Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 12.04.2023 10:47:35
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_23_»_03_____ 2023 г.

ИЗУЧЕНИЕ МЕХАНИЗМОВ БЕЗОПАСНОСТИ СЕТЕЙ WI-FI

Методические указания по выполнению лабораторных работ для студентов укрупненной группы специальностей и направлений подготовки 10.00.00

Курск 2023

УДК 004.056.5

Составитель: А.В. Митрофанов

Рецензент

Кандидат технических наук, доцент кафедры «Информационная безопасность» А.Л. Марухленко

Изучение механизмов безопасности сетей Wi-Fi: методические указания по выполнению лабораторной работы по дисциплине «Проектирование защищенных телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: А.В. Митрофанов. Курск, 2023. 10с. Библиогр.: с. 10.

Рассматриваются методы защиты беспроводной сети WI-FI. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания по выполнению лабораторных работ по дисциплине «Проектирование защищенных телекоммуникационных систем», предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00

Текст печатается в авторской редакции

Подписано в печать _____. Формат 60×84 1/16.
Усл.печ.л. . Уч.-изд.л. . Тираж 50 экз. Заказ 136. Бесплатно
Юго–Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ЦЕЛЬ РАБОТЫ

Изучение механизмов обеспечения безопасности беспроводной Wi-Fi сети на базе Windows клиентов.

Изучить технологии:

– Шифрование WEP/WPA/WPA2/AES;
– Фильтрация MAC-адресов;
– Запрет широковещания SSID.

ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

Под беспроводной сетью будем понимать такую сеть, в которой есть хотя бы один сегмент, соединяющий два и более беспроводных устройства по радиоканалу стандарта 802.11. Топологически такие сети можно разделить на два вида: с точкой доступа (через сервер с радиоустройством, одновременно подключенный к радиосети), ad hoc (клиенты взаимодействуют напрямую без точки доступа).

Рассмотрим беспроводную сеть с точкой доступа, реализованная по любому коммерческому стандарту 802.11 (a, b, g, i), кроме 802.1x. Вне зависимости от количества точек доступа беспроводной сетевой сегмент идентифицируется единственным идентификатором (SSID). Существуют три встроенных механизма безопасности для защиты беспроводных сетей: проверка подлинности, шифрование, WPA.

Подлинность проверяется двумя механизмами: открытой проверкой (на точке доступа задаются ограничения MAC-адресов беспроводных сетевых устройств), закрытым ключом (пользователям беспроводной сети сообщается пароль, который они вводят вручную при установке соединения).

Шифрование в беспроводных сетях осуществляется по алгоритму RC4. Шифрование поддерживает два вида ключей: глобальный и сеансовый. Глобальный ключ применяется для защиты группового и широковещательного исходящего трафика точки доступа, а сеансовый ключ – для одноадресного исходящего трафика точки доступа, а также группового и широковещательного

входящего трафика точки доступа. Оба типа ключей распространяются между клиентами сети и вводятся вручную.

WPA обеспечивает улучшенное шифрование по протоколу TKIP, который контролирует и целостность данных. Проверка подлинности проверяется протоколом IAP.

Через беспроводные сети могут осуществляться следующие виды атак:

– перехват трафика,

– взлом адресов протокола ARP,

– атаки вирусов, попавших в сеть с компьютера взломщика,

– перенаправления (в данном случае осуществляется взлом на уровне SSL. Взломщик подделывает MAC-адрес точки доступа и направляет пользователю запрос на прием удостоверений нового сервера, подконтрольного ему.),

– несанкционированные подключения (к любой беспроводной сети можно подключить, приблизившись на достаточное расстояние. При использовании открытой системы идентификации любой может получить доступ к корпоративной сети.),

– подключение несанкционированных точек доступа (пользователи могут сами установить необходимое оборудование, не включив на нем защитных механизмов), перегрузка сети (атака типа DoS),

– радиопомехи.

Чтобы усилить защиту беспроводной сети следует:

– изменить заводской SSID,

– отключить широковещательную рассылку SSID,

– необходимо использовать шифрование с уникальными ключами,

– защитить протокол SSNP (изменить сообщество для этого протокола, заданное по умолчанию, продумать защиту от PROTOS),

– использовать фильтрацию MAC-адресов, установив в списке допустимых беспроводных клиентов,

– совместно со службой безопасности предприятия нужно бороться с установкой несанкционированных точек доступа

(необходимо проверять какое оборудование вносят на предприятие и обнаруживать точки доступа с помощью SSNP-агентов.

Безусловно необходимо уделить внимание выбору и установке антенн у точек доступа. По возможности нужно использовать антенны направленного действия или передатчики с малым радиусом действия, чтобы не расширять территориальных границ беспроводной сети. Целесообразно считать точку доступа частью демилитаризованной зоны или сети, не пользующейся доверием. Поэтому рекомендуется отделять точки доступа от проводных сетей брандмауэром.

Качественным скачком в безопасности беспроводных сетей является стандарт 802.1x. Он позволяет использовать максимально безопасную проверку подлинности беспроводных клиентов и осуществлять безопасную шифрованную передачу данных. В этом стандарте для шифрования используются динамические ключи, которые не нужно устанавливать вручную. Однако для внедрения данного стандарта необходимо три вещи:

– для аутентификации клиентов беспроводной сети необходимо настраивать RADIUS-сервер со специальной политикой удаленного доступа для беспроводных сетей;

– в организации должна быть внедрена система Открытых ключей, т.к. для проверки подлинности стандарт 802.1x использует протокол EAP-TLS;

– точку доступа можно организовать только под WS2003, а беспроводные клиенты должны управляться Windows XP SP1 или выше.

Таким образом, внедрение RADIUS-сервера может потребовать коренного изменения топологии корпоративной сети. Внедрение системы Открытых ключей потребует либо развертывание собственной иерархии центров сертификации, или приобретение сертификатов у сторонних фирм. Внедрение стандарта 802.1x обеспечивает максимальный уровень защиты беспроводной сети, но требует большой административной настройки и финансовых затрат.

ЗАДАНИЕ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1) Соберите топологию сети, представленную на рисунке 1.

Рисунок 1 – Сеть «Ad–Hoc»

2) Настройте сеть в режиме Ad-Hoc, используя два ноутбука, на основе WEP– шифрования.

3) Используя утилиту «Speed Test» сравните полезную пропускную способность канала до и после использования WEP шифрования.

4) Соберите топологию, представленную на рисунке 2.

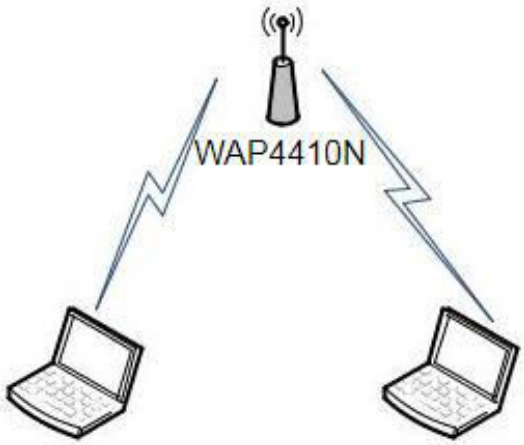

Рисунок 2 – Режим «точка доступа»

5) Настройте защищенную беспроводную сеть (режим инфраструктуры) с использованием WEP шифрования.

6) Используя утилиту «Speed Test» сравните полезную пропускную способность канала до и после использования WEP шифрования.

7) Используя утилиту «Wireshark» осуществите перехват пакетов. Изучите содержимое перехваченных пакетов до и после применения шифрования. Расскажите о результатах преподавателю.

8) Используя сеть, представленную на рисунке 2, настройте защищенную сеть (режим инфраструктуры) с использованием аутентификации WPA и алгоритмом шифрования TKIP.

9) Используя утилиту «Speed Test», сравните полезную пропускную способность канала до и после использования WPA.

10) Используя утилиту «Wireshark» осуществите перехват пакетов. Изучите содержимое перехваченных пакетов до и после применения WPA. Сравните с результатами, полученными с использованием WEP шифрования. Расскажите о результатах преподавателю.

11) Используя сеть, представленную на рисунке 2, настройте защищенную сеть (режим инфраструктуры) с использованием аутентификации WPA2/PSK и системой шифрования TKIP.

12) Используя утилиту «Speed Test», сравните полезную пропускную способность канала до и после использования WPA2/PSK.

13) Используя сеть, представленную на рисунке 2, настройте защищенную сеть (режим инфраструктуры) с использованием аутентификации WPA2/PSK и системой шифрования AES

14) Используя утилиту «Speed Test», сравните полезную пропускную способность канала с использованием системы шифрования TKIP с системой шифрования AES.

15) Постройте сеть, топология которой представлена на рисунке 3.

16) Настройте защищенную сеть (режим инфраструктуры) с использованием аутентификации WPA2/EAP и системой шифрования TKIP.

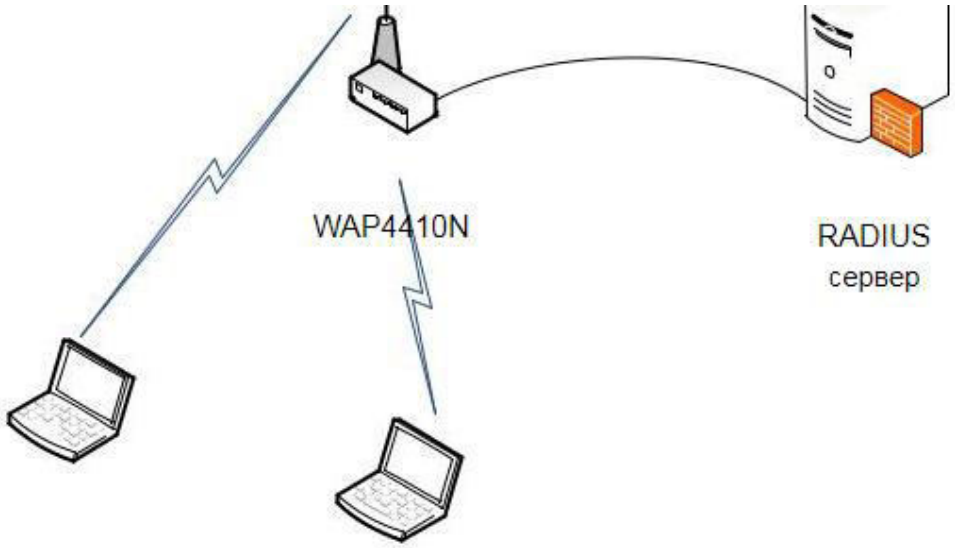

Рисунок 3 – Использование RADIUS-сервера

17) Используя утилиту freeradius, настройте RADIUS-сервертаким образом, чтобы только абоненты, занесенные в базу данных пользователей смогли пройти процедуру аутентификации.

18) Отключите в настройках точки доступа широковещание SSID.

19) На клиентских машинах настройте встроенные беспроводные адаптеры средствами ОС Windows. В параметрах настройки укажите в поле SSID имя сети, указанное в настройках точки доступа. Проверьте работоспособность вашей сети.

20) Как ведет себя точка доступа при отключении SSID? Для чего нужна эта функция?

21) Соберите топологию, представленную на рисунке 4.

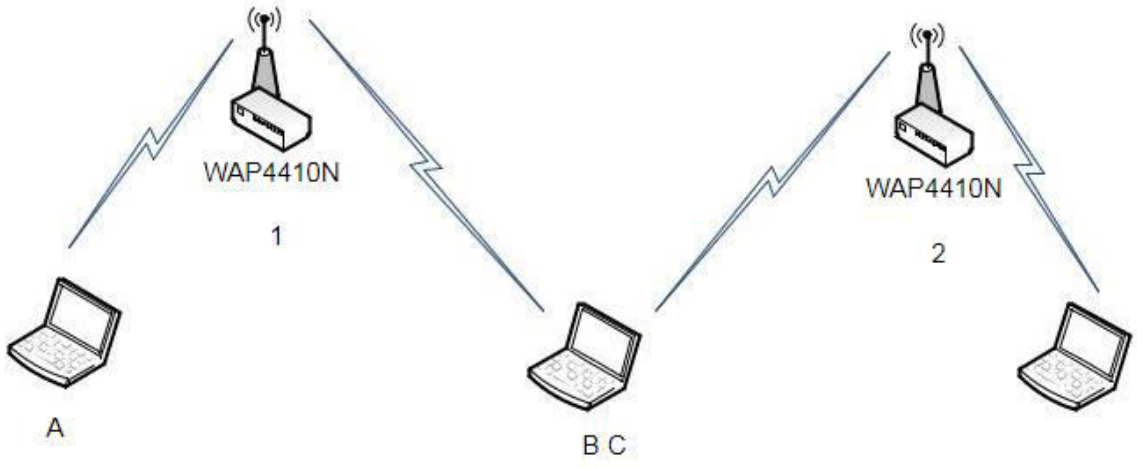

Рисунок 4 – Использование фильтрации по MAC-адресам

22) К точке доступа 1 разрешить подключение ноутбуков A и B с помощью разрешенных списков MAC-адресов. К точке

доступа 2 запретить подключение с ноутбука А с помощью запрещенных списков MAC-адресов.

23) Проверьте правильность выполненных настроек.

24) Подготовьте отчет о проделанной работе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Шувалов В.П., Величко В.В., Субботин Е.А., Ярославцев А.Ф. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети (2005)

2) Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

3) Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2-е изд. – М.: Горячая линия – Телеком, 2003.–232 с.

4) Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. - СПб.: БХВ-Петербург, 2010. - 400 с.

5) Башарин Г.П. Лекции по математической теории телетрафика: Учеб. пособие. Изд. 3-е, испр. и доп. - М.: РУДН, 2009.-342 с.

6) Буч Г. Объектно-ориентированный анализ и проектирование. – М.: Вильямс, 2008.

7) Леоненков А.В. Самоучитель языка UML. – СПб.: БХВ-Петербург, 2004.

8) Розенберг Д., Скотт К. Применение объектного моделирования с использованием UML и анализ прецедентов. – М.: ДМК Пресс, 2002.

9) А.В. Росляков. Виртуальные частные сети. Основы построения и применения. - М.: Эко-Трендз, 2006. - 242 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_23_» _03_ 2023 г.

РАЗРАБОТКА ПРОЕКТА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

Методические указания по выполнению лабораторных работ для студентов укрупненной группы специальностей и направлений подготовки 10.00.00

Курск 2023

УДК 004.056.5

Составитель: А.В. Митрофанов

Рецензент

Кандидат технических наук, доцент кафедры «Информационная безопасность» А.Л. Марухленко

Разработка проекта локальной вычислительной сети предприятия: методические указания по выполнению лабораторной работы по дисциплине «Проектирование защищенных телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: А.В. Митрофанов. Курск, 2023. 10с. Библиогр.: с. 10.

Рассматриваются основные этапы проектирования локальной вычислительной сети. Указывается порядок выполнения лабораторной работы и содержание отчета.

Методические указания по выполнению лабораторных работ по дисциплине «Проектирование защищенных телекоммуникационных систем», предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00

Текст печатается в авторской редакции

Подписано в печать _____. Формат 60×84 1/16.
Усл.печ.л. . Уч.-изд.л. . Тираж 50 экз. Заказ 184. Бесплатно
Юго–Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ЦЕЛЬ РАБОТЫ

Целью выполнения лабораторной работы является формирование у студентов навыков и умений по разработке проекта локальной вычислительной сети предприятия.

ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

Локальная вычислительная сеть (ЛВС) представляет собой коммуникационную систему, объединяющую компьютеры и периферийное оборудование на ограниченной территории, обычно не больше нескольких зданий или одного предприятия. В настоящее время ЛВС стала неотъемлемым атрибутом в любых вычислительных системах, имеющих более 1 компьютера.

Основные преимущества, обеспечиваемые локальной сетью – возможность совместной работы и быстрого обмена данными, централизованное хранение данных, разделяемый доступ к общим ресурсам, таким как принтеры, сеть Internet и другие.

Еще одной важнейшей функцией локальной сети является создание отказоустойчивых систем, продолжающих функционирование (пусть и не в полном объеме) при выходе из строя некоторых входящих в них элементов. В ЛВС отказоустойчивость обеспечивается путем избыточности, дублирования; а также гибкости работы отдельных входящих в сеть частей (компьютеров).

Конечной целью создания локальной сети на предприятии или в организации является повышение эффективности работы вычислительной системы в целом.

Построение надежной ЛВС, соответствующей предъявляемым требованиям по производительности и обладающей наименьшей стоимостью, требуется начинать с составления плана. В плане сеть разделяется на сегменты, подбирается подходящая топология и аппаратное обеспечение.

Информация в локальных сетях, как правило, передается отдельными порциями, кусками, называемыми пакетами. Причем

предельная длина этих пакетов строго ограничена (обычно величиной в несколько килобайт). Ограничена длина пакета и снизу (как правило, несколькими десятками байт). Выбор пакетной передачи связан с несколькими важными соображениями.

Локальная сеть, как уже отмечалось, должна обеспечивать качественную, связь всем абонентам сети. Важнейшим параметром является так называемое время доступа к сети (access time), которое определяется как временной интервал между моментом готовности абонента к передаче (когда ему есть, что передавать) и моментом начала этой передачи. Это время ожидания абонентом начала своей передачи. Естественно, оно не должно быть слишком большим, иначе величина реальной, интегральной скорости передачи информации между приложениями сильно уменьшится даже при высокоскоростной связи.

Ожидание начала передачи связано с тем, что в сети не может происходить несколько передач одновременно (во всяком случае, при топологиях шина и кольцо). Всегда есть только один передатчик и один приемник (реже – несколько приемников). В противном случае информация от разных передатчиков смешивается и искажается. В связи с этим абоненты передают свою информацию по очереди. И каждому абоненту, прежде чем начать передачу, надо дождаться своей очереди. Вот это время ожидания своей очереди и есть время доступа.

Если бы вся требуемая информация передавалась каким-то абонентом сразу, непрерывно, без разделения на пакеты, то это привело бы к монопольному захвату сети этим абонентом на довольно продолжительное время. Все остальные абоненты вынуждены были бы ждать окончания передачи всей информации, что в ряде случаев могло бы потребовать десятков секунд и даже минут (например, при копировании содержимого целого жесткого диска). С тем чтобы уравнять в правах всех абонентов, а также сделать примерно одинаковыми для всех них величину времени доступа к сети и интегральную скорость передачи информации, как раз и применяются пакеты ограниченной длины.

Каждый пакет помимо собственно данных, которые требуется передать, должен содержать некоторое количество служебной информации. Прежде всего, это адресная информация, которая определяет, от кого и кому передается данный пакет.

Таким образом, процесс информационного обмена в сети представляет собой чередование пакетов, каждый из которых содержит информацию, передаваемую от абонента к абоненту.Термин «топология», или «топология сети», характеризует физическое расположение компьютеров, кабелей и других компонентов сети. Топология — это стандартный термин, который используется профессионалами при описании основной компоновки сети. Топология сети обуславливает ее характеристики. В частности, выбор той или иной топологии влияет:

- на состав необходимого сетевого оборудования;
- характеристики сетевого оборудования;
- возможности расширения сети;
- способ управления сетью.

На сегодняшний день подавляющая часть компьютерных сетей использует для соединения провода или кабели. Они выступают в качестве среды передачи сигналов между компьютерами. Существуют различные типы кабелей, которые удовлетворяют потребности всевозможных сетей, от малых до больших.

Выделяют три основные группы кабелей:

- коаксиальный кабель (coaxial cable);
- витая пара (twisted pair):
  - неэкранированная (unshielded);
  - экранированная (shielded);
- оптоволоконный кабель (fiber optic).

Конечное сетевое оборудование является источником и получателем информации, передаваемой по сети:

- Компьютер (рабочая станция), подключенный к сети, является самым универсальным узлом. Прикладное использование компьютера в сети определяется программным обеспечением и установленным дополнительным оборудованием. Для дальних коммуникаций используется модем, внутренний или внешний. С точки зрения сети, «лицом» компьютера является его сетевой адаптер. Тип сетевого адаптера должен соответствовать назначению компьютера и его сетевой активности.

- Сервер является также компьютером, но с большими ресурсами. Это подразумевает его более высокую сетевую активность и значимость. Серверы желательно подключать к выделенному порту коммутатора. При установке двух и более сетевых интерфейсов (в том числе и модемного подключения) и соответствующего программного обеспечения сервер может играть роль маршрутизатора или моста. Серверы, как правило, должны иметь высокопроизводительную операционную систему.

Для надёжной работы и повышения производительности сети следует вносить изменения в структуру сети только с учётом требований стандарта.

Для защиты данных от вирусов необходимо установить антивирусные программы, а для восстановления повреждённых или ошибочно удалённых данных следует использовать специальные утилиты.

Следует беречь сетевой трафик, поэтому с помощью программы для администрирования следить за целевым использованием внутрисетевого и интернет-трафика. Также следует разделить во времени загрузку информации из другого сегмента т.е. постараться чтобы каждый сегмент обращался к другому в отведённое ему время. Установка программ, не имеющих отношения к непосредственной области деятельности компании, должна пресекаться администратором. При монтаже сети необходимо маркировать кабель, чтобы не столкнуться с трудностями при обслуживании сети.

Монтаж сети следует осуществлять через существующие каналы и короба.

Для надежной работы сети необходимо наличие сотрудника отвечающего за всю локальную сеть и занимающегося ее оптимизацией и повышением производительности.

Периферийное (принтеры, сканеры, проекторы) оборудование следует устанавливать уже после конкретного распределения обязанностей рабочих станций.

В целях профилактики следует периодически проверять целостность кабелей в секретном полу. При демонтаже оборудования следует аккуратно обращаться с оборудованием, для возможности его последующего использования.

Кроме того, необходимо ограничить доступ в серверную комнату и к тумбам с коммутаторами.

Лабораторная работа предполагает развитие **следующих умений и навыков**:

– развитие практических умений по разработке проекта локальной сети;

– применение современного оборудования, технологий и программных продуктов;

– проведение технико-экономического обоснования внедрения оборудования;

– применение мер безопасности для сохранения конфиденциальности информации.

ЗАДАНИЕ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Необходимо обеспечить локальной сетью Фирму, состоящую из «А» сотрудников, занимающую «Б» этажей в одном здании, размещающуюся в «В» комнатах (кол-во комнат на этажах выбрать самостоятельно). Предусмотреть увеличение штата работников до «Г» человек. (Значения А,Б,В,Г указаны в таблице №1).

Таблица 1 – Варианты заданий

№ варианта	«А»	«Б»	«В»	«Г»
1	10	2	3	5
2	12	1	4	5
3	12	2	3	8
4	10	1	2	5
5	7	1	2	3
6	8	1	4	5
7	9	1	3	7
8	10	2	2	5
9	12	2	5	5
10	12	1	2	8

2. Разработать проект локальной сети для Фирмы, учитывая следующее:

- у каждого сотрудника есть компьютер;

- информация хранимая и обрабатываемая на компьютерах строго конфиденциальна;
- планируется установка МФУ (выбрать оптимальное кол-во МФУ для нормальной работы фирмы);
- необходим сервер для хранения информации.

3. Проект локальной сети должен включать:

- примерный план размещения сотрудников по комнатам;
- перечень необходимого сетевого оборудования с обоснованием выбора;
- описание топологии, которой Вы будете придерживаться, проектируя сеть, обосновать выбор.
- описание мер безопасности для сохранения конфиденциальности информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Шувалов В.П., Величко В.В., Субботин Е.А., Ярославцев А.Ф. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети (2005)

2) Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

3) Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2-е изд. – М.: Горячая линия – Телеком, 2003. – 232 с.

4) Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. - СПб.: БХВ-Петербург, 2010. - 400 с.

5) Башарин Г.П. Лекции по математической теории телетрафика: Учеб. пособие. Изд. 3-е, испр. и доп. - М.: РУДН, 2009. - 342 с.

6) Буч Г. Объектно-ориентированный анализ и проектирование. – М.: Вильямс, 2008.

7) Леоненков А.В. Самоучитель языка UML. – СПб.: БХВ-Петербург, 2004.

8) Розенберг Д., Скотт К. Применение объектного моделирования с использованием UML и анализ прецедентов. – М.: ДМК Пресс, 2002.

9) А.В. Росляков. Виртуальные частные сети. Основы построения и применения. - М.: Эко-Трендз, 2006. - 242 с.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«23» 03 2023 г.

УСТРАНЕНИЕ УЯЗВИМОСТЕЙ СЕТЕВЫХ ПОРТОВ

Методические указания по выполнению лабораторных работ для студентов укрупненной группы специальностей и направлений подготовки 10.00.00

Курск 2023

УДК 004.056.5

Составитель: А.В. Митрофанов

Рецензент

Кандидат технических наук, доцент кафедры «Информационная безопасность» А.Л. Марухленко

Устранение уязвимостей сетевых портов: методические указания по выполнению лабораторной работы по дисциплине «Проектирование защищенных телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: А.В. Митрофанов. Курск, 2023. 10 с. Библиогр.: с. 10.

Рассматриваются особенности протокола NetBIOS. Указывается порядок выполнения лабораторной работы, теоретические сведения и необходимый для выполнения перечень литературы.

Методические указания по выполнению лабораторных работ по дисциплине «Проектирование защищенных телекоммуникационных систем», предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00

Текст печатается в авторской редакции

Подписано в печать _____. Формат 60×84 1/16.
Усл.печ.л. . Уч.-изд.л. . Тираж 50 экз. Заказ 175. Бесплатно
Юго–Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ЦЕЛЬ РАБОТЫ

По результатам сканирования сетевых портов на машине с установленным брандмауэром, произвести его настройку для скрытия или устранения найденных уязвимостей.

ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

Выполнение данной лабораторной работы заключается в том, чтобы правильно настроить брандмауэр для устранения или скрытия найденных ранее уязвимостей. Данная работа посвящена настройке правил реагирования брандмауэра на различные события. Для выполнения работы необходимо изучить и освоить работу брандмауэра. Agnitum Outpost Firewall Pro версии 4.0

Протокол NetBIOS был создан для работы в локальных сетях. Система NetBIOS предназначена для персональных ЭВМ типа IBM/PC в качестве интерфейса, независящего от фирмы-производителя. NetBIOS использует в качестве транспортных протоколов TCP и UDP. Описание NetBIOS содержится в документе IBM 6322916 "Technical Reference PC Network".

Пакет NETBIOS создан для использования группой ЭВМ, поддерживает как режим сессий (работа через соединение), так и режим дейтограмм (без установления соединения). 16-и символьные имена объектов в netbios распределяются динамически. netbios имеет собственную dns, которая может взаимодействовать с интернетовским. Имя объекта при работе с NETBIOS не может начинаться с символа *.

Приложения могут через netbios найти нужные им ресурсы, установить связь и послать или получить информацию. NETBIOS использует для службы имен порт - 137, для службы дейтограмм - порт 138, а для сессий - порт 139.

Любая сессия начинается с netbios-запроса, задания ip-адреса и определения tcp-порта удаленного объекта, далее следует обмен NETBIOS-сообщениями, после чего сессия закрывается. Сессия осуществляет обмен информацией между двумя netbios-

приложениями. Длина сообщения лежит в пределах от 0 до 131071 байт. Допустимо одновременное осуществление нескольких сессий между двумя объектами.

При организации IP-транспорта через NETBIOS IP-дейтограмма вкладывается в NETBIOS-пакет. Информационный обмен происходит в этом случае без установления связи между объектами. Имена Netbios должны содержать в себе IP-адреса. Так часть NETBIOS-адреса может иметь вид, ip.**.**.**.**, где IP указывает на тип операции (IP через Netbios), а **.**.**.** - ip-адрес. Система netbios имеет собственную систему команд (call, listen, hang up, send, receive, session status, reset, cancel, adapter status, unlink, remote program load) и примитивов для работы с дейтограммами (send datagram, send broadcast datagram, receive datagram, receive broadcast datagram). Все оконечные узлы netbios делятся на три типа: широковещательные ("b") узлы; узлы точка-точка ("p"); узлы смешанного типа ("m").

IP-адрес может ассоциироваться с одним из указанных типов. B-узлы устанавливают связь со своим партнером посредством широковещательных запросов. P- и M-узлы для этой цели используют netbios сервер имен (NBNS) и сервер распределения дейтограмм (NBDD).

После сканирования удаленной виртуальной машины с установленным брандмауэром со стандартными настройками, сканер находит несколько уязвимостей, в том числе, и уязвимость по сессии NetBIOS на 139 порту. Для устранения данной проблемы необходимо использовать обходной путь, потому что «грубо» этот порт закрыть нельзя. Чтобы устранить проблему 139-го порта, необходимо определить доверенную группу IP-адресов, члены которой смогут взаимодействовать по сети. Для других уязвимых портов необходимо создать правило реагирования брандмауэра. Глобальные правила брандмауэра применяются ко всем процессам и приложениям на вашем компьютере, которые запрашивают доступ в сеть. Например, создав соответствующие правила, вы можете блокировать весь трафик, идущий по данному протоколу или с данного удаленного узла. Некоторые из установок глобальных правил, подобранные оптимальным образом, Outpost Firewall Pro задает по умолчанию.:

Каждый компьютер в локальной сети может получить один из трех уровней доступа к компьютеру:

- NetBIOS. Разрешает разделение доступа к файлам и принтерам между компьютером из локальной сети и вашим компьютером. Чтобы установить этот уровень, отметьте соответствующий флажок NetBIOS для этого адреса;

- Доверенные. Все соединения к и из этой сети разрешены. Чтобы установить этот уровень, отметьте флажок Доверенные для этого адреса;.

- Ограниченный доступ к LAN. NetBIOS соединения блокируются, все остальные соединения обрабатываются, согласно глобальным правилам и правилам для приложений. Чтобы установить этот уровень, уберите оба флажка NetBIOS и Доверенные для этого адреса.

Важно помнить, что узел, относящийся к числу Доверенных, имеет наивысший приоритет. С таким узлом могут соединяться даже запрещенные приложения. Рекомендуется помещать в список Доверенных только СОВЕРШЕННО БЕЗОПАСНЫЕ компьютеры. Если вам нужно только разделение доступа к файлам и принтерам, лучше использовать уровень NetBIOS, а не Доверенные. Нажав на кнопку «добавить», в обработку можно включить как отдельный IP-адрес, так и диапазон IP-адресов или отдельный домен.

Одной из наиболее важных характеристик системы Agnitum Outpost Firewall Pro является политика или режим работы с сетью. Существует пять режимов или политик с сетью.

Режим бездействия (Отключить) – разрешены все сетевые взаимодействия; брандмауэр отключен.

Режим разрешения (Разрешить) – разрешены все сетевые взаимодействия, которые явно не заблокированы.

Режим обучения (Обучения) – первое сетевое взаимодействие каждого приложения сопровождается предупреждением и дает вам возможность создать правило для работы этого приложения с сетью. Созданное правило будет немедленно задействовано брандмауэром для обработки соединений.

Режим блокировки (Блокировать) – запрещены все сетевые взаимодействия, за исключением явно разрешенных. Для каждого приложения, которому необходим доступ в Интернет, потребуется создать правило брандмауэра.

Блокировать все (Запрещать) – запрещены сетевые взаимодействия.

Сразу после установки программа по умолчанию функционирует в режиме обучения. Этот режим выявляет любые приложения, взаимодействующие с сетью, и выдает диалог с предупреждением сообщающем. Это все данные о приложение (т.е, в каком направлении запрашивается соединение, исходящие или входящие, через какой порт и по какому протоколу). Основываясь на предупреждении, пользователь выбирает соответствующие действия. Он может разрешить приложению выполнять любые действия либо запретить. Также можно создать правило, где все параметры задаются пользователем.

ЗАДАНИЕ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Задание:

1) Защитить машину брандмауэром и произвести сканирование.
2) Произвести настройку брандмауэра для устранения или скрытия найденных путем сканирования портов уязвимостей
3) Запретить доступ на виртуальной машине для HOST-компьютера и осуществить новое сканирование на уязвимости.
4) По завершении сканирования создать отчет и сравнить с сохраненными ранее.
5) Настроить правила для портов согласно Таблице №1.

Таблица 1 – Варианты заданий

№ варианта	Задание
1	Запретить исходящее соединение по протоколу TCP с адресом 192.168.120.1 через порт 110;
2	Запретить входящие данные по протоколу UDP от адреса 192.168.124.0 через порт 4000. При попытке установления связи через данный порт и адрес автоматически запустить антивирусную программу;
3	Разрешить входящие данные по протоколу IP, где протокол: 6 – Transmission Control Protocol, для IP-адресов следующего диапазона: 192.168.10.0-192.168.11.255;

№ варианта	Задание
4	Разрешить исходящее соединение для адреса 192.168.0.1
5	Запретить исходящее соединение с адресом 192.168.0.12 по протоколу TCP с портом 43;
6	Разрешить входящее соединение по протоколу IP с диапазоном адресов 192.168.0.1-192.168.3.255, где протокол: Internet Control Message Protocol-1;
7	Запретить входящие данные по протоколу UDP для диапазона адресов: 192.168.12.3-192.168.13.255;
8	Запретить исходящие данные по протоколу TCP по порту 145 для диапазона адресов: 192.168.12.3-192.168.13.255;
9	Разрешить исходящие данные для адреса 192.168.0.34 по протоколу TCP для порта 4000;
10	Запретить входящие данные по протоколу IP, где протокол: Internet Control Message Protocol-1, для диапазона адресов: 192.168.12.3-192.168.13.255.

Порядок выполнения работы:

1) Для того, чтобы просмотреть список глобальных правил, щелкните на панели инструментов кнопку Параметры, выберите вкладку Системные и щелкните Правила в группе Глобальные правила и доступ к rawsocket.

2) Для того, чтобы добавить новое правило, щелкните Добавить в окне диалога Глобальные правила. В окне редактирования правила укажите параметры.

3) Выберите событие для правила.

4) Выберите действие для правила.

5) Для защиты сессии NetBIOS необходимо добавить в область сетевого взаимодействия лишь те IP-адреса, которым вы полностью доверяете. Для этого перейдите в настройку системных параметров брандмауэра и нажмите на кнопку «Параметры» для настройки локальной сети. Нажав на кнопку «добавить», в обработку можно включить как отдельный IP-адрес, так и диапазон IP-адресов или отдельный домен

6) Выберите действия - соответствующие сообщения появятся в поле Описание правила. Если вы хотите, чтобы действием на событие стал запуск определенного приложения или команды, поставьте флажок в соответствующем поле и укажите приложение или команду, нажав на подчеркнутое значение в поле Описание правила.

7) Убедитесь, что в поле Описание правила не осталось неопределенных параметров. Outpost Firewall Pro автоматически сгенерирует Имя правила на основе заданных параметров. Щелкните OK, чтобы сохранить правило. Правило отобразится в списке.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Шувалов В.П., Величко В.В., Субботин Е.А., Ярославцев А.Ф. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети (2005)

2) Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

3) Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2-е изд. – М.: Горячая линия – Телеком, 2003.–232 с.

4) Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. - СПб.: БХВ-Петербург, 2010. - 400 с.

5) Башарин Г.П. Лекции по математической теории телетрафика: Учеб. пособие. Изд. 3-е, испр. и доп. - М.: РУДН, 2009.-342 с.

6) Буч Г. Объектно-ориентированный анализ и проектирование. – М.: Вильямс, 2008.

7) Леоненков А.В. Самоучитель языка UML. – СПб.: БХВ-Петербург, 2004.

8) Розенберг Д., Скотт К. Применение объектного моделирования с использованием UML и анализ прецедентов. – М.: ДМК Пресс, 2002.

9) А.В. Росляков. Виртуальные частные сети. Основы построения и применения. - М.: Эко-Трендз, 2006. - 242 с.