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

Институт комплексной безопасности и специального приборостроения

КБ-4 «Интеллектуальные системы информационной безопасности»

Отчёт

по практической работе

по дисциплине «Управление информационной безопасностью»

на тему: «2.2 Snort IDS»

Выполнил студент:

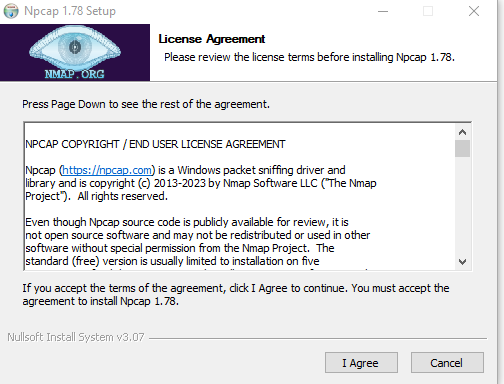
Группы: ББМО-02-22

Исаев А.М.

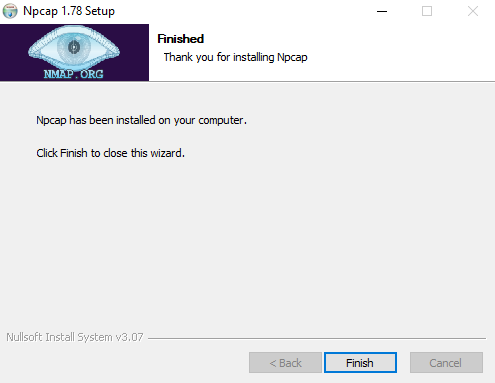
Проверил: Пимонов Р.В.

**Москва 2023**

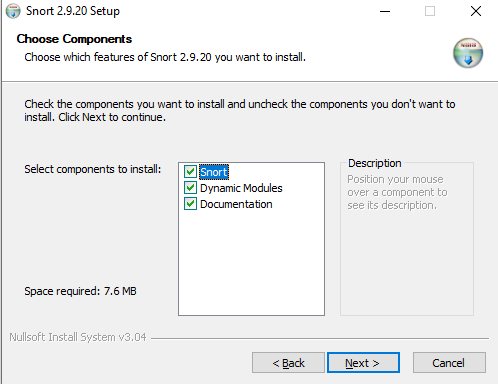
Для начала – установим npcap



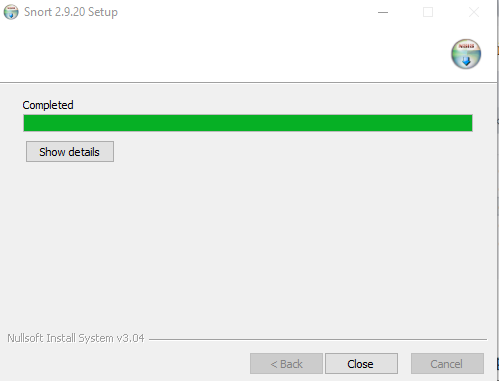
Все было успешно установлено!



Далее, установим сам Snort

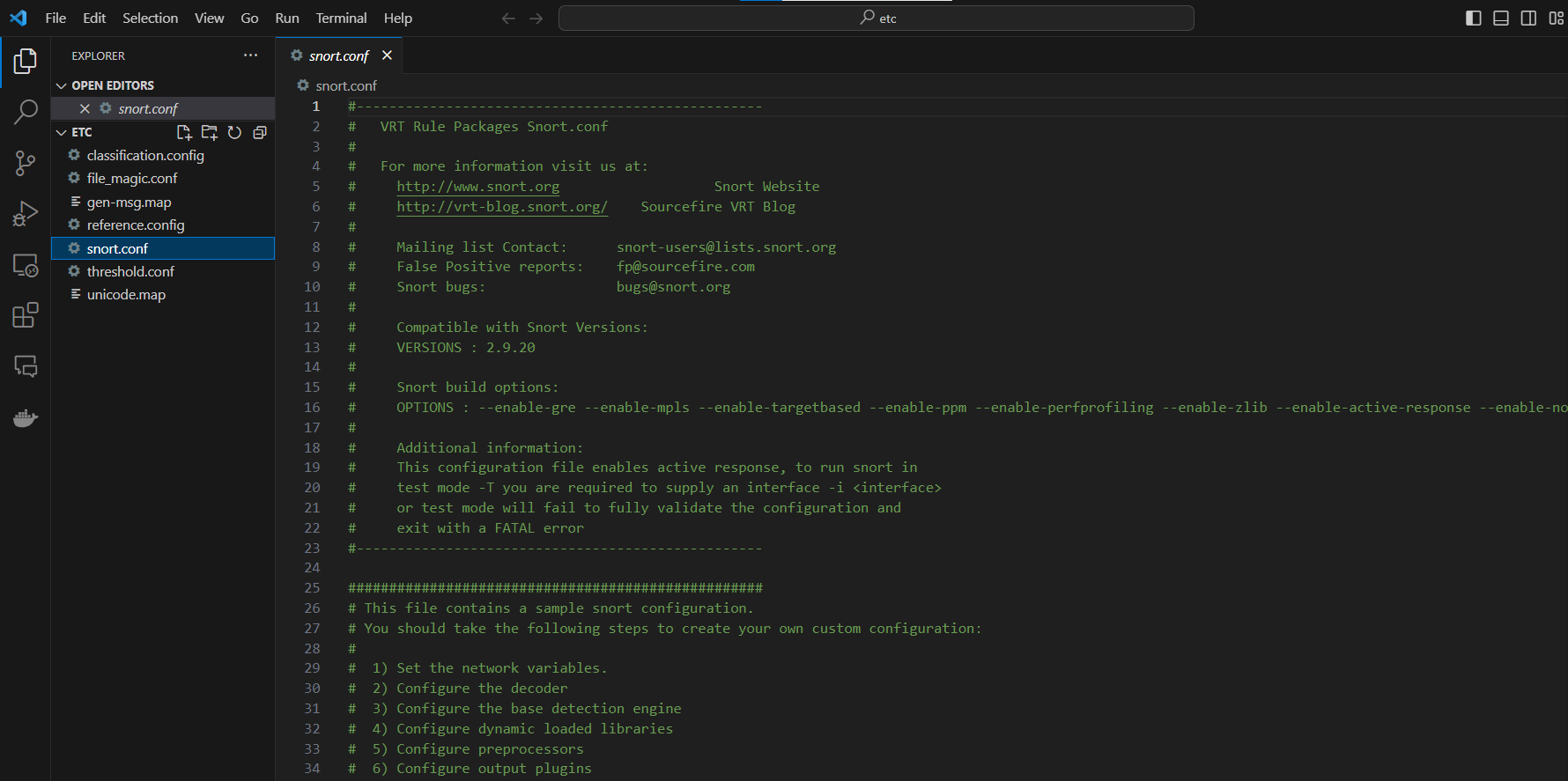


Все было успешно сделано.

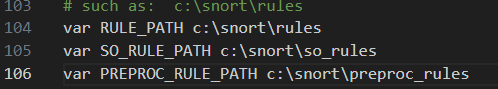


Далее, настроим конфигурационный файл для успешной и правильной работы Snort

Откроем snort.conf



Изменим 103-106 строки



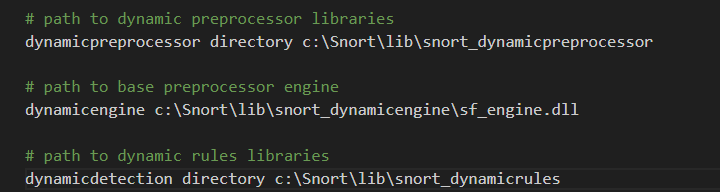
Изменим 113-114 строки



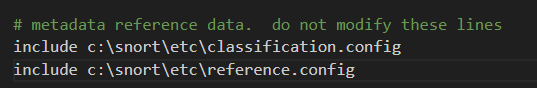
И 186 строку



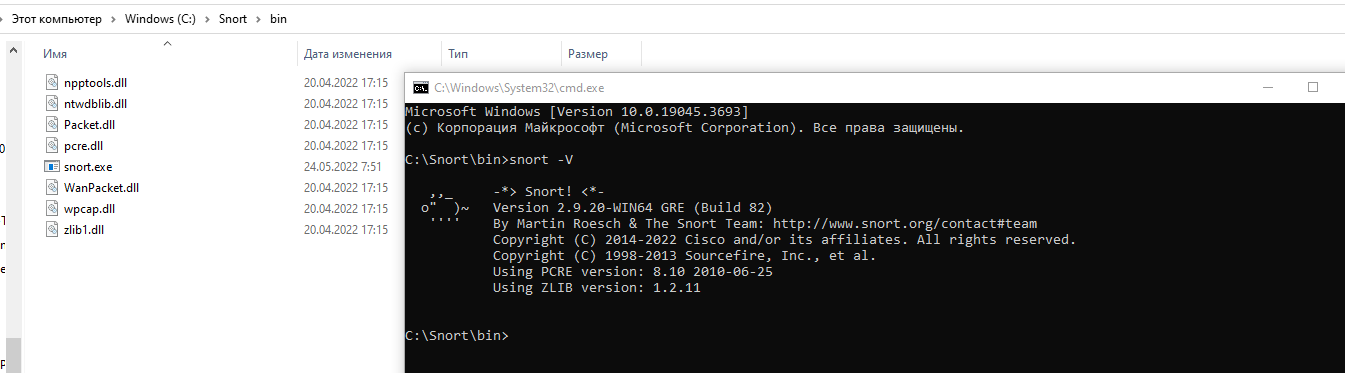
Укажем пути к библиотекам и движку

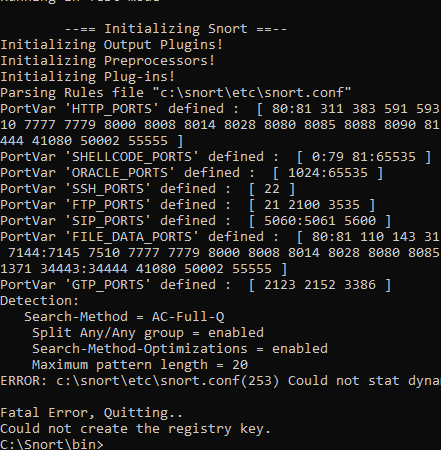


Укажем c:\snort для корректной работы



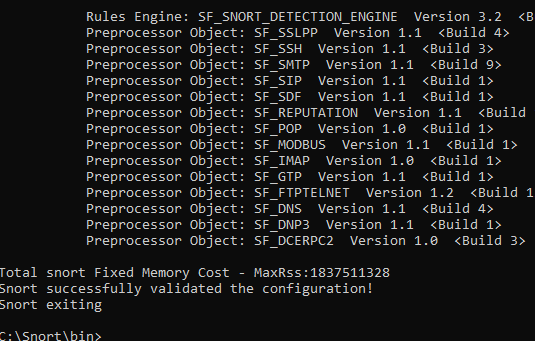
Необходимо добавить white\_list.rules и black\_list.rules



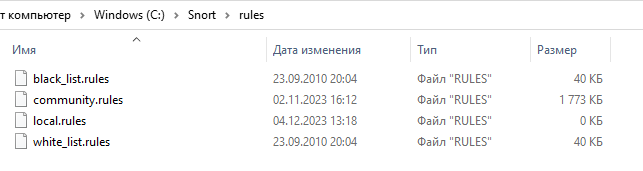


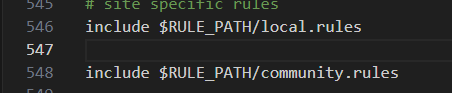
Введем команду, с помощью которой мы сможем протестировать конф.файл

**snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 4**



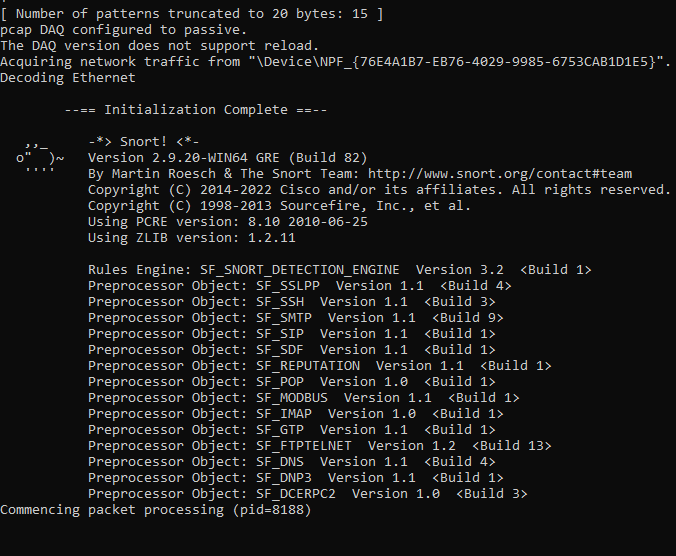
Все работает! Добавим community.rules и укажем путь на него



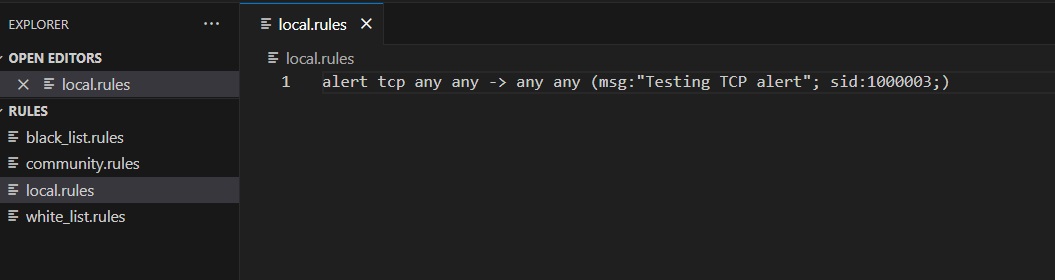


Запускаем Snort в режиме IDS, введя данную команду в командной строке: **snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 2**

Ключ -A показывает, что все предупреждения (alerts) будут дублироваться выводом на консоль. Snort проверил файл конфигурации и начал свою работу в режиме IDS:



Теперь самостоятельно попробуем написать правило для IDS Snort. Открываем файл в текстовом редакторе и вводим строку, как показано на рисунке ниже.



alert: Это действие, которое предписывает системе генерировать предупреждение при срабатывании данного правила.

tcp: Это протокол, к которому применяется правило, в данном случае, это TCP (Transmission Control Protocol), один из основных протоколов передачи данных интернета.

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).

any any: Эти части указывают на IP-адрес и порт назначения.

Аналогично "any" означает "любой", применение правила ко всем IP-адресам и портам назначения.

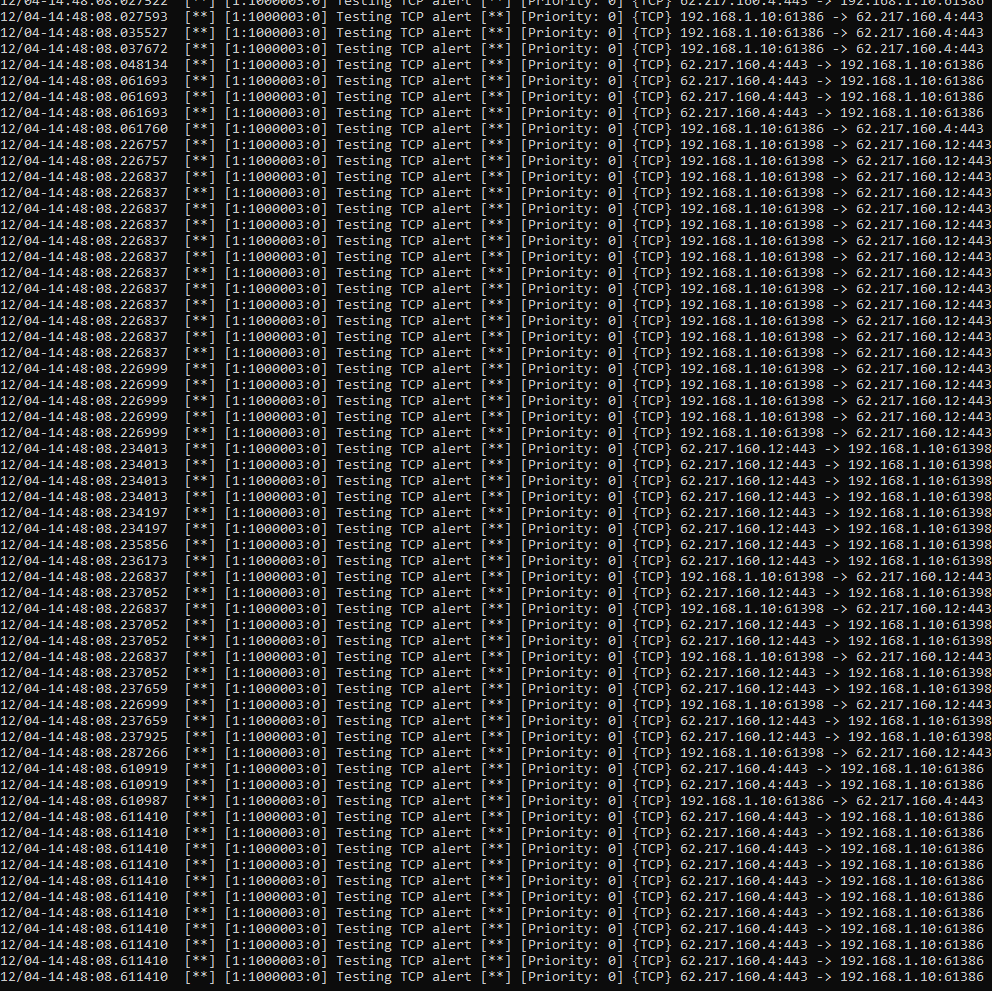
(msg:"Testing TCP alert"; sid:1000003;): Это дополнительная информация к правилу. msg указывает на сообщение или описание правила, в данном случае, это "Testing TCP alert".

sid (идентификатор сигнала) представляет собой уникальный числовой идентификатор этого правила в рамках системы IDS/IPS.

Введенное правило в файле local.rules означает следующее: "Генерировать предупреждение при обнаружении любых TCP пакетов от любого источника к любому назначению, с сообщением 'Testing TCP alert' и идентификатором сигнала 1000003".

Введем команду и убедимся что алерты работают.

**snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 2**

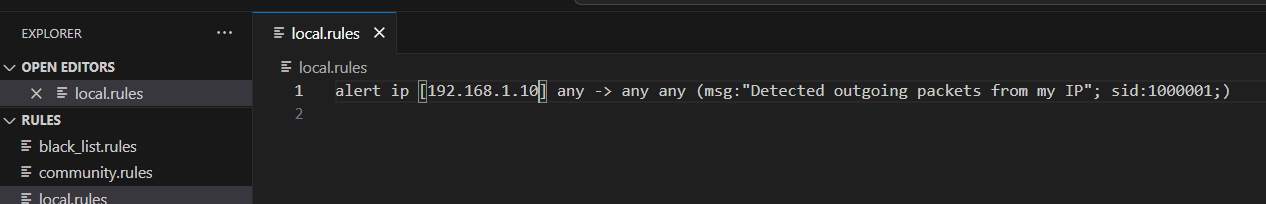


Вопрос 2. Разработка правил для IDS Snort 1. Определить номер выполняемого задания по формуле: N = n mod m + 1, где N – номер задания; m – количество заданий; n – номер строки с Фамилией в файле: https://docs.google.com/spreadsheets/d/1S\_t5WzsKG52ednX4scHOn8WHz k7823kHENAm9C2ssnw/edit#gid=0

N = 9 + 1 = 10. – 10 номер задания

10. Создать правило для Snort, которое срабатывает при обнаружении всех исходящих ip-пакетов с Вашим ip-адресом с выводом соответствующего сообщения.

Создадим правило по аналогии: но вместо tcp укажем собственный ip-адрес



Убедимся что все работает.

