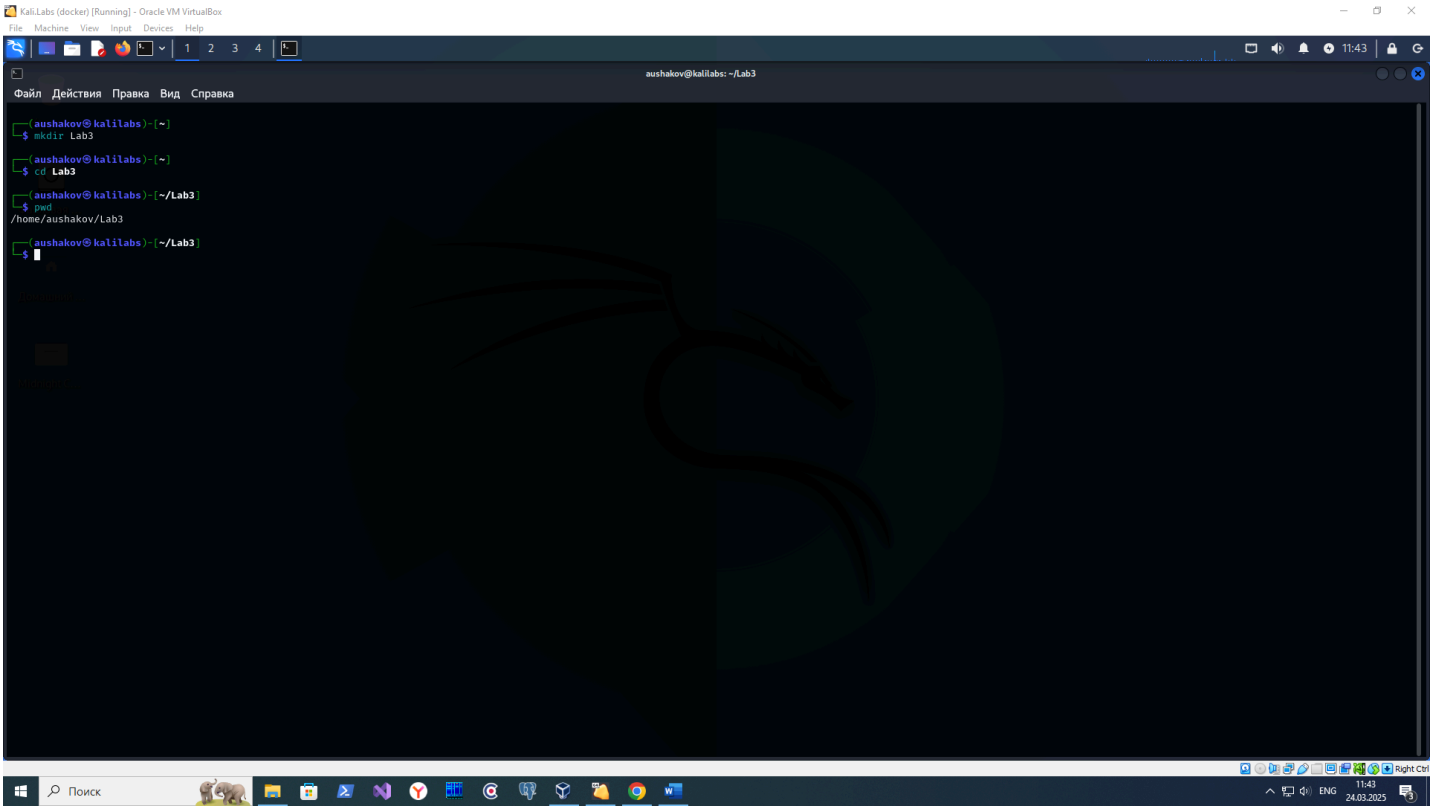
Устанавливаю Nuclei



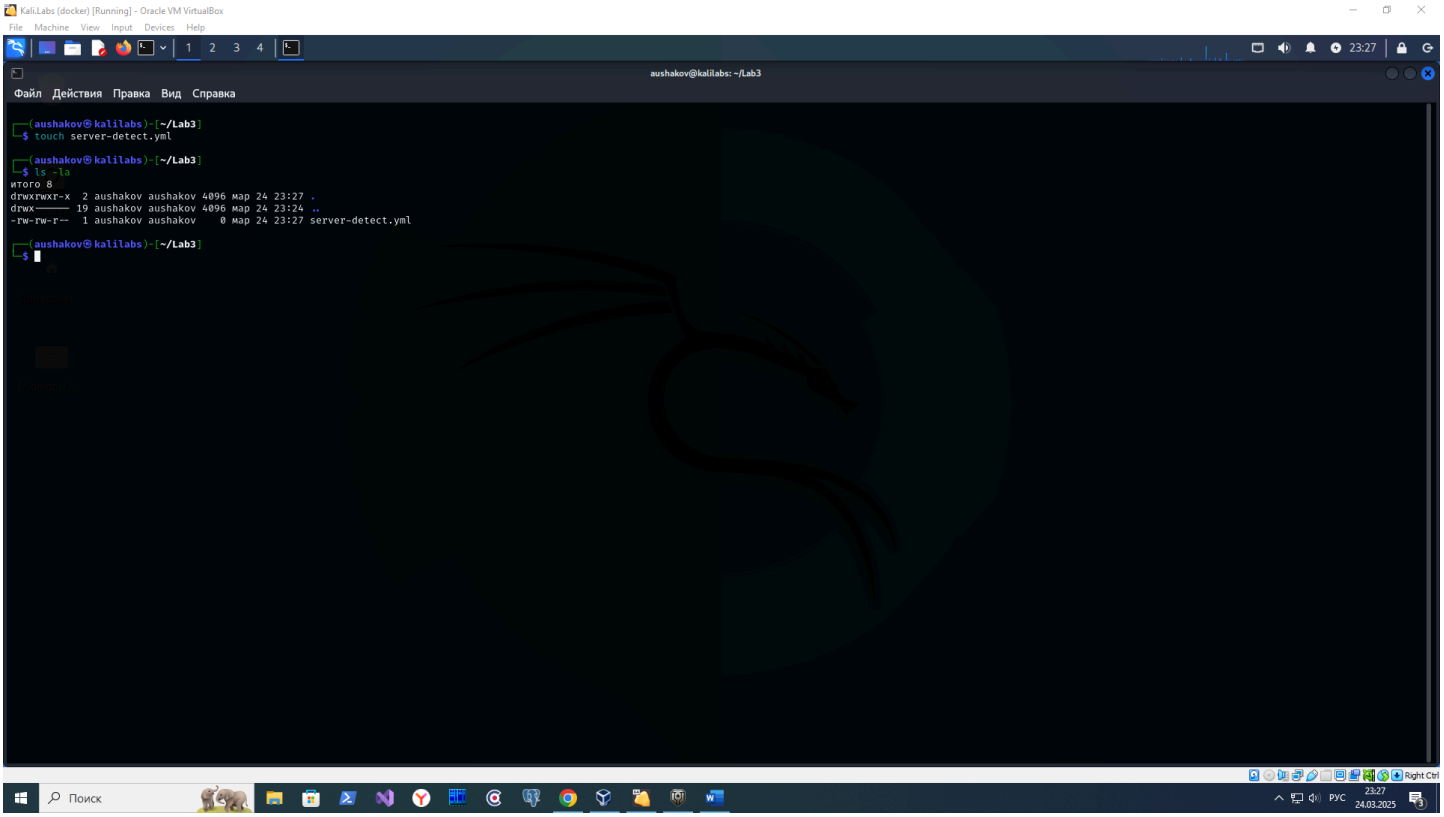
Проверяю версию Nuclei

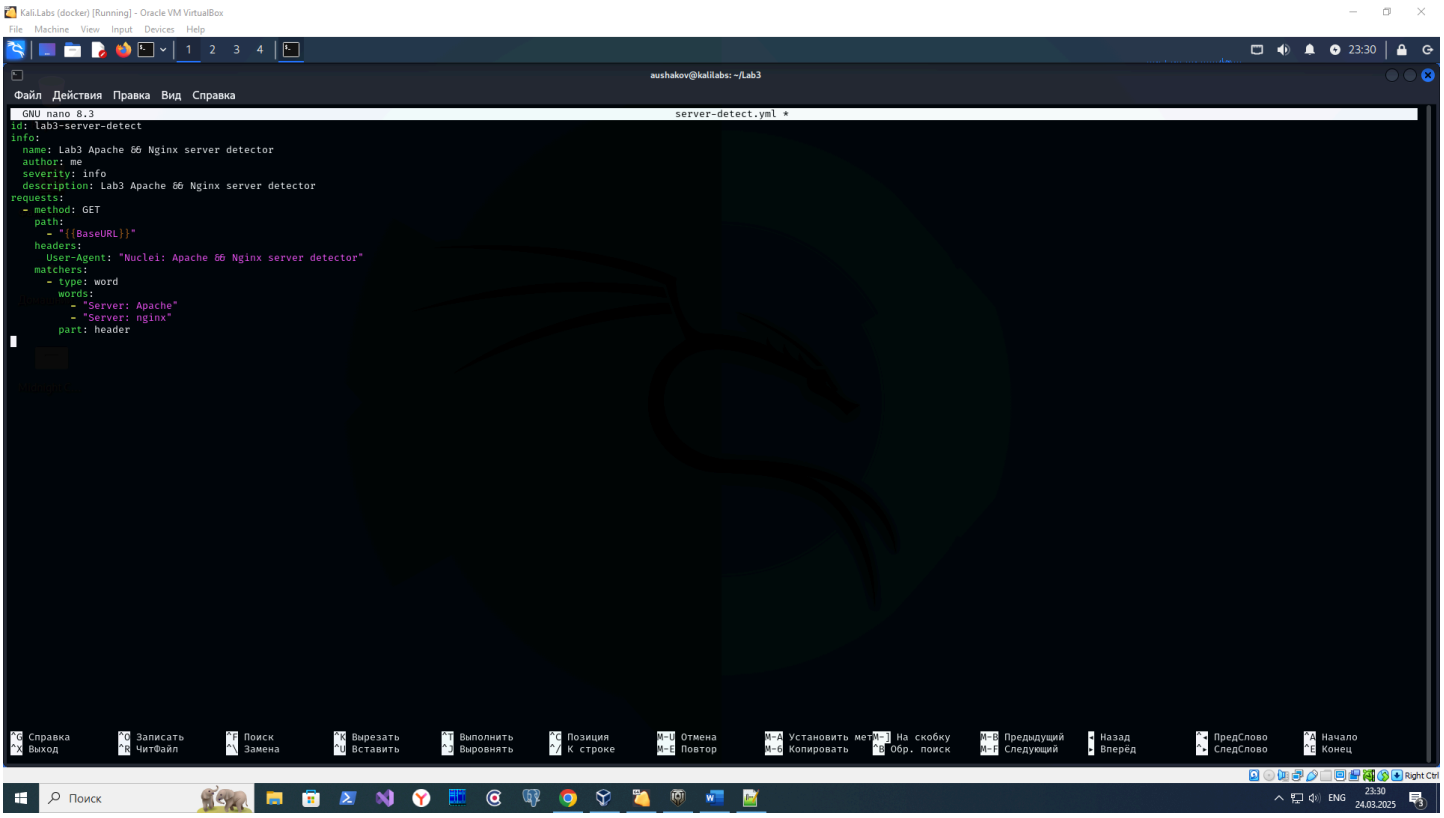


Создаю директорию для моих шаблонов Nuclei



Создаю файл для шаблона Nuclei для детектирования типа веб-сервера (сам шаблон приложен отдельным файлом)

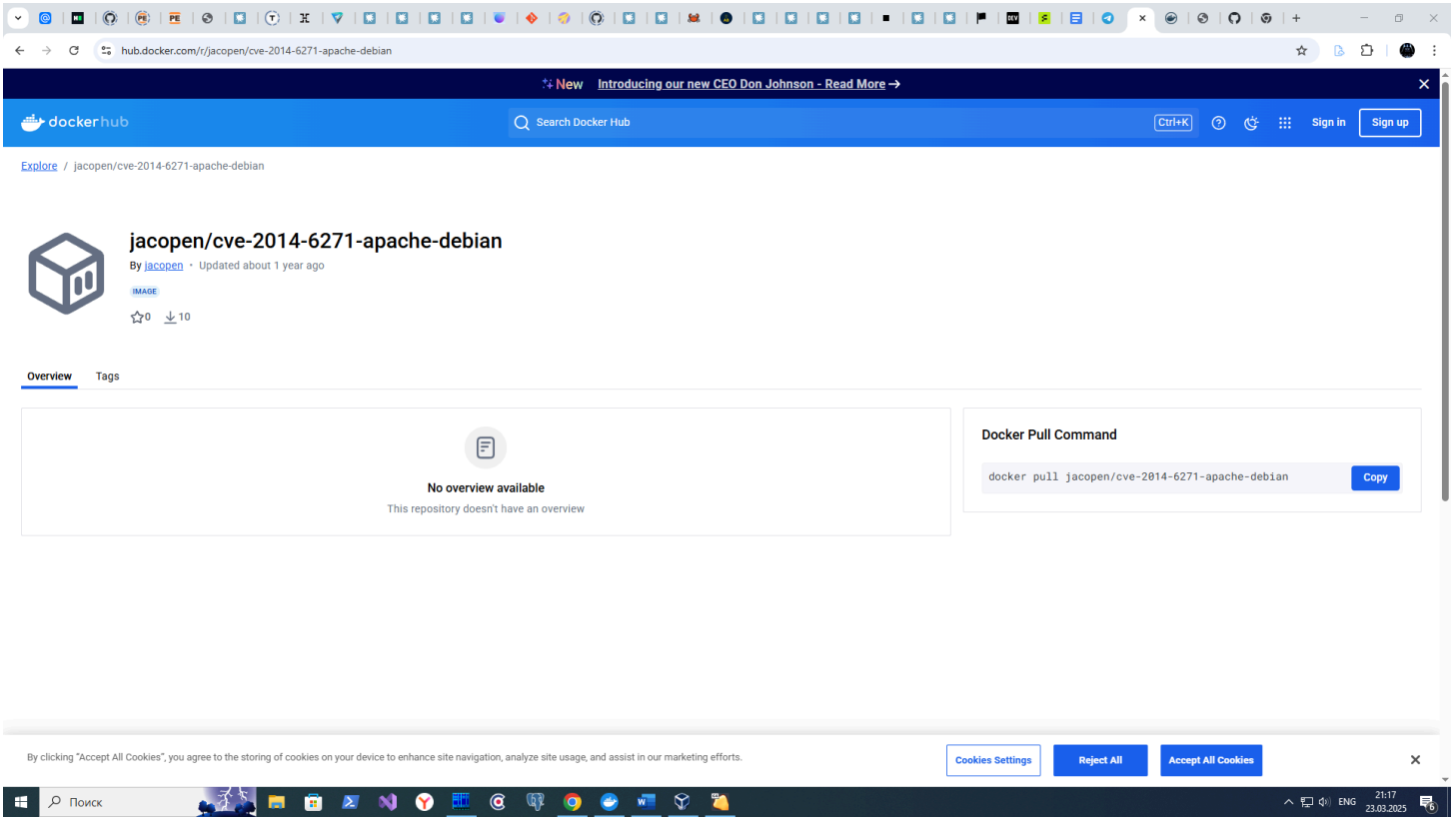




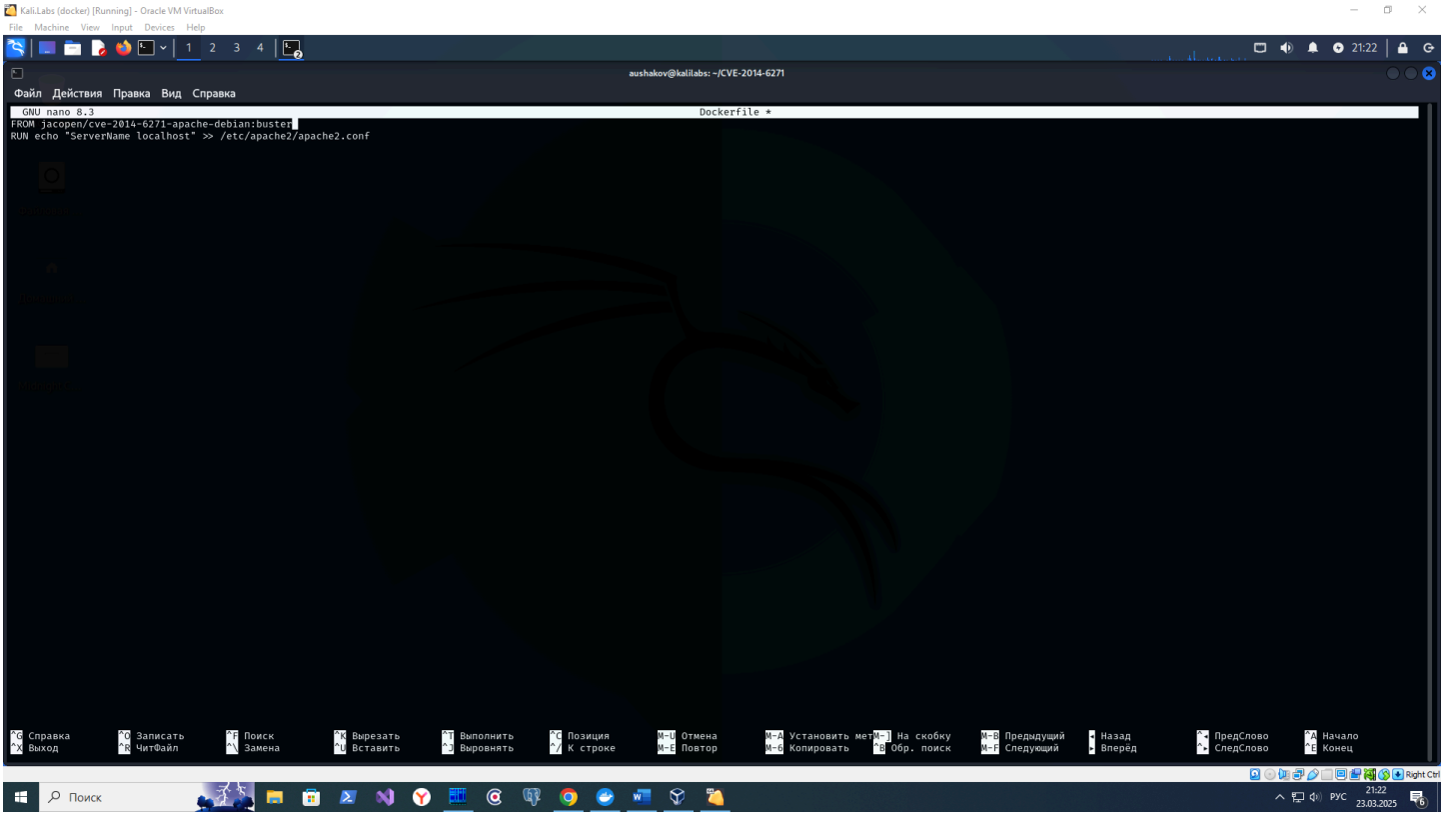
Описание шаблона:

Этот шаблон Nuclei предназначен для обнаружения веб-серверов Apache и Nginx, основываясь на заголовке Server в HTTP-ответе. Шаблон отправляет GET-запрос к целевому хосту и проверяет заголовок ответа. Если в заголовке Server присутствует строка Apache или nginx, то шаблон определяет, что соответствующий веб-сервер был найден.

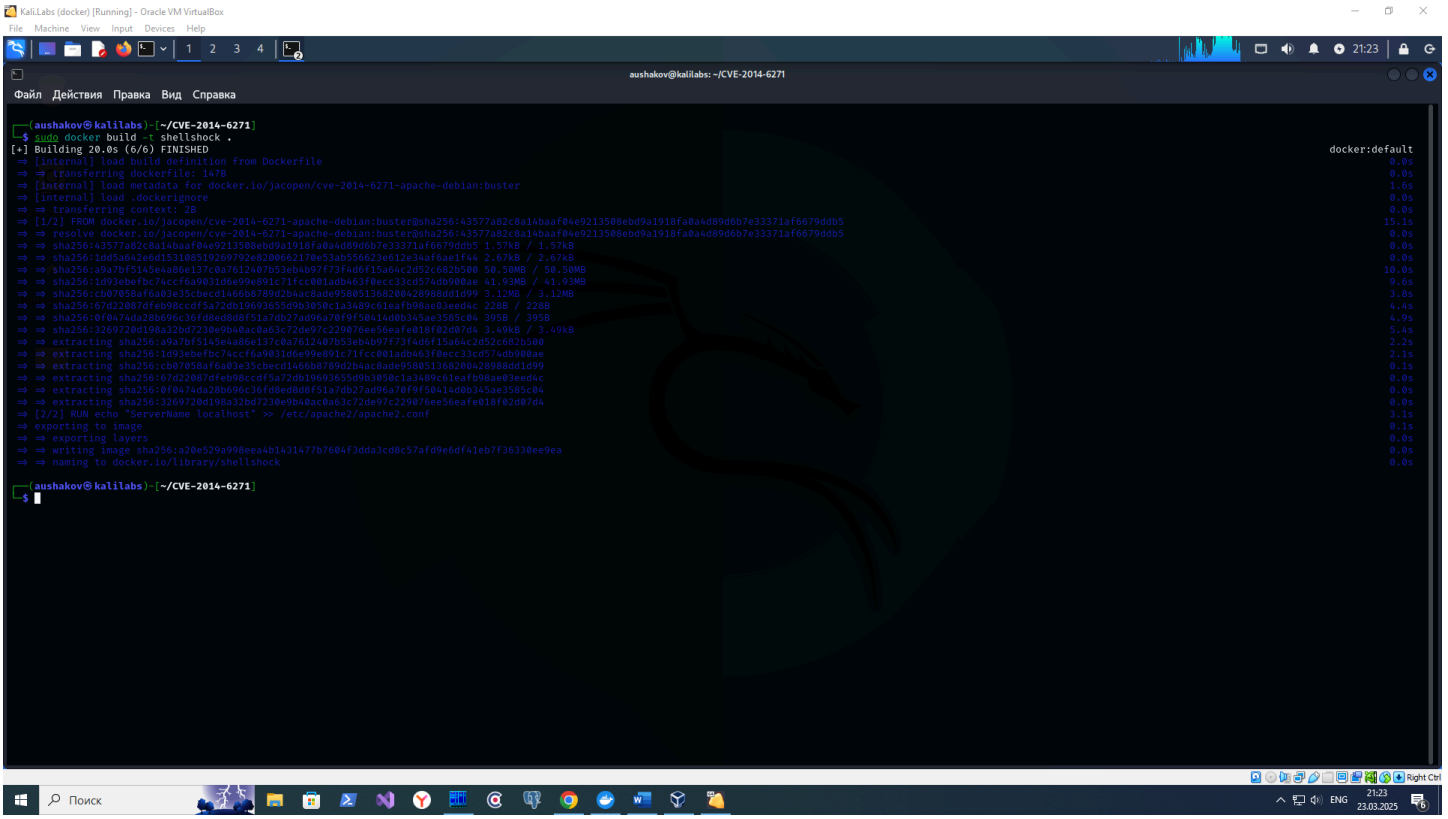
В качестве сервера, который я буду проверять с помощью моего шаблона Nuclei, я возьму образ jacopen/cve-2014-6271-apache-debian для создания docker контейнера, который я использовал в прошлых лабораторных (я знаю, что в нем используется Apache в качестве веб-сервера).



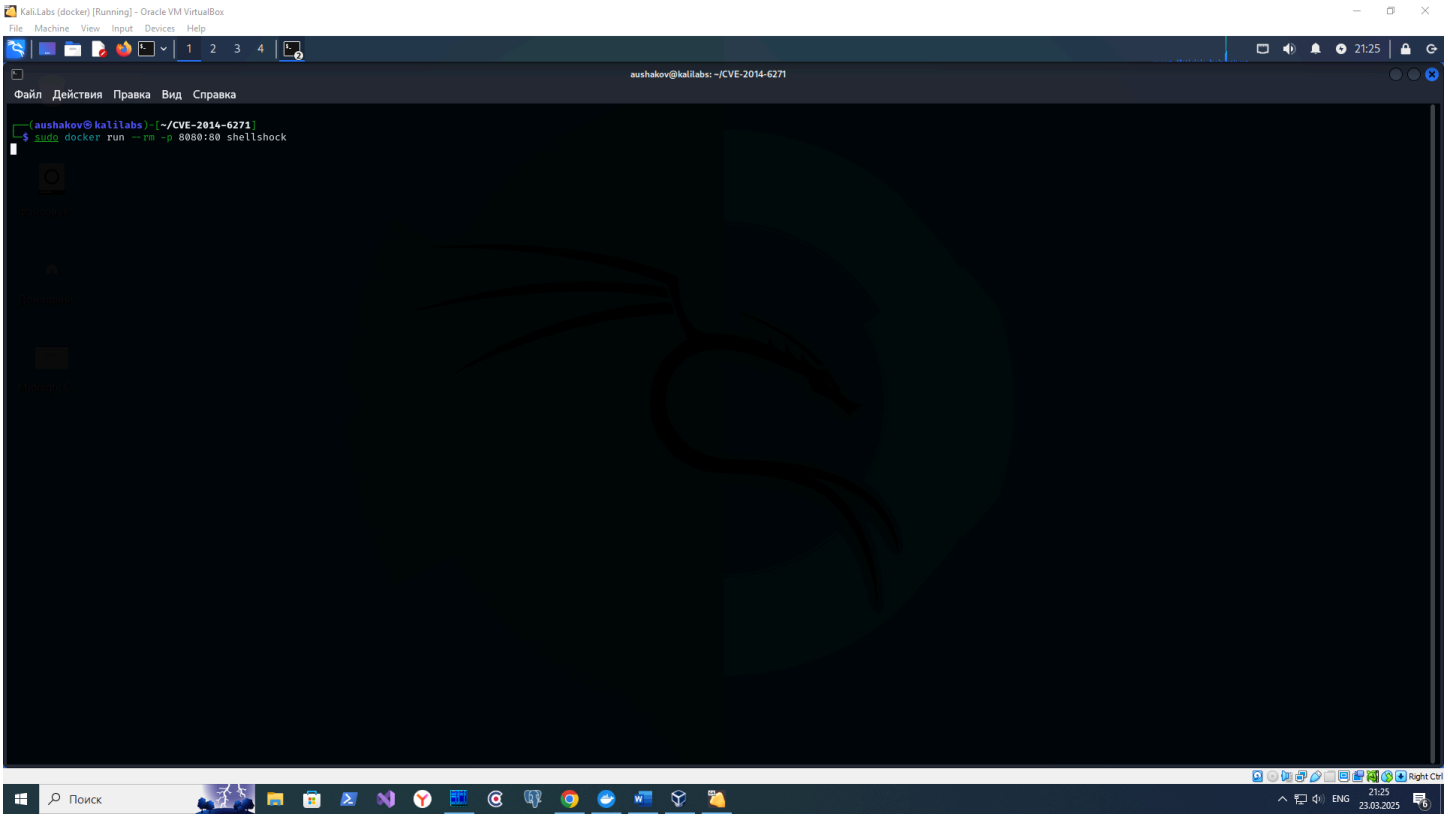
Создаю Dockerfile на основе образа jacopen/cve-2014-6271-apache-debian:

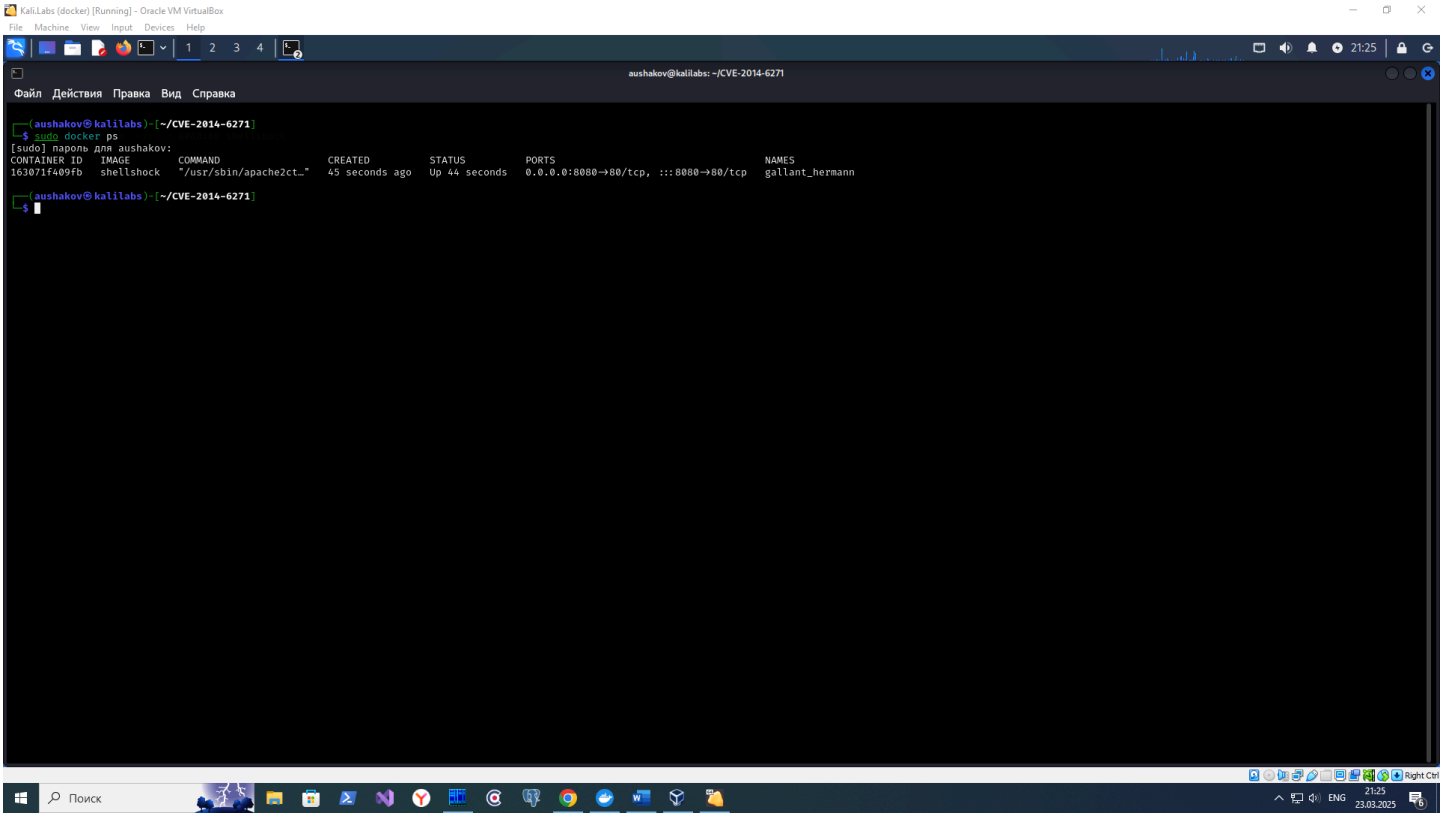


Запускаю сборку образа моего контейнера docker

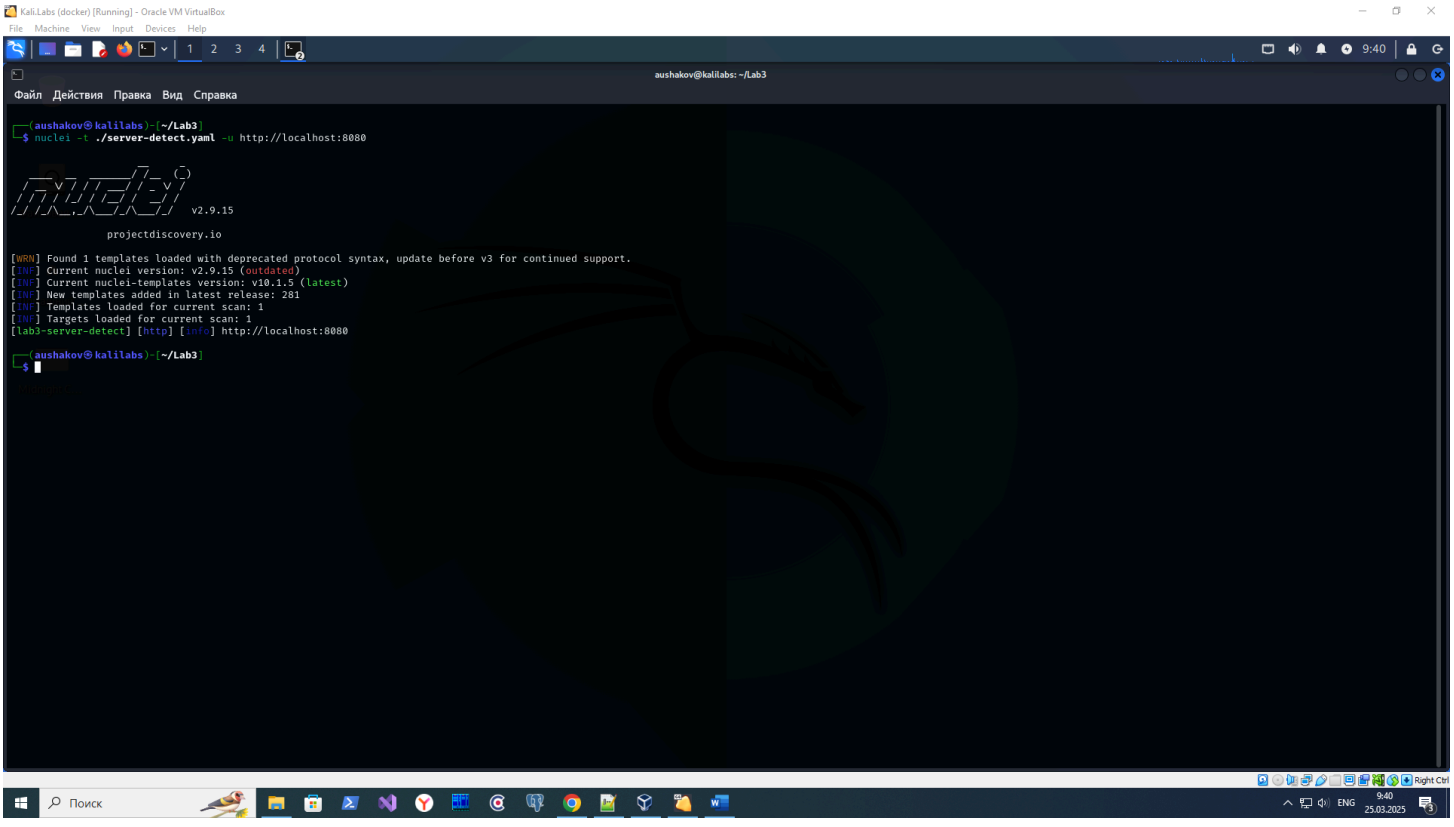


Запускаю созданный контейнер docker (с учетом необходимости проброса портов)





Запускаю выполнение Nuclei только на моем созданном шаблоне



Видно, что Nuclei определил, что на испытуемом веб-сервере используется Apache с помощью моего созданного шаблона. Это означает, что шаблон создан корректно.