Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5

САМАКЕ
Баче Александр

МЕТОДИКА ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СЕТЕЙ

Автореферат
на соискание степени магистра
по специальности 1-98 80 01 Информационная безопасность

_____

Научный руководитель
канд. техн. н., доцент
БЕЛОУСОВА Елена Сергеевна

_____

Минск 2024

ВВЕДЕНИЕ

В современном мире, где информация является ценным ресурсом, а киберугрозы становятся все более изощренными, обеспечение безопасности корпоративной сети является первостепенной задачей для любой организации. Неэффективная система безопасности может привести к утечке конфиденциальных данных, финансовым потерям, нарушению деловой репутации и даже остановке работы компании.

Поэтому тестирование безопасности корпоративной сети является неотъемлемой частью ее защиты. Оно позволяет выявить уязвимости, которые могут быть использованы нарушителями, и разработать эффективные меры по их устранению.

Целью диссертационной работы является разработка методики тестирование безопасности корпоративной сети на основе анализа уязвимостей сетевых протоколов.

Для достижения поставленной цели в диссертации решены следующие задачи:

1 Изучение архитектуры построения корпоративных сетей, уязвимостей сетевых протоколов.

2 Обзор стандартов и методик тестирование безопасности.

3 Обоснование выбора инструментов для тестирования безопасности корпоративных сетей, построение модели корпоративной сети с целью анализа уязвимостей сетевых протоколов.

4 Разработка методики тестирование безопасности корпоративной сети и ее апробация для построенной модели корпоративной сети.

5 Составление рекомендации по совершенствованию информационной безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту 6 приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «*Обеспечение безопасности человека, общества, государства*». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной работы является разработка методики тестирование безопасности корпоративной сети на основе анализа уязвимостей сетевых протоколов.

Для достижения поставленной цели в диссертации решены следующие задачи:

1 Изучение архитектуры построения корпоративных сетей, уязвимостей сетевых протоколов.

2 Обзор стандартов и методик тестирование безопасности.

3 Обоснование выбора инструментов для тестирования безопасности корпоративных сетей, построение модели корпоративной сети с целью анализа уязвимостей сетевых протоколов.

4 Разработка методики тестирование безопасности корпоративной сети и ее апробация для построенной модели корпоративной сети.

5 Составление рекомендации по совершенствованию информационной безопасности.

Личный вклад соискателя ученой степени

Содержание диссертации отображает личный вклад автора. Он заключается в построение корпоративной сети с помощью программного симулятора сетевого оборудования для проведения кибератак, определение уязвимостей, составления методики тестирование безопасности корпоративной сети, проведение ее апробации, составление рекомендаций для использования разработанной методики.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем, кандидатом технических наук, доцентом Е.С. Белоусовой.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на: 59-ой научно-технической конференции аспирантов, магистрантов и студентов БГУИР и на 60-ой научно-технической конференции аспирантов, магистрантов и студентов БГУИР.

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 2 печатные работы, в том числе 2 статьи в сборниках и материалах конференций.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трех глав с выводами по каждой главе, заключения, библиографического списка.

Общий объем диссертационной работы составляет 73 страниц, из них 65 страниц текста, 35 рисунков на 19 страницах, 2 таблицы на 1 страницу, список использованных библиографических источников (20 наименований на 2 страницы), список публикаций автора по теме диссертации (2 наименование на 1 страницу), графический материал на 7 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Самаке Бач Александр «Методика тестирование безопасности корпоративной сети» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) в on-line режиме 11.06.2024 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 72 %). Отчет о результатах проверки представлен в Приложении А.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении рассмотрена актуальность проведения тестирования безопасности корпоративной сети, которая является неотъемлемой частью ее защиты от утечки конфиденциальных данных, финансовых потерь, нарушения деловой репутации и остановке работы компании.

В общей характеристике работы показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени, апробация результатов диссертации.

В первой главе рассмотрены архитектуры защищенных локальных сетей, такие как распределенная архитектура, централизованная архитектура и централизованно-распределенная архитектура. Проведен анализ уязвимостей сетевых протоколов такие как: протокол разрешения адресов (ARP), система доменных имен (DNS), протокол передачи файлов, протокол передачи гипертекста, почтовый протокол и другие.

Выполнен обзор стандартов и методик тестирования безопасности, среди которых методика OSSTMM, методика OWASP, Методика ISSAF. Были изучены такие стандарты как стандарт проведения тестирования на проникновение PTES и стандарт NIST SP 800–115.

Во второй главе был обоснован выбор инструментов для тестирования безопасности корпоративных сетей, среди них отметили Nmap (Network Mapper) для сканирования сети, предоставляющий информацию об устройствах в сети, открытых портах, операционных системах, службах и многом другом, Wireshark, который позволяет анализировать активность в компьютерных сетях и Hping, которая позволяет проверить доступность и проанализировать качество соединения с удаленным устройством. Она может использоваться для проверки статуса устройства в сети, определения времени отклика и оценки качества соединения. Была реализована модель сети для реализации тестирования (рисунок 1).

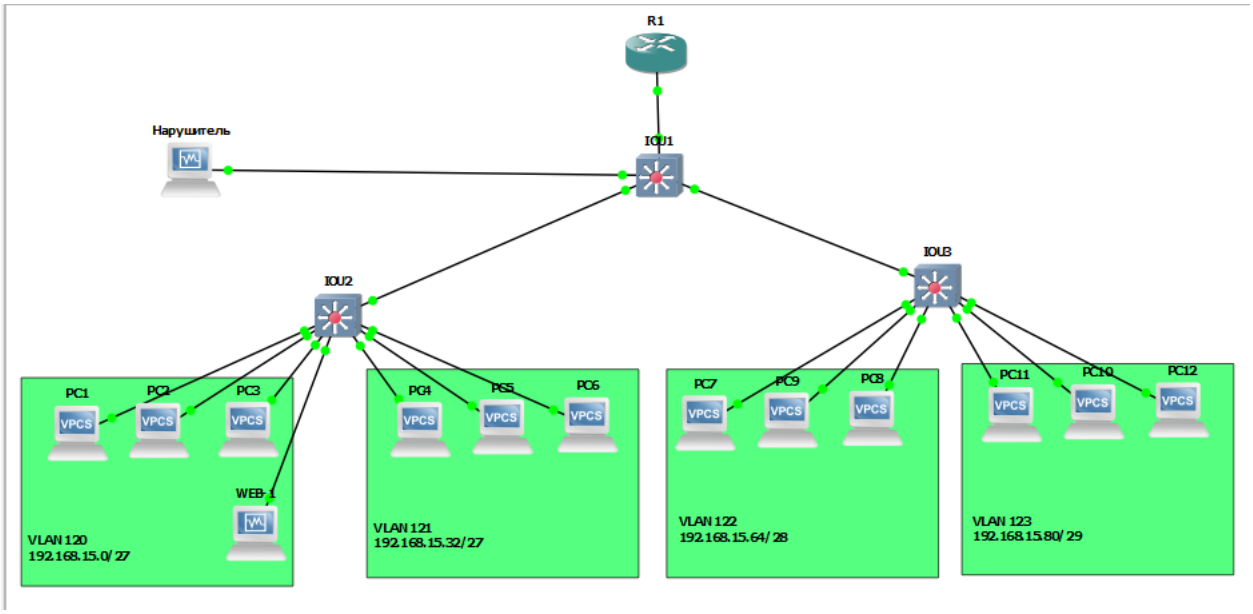

Рисунок 1 – Модель корпоративной сети

В результате анализа уязвимостей корпоративной сети и векторов атак для их эксплуатации был выбран один из наиболее эффективных приемов моделирование сценариев реализации угроз с помощью модели Cyber Kill Chain. Посредством техник модели Cyber Kill Chain была исследована уязвимость, связанная с ARP протоколом, который используется для идентификации MAC-адреса устройства по его известному IP-адресу, а также для формирования таблиц MAC-адресов на коммутаторах и ARP-таблиц на устройствах в сети. Уязвимость данного протокола заключается в попытке перехвата широковещательной рассылки ARP-пакетов, в которых есть IP и MAC-адреса устройств в сети. Таким образом, нарушитель может получить данные об устройствах в сети и реализовать атаку ARP spoofing. Было установлено, что нарушитель с помощью уязвимости, связанной с рассылкой ARP пакетов, получил информацию о IP-адресе легитимного пользователя, как предоставлено на рисунке 2. Таким образом, нарушитель способен перехватывать пакеты, которые будут адресованы доверенному пользователю и изменить таблицу ARP на маршрутизаторе как видна на рисунке 3. после чего выполнить DDoS-атаку на веб-сервере.

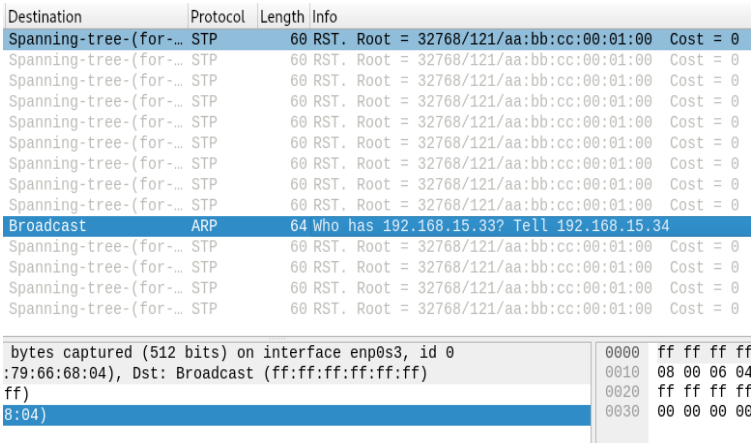

Рисунок 2. – Результат перехвата ARP-протокола

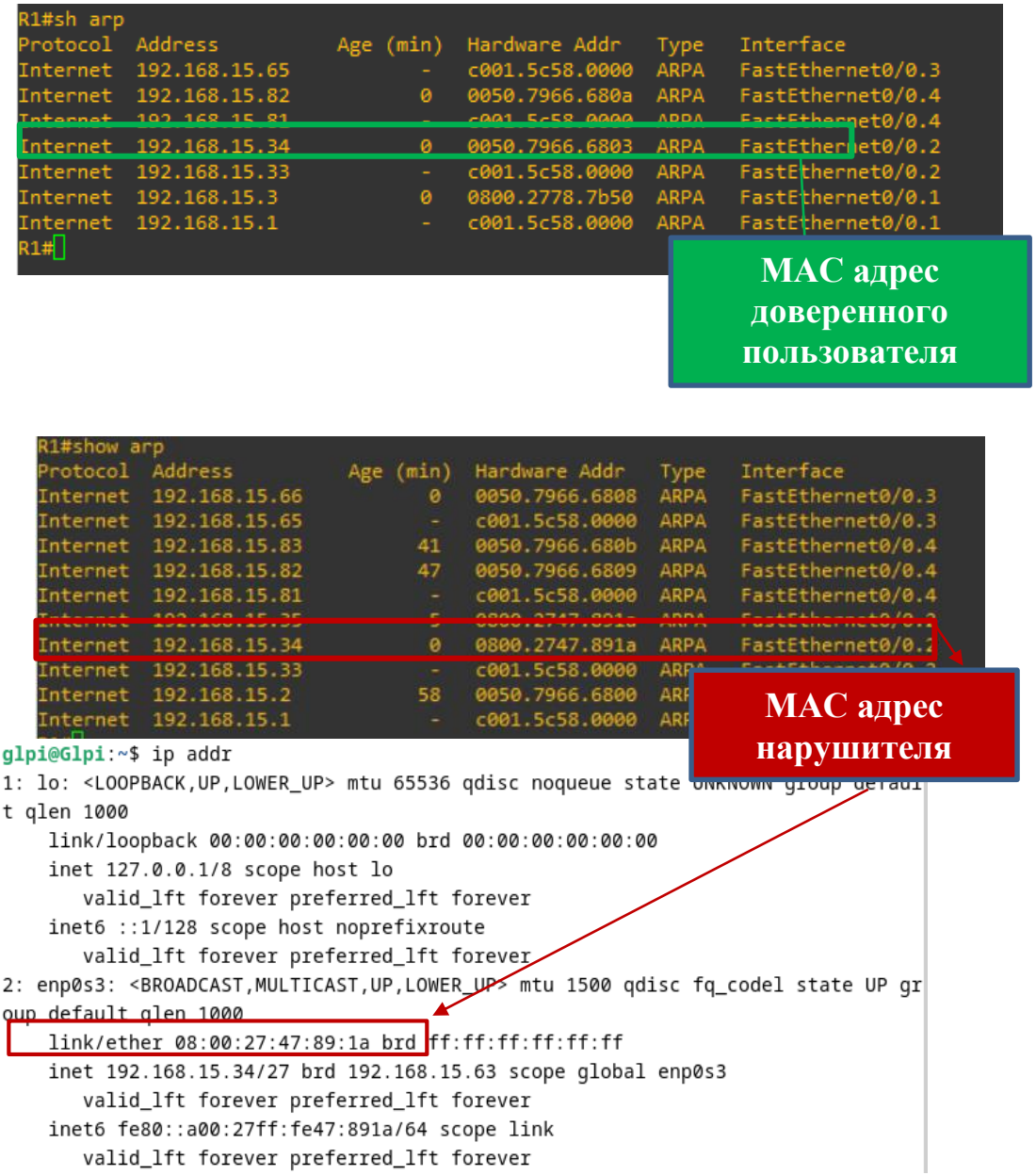

Рисунок 3 – Результат подмены записи в ARP-таблицы на устройстве R1

Далее была реализована DDoS-атака с помощью hping с целью проверки работы сервера, результат представлен на рисунке 5.

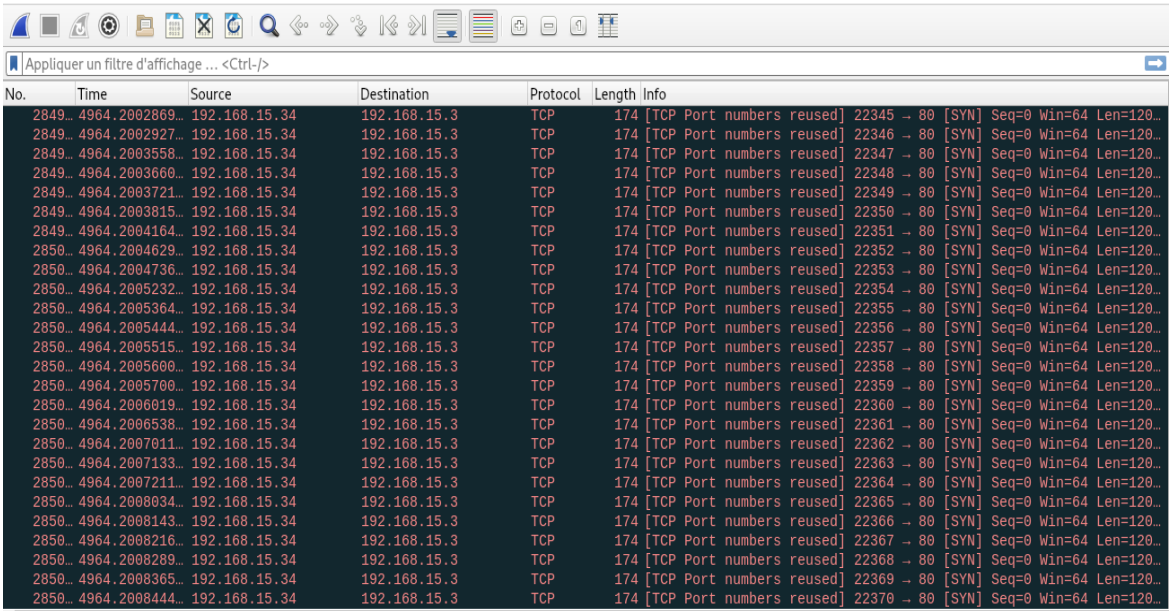

Рисунок 4 – Признак DDoS атаки представлена через Wireshark

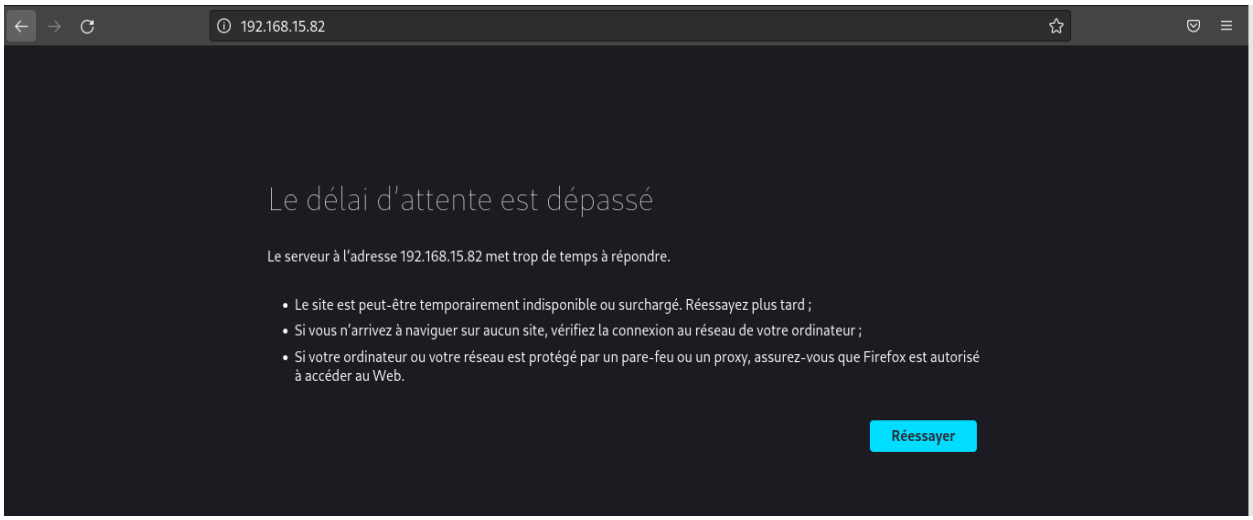

Рисунок 5 –Незультат выполнение DDoS-атак

В третьей главе разработан методика тестирования безопасности корпоративной сети, которая состоит из следующих этапов:

– получения разрешения на проведение тестирования безопасности сети;
– определение целей тестирования;
– планирование тестирование;
– проведение тестирования;
– анализ результатов;
– рекомендации по обеспечению безопасности.

После проведения апробации методики тестирования на сервера в

разработанной модели корпоративной сети, были выявлены уязвимости. Первая уязвимость, которая была рассмотрена, эта уязвимость, которая может возникнуть в том случае, когда у нарушителя не получается подключиться к локальной сети организации, и этот метод является самая распространенная, и это социальная инженерия. Этот метод заключается в несанкционированном доступе к информации или системам хранения информации без использования технических средств.

Данная уязвимость, связана с человеческим фактором может привести к таким серьезным кибератакам как:

– фишинг, отправка электронных писем с инфицированным файлами или ссылками на зараженные сайты;

– спам, массовая реклам;

– fraud, электронные письма с подмененными адресами отправителей, чтобы убедить получателя выполнить определенные действия.

Цель этих кибератак заключаются в инфицирование компьютеров, сборе определенной информации. Были формированы рекомендации для снижения риска, так как эти атаки в основном зависят от человеческого фактора, для его снижения необходима проводить мероприятия, в котором будет объяснятся риски таких атак, научить сотрудников не взаимодействовать с такими письмами и не сохранять рабочие адреса в разных сервисах для снижение полученных писем.

Вторая уязвимость связана с DDoS-атаками, которые были рассмотрены во втором разделе. Для защиты использовались модули apache. На рисунке 5 представлена настройка от DDoS-атаки с помощью mod-evasive.

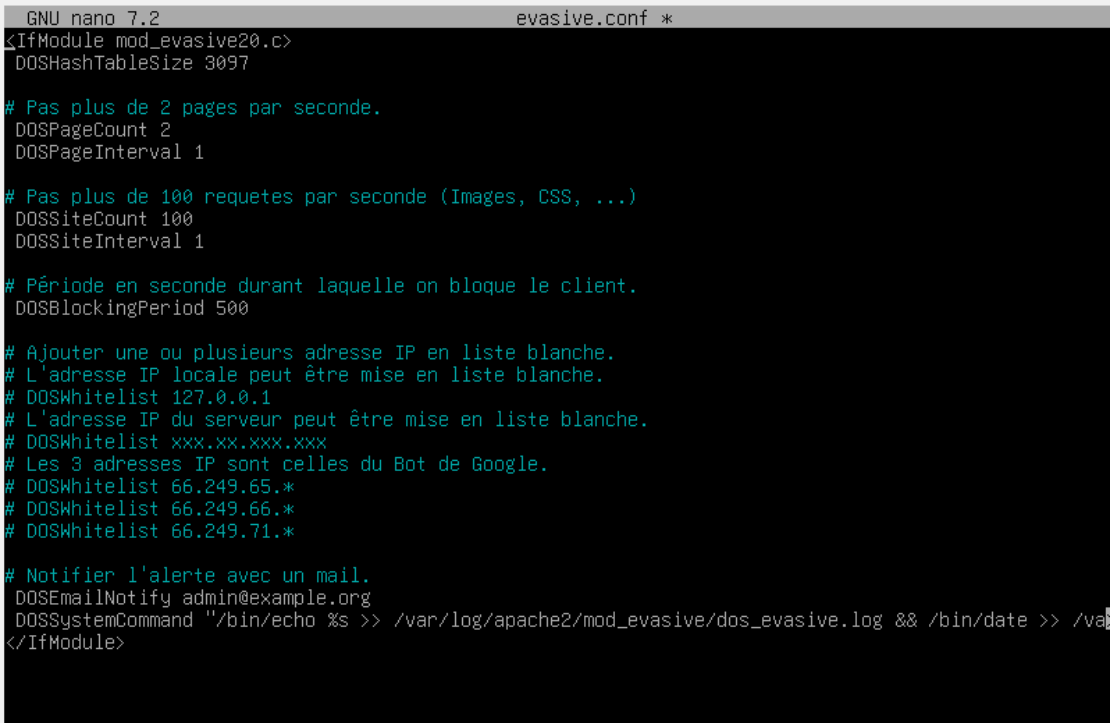

Рисунок 6 – Настройка модуля от DDoS атаки с помощью apache

Для обеспечения безопасности рекомендуется настраивать таблицы правил фильтрации пакетов, используя программу iptable. Результат этой настройки представлена на рисунке 7.

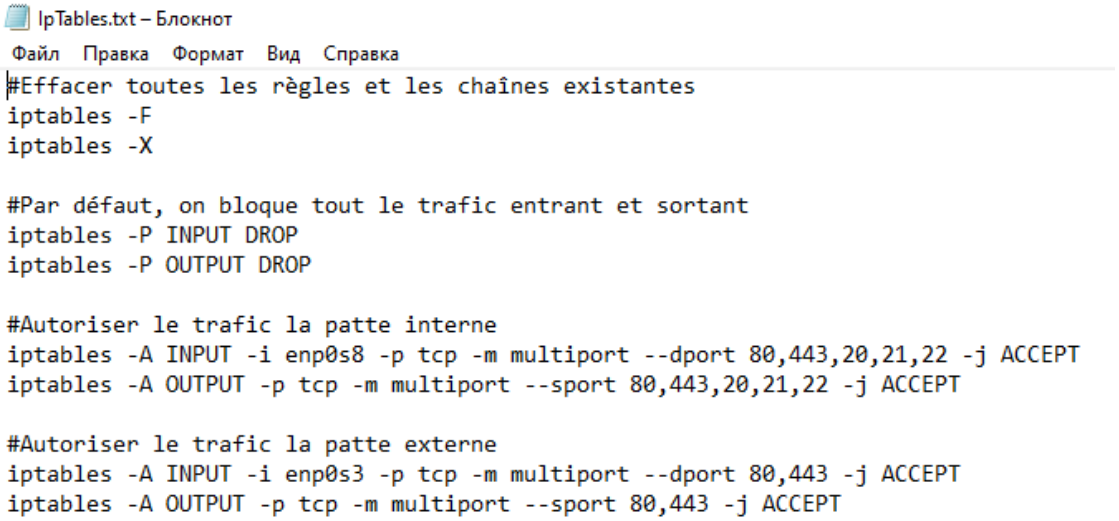

Рисунок 7 – Настройка фильтрации пакета с помощью iptable

После тестирования веб-сервера, было проведено тестирование на VSFTPD сервер, цель данного тестирование заключалось в перехвате пакетов при подключении к серверу VSFTPD. На рисунке 8 видно, что при попытке авторизации пользователя на сервере его login и пароль передается без шифрования, что может привести к утечке данных пользователя, если нарушитель имеет доступ к сети организации.

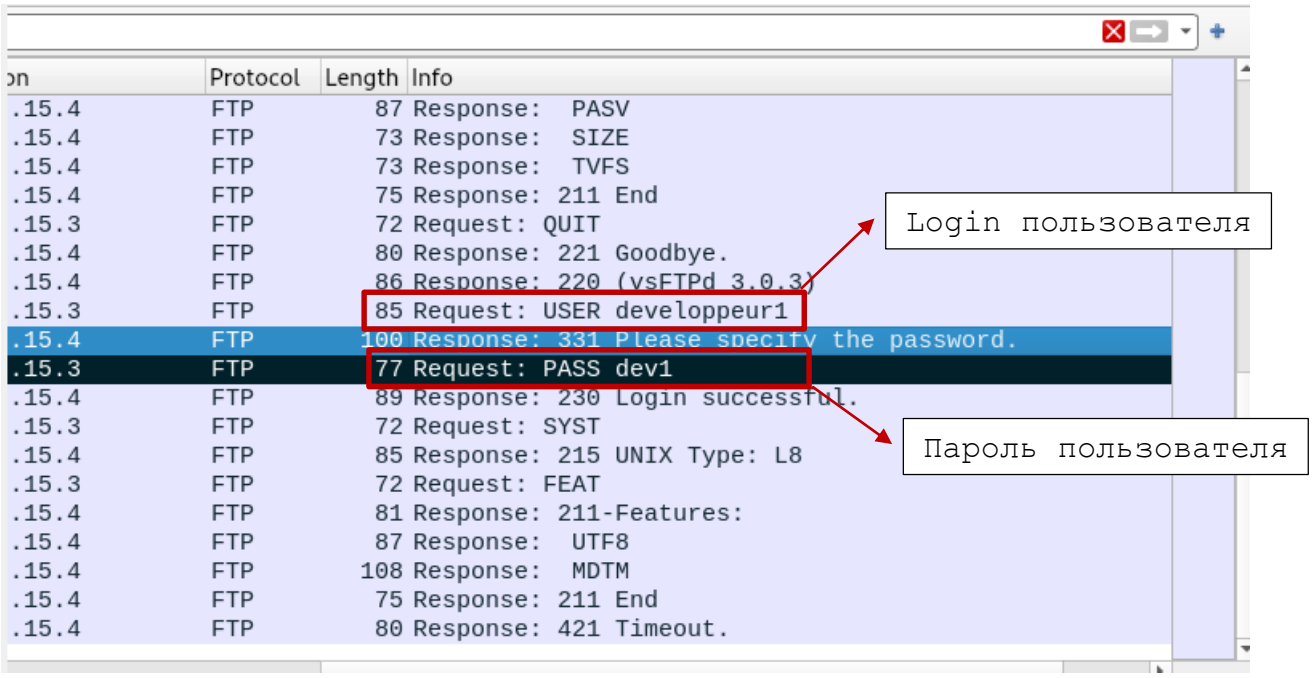

Рисунок 8 – Результат перехвата пакеты FTP при подключений

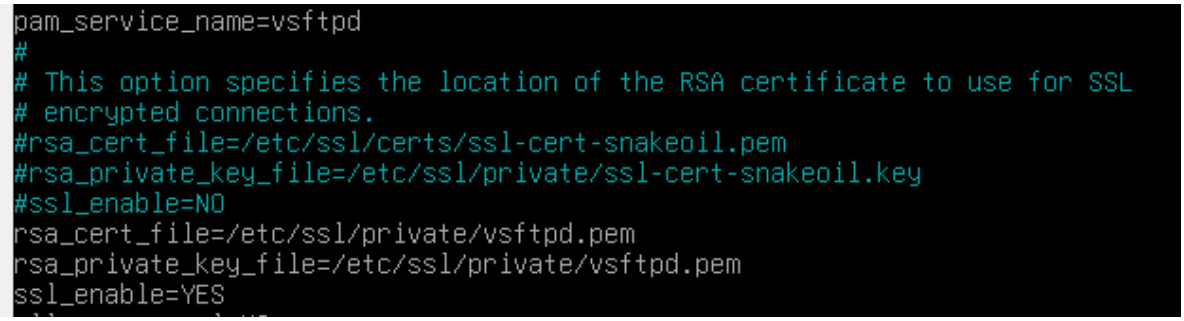

Рисунок 9 – Рекомендация для устранение уязвимости связана с FTP протоколом

Таким образом, посредством методики тестирования были составлены рекомендации по совершенствованию информационной безопасности корпоративной сети, которые включают следующие действия: стратегия и политика, технические меры, использование процессов и процедур, инфраструктура, которая должна состоят из облачных сервисов и виртуализации, для упрощения управления и обеспечения безопасности серверов и других сетевых устройств.

ЗАКЛЮЧЕНИЕ

В ходе работы над диссертацией были изучены основные архитектуры защищенных локальных сетей, такие как распределенная, централизованная и централизованно-распределенная архитектура. Были также изучены разные методики такие как OSSTMM, OWASP. Проведен анализ стандартов проведения тестирования на проникновение PTES и стандарт NIST SP 800–115.

Была также смоделирована корпоративная сеть с помощью GNS3 для создания серверов, на которых проводилась апробация методики тестирования. После моделирования, осуществлены кибератаки на данную сеть такие как ARP-spoofing и DDoS. Таким образом показано, что разработанная модель сети, является уязвимой к различным кибератакам.

В разработанной методике тестирования безопасности корпоративной сети описана последовательность действий, имитирующих действия нарушителя. В результате апробации методики на сервера корпоративной сети были выявлены уязвимости, связанные с социальной инженерии, DDoS-атаки и уязвимость VSFTPD, которая передавала login и пароли пользователей по сети в открытом виде. В разработанной методике для каждой из выявленных уязвимостей был предложен способ их устранения.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Тезисы конференций

1–А. Самаке, Б. А. Модель эксплуатации уязвимости ARP-протокола / Самаке Б. А. // Информационная безопасность : сборник материалов 59-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 17–21 апреля 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023. – С. 52–54.

2–А. Самаке, Б. А. Анализ и защита от DDoS-атак в сетях на базе GNS3 / Самаке Б. А. // Информационная безопасность : сборник материалов 60-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 22–26 апреля 2024 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2024.