МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ИКБ направление «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Практическая работа

по дисциплине

«Управление информационной безопасностью»

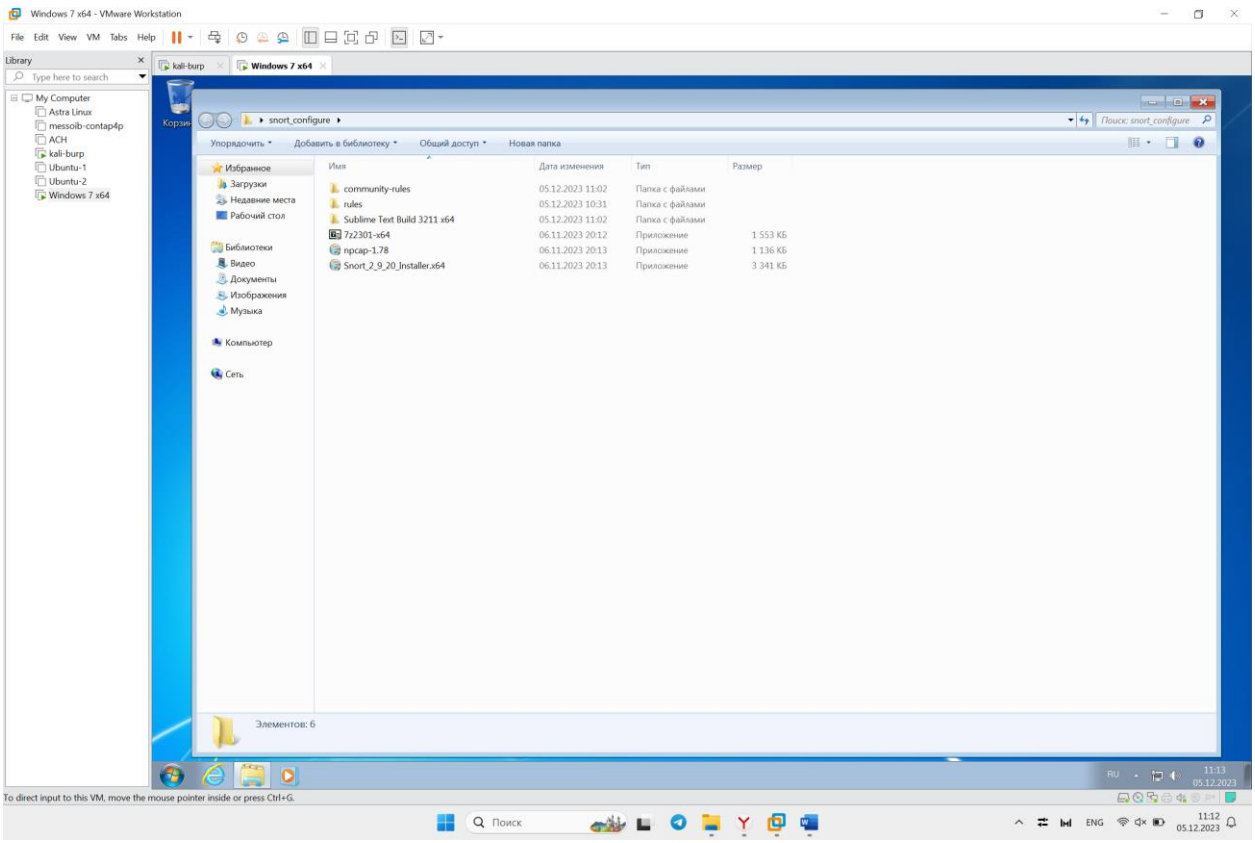
Группа:
ББМО-01-22
Выполнила:
Огольцова Н.Д.

Проверил:
Пимонов Р.В.

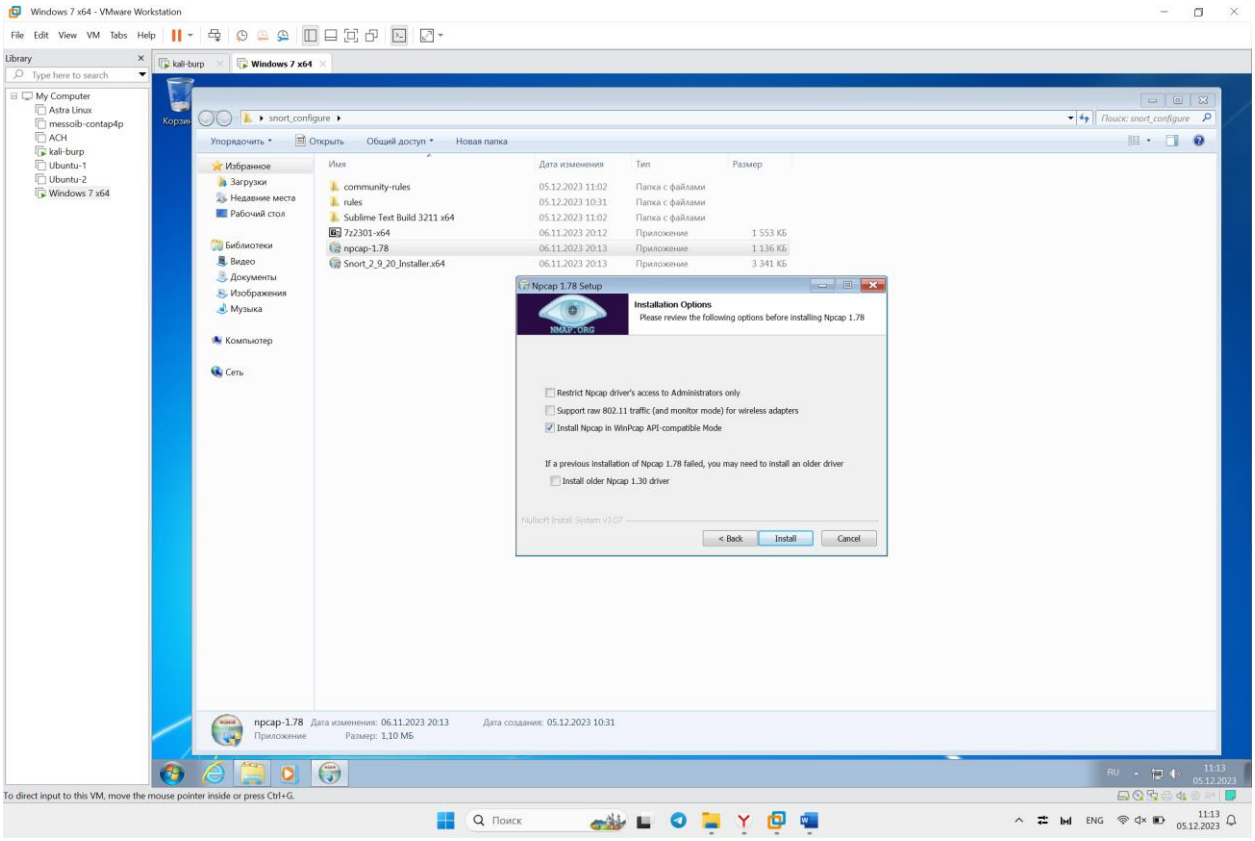
Москва 2023

Ход работы:

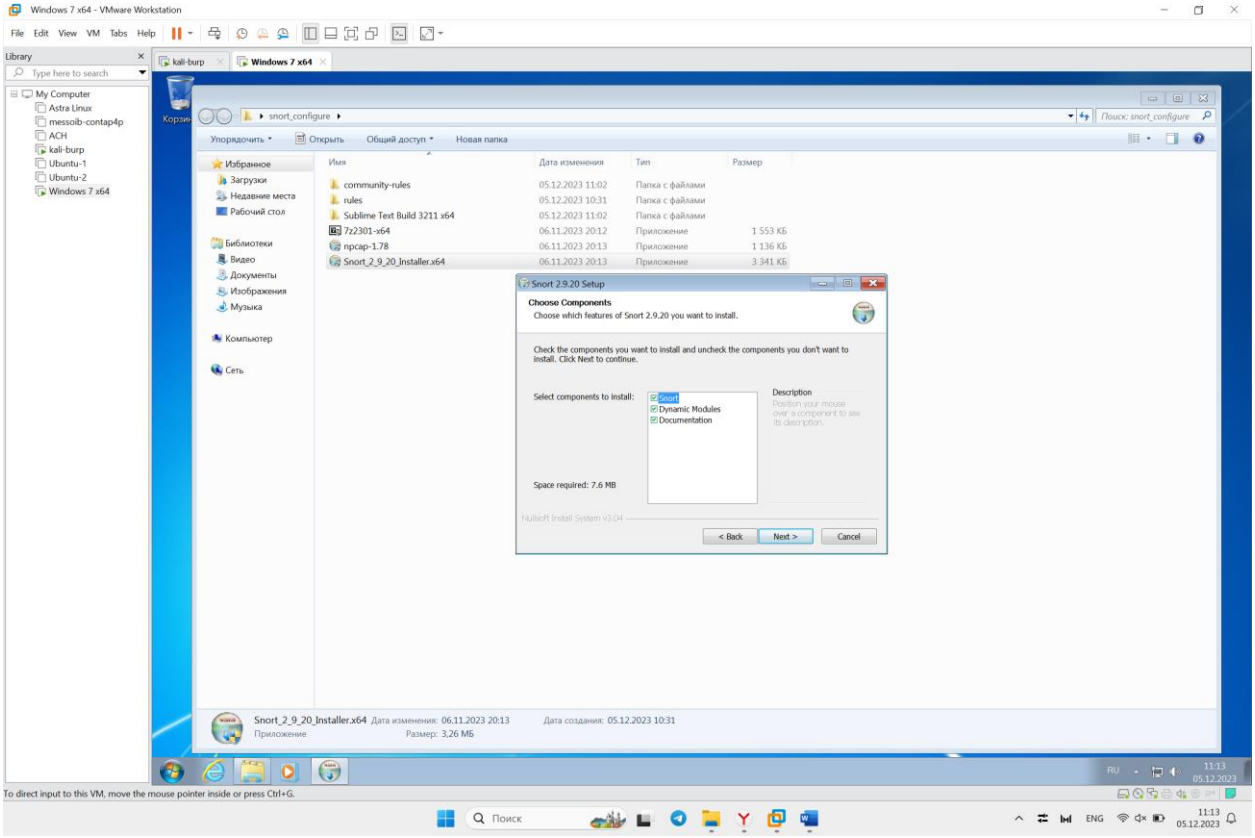
1. На виртуальную машину добавим папку с заданием.



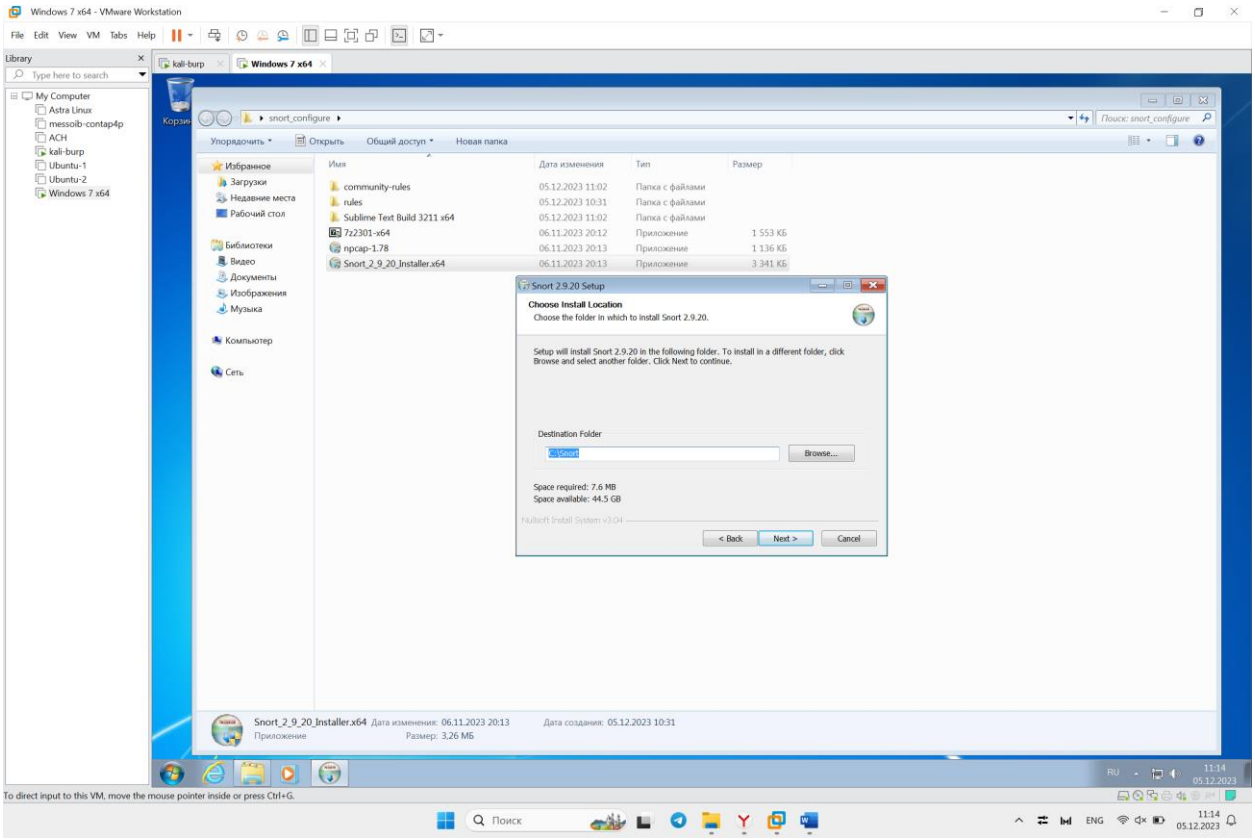
2. Выполним установку ncap.



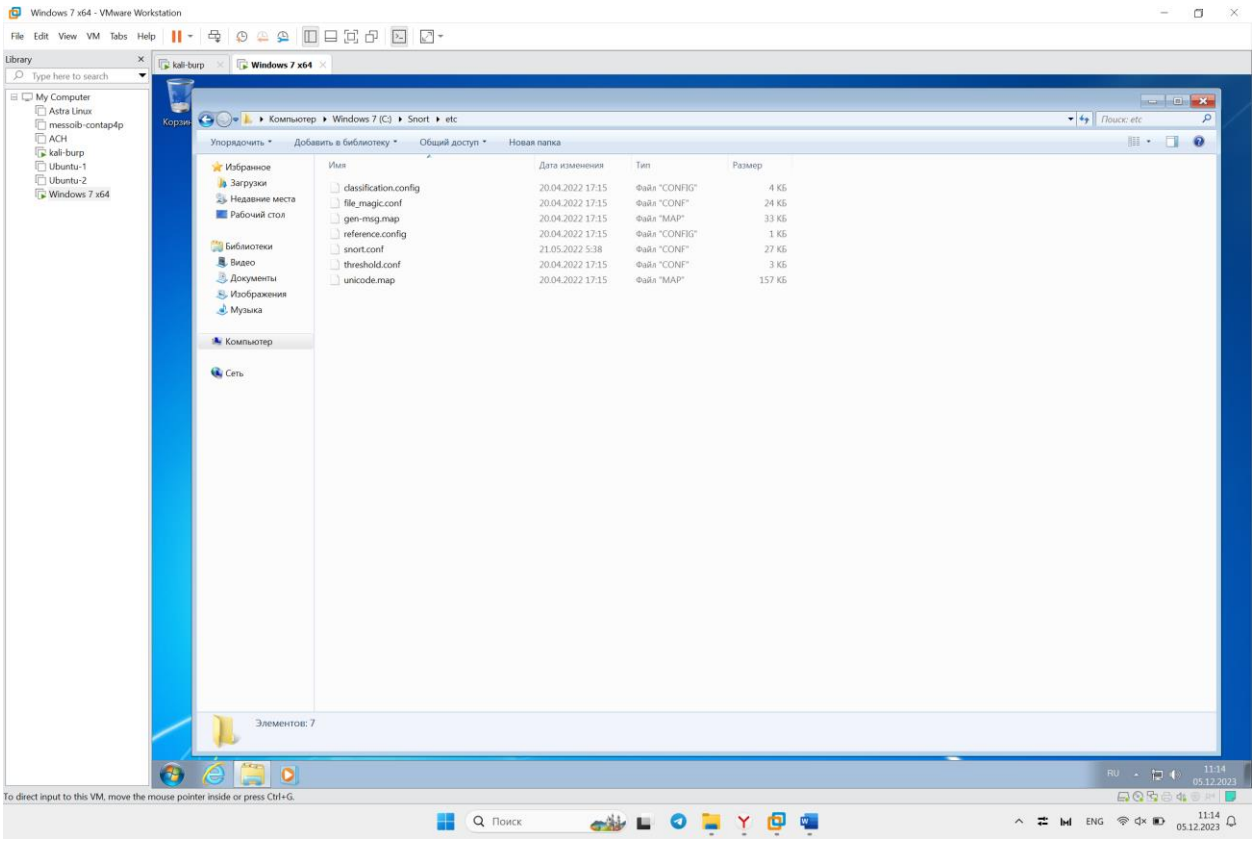
3. Выполним установку Snort.



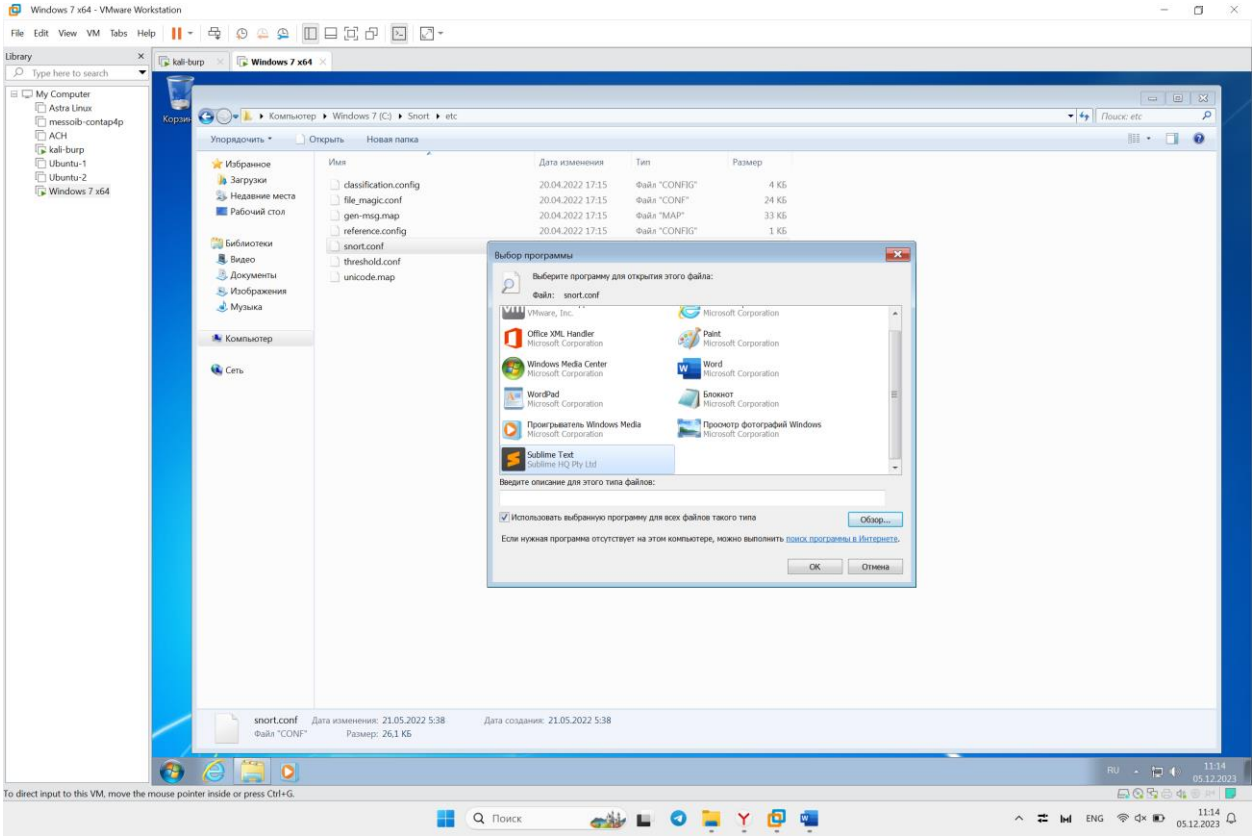
4. Выберем необходимую директорию для установки.



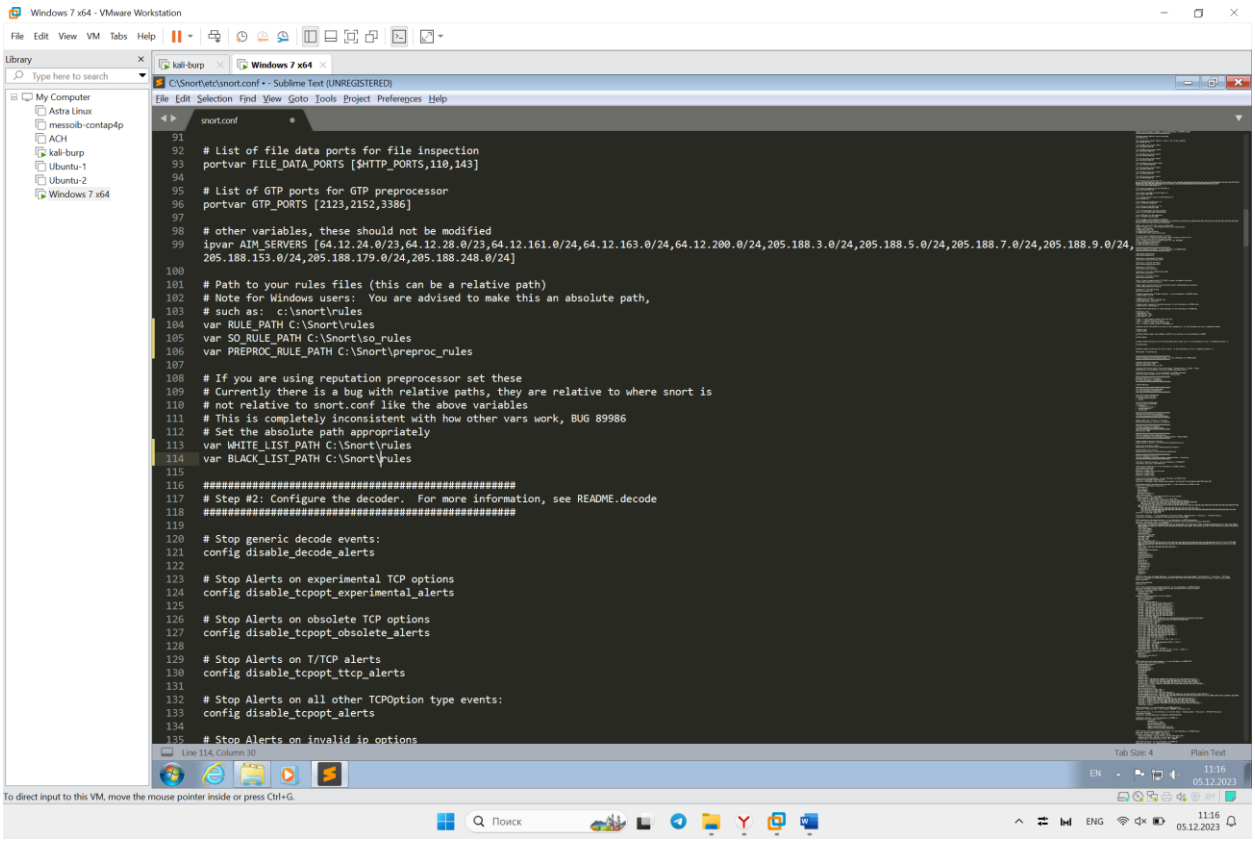
5. Откроем папку с конфигурационными файлами.



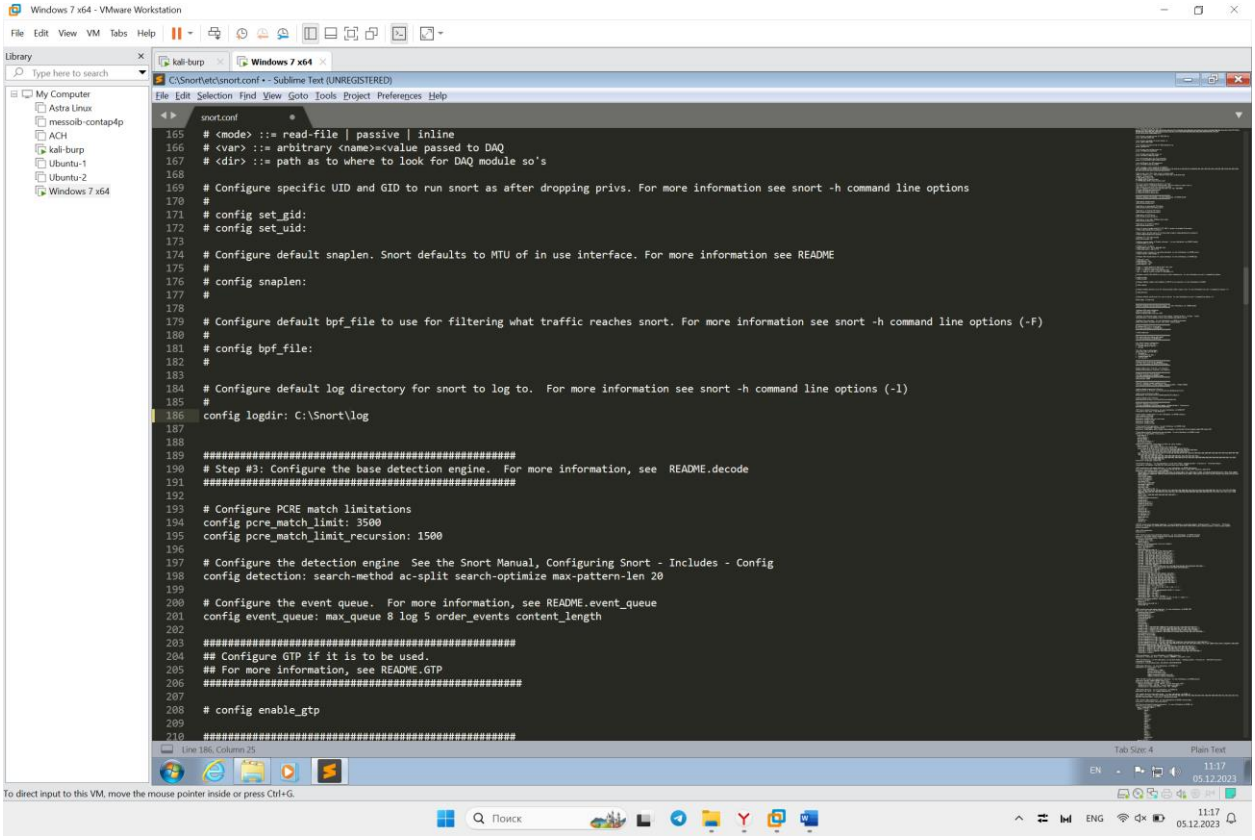
6. Выберем необходимое приложение для открытия файла конфигурации.



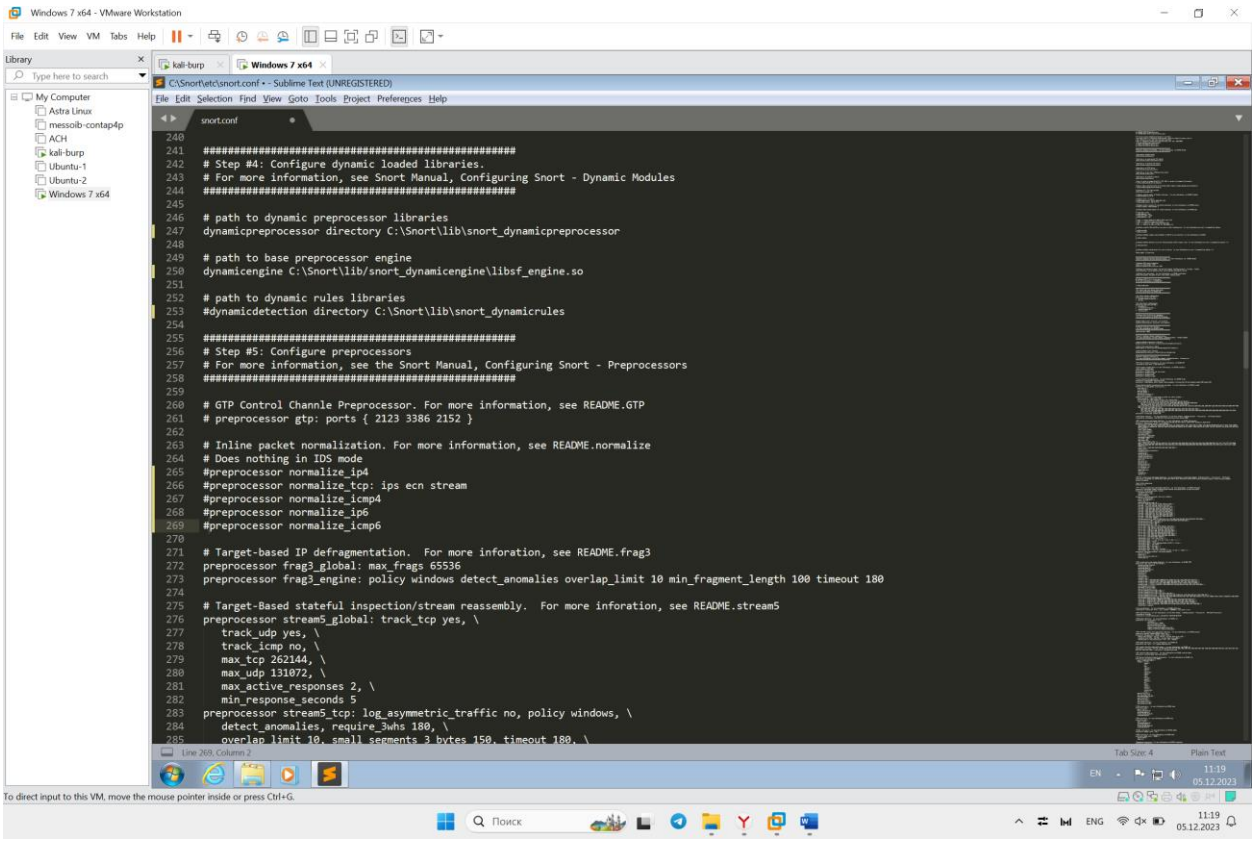
7. Постепенно исправляем файл.



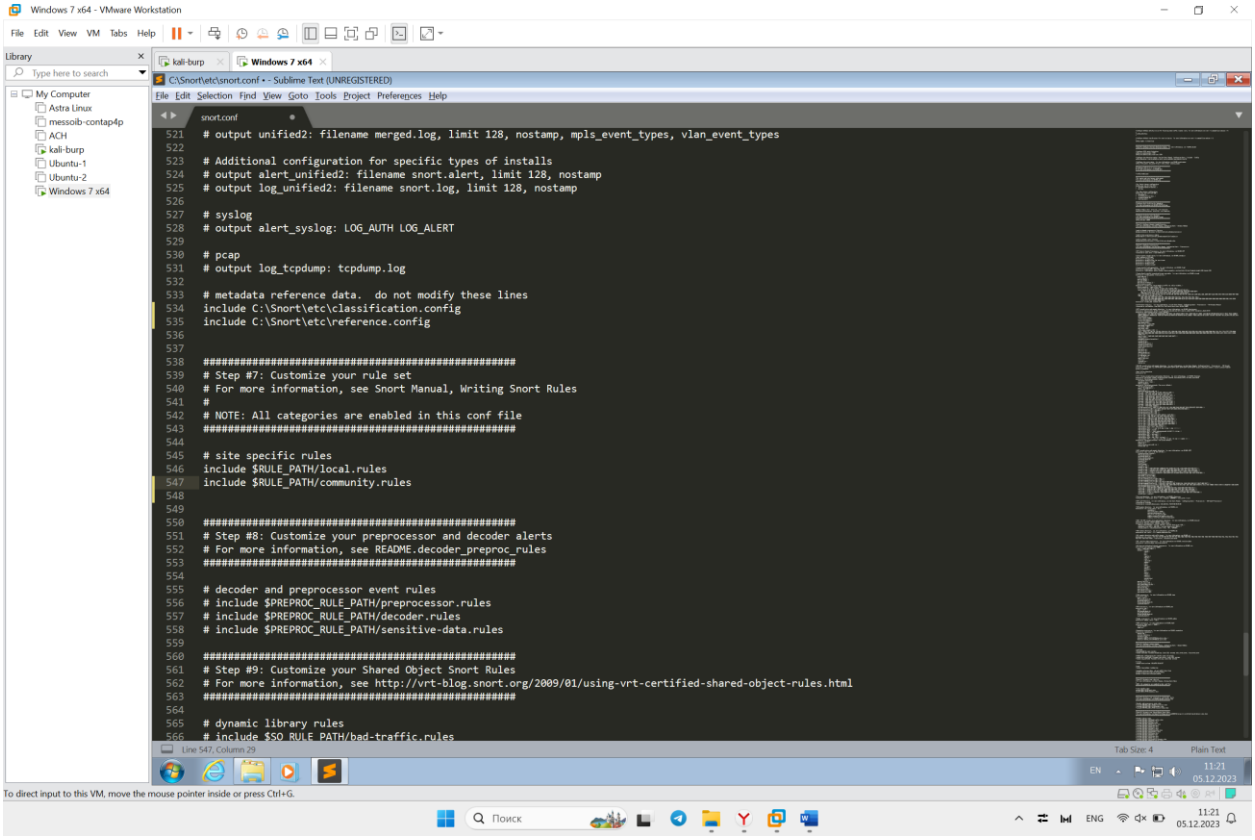
8. Добавляем пути лог файлов.



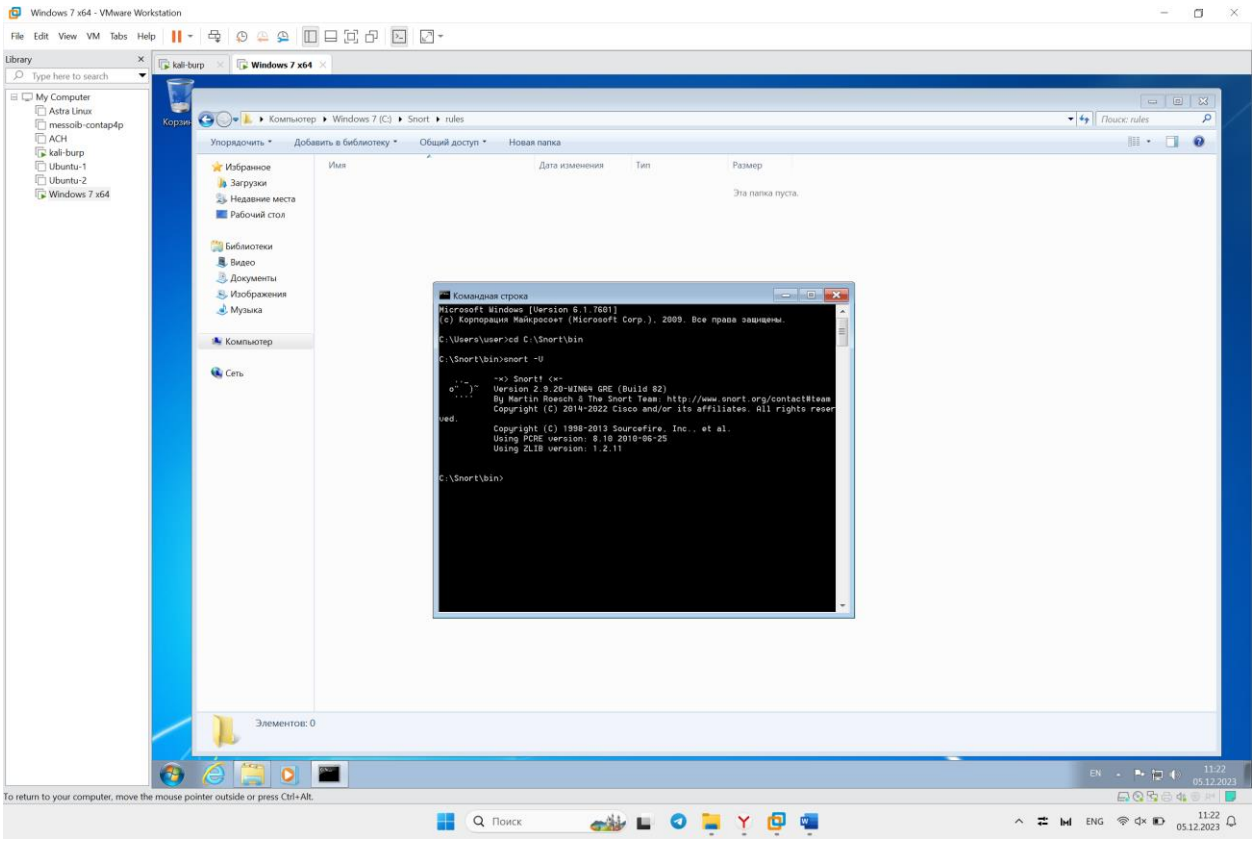
9. Комментируем необходимые строки.



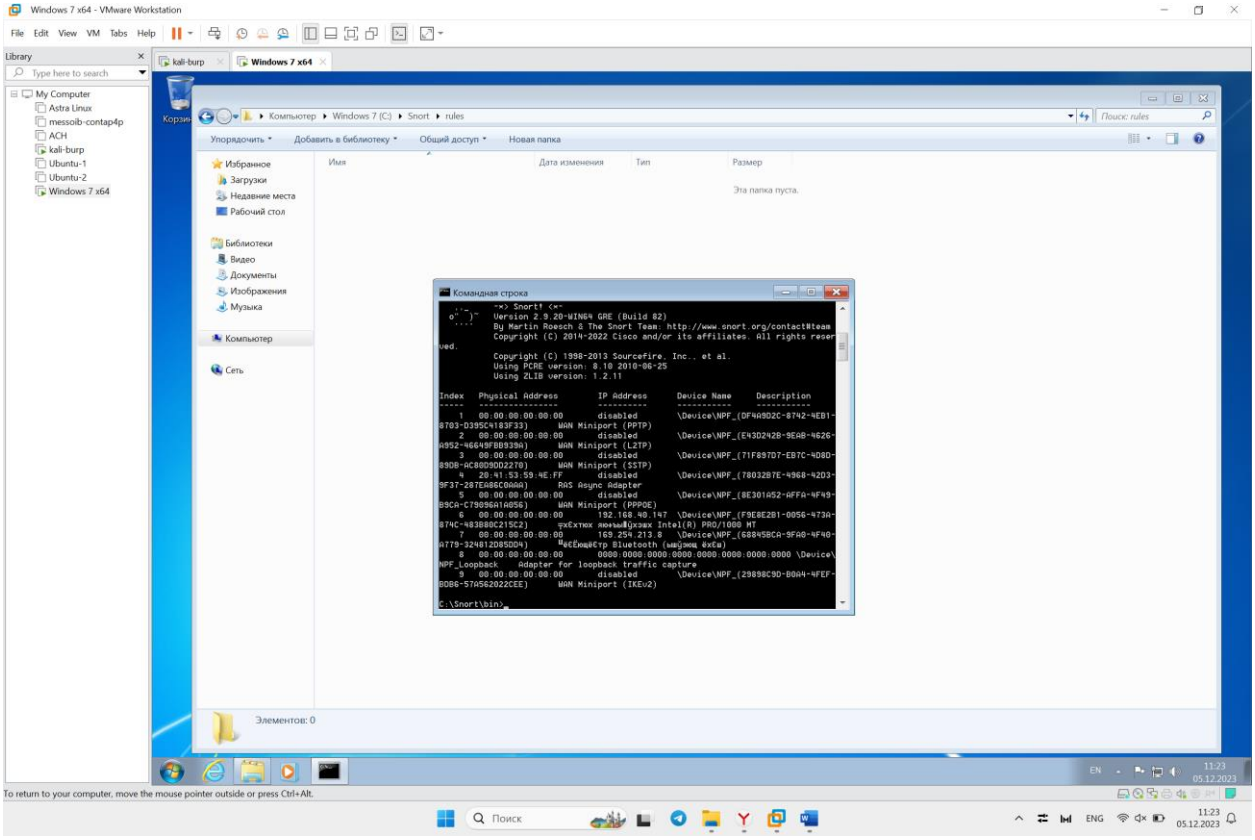
10.Добавляем строки с правилами.



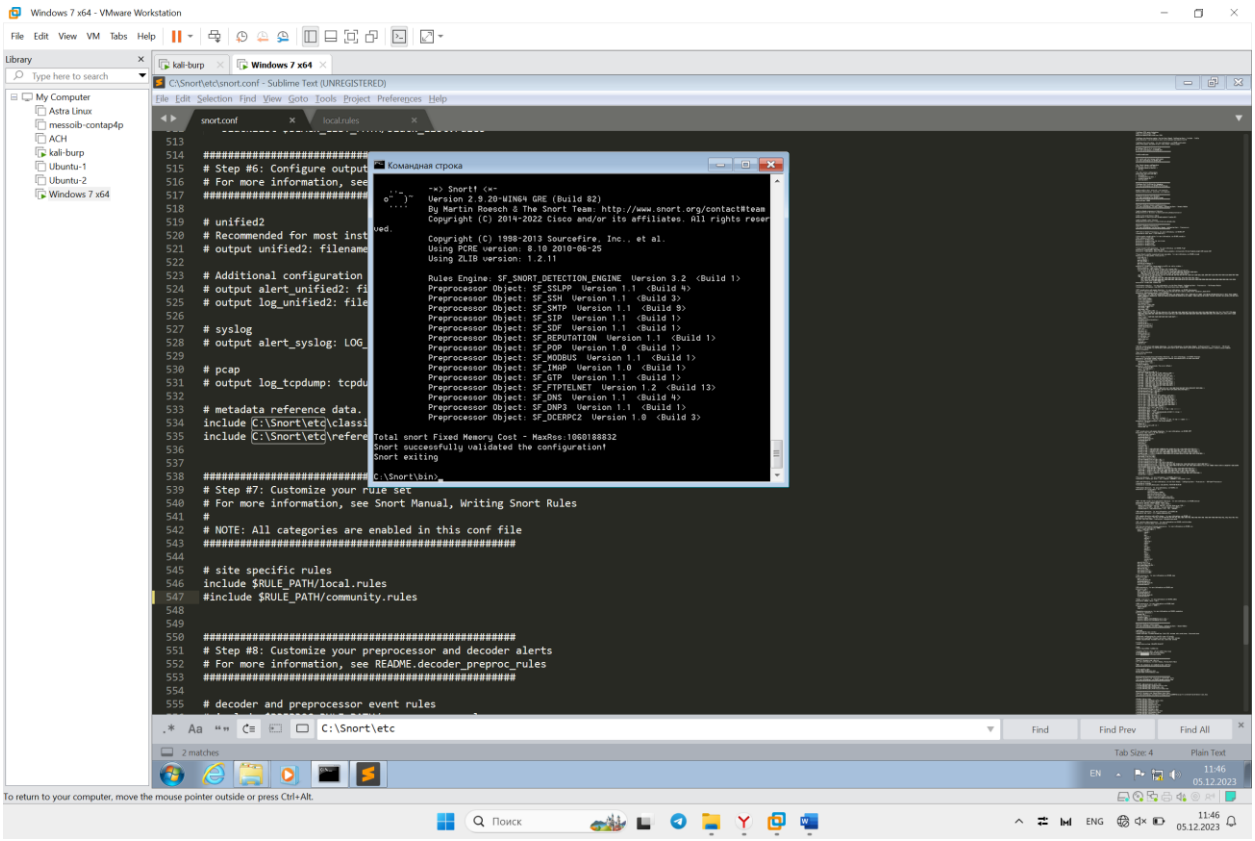
11.Запускаем snort, т.е. проверяем версию. Snort -V



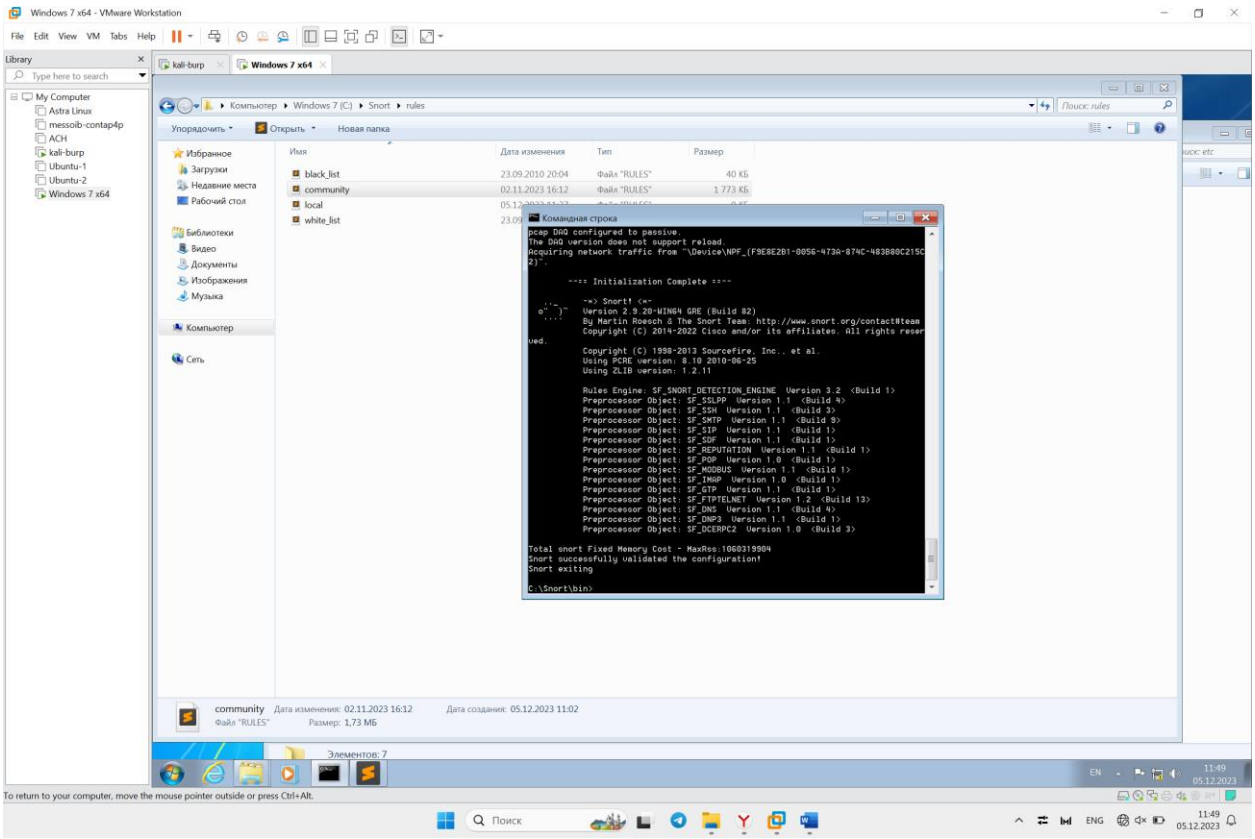
12.Проверяем работающий интерфейс – получаем шестой. Snort -W



13.Запускаем snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 6



14.Добавляем файл community.rules, меняем конфигурацию и запускаем тест заново.



15. Разработаем правило для варианта 9 (Номер по списку 18). Создать правило для Snort, которое срабатывает при обнаружении строки "hack" в DNS-запросе с выводом соответствующего сообщения.

alert tcp any any -> any any (msg: "TCP DNS request includes hack"; content: "hack"; sid: 10000004;)

alert udp any any -> any any (msg: "UDP DNS request includes hack"; content: "hack"; sid: 10000005;)

Описание введенной строки по частям:

alert: Это действие, которое предписывает системе генерировать

предупреждение при срабатывании данного правила.

tcp udp: Это протокол, к которому применяется правило, в данном случае.

any any: Эти части указывают исходный IP-адрес и порт отправителя. "any" – означает "любой", то есть правило применяется ко всем исходящим IP-адресам и портам.

->: Эта часть разделяет данные об исходе (source) и данных о назначении

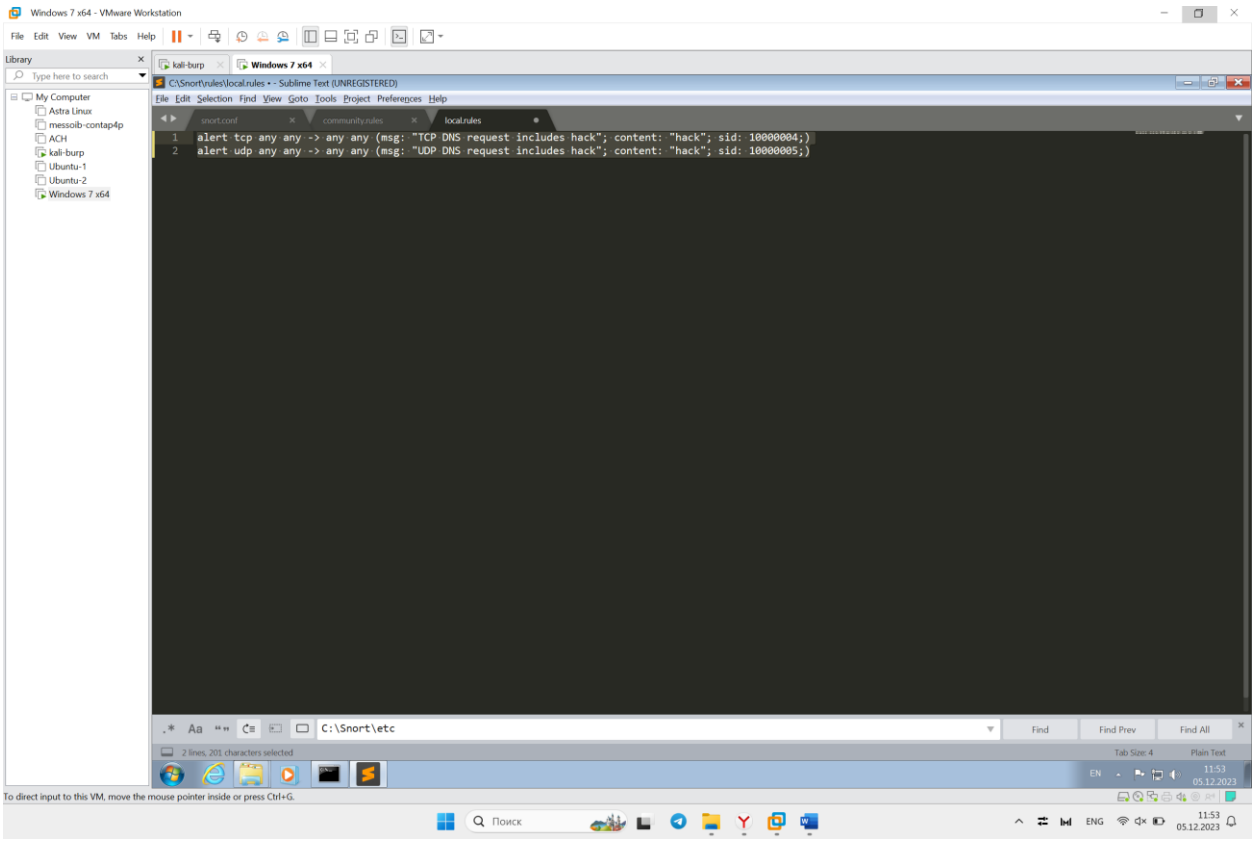
(destination).

msg: Надпись, которая будет появляется при срабатывании данного правила.

content: Позволяет устанавливать условие в правила, которые ищут определённое содержание (контент) в полезной нагрузке пакетов. В данном случае ищем любое упоминание hack.

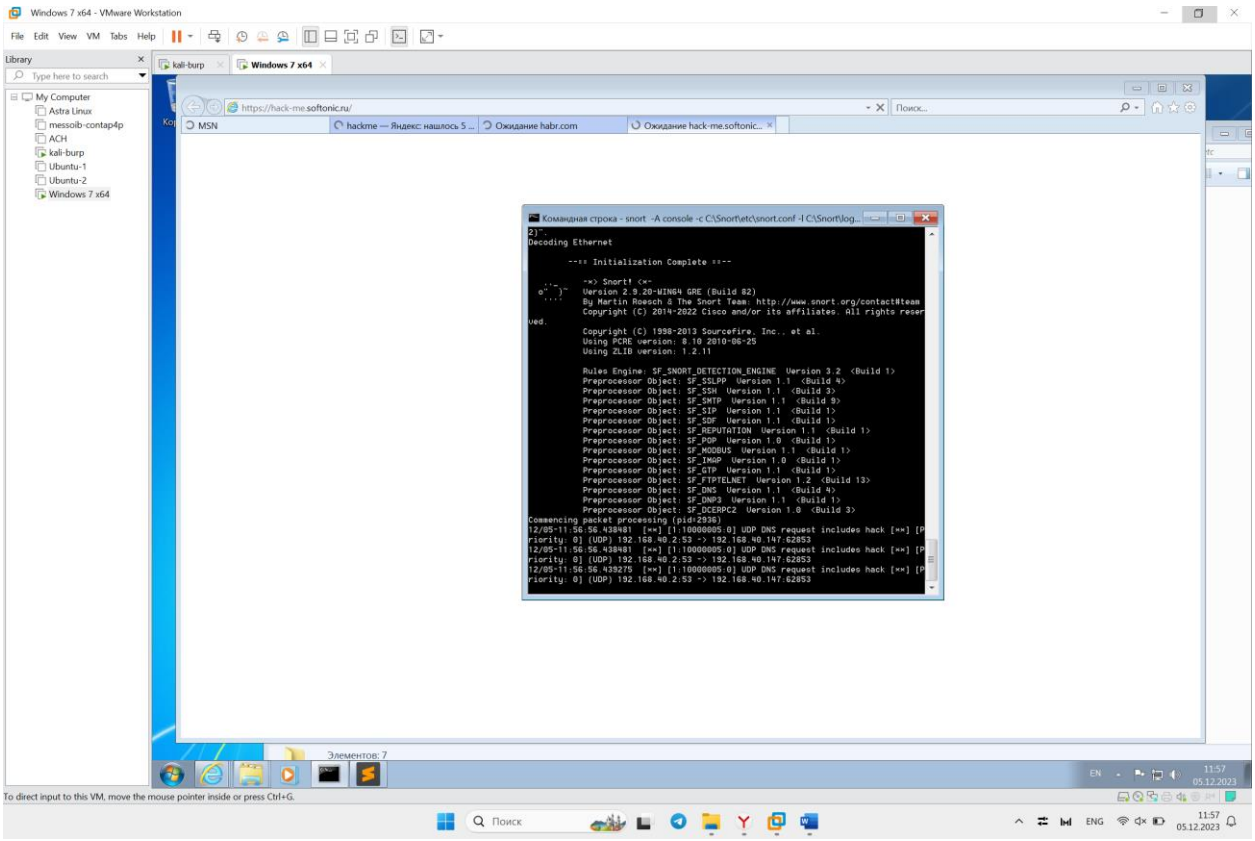
sid: Ключевое слово sid (Snort id или иногда упоминается как signature id) используется для уникальной идентификации правил Snort. По значению его аргумента можно легко идентифицировать правило.

16. Добавим данные правила в файл local.rules.



17. Запустим Snort в режиме IDS: snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 6

На скриншоте также видно, что в поисковике ищутся страницы с dns содержанием hack.



Программа смогла засечь данные запросы.