

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.

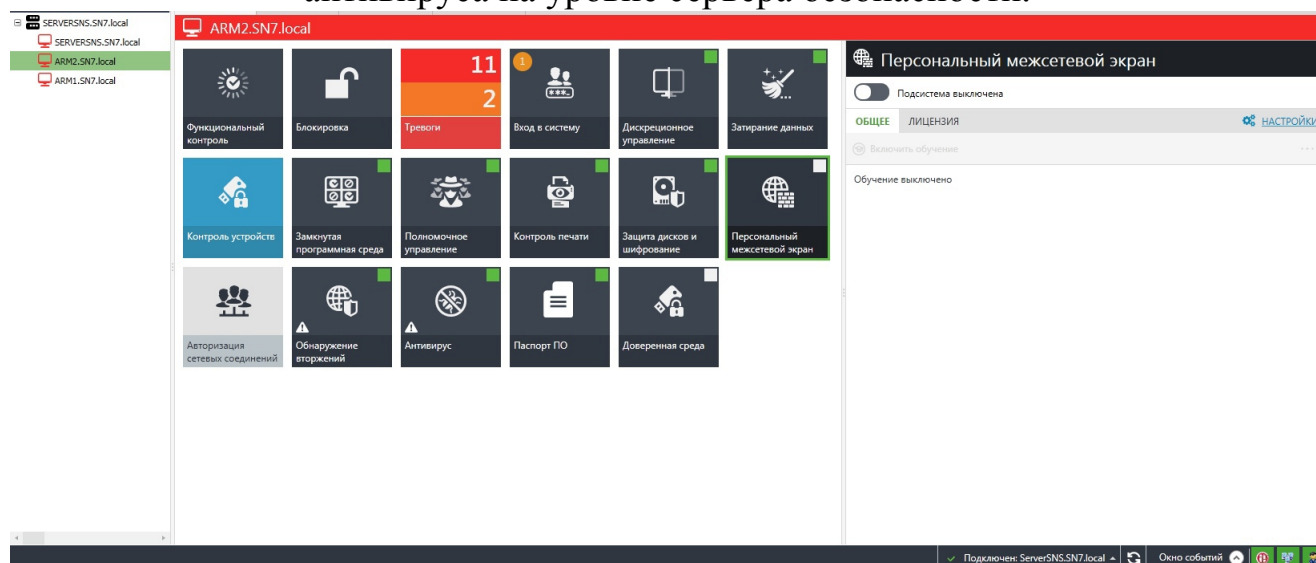


Рис 1. Персональный межсетевой экран.

## Пункт 3

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

### Обнаружение вторжений

#### Детекторы сетевых атак

- ☒ Включить детекторы атак
  - ☒ Блокировка атакующего хоста при обнаружении атак
    - Время блокировки:  минута
  - ☒ Использовать черный список IP-адресов

Рис 2. Основное окно настройки.

#### Детекторы

- ☒ Сканирование портов

Период обнаружения:

секунд

Максимальное количество обращений к портам за указанный период:

Рис 3. Детекторы.

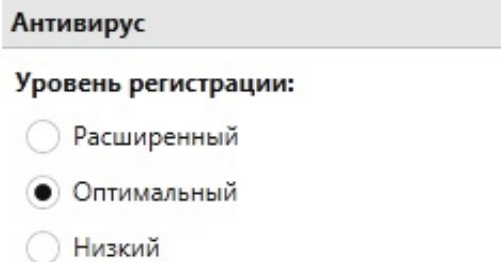


Рис 4. Регистрация событий.

#### Пункт 4

В данном пункте мы имитировали атаку на компьютер ServerSNS.

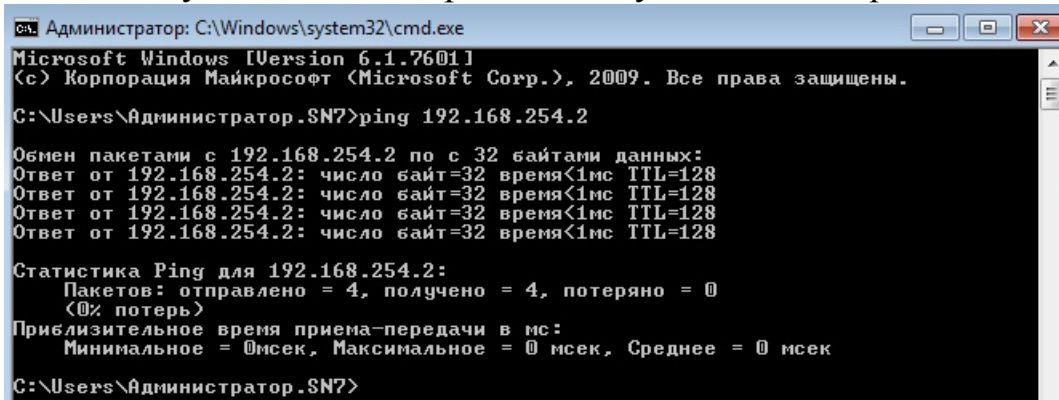


Рис 5. Компьютер ServerSNS доступен.

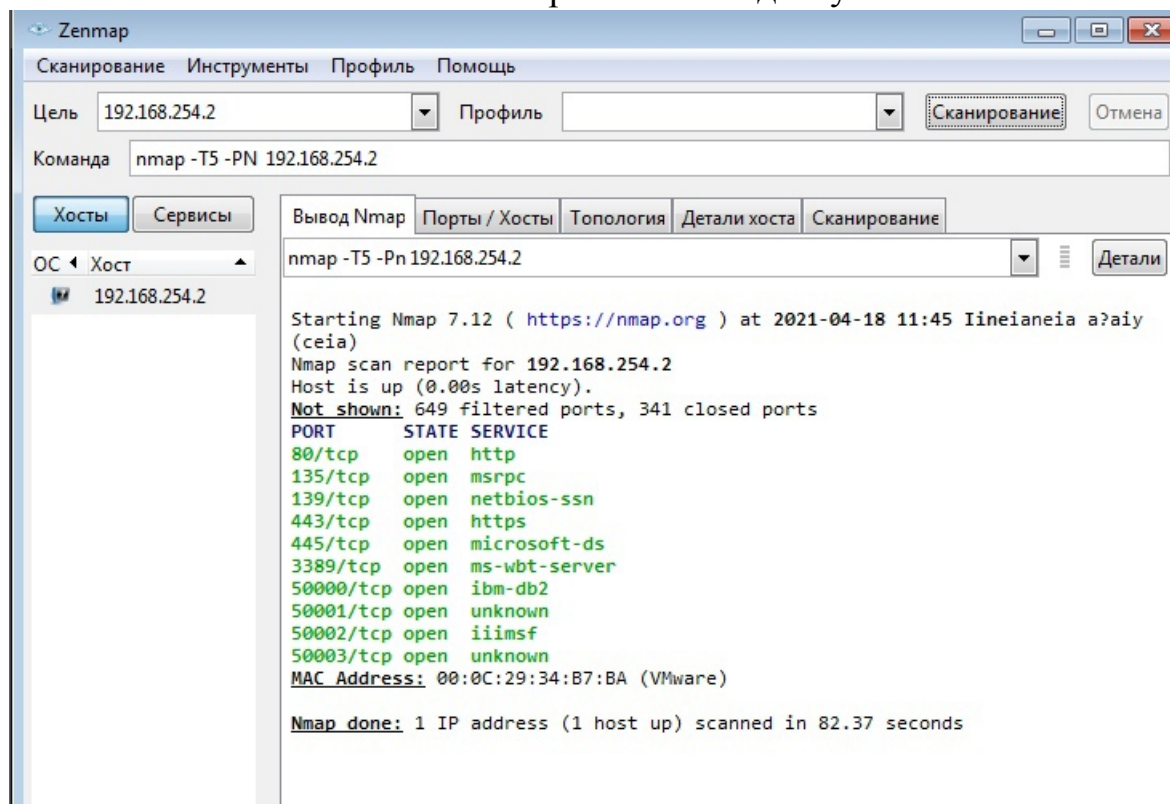


Рис 6. Проводим сканирование портов защищаемого сервера.

```

C:\Администратор: C:\Windows\system32\cmd.exe
C:\Users\Администратор.SN7>ping 192.168.254.2

Обмен пакетами с 192.168.254.2 по 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% потеря>

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.

СОБЫТИЯ		УГРОЗЫ							
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...		

ДЕТАЛЬНО	ОБЩЕЕ	ПАРАМЕТРЫ	КВИТИРОВАНИЕ
<b>Описание</b>  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 COB на клиенте SNS.

☒ ARP-spoofing

Время после ARP-запроса, в течение которого ожидается ARP-ответ:  миллисекунд

Действие с ARP-ответами, полученными без ARP-запросов:

Рис 10. ARP-spoofing

## Пункт 7

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

```
C:\Users\Администратор.SN7>arp -a

Интерфейс: 192.168.254.2 --- 0xb
  адрес в Интернете      Физический адрес      Тип
192.168.254.1            00-0c-29-9e-80-2e      динамический
192.168.254.21           00-0c-29-9b-8e-74      динамический
192.168.254.22           00-0c-29-69-45-83      динамический
192.168.254.255          ff-ff-ff-ff-ff-ff      статический
224.0.0.22               01-00-5e-00-00-16      статический
224.0.0.252              01-00-5e-00-00-fc      статический

Интерфейс: 172.17.111.247 --- 0xc
  адрес в Интернете      Физический адрес      Тип
172.17.111.255           ff-ff-ff-ff-ff-ff      статический
224.0.0.22               01-00-5e-00-00-16      статический
224.0.0.252              01-00-5e-00-00-fc      статический
```

Рис 11. Определяем mac-адрес компьютера.

```
netsh interface ipv4>set interface "11" forwarding=enabled
OK.
```

Рис 12. Переводим интерфейс в статус пересылки ipv4 пакетов.

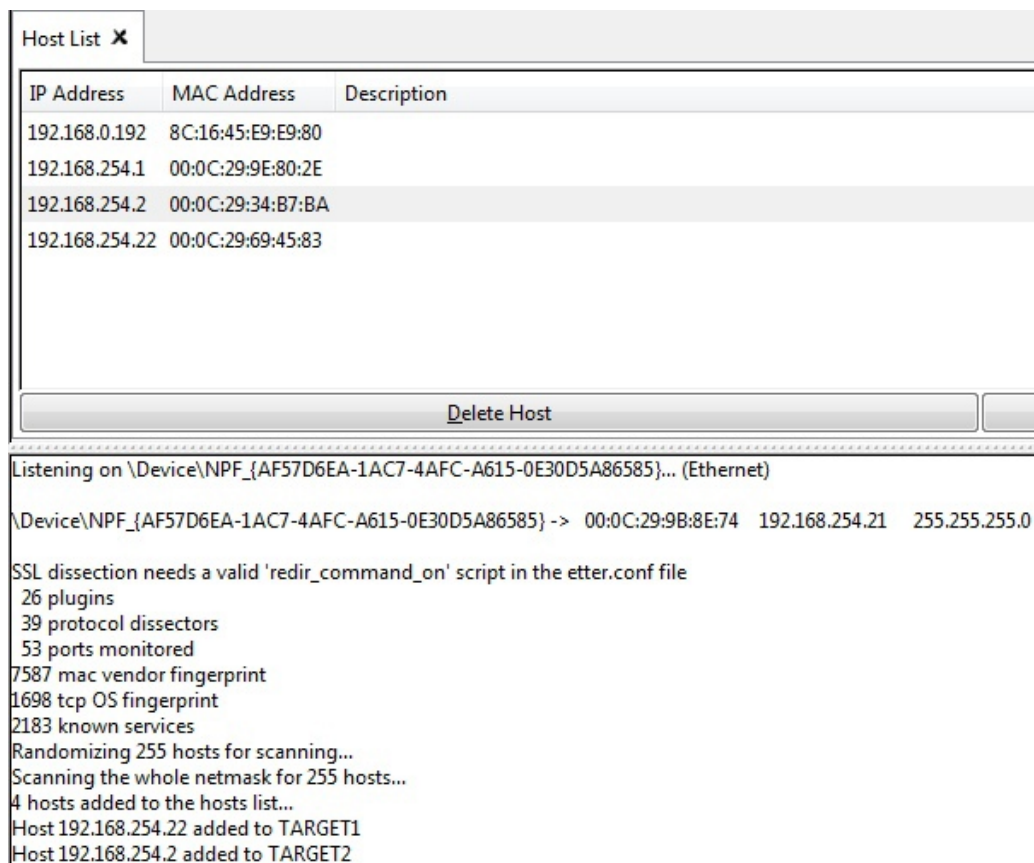


Рис 13. Список доступных хостов в сети.

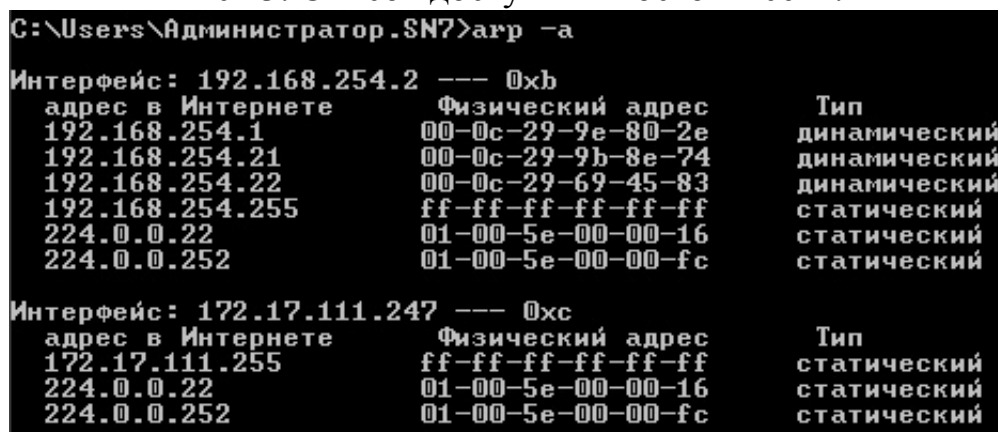


Рис 14. Убеждаемся, что верно определили mac-адрес.

```
ARP poisoning victims:

GROUP 1 : 192.168.254.22 00:0C:29:69:45:83

GROUP 2 : 192.168.254.2 00:0C:29:34:B7:BA
ARP poisoner deactivated.
RE-ARPing the victims...
```

Рис 15. Останавливаем атаку.

## Пункт 8

В данном пункте мы остановили команду ping.

```
Статистика Ping для 192.168.254.22:
Пакетов: отправлено = 836, получено = 835, потеряно = 1
<0% потерь>
Приблизительное время приема-передачи в мс:
Минимальное = 0мсек, Максимальное = 22 мсек, Среднее = 0 мсек
Control-C
^C
C:\Users\Администратор.SN7>
```



Рис 16. Остановка ping

## Пункт 9

В данном пункте мы провели проверку журнала тревог.

СОБЫТИЯ		УГРОЗЫ							
Дата	Событие	Категория	Источник	Комп...	Домен	Польз...	Уро...		
18.04.2021 12:14:12	СОВ забло...	Сетевая активность	NetworkPro...	ServerSNS.SN...			Повыше...		
18.04.2021 12:14:09	СОВ забло...	Сетевая активность	NetworkPro...	ServerSNS.SN...			Повыше...		
18.04.2021 11:51:11	СОВ разбл...	Проверка ПРД	NetworkPro...	ServerSNS.SN...			Низкий		
18.04.2021 11:50:07	СОВ забло...	Сетевая активность	NetworkPro...	ServerSNS.SN...			Повыше...		
18.04.2021 11:50:03	СОВ разбл...	Проверка ПРД	NetworkPro...	ServerSNS.SN...			Низкий		
18.04.2021 11:49:02	СОВ забло...	Сетевая активность	NetworkPro...	ServerSNS.SN...			Повыше...		
ДЕТАЛЬНО									
ОБЩЕЕ									
ПАРАМЕТРЫ									
КВИТИРОВАНИЕ									
<p>СОВ заблокировала удаленный узел (событий: 1).</p> <p>Подсистема: Детектор ARP-spoofing атак</p> <p>Локальный узел: 192.168.254.2 (00-0C-29-34-B7-BA)</p> <p>Удаленный узел: 192.168.254.22 (00-0C-29-98-8E-74)</p> <p>Параметры:</p> <p>Протокол: ARP</p> <p>Локальный порт: 0</p> <p>Удаленный порт: 0</p> <p>Направление: входящий</p> <p>Причина: Обнаружены одинаковые IP-адреса в сети. IP: 192.168.254.22; MAC1: 00-0C-29-69-45-83; MAC2: 00-0C-29-98-8E-74</p>									
Данные									
Тип	Дата и время	Событие	Описание						
	18.04.2021 12:18:07	Запрос журнала тревог.	<a href="#">Журнал получен.</a>						
	18.04.2021 12:14:22	Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).	<a href="#">Получить описание тревоги.</a>						
	18.04.2021 12:14:12	Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).	<a href="#">Получить описание тревоги.</a>						

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. **Какими программными средствами Secret Net Studio выполняется настройка компонентов "Антивирус" и "СОВ"?**

Панель управления SNS, компоненты "Антивирус" и "Обнаружение вторжений"

2. **Какие функции защиты реализуются компонентом "Антивирус" в Secret Net Studio?**

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. **Какие функции защиты реализуются компонентом "СОВ" в Secret Net Studio?**

Детектор сетевых атак, сигнатурный анализ, блокировка доступа к опасным веб-ресурсам.

4. **Какое программное средство в Secret Net Studio используется для централизованного обновления антивирусных баз и баз решающих правил на защищаемых компьютерах?**

Сервер обновлений.