

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.)

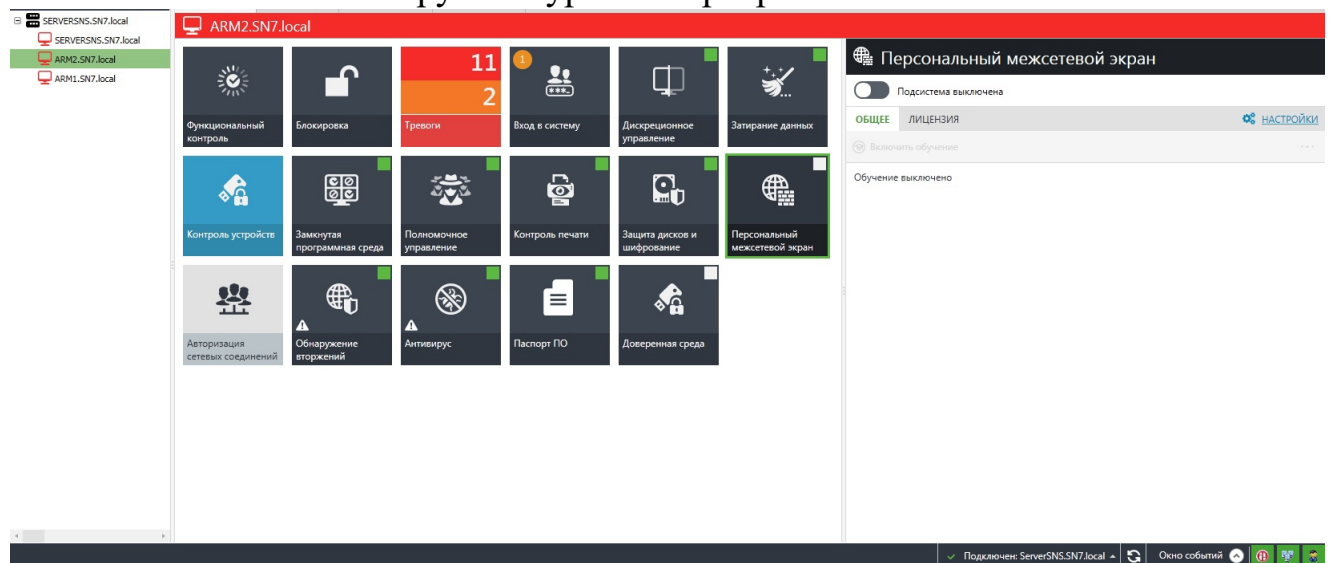
(подпись)

Санкт-Петербург

2021

## Пункт 1

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



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

Основное окно настройки.

#### Детекторы

- ☒ Сканирование портов
  - Период обнаружения:  секунд
  - Максимальное количество обращений к портам за указанный период:

Детекторы.

## Антивирус

Уровень регистрации:

- ☐ Расширенный
- ☒ Оптимальный
- ☐ Низкий

Регистрация событий.

## Пункт 4

В данном пункте мы имитировали атаку на компьютер ServerSNS.

```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

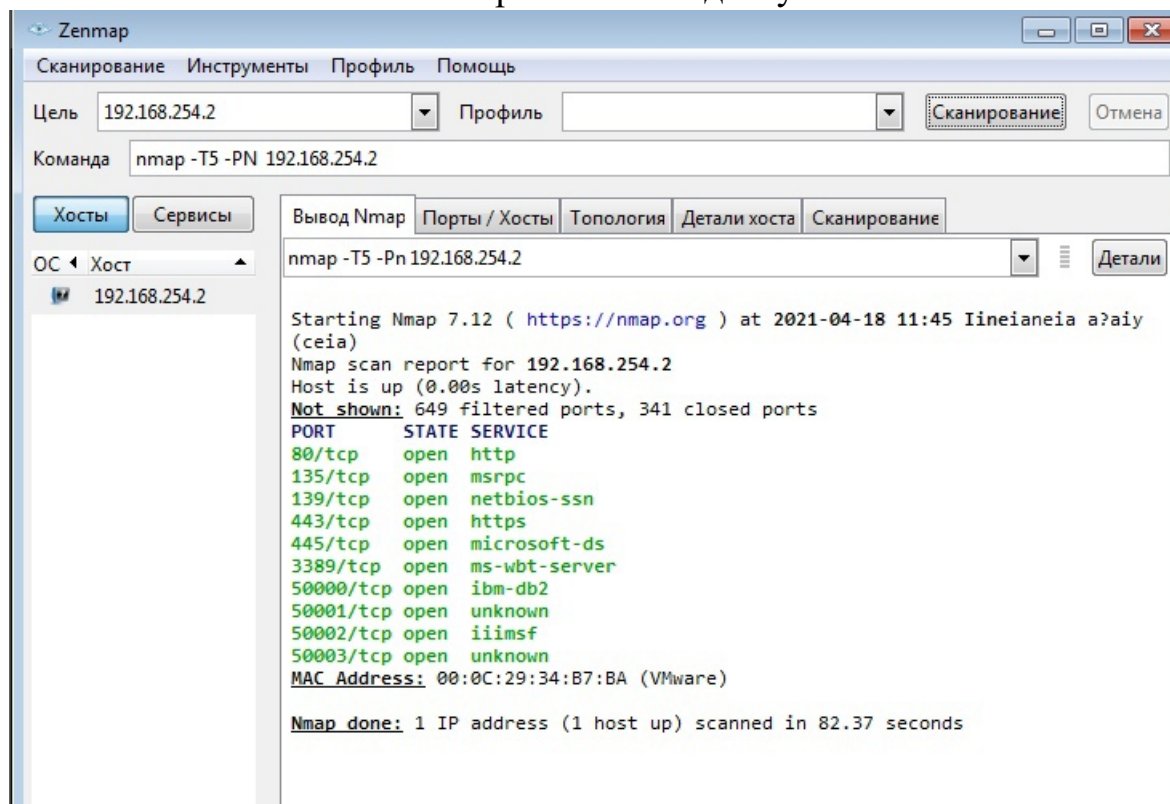
C:\Users\Администратор.SN7>ping 192.168.254.2

Обмен пакетами с 192.168.254.2 по с 32 байтами данных:
Ответ от 192.168.254.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.254.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.254.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.254.2: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.254.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Администратор.SN7>
```

Компьютер ServerSNS доступен.



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>

```

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).

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...	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.Io...			Повыше...	
	18.04.2021...	Антивирус...	Антивирус	Antivirus	ARM1.SN7.Io...	NT AUTHO...	система	Повыше...	
	18.04.2021...	Базы СОВ у...	Администр...	NetworkPro...	ARM2.SN7.Io...			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.Io...	NT AUTHO...	система	Повыше...	
ДЕТАЛЬНО		ОБЩЕЕ ПАРАМЕТРЫ КВИТИРОВАНИЕ							
Описание									
<p>СОВ заблокировала удаленный узел (событий: 1).</p> <p>Подсистема: Детектор сканирования портов</p> <p>Локальный узел: 192.168.254.2</p> <p>Удаленный узел: 192.168.254.21</p> <p>Параметры:</p> <p>Протокол: TCP</p> <p>Локальный порт: 64680</p> <p>Удаленный порт: 48799</p> <p>Направление: входящий</p> <p>Причина: Детектор вторжений заметил подозрительную сетевую активность</p>									

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:

## 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
```

Определяем mac-адрес компьютера.

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

Переводим интерфейс в статус пересылки ipv4 пакетов.

Host List X

IP Address	MAC Address	Description
192.168.0.192	8C:16:45:E9:E9:80	
192.168.254.1	00:0C:29:9E:80:2E	
192.168.254.2	00:0C:29:34:B7:BA	
192.168.254.22	00:0C:29:69:45:83	

Delete Host

Listening on \Device\NPF\_{AF57D6EA-1AC7-4AFC-A615-0E30D5A86585}... (Ethernet)  
\Device\NPF\_{AF57D6EA-1AC7-4AFC-A615-0E30D5A86585} -> 00:0C:29:9B:8E:74 192.168.254.21 255.255.255.0  
SSL dissection needs a valid 'redir\_command\_on' script in the etter.conf file  
26 plugins  
39 protocol dissectors  
53 ports monitored  
7587 mac vendor fingerprint  
1698 tcp OS fingerprint  
2183 known services  
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
4 hosts added to the hosts list...  
Host 192.168.254.22 added to TARGET1  
Host 192.168.254.2 added to TARGET2

Список доступных хостов в сети.

```
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
```

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...
```

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>
```



## Остановка ping

### Пункт 9

В данном пункте мы провели проверку журнала тревог.

Новый

Открыть

СТАНДАРТНЫЕ ЗАПРОСЫ

За все время

За час

За сутки

За 7 суток

Все высокого уровня

Все повышенного уровня

Все низкого уровня

Последние 1000 событий

ЗАПРОСЫ

ВНЕШНИЕ ЖУРНАЛЫ

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

СОВ заблокировала удаленный узел (событий: 1).  
Подсистема: Детектор ARP-spoofing атак  
Локальный узел: 192.168.254.2 (00-0C-29-34-B7-BA)  
Удаленный узел: 192.168.254.22 (00-0C-29-98-8E-74)  
Параметры:  
Протокол: ARP  
Локальный порт: 0  
Удаленный порт: 0  
Направление: входящий  
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

Данные

Тип	Дата и время	Событие	Описание
	18.04.2021 12:18:07	Запрос журнала тревог.	Журнал получен.
	18.04.2021 12:14:22	Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).	Получить описание тревоги.
	18.04.2021 12:14:12	Тревоги на станции. Компьютер: SERVERSNS.SN7.local. Тревоги: 1(1).	Получить описание тревоги.

В журнале тревог появились сообщения детектора атак об arp-спуфинге

### 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.