

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 №2

Авторизация сетевых соединений

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 2

В данном пункте мы убедились, что передается открытый трафик с помощью программы Wireshark.

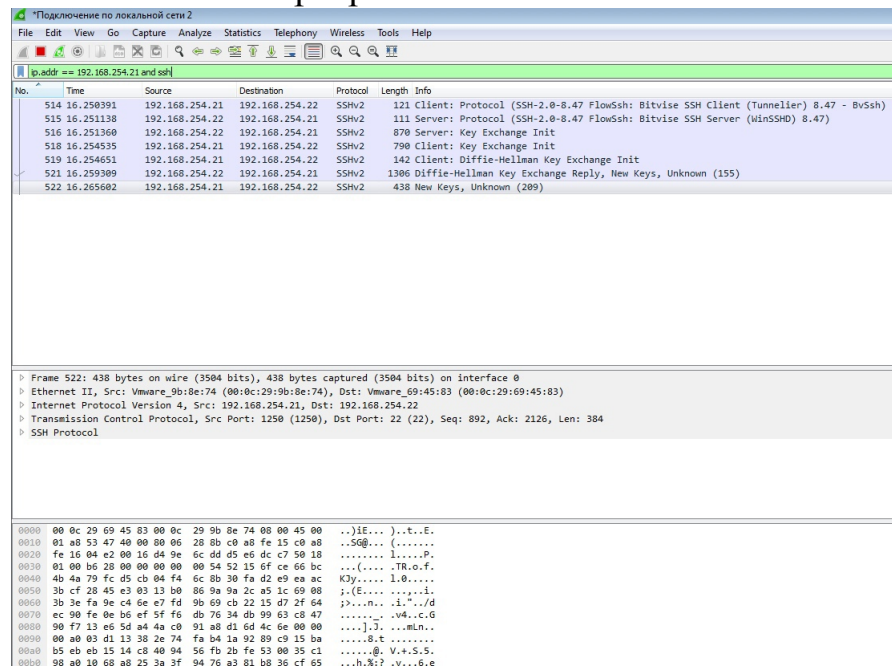


Рис. 1 Открытый трафик.

Пункт 3

В данном пункте мы настроили правила доступа, разрешающее всем сетевым сервисам входящее подключение.

Правила доступа						
Правила, регламентирующие доступ к сетевым сервисам (TCP/IP v4) данного компьютера.						
Вкл	Субъект	Сетевой сервис	Тип доступа	Направление	Удаленный адрес	Приложение
<input checked="" type="checkbox"/>	everyone	Secret Net Studio	Все входящие (UDP, TCP)	Разрешен	Входящее	*

Рис. 2 Парвило доступа.

Пункт 4

В данном пункте мы настроили режим защиты сетевых соединений.

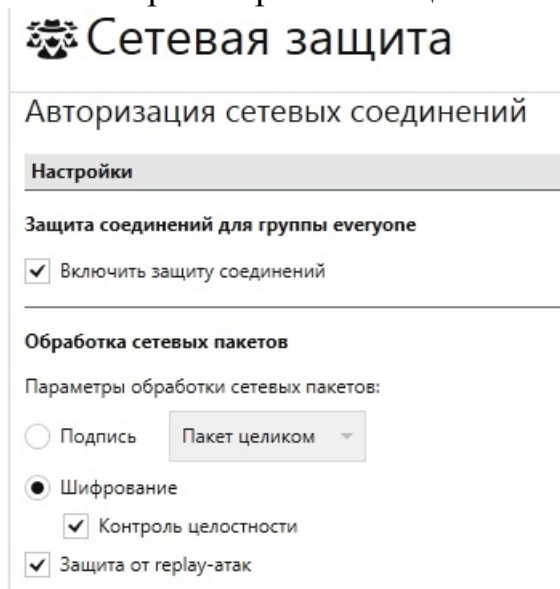


Рис. 3 Экран настроек.

Пункт 5

В данном пункте мы убедились, что передается зашифрованный трафик

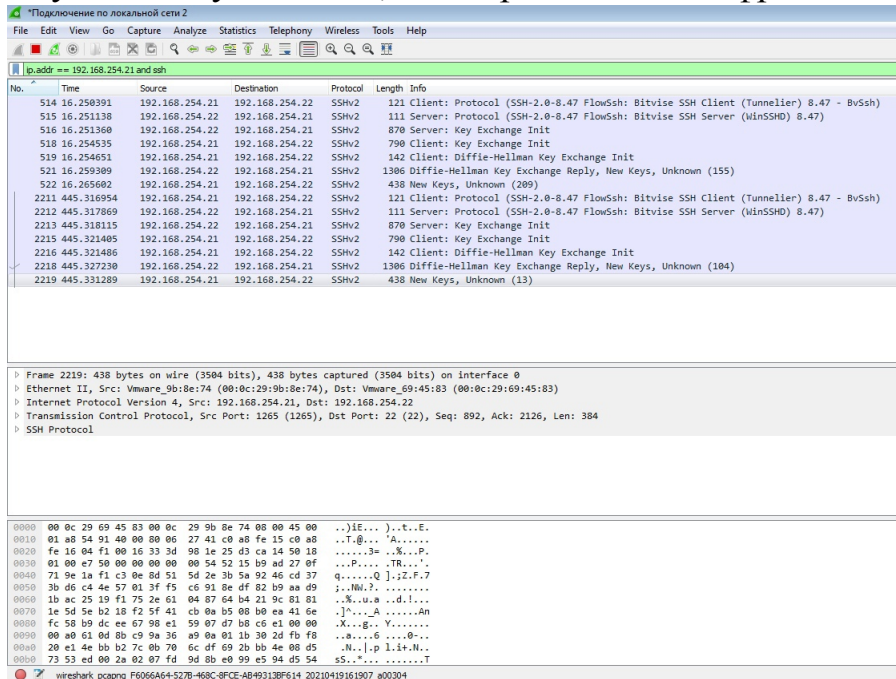


Рис. 4 Не удалось зашифровать трафик.

Пункт 7

В данном пункте мы настроили блокировку соединений для неавторизованных на СБ пользователей

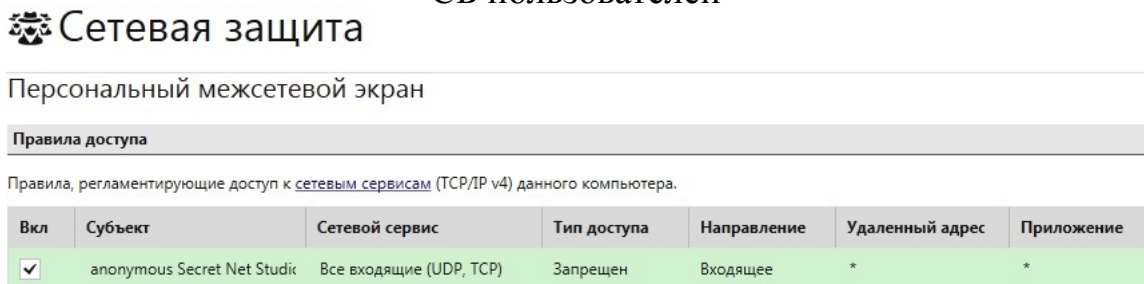


Рис. 5 Парвило доступа.

Вывод

Выполнив данную лабораторную работу, мы протестировали компонент ”Авторизация сетевых соединений” в Secret Net Studio. Нами была реализована защита протокола SSH от перехвата передаваемых по нему данных.

Ответы на контрольные вопросы.

- 1. В чем заключается особенность функционирования ПМЭ в Secret Net Studio, отличающая его от традиционных, "периметровых" МЭ?**

В отличие от традиционных, "периметровых" МЭ, реализованный в SNS распределенный межсетевой экран предназначен именно для защиты информации внутри сети организации, функционирует непосредственно на ее защищаемых объектах (сервер БД, рабочие места руководителей или сотрудников и т.д.) и обеспечивает их защиту от сетевых угроз со стороны внешнего и внутреннего нарушителей.

- 2. Какие группы правил проверки сетевого трафика реализованы в ПМЭ Secret Net Studio?**

Правила доступа, прикладные правила, системные правила, сетевые протоколы.

- 3. Какая из групп правил проверки сетевого трафика в ПМЭ Secret Net Studio имеет наивысший приоритет? Что регламентируется правилами этой группы?**

Системные правила

- 4. По каким протоколам может ограничиваться доступ к защищаемым ресурсам с помощью системных правил?**

Все IP-based протоколы (RDP)

- 5. Какая из групп правил проверки сетевого трафика в ПМЭ Secret Net Studio имеет минимальный приоритет? Что регламентируется правилами этой группы?**

Прикладные правила. Регламентируют доступ пользователей к сетевым сервисам защищаемого компьютера (например, общие папки).

- 6. Каков порядок обработки заданных в параметрах ПМЭ Secret Net Studio правил доступа?**

Чем выше правило в таблице, тем больше его приоритет

- 7. Через какой промежуток времени после сохранения изменений вступают в силу новые настройки правил доступа ПМЭ Secret Net Studio?**

4 - 6 минут

- 8. Какой режим работы ПМЭ в Secret Net Studio позволяет составить на основе информации о сетевой активности приложений базовый набор правил доступа, необходимый для функционирования защищаемого компьютера?**

Сетевой режим

9. В чем заключается особенность аутентификации пользователей механизмом авторизации сетевых соединений Secret Net Studio?

Механизм авторизации сетевых соединений обеспечивает защиту взаимодействия только между авторизованными на СБ клиентами Secret Net Studio. Если на компьютере пользователя не установлен Secret Net Studio или пользователь по каким-либо причинам не прошел аутентификацию на СБ SNS (anonymous), то трафик между ним и авторизованным клиентом SNS не будет защищаться.

10. Какими средствами обеспечивается защита и целостность передаваемых данных в механизме авторизации сетевых соединений?

Средствами протоколов семейства IPsec, а именно АН (Authentication Header) - гарантирует аутентичность и целостность и ESP (Encapsulation Security Payload) - шифрование и контроль целостности.

11. Что необходимо для возможности выбора пользователя или группы пользователей, доступ к которой будет контролироваться при создании нового правила доступа в параметрах настроек политик ПМЭ?

Необходима лицензия на использование механизма авторизации сетевых соединений.

12. Наличие каких правил необходимо для работы прикладных правил доступа к общим папкам на защищаемом компьютере?

Если прохождение пакетов по протоколу SMB запрещается системными правилами или правилами доступа, то прикладные правила не работают, так как на транспортном уровне IP-пакеты блокируются.