ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №3

Настройка антивируса и СОВ

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С., Мазеин Д.С.

_____

(Ф.И.О., № группы) *(подпись)*

Проверил:

Казанцев А.А. _____

(*уч. степень, уч. звание, Ф.И.О.)* *(подпись)*

Санкт-Петербург

2021

Пункт 1

В данном пункте мы ознакомились с параметрами настройки групповых политик антивируса на уровне сервера безопасности.

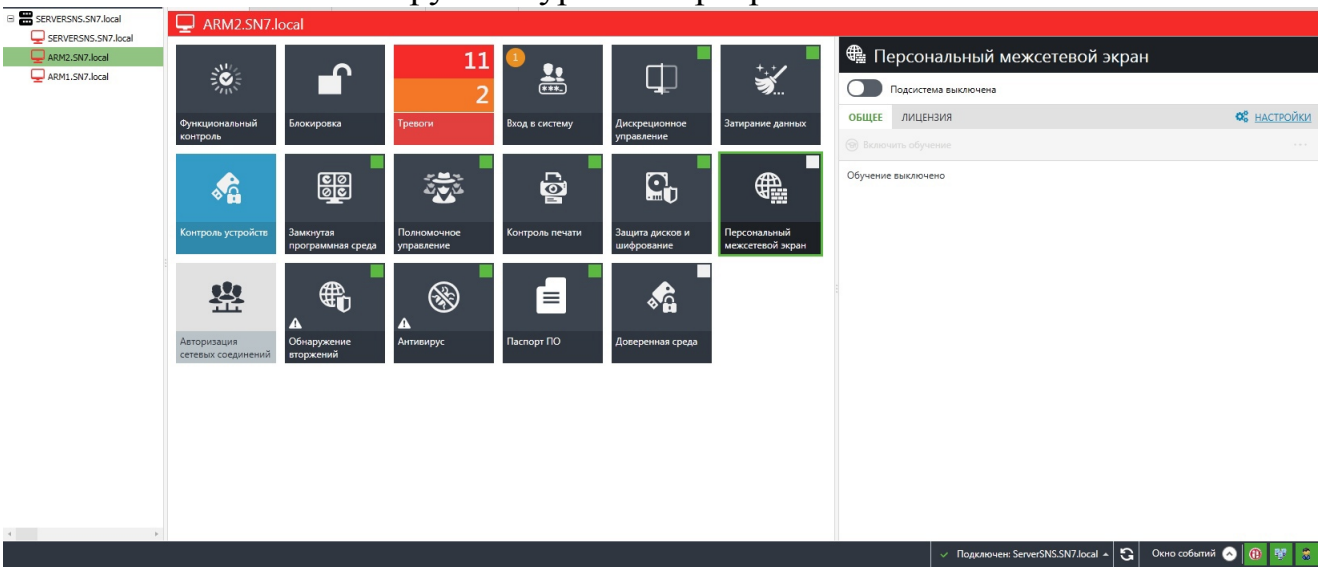


Рис 1. Персональный межсетевой экран.

Пункт 3

В данном пункте мы настроили политики СОВ на клиенте SNS, установленном на СБ.

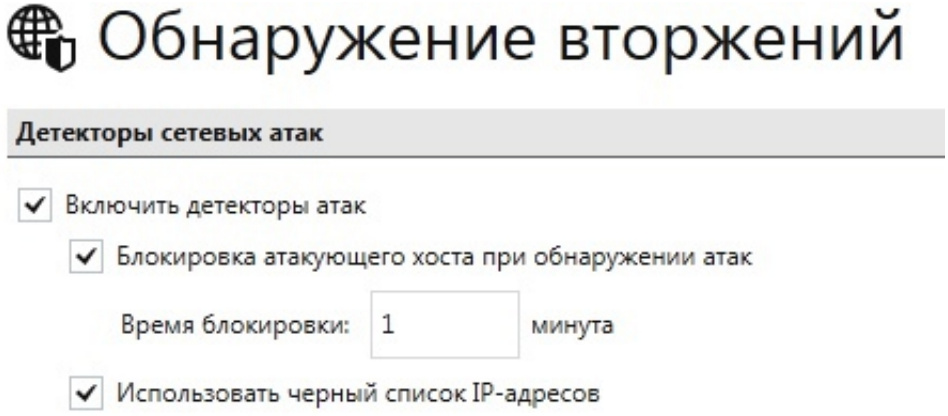


Рис 2. Основное окно настройки.

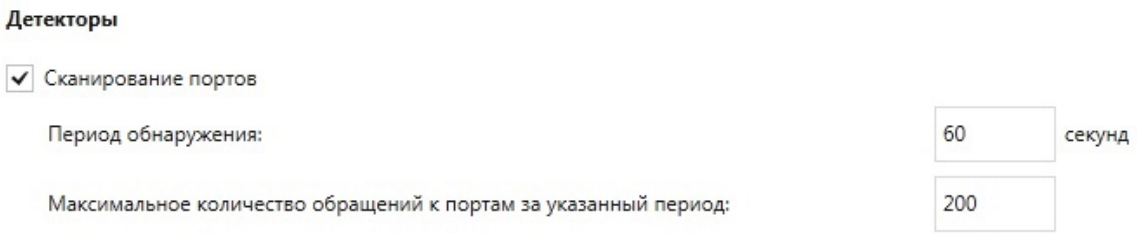


Рис 3. Детекторы.

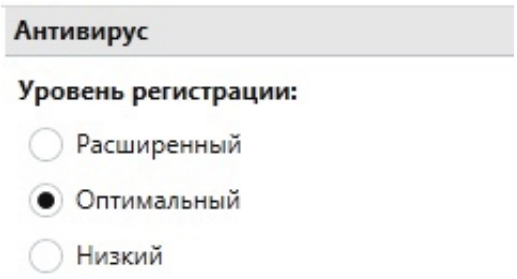


Рис 4. Регистрация событий.

Пункт 4

В данном пункте мы имитировали атаку на компьютер ServerSNS.

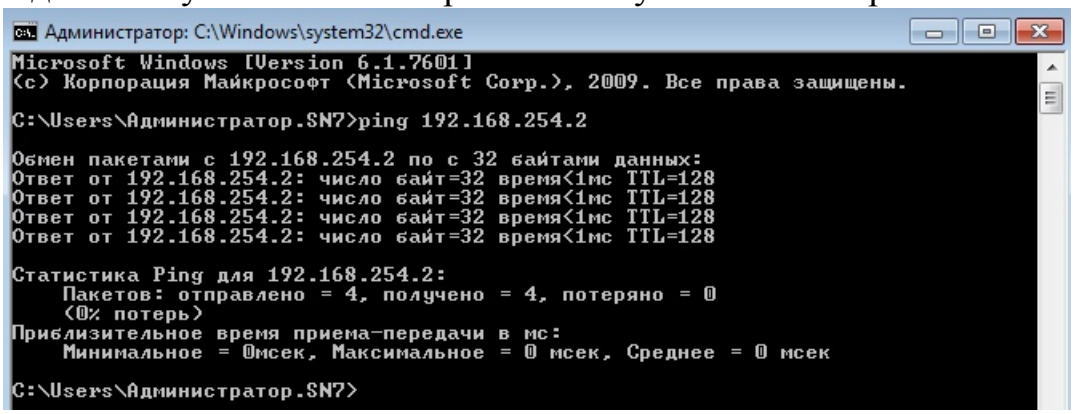


Рис 5. Компьютер ServerSNS доступен.

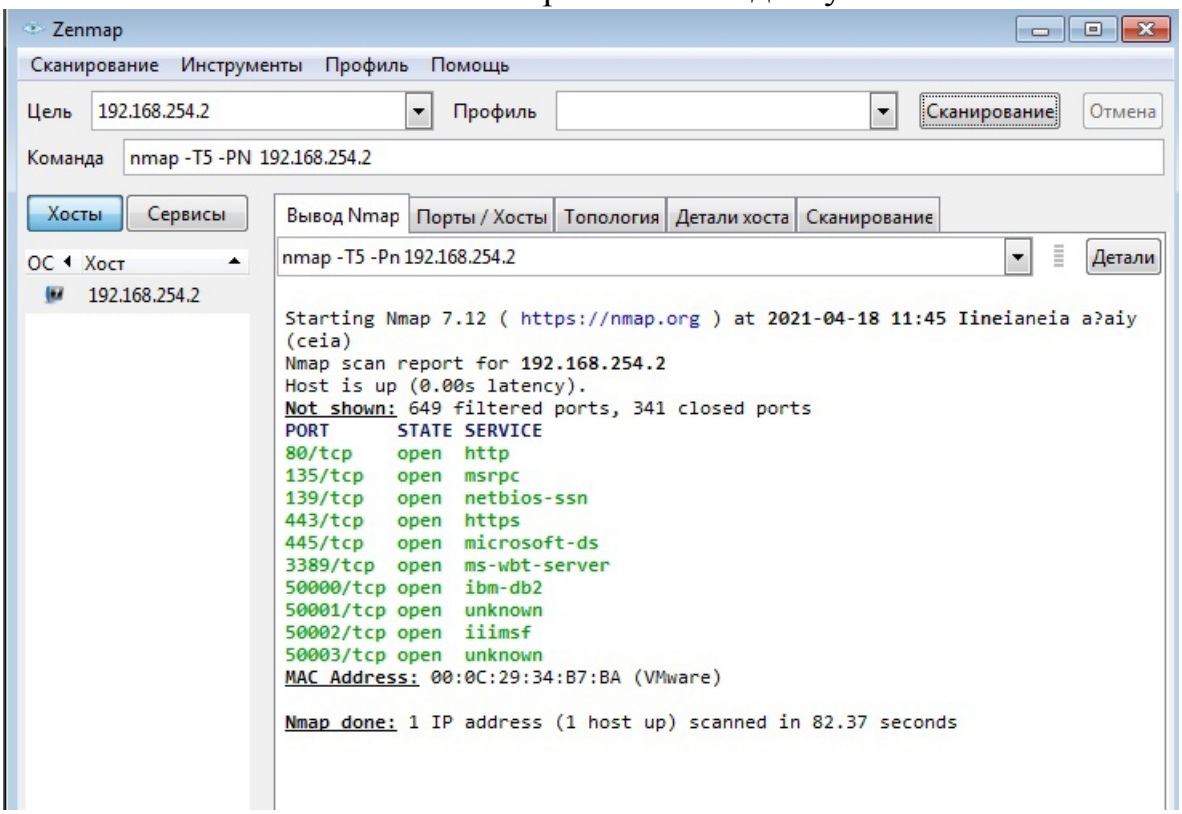
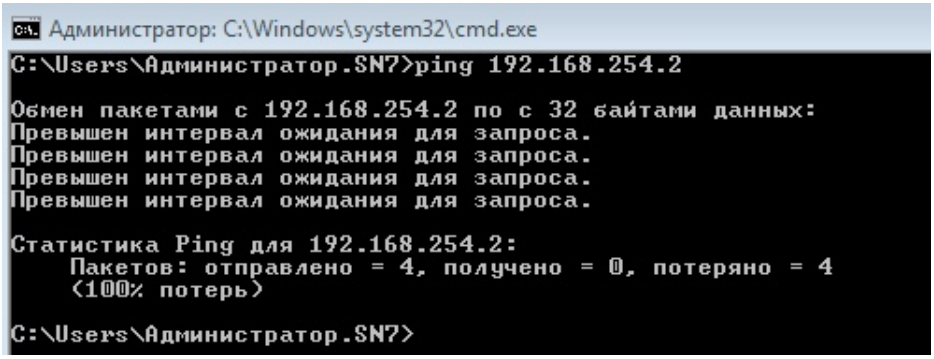


Рис 6. Проводим сканирование портов защищаемого сервера.



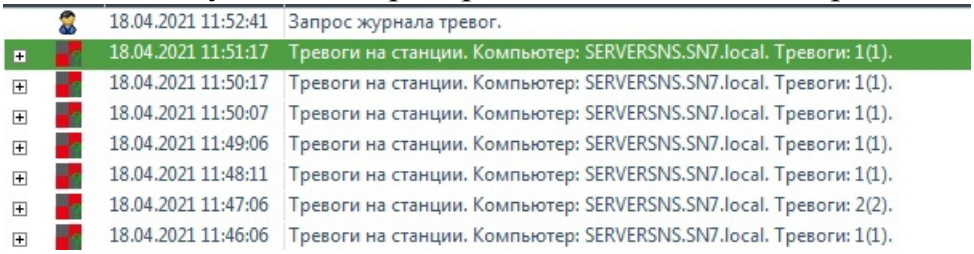
Администратор: C:\Windows\system32\cmd.exe

```
C:\Users\Администратор.SN7>ping 192.168.254.2

Обмен пакетами с 192.168.254.2 по с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 192.168.254.2:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)

C:\Users\Администратор.SN7>
```

Рис 7. Компьютер ServerSNS недоступен.

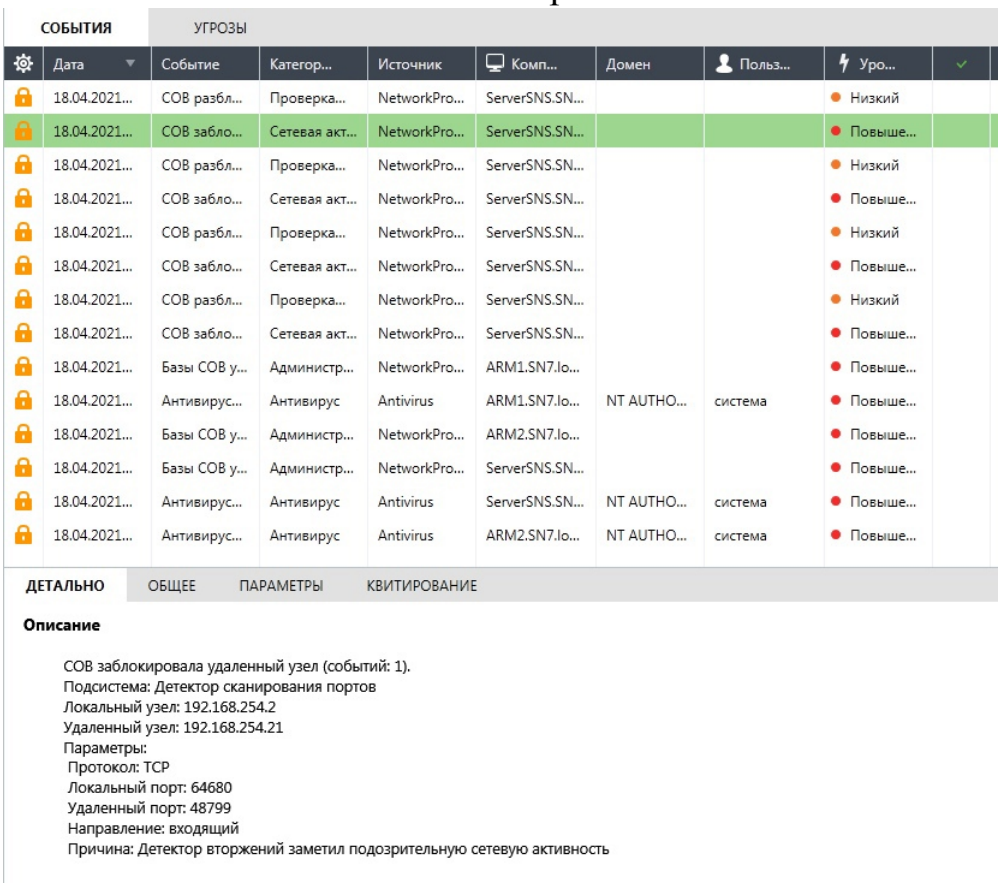
Пункт 5

В данном пункте мы проверили наличие записи тревоги.



18.04.2021 11:52:41 Запрос журнала тревог.
18.04.2021 11:51:17 Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).
18.04.2021 11:50:17 Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).
18.04.2021 11:50:07 Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).
18.04.2021 11:49:06 Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).
18.04.2021 11:48:11 Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).
18.04.2021 11:47:06 Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 2(2).
18.04.2021 11:46:06 Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).

Рис 8. Появились записи о событиях тревоги на СБ в панели событий.



	Дата	Событие	Категор...	Источник	Комп...	Домен	Польз...	Уро...	✓
🔒	18.04.2021...	СОВ разбл...	Проверка...	NetworkPro...	ServerSNS.SN...			● Низкий	
🔒	18.04.2021...	СОВ забло...	Сетевая акт...	NetworkPro...	ServerSNS.SN...			● Повыше...	
🔒	18.04.2021...	СОВ разбл...	Проверка...	NetworkPro...	ServerSNS.SN...			● Низкий	
🔒	18.04.2021...	СОВ забло...	Сетевая акт...	NetworkPro...	ServerSNS.SN...			● Повыше...	
🔒	18.04.2021...	СОВ разбл...	Проверка...	NetworkPro...	ServerSNS.SN...			● Низкий	
🔒	18.04.2021...	СОВ забло...	Сетевая акт...	NetworkPro...	ServerSNS.SN...			● Повыше...	
🔒	18.04.2021...	СОВ разбл...	Проверка...	NetworkPro...	ServerSNS.SN...			● Низкий	
🔒	18.04.2021...	СОВ забло...	Сетевая акт...	NetworkPro...	ServerSNS.SN...			● Повыше...	
🔒	18.04.2021...	Базы СОВ у...	Администр...	NetworkPro...	ARM1.SN7.lo...			● Повыше...	
🔒	18.04.2021...	Антивирус...	Антивирус	Antivirus	ARM1.SN7.lo...	NT AUTHO...	система	● Повыше...	
🔒	18.04.2021...	Базы СОВ у...	Администр...	NetworkPro...	ARM2.SN7.lo...			● Повыше...	
🔒	18.04.2021...	Базы СОВ у...	Администр...	NetworkPro...	ServerSNS.SN...			● Повыше...	
🔒	18.04.2021...	Антивирус...	Антивирус	Antivirus	ServerSNS.SN...	NT AUTHO...	система	● Повыше...	
🔒	18.04.2021...	Антивирус...	Антивирус	Antivirus	ARM2.SN7.lo...	NT AUTHO...	система	● Повыше...	

Описание

СОВ заблокировала удаленный узел (событий: 1).
Подсистема: Детектор сканирования портов
Локальный узел: 192.168.254.2
Удаленный узел: 192.168.254.21
Параметры:
Протокол: TCP
Локальный порт: 64680
Удаленный порт: 48799
Направление: входящий
Причина: Детектор вторжений заметил подозрительную сетевую активность

Рис 9. В журнале тревог появились сообщения о блокировке атакующего узла.

Пункт 6

В данном пункте мы провели дополнительную настройку политик СОВ на клиенте SNS.

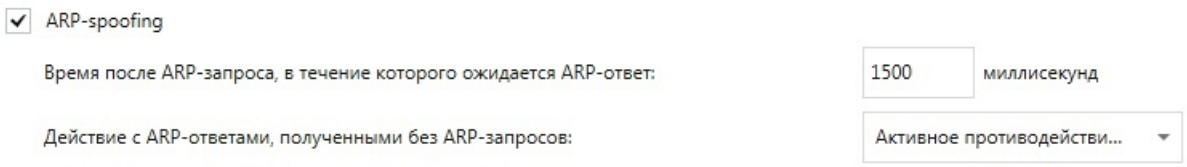


Рис 10. ARP-spoofing

Пункт 7

В данном пункте мы имитировали атаку ARP-spoofing на компьютер ServerSNS.

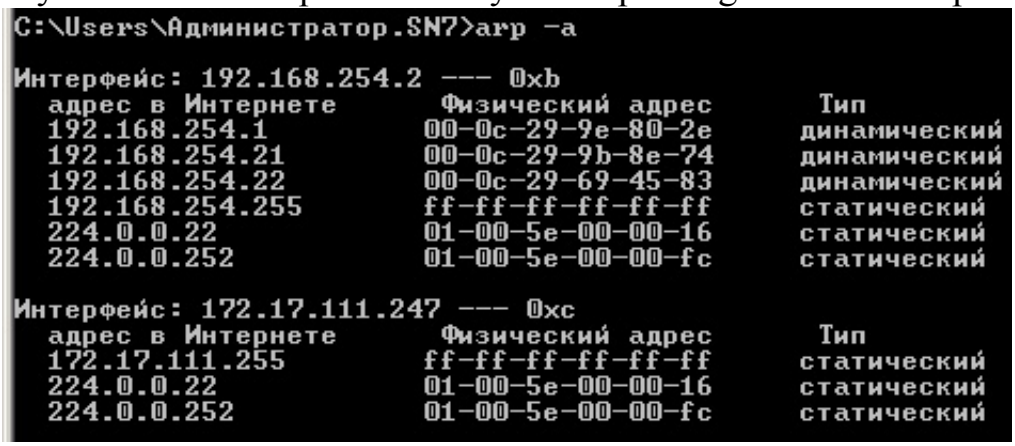


Рис 11. Определяем mac-адрес компьютера.

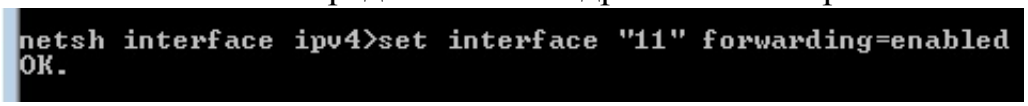


Рис 12. Переводим интерфейс в статус пересылки ipv4 пакетов.

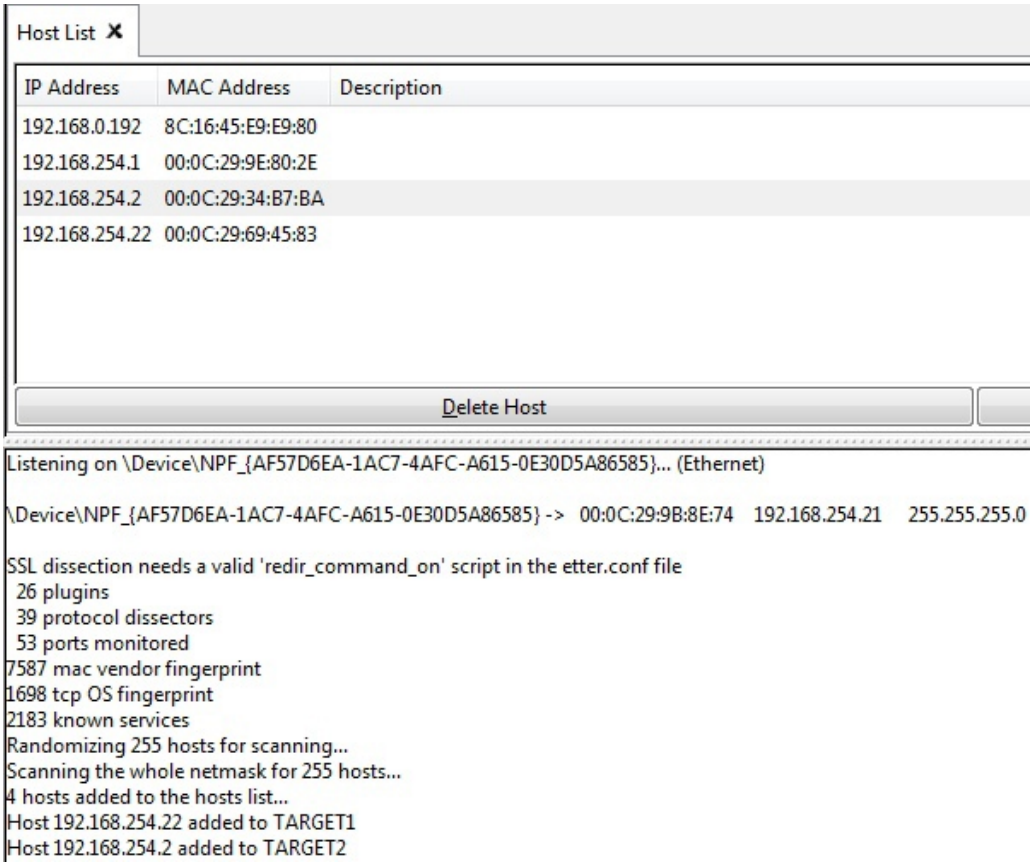


Рис 13. Список доступных хостов в сети.

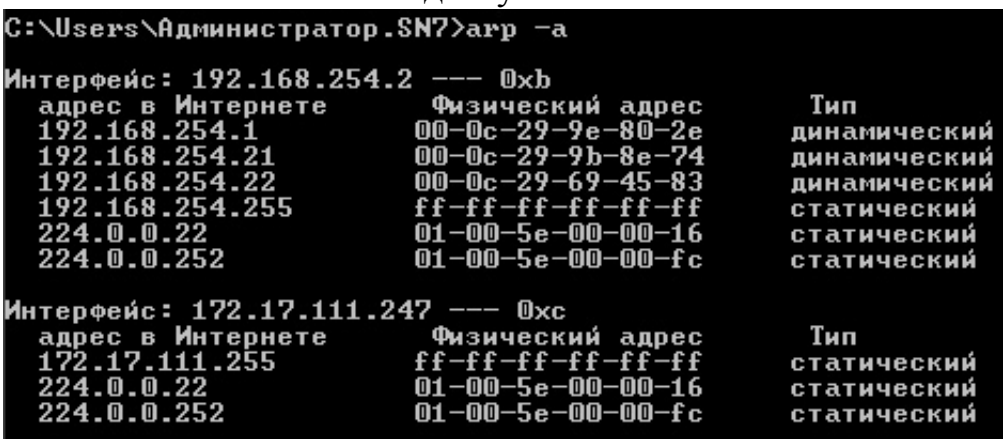


Рис 14. Убеждаемся, что верно определили mac-адрес.

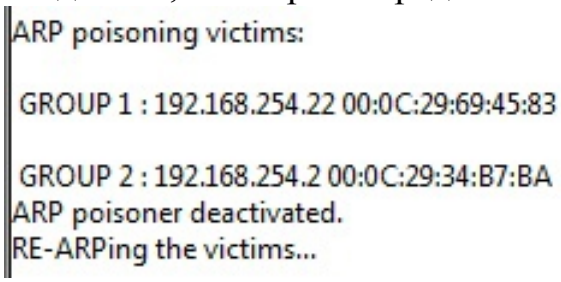


Рис 15. Останавливаем атаку.

Пункт 8

В данном пункте мы останавили команду ping.

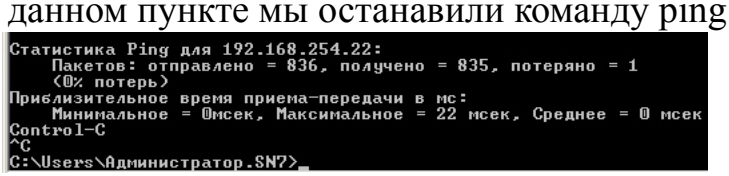


Рис 16. Остановка ping

Пункт 9

В данном пункте мы провели проверку журнала тревог.

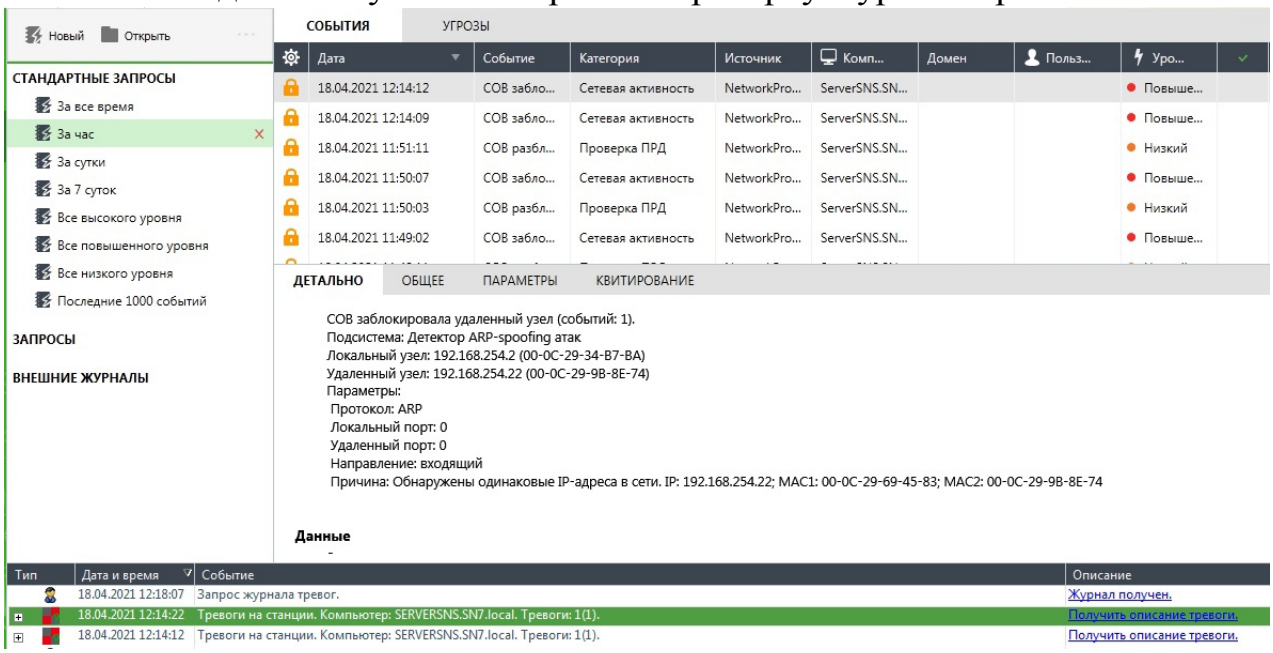


Рис 17. В журнале тревог появились сообщения детектора атак об arp-спуфинге

Вывод

В ходе данной лабораторной работы была исследована функциональность модулей ”Антивирус” и ”Система обнаружения вторжений”. Также мы протестировали их работоспособность с помощью программ Nmap и Etthercap.

Ответы на контрольные вопросы.

1. Панель управления SNS, компоненты “Антивирус” и “Обнаружение вторжений”
2. Постоянная защита, контекстное сканирование, быстрое/полное сканирование, автопроверка съемных носителей, выбор уровня защиты, выбор объектов для сканирования, список исключений и выбор действий над вирусами.
3. Детектор сетевых атак, сигнатурный анализ, блокировка доступа к опасным веб-ресурсам.
4. Сервер обновлений.