

Министерство науки и высшего образования Российской Федерации

Калужский филиал
федерального государственного бюджетного образовательного
учреждения высшего образования
**«Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)»**
(КФ МГТУ им. Н.Э. Баумана)

Ю.С. Белов, А.Н. Молчанов

АНАЛИЗ УЯЗВИМОСТЕЙ В БЕСПРОВОДНЫХ СЕТЯХ
Методические указания к выполнению лабораторной работы
по курсу «Беспроводные технологии передачи данных»


Калуга – 2019

УДК 004.71
ББК 32.972.5
Б435


Методические указания составлены в соответствии с учебным планом КФ МГТУ им. Н.Э. Баумана по направлению подготовки 09.03.04 «Программная инженерия» кафедры «Программного обеспечения ЭВМ, информационных технологий».

Методические указания рассмотрены и одобрены:


- Кафедрой «Программного обеспечения ЭВМ, информационных технологий» (ИУ4-КФ) протокол № 51.4/6 от «20» февраля 2019 г.


Зав. кафедрой ИУ4-КФ  к.т.н., доцент Ю.Е. Гагарин

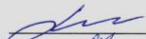

- Методической комиссией факультета ИУ-КФ протокол № 9 от «04» 03 2019 г.

Председатель методической комиссии факультета ИУ-КФ  к.т.н., доцент М.Ю. Адкин

- Методической комиссией КФ МГТУ им.Н.Э. Баумана протокол № 5 от «5» 03 2019 г.

Председатель методической комиссии КФ МГТУ им.Н.Э. Баумана  д.э.н., профессор О.Л. Перерва

Рецензент:
к.т.н., доцент кафедры ИУ3-КФ  А.В. Фиошин

Авторы
к.ф.-м.н., доцент кафедры ИУ4-КФ  Ю.С. Белов
ст. преп. кафедры ИУ6-КФ  А.Н. Молчанов

Аннотация

Методические указания по выполнению лабораторной работы по курсу «Беспроводные технологии передачи данных» содержат описание механизмов обеспечения безопасности в беспроводных сетях и анализа уязвимостей в беспроводных сетях.

Предназначены для студентов 4-го курса бакалавриата КФ МГТУ им. Н.Э. Баумана, обучающихся по направлению подготовки 09.03.04 «Программная инженерия».

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
ЦЕЛЬ И ЗАДАЧИ РАБОТЫ, ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ЕЕ ВЫПОЛНЕНИЯ.....	5
КРАТКАЯ ХАРАКТЕРИСТИКА ОБЪЕКТА ИЗУЧЕНИЯ, ИССЛЕДОВАНИЯ	6
ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ	27
КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ	28
ФОРМА ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ	28
ОСНОВНАЯ ЛИТЕРАТУРА.....	29
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА	29

ВВЕДЕНИЕ

Настоящие методические указания составлены в соответствии с программой проведения лабораторных работ по курсу «Беспроводные технологии передачи данных» на кафедре «Программное обеспечение ЭВМ, информационные технологии» факультета «Информатика и управление» Калужского филиала МГТУ им. Н.Э. Баумана.

Методические указания, ориентированные на студентов 4-го курса направления подготовки 09.03.04 «Программная инженерия», содержат краткое описание настройки безопасности в беспроводных сетях, анализа уязвимостей в беспроводных сетях и задание на выполнение лабораторной работы.

Методические указания составлены для ознакомления студентов с возможностями оборудования для беспроводных локальных сетей. Для выполнения лабораторной работы студенту необходимы минимальные знания архитектуры ЭВМ, компьютерных сетей и технологии локальных вычислительных сетей.

ЦЕЛЬ И ЗАДАЧИ РАБОТЫ, ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ЕЕ ВЫПОЛНЕНИЯ

Целью выполнения лабораторной работы является получение практических навыков анализа уязвимостей при передаче данных в беспроводных сетях.

Основными задачами выполнения лабораторной работы являются:

1. Ознакомиться с наиболее распространенными уязвимостями в беспроводных сетях.
2. Научиться использовать механизмы поиска уязвимостей в беспроводных сетях.
3. Ознакомиться с основными методами повышения безопасности передаваемых данных.

Результатами работы являются:

- Проведенная на беспроводную сеть «атака по середине», позволяющая прослушивать клиентский трафик
- Подготовленный отчет

КРАТКАЯ ХАРАКТЕРИСТИКА ОБЪЕКТА ИЗУЧЕНИЯ, ИССЛЕДОВАНИЯ

Атака посредника

Атака «человек посередине», МИТМ-атака (Man in the middle) — термин в криптографии, обозначающий ситуацию, когда криптоаналитик (атакующий) способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причём ни один из последних не может догадаться о его присутствии в канале.

Метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

Принцип атаки

Атака обычно начинается с прослушивания канала связи и заканчивается тем, что криптоаналитик пытается подменить перехваченное сообщение, извлечь из него полезную информацию, перенаправить его на какой-нибудь внешний ресурс.

Предположим, объект А планирует передать объекту В некую информацию. Объект С обладает знаниями о структуре и свойствах используемого метода передачи данных, а также о факте планируемой передачи собственно информации, которую С планирует перехватить. Для совершения атаки С «представляется» объекту А как В, а объекту В — как А. Объект А, ошибочно полагая, что он направляет информацию В, посылает её объекту С. Объект С, получив информацию, и совершив с ней некоторые действия (например, скопировав или модифицировав в своих целях) пересылает данные собственно получателю — В; объект В, в свою очередь, считает, что информация была получена им напрямую от А.

Пример атаки

Предположим, что Алиса хочет передать Бобу некоторую информацию. Мэлори хочет перехватить сообщение и, возможно, изменить его так, что Боб получит неверную информацию.

Мэлори начинает свою атаку с того, что устанавливает соединение с Бобом и Алисой, при этом они не могут догадаться о том, что кто-то третий присутствует в их канале связи. Все сообщения, которые посылают Боб и Алиса, приходят Мэлори.

Алиса просит у Боба его открытый ключ. Мэлори представляется Алисе Бобом и отправляет ей свой открытый ключ. Алиса, считая, что это ключ Боба, шифрует им сообщение и отправляет его Бобу. Мэлори получает сообщение, расшифровывает, затем изменяет его, если нужно, шифрует его открытым ключом Боба и отправляет его ему. Боб получает сообщение и думает, что оно пришло от Алисы:

1. Алиса отправляет Бобу сообщение, которое перехватывает Мэлори:

Алиса «Привет Боб, Это Алиса. Пришли мне свой открытый ключ» → Мэлори Боб

2. Мэлори пересылает сообщение Бобу; Боб не может догадаться, что это сообщение не от Алисы:

Алиса Мэлори «Привет Боб, Это Алиса. Пришли мне свой открытый ключ» → Боб

3. Боб посылает свой ключ:

Алиса Мэлори ← [ключ Боба] Боб

4. Мэлори подменяет ключ Боба своим и пересылает сообщение Алисе:

Алиса ← [ключ Мэлори] Мэлори Боб

5. Алиса шифрует сообщение ключом Мэлори, считая, что это ключ Боба, и только он может расшифровать его:

Алиса «Встретимся на автобусной остановке!» [зашифровано ключом Мэлори] → Мэлори Боб

6. Мэлори расшифровывает сообщение, читает его, модифицирует его, шифрует ключом Боба и отправляет его:

Алиса Мэлори «Жди меня у входа в музей в 18:00!» [зашифровано ключом Боба] → Боб

7. Боб считает, что это сообщение Алисы.

Этот пример демонстрирует необходимость использования методов для подтверждения того, что обе стороны используют правильные открытые ключи, то есть что у стороны А открытый ключ стороны Б, а у стороны Б открытый ключ стороны А. В противном случае, канал может быть подвержен атаке «человек посередине».

Сценарий атаки

— Обмен открытыми ключами

Атаки «человек посередине» представляют угрозу для систем, совершающих финансовые операции через интернет — например, электронный бизнес, интернет-банкинг, платёжный шлюз. Применяя данный вид атаки, злоумышленник может получить доступ к учетной записи пользователя и совершать всевозможные финансовые махинации.

В случае системы с открытым ключом, криптоаналитик может перехватить сообщения обмена открытыми ключами между клиентом и сервером и изменить их, как в примере выше. Для того, чтобы оставаться незамеченным, криптоаналитик должен перехватывать все сообщения между клиентом и сервером и шифровать, и расшифровывать их соответствующими ключами. Такие действия могут показаться слишком сложными для проведения атаки, однако они представляют реальную угрозу для небезопасных сетей (например, интернет и беспроводные сети).

— Внедрение вредоносного кода

Внедрение кода в атаке «[человек посередине](#)» главным образом применяется для захвата уже авторизованной сессии, выполнения собственных команд на сервере и отправки ложных ответов клиенту.

Атака «человек посередине» позволяет криптоаналитику вставлять свой код в электронные письма, SQL выражения и веб-страницы (то есть позволяет осуществлять SQL-инъекции, HTML/script-инъекции или XSS-атаки), и даже модифицировать загружаемые пользователем бинарные файлы для того, чтобы получить доступ к учетной записи

пользователя или изменить поведение программы, загруженной пользователем из интернета.

— Downgrade Attack

Термином «Downgrade Attack» называют такую атаку, при которой криптоаналитик вынуждает пользователя использовать менее безопасные функции, протоколы, которые всё ещё поддерживаются из соображений совместимости. Такой вид атаки может быть проведён на протоколы SSH, IPsec и PPTP.

Для защиты от Downgrade Attack небезопасные протоколы должны быть отключены как минимум на одной стороне; просто поддержки и использования по умолчанию безопасных протоколов недостаточно!

SSH V1 вместо SSH V2

Атакующий может попытаться изменить параметры соединения между сервером и клиентом при установлении между ними соединения. Криптоаналитик может «заставить» клиента начать сессию SSH1 вместо SSH2 изменив номер версии «1.99» для SSH сессии на «1.51», что означает использование SSH V1. Протокол SSH-1 имеет уязвимости, которыми может воспользоваться криптоаналитик.

IPsec

При таком сценарии атаки криптоаналитик вводит свою жертву в заблуждение, заставляя её думать, что IPsec сессия не может начаться на другом конце (сервере). Это приводит к тому, что сообщения будут пересылаться в явном виде, в случае если хост-машина работает в rollback режиме.

РРТР

На этапе согласования параметров РРТР сессии атакующий может вынудить жертву использовать менее безопасную PAP аутентификацию, MSCHAP V1 (то есть «откатиться» с MSCHAP V2 до версии 1), либо не использовать шифрование вообще.

Атакующий может вынудить свою жертву повторить этап согласования параметров РРТР сессии (послать Terminate-Ask-пакет), выкрасть пароль из существующего туннеля и повторить атаку.

Публичные средства коммуникаций без защиты достоверности, конфиденциальности, доступности и целостности информации

Наиболее распространенные средства коммуникаций этой группы - это социальная сеть, публичный сервис электронной почты и система мгновенного обмена сообщениями.

Владелец ресурса, обеспечивающего сервис коммуникаций имеет полный контроль над информацией, которой обмениваются корреспонденты и, по своему усмотрению, в любой момент времени беспрепятственно может осуществить атаку.

В отличие от предыдущих сценариев, основанных на технических и технологических аспектах средств коммуникаций, в данном случае атака основана на ментальных аспектах, а именно на укоренении в сознании пользователей концепции игнорирования требований информационной безопасности.

Спасет ли шифрование?

Рассмотрим случай стандартной HTTP-транзакции. В этом случае злоумышленник достаточно легко может разбить оригинальное TCP-соединение на два новых: одно между собой и клиентом, другое между собой и сервером. Это довольно просто сделать, так как очень редко соединение между клиентом и сервером прямое, и в большинстве случаев они связаны через некоторое количество промежуточных серверов. MITM-атаку можно проводить на любом из этих серверов.

Однако в случае, если клиент и сервер общаются по HTTPS — протоколу, поддерживающему шифрование — тоже может быть проведена атака «человек посередине». При таком виде соединения

используется TLS или SSL для шифрования запросов, что, казалось бы, делает канал защищённым от сниффинга и MITM-атак.

Атакующий может для каждого TCP-соединения создать две независимые SSL-сессии. Клиент устанавливает SSL-соединение с атакующим, тот в свою очередь создает соединение с сервером. Браузер в таких случаях обычно предупреждает о том, что сертификат не подписан доверенным центром сертификации, но рядовой пользователь с легкостью игнорирует данное предупреждение. К тому же, у злоумышленника может оказаться сертификат, подписанный центром сертификации (например, такие сертификаты иногда используются для DLP). Кроме того, существует ряд атак на HTTPS. Таким образом, HTTPS протокол нельзя считать защищенным от MITM-атак у рядовых пользователей.

Обнаружение MITM-атаки

Для обнаружения атаки «[человек посередине](#)» необходимо проанализировать сетевой трафик. К примеру, для детектирования атаки по SSL следует обратить внимание на следующие параметры:

1. IP-адрес сервера
2. DNS-сервер
3. X.509-сертификат сервера
 - Подписан ли сертификат самостоятельно?
 - Подписан ли сертификат центром сертификации?
 - Был ли сертификат аннулирован?
 - Менялся ли сертификат недавно?
 - Получали ли другие клиенты в интернете такой же сертификат?

Реализации MITM-атаки

- **dsniff** — инструмент для SSH и SSL атак
- **Cain** — инструмент для проведения атаки «человек посередине». Имеет графический интерфейс. Поддерживает sniffing и ARP-spoofing
- **Etterscap** — инструмент для проведения атак в локальной сети
- **Karma** — использует атаку злой двойник (Evil Twin) для проведения MITM-атак
- **AirJack** — программа демонстрирует основанные на стандарте 802.11 MITM-атаки
- **SSLStrip** — инструмент для MITM-атаки на SSL
- **SSLSniff** — инструмент для MITM-атаки на SSL. Изначально был создан для обнаружения уязвимостей в Internet Explorer.
- **Mallory** — прозрачный прокси-сервер, осуществляющий TCP- и UDP-MITM-атаки. Может быть также использован для атаки на протоколы SSL, SSH и многие другие
- **wsniff** — инструмент для проведения атак на 802.11 HTTP/HTTPS протокол

Перечисленные программы могут быть использованы для осуществления атак «человек посередине», а также для их обнаружения и тестирования системы на уязвимости.

Системы обнаружения беспроводных атак

Системы обнаружения беспроводных атак (Wireless Intrusion Detection Systems, WIDS) сочетают в себе функции сигнатурных и поведенческих IDS. С их помощью также решается ряд задач, характерных для сканеров уязвимостей. В настоящее время существует достаточно много разнообразных реализаций подобных систем.

Возможности WIDS

Поскольку системы обнаружения беспроводных атак являются молодым классом средств защиты, набор функций и подходов к их реализации у различных производителей довольно серьезно различаются. Несмотря на это, можно выделить следующие основные задачи, решаемые с их помощью:

- составление карты беспроводной сети, инвентаризация сетевых устройств;
- диагностика проблем с пропускной способностью беспроводной сети;
- контроль политики безопасности;
- определение уязвимостей конфигурации беспроводных сетей;
- обнаружение и противодействие атакам в беспроводных сетях;
- позиционирование сетевых устройств;

Все приведенные категории задач в той или иной мере пересекаются, например, неверная конфигурация может приводить к отклонению от политики безопасности, или снижению производительности сети.

Основным механизмом, используемым [WIDS](#), является пассивный мониторинг трафика. В связи с этим большинство подобных систем может быть использовано в качестве беспроводного сетевого анализатора, и наоборот – многие системы обнаружения атак основаны на сетевых анализаторах.

Инвентаризация беспроводных устройств

Функция инвентаризации позволяет администратору составить списки беспроводных устройств, формирующих сеть. Списки могут составляться либо вручную, либо на основе анализа текущего сетевого трафика. Основным параметром при настройке списков устройств является MAC-адрес узла. Дополнительно могут быть задействованы другие параметры беспроводных устройств, такие как:

- используемый канал 802.11b/g/a;
- идентификатор производителя в MAC-адресе (IEEE OUI);

- используемый вариант протокола 802.11 (802.11a, 802.11b, 802.11g или различные сочетания);
- идентификатор сети (SSID).

В качестве дополнительного динамического параметра может использоваться минимальный уровень сигнала. Как правило, в WIDS можно задавать несколько различных списков, например: корпоративных сетей, гостевых сетей, сетей соседей.

Полученные списки являются основой для дальнейшей настройки системы, но и сами могут быть источниками событий. Например, обнаружение точки доступа с SSID корпоративной сети, но отсутствующей в списке легальных устройств, может быть признаком атаки «человек посередине».

Диагностика пропускной способности

Большинство систем обнаружения беспроводных атак имеют возможность контроля состояния физического и канального уровней сети 802.11. Ситуации, приводящие к срабатыванию системы, можно разбить на следующие категории:

1. Перегрузка канала или устройства
 - большое количество клиентов на точку доступа;
 - чрезмерная загрузка беспроводной сети или точки доступа;
 - падение качества сигнала;
 - большое количество широковещательных пакетов.
2. Ошибки в настройке
 - перекрытие каналов;
 - точка доступа не поддерживает максимально доступную для стандарта скорость передачи;
 - конфликтующие настройки точек доступа с одним идентификатором сети;
 - большое количество неассоциированных клиентов, рассылающих Probe Request на скорости 1 Мбит/сек.
3. Проблемы совместимости
 - передатчик не использует методы предотвращения конфликтов для смешанных (802.11 b/g) сетей;

- клиентская станция постоянно переключается между 802.11g и 802.11b;
 - использование нестандартных скоростей передачи.
4. Аномальный трафик в сети
- высокий процент фрагментированных фреймов;
 - большое количество повторных передач;
 - передача данных на низких скоростях;
 - большое количество ошибок при подсчете контрольной суммы;
 - большое количество переключений между точками доступа;
 - сеть перегружена управляющим трафиком.

Контроль политики безопасности

Контроль политики безопасности осуществляется на основе заранее сформулированных списков корпоративных точек доступа и клиентов и заключается в обнаружении отклонения от некоторого базового состояния, заданного администратором. В большинстве систем предусмотрены следующие возможности контроля принятой в компании политики безопасности беспроводной сети:

- обнаружение несанкционированных клиентов;
- обнаружение несанкционированных точек доступа;
- обнаружение нарушений принятой политики защиты трафика.

Проверки каждой из групп могут применяться либо ко всем обнаруживаем сетевым пакетам, либо для определенных групп точек доступа на основе SSID и списков контроля доступа по MAC-адресам. Это позволяет задавать разные правила для различных сетей, например, контролировать клиентов, точки доступа и применение 802.1x и WPA в основной сети и не обращать внимания на незащищенные взаимодействия в рядом расположенной сети соседней компании. Кроме того, в разных частях корпоративной

WLAN (основная сеть, гостевая сеть) могут действовать различные политики безопасности. Может контролироваться использование следующих технологий защиты беспроводных сетей:

- шифрование (любое);
- использование WEP;

- аутентификация Open System/Shared Key;
- применение виртуальных частных сетей на основе L2TP, IPSec, PPTP, SSH и т.д.;
- использование 802.1x с динамическим распределением ключей WEP;
- шифрование TKIP (WPA);
- аутентификация Protected EAP (PEAP);
- аутентификация на общих ключах (WPA-PSK, 802.11i-PSK);
- аутентификация EAP-FAST/LEAP;
- шифрование AES (802.11i).

Соответственно, если администратор указывает что в сети с SSID «Corporate» должно использоваться шифрование TKIP с аутентификацией PEAP, любые точки доступа с таким же идентификатором сети, пытающиеся использовать другие технологии защиты, будут вызывать срабатывание системы обнаружения атак.

Определение уязвимостей сети

Задача определения ошибок в конфигурации беспроводных сетей тесно переплетается с задачей контроля соблюдения [политики безопасности](#). В проводных сетях подобные функции реализуются с помощью средств анализа защищенности (сканеров), представляющих собой активные утилиты. В беспроводных сетях используется комбинированный подход, сочетающий активные и пассивные методы с приоритетом последних.

Ошибки в конфигурации можно разбить на следующие группы:

- ошибки в настройке беспроводных клиентов;
- ошибки в настройке точек доступа;
- ошибки в настройке механизмов защиты.

Можно выделить следующие типичные ошибки в настройке различных компонентов беспроводной сети:

1. Рабочие места пользователей

- наличие рабочих станций в режиме Ad-Hoc;
- клиент с несколькими профилями соединений;
- наличие неассоциированных клиентов;

- использование аутентификации типа Open System/Shared Key;
 - использование клиентом в режиме Ad-Нос идентификатора SSID точки доступа.
2. Точки беспроводного доступа
- использование настроек «по умолчанию»;
 - широковещательная рассылка SSID;
 - использование аутентификации типа Open System/Shared Key;
 - работа точки доступа в режиме сетевого моста.
3. Механизмы защиты
- использование LEAP;
 - не использование шифрования на точке доступа или клиенте;
 - повторное использование вектора инициализации WEP;
 - слишком большой промежуток смены ключей WEP (при использовании стандарта 802.1x);
 - использование векторов инициализации WEP, уязвимых для FSM-атак (представляет чисто исторический интерес);
 - отсутствие шифрования широковещательного трафика при использовании стандарта 802.1x;
 - несоответствие используемых протоколов защиты заданному профилю.

Часть приведенных проверок требует дополнительного внимания со стороны администратора. Так, для определения точек доступа со стандартными настройками система обнаружения атак должно обладать списком, содержащим OUI производителя и стандартный идентификатор сети. Как правило, подобные списки предоставляются производителем, но практика показывает, что они немного отстают от действительности.

В связи с этим рекомендуется следить за списками стандартных настроек точек доступа и добавлять их в конфигурацию WIDS.

Собственно, атаки

Количество обнаруживаемых беспроводной [IDS](#) атак сильно отстает по количеству от подобной характеристики проводных систем, где список правил обнаружения атак может исчисляться тысячами. Это

связанно с тем, что WIDS сконцентрированы на канальном уровне модели OSI, обладающем гораздо меньшей энтропией, чем, например, прикладной, для которого создана большая часть сигнатур проводных систем обнаружения атак.

Конечно, система обнаружения атак может расшифровать трафик WEP, WPA или 802.11i в случае использования для аутентификации статических ключей, но в корпоративной сети это скорее исключение, чем правило. Если в сети используется аутентификация 802.1X, система обнаружения атак просто не имеет доступа к ключам шифрования и не может анализировать данные и заголовки более высоких уровней, чем канальный.

Ниже приведен список атак, обнаруживаемых системами AirMagnet.

Таблица 1. Атаки, обнаружимые AirMagnet

Название атаки	Описание
Airsnarf attack detected	Обнаружены попытки использования утилиты Airsnarf для организации ложных точек доступа и fishing-атак
ARP Request Replay attack	Проводится атака с повтором перехваченного зашифрованного пакета для ускорения вскрытия WEP
Device probing for AP	Клиент настроен на установление соединения с любой точкой доступа
Dictionary attack on EAP methods	Большое количество неудачных попыток установить сессию по протоколу EAP
Faked APs detected	Обнаружено большое количество точек доступа, с которыми не установлено не одного соединения. Это характерно для ситуаций, когда используется утилита FakeAP
Fake DHCP server detected	В беспроводной сети обнаружен сервер DHCP

Таблица 1 (продолжение)

Hotspotter tool detected	Обнаружены попытки использования утилиты Hotspotter для организации ложных точек доступа и fishing-атак
Illegal 802.11 packets detected	Обнаружен пакет, нарушающий правила стандарта 802.11
Man-in-the middle attack detected	Обнаружена попытка организации атаки «человек посередине»
NetStumbler detected	Обнаружен трафик, характерный для утилиты NetStumbler
Potential ASLEAP attack detected	Обнаружен трафик, характерный для атак на протокол LEAP с использованием утилиты ASLEAP
Potential Honey Pot AP detected	Обнаружена точка доступа, маскирующаяся под корпоративную
PSPF violation	Обнаружена прямая передача пакетов между клиентами, что является нарушением политики Publicly Secure Packet Forwarding (PSPF)
Soft AP or Host AP detected	Обнаружено использование программной реализации точки доступа (HostAP, SoftAP)
Spoofed MAC address detected	Обнаружена подмена MAC-адреса, с целью обхода фильтров на основе MAC-адресов
Wellenreiter detected	Обнаружен трафик, характерный для утилиты Wellenreiter

В последнее время, в связи с большим количеством обнаруженных уязвимостей в драйверах беспроводных адаптеров, в системы WIDS стали включать сигнатуры для подобных атак.

Естественно сигнатуры такого рода не свободны от ошибок первого и второго рода. Например, использование карточки Orinoco 802.11b со стандартными драйверами для Windows приводило к срабатыванию

сигнатуры обнаруживающей заполнение Clear To Send (CTF) пакетами. Инициализация сетевой карточки или переключение ее на другую точку доступа может вызвать обнаружение подмена (spoofing) MAC-адреса. Проблемы могут возникать при использовании злоумышленником нестандартных средств. Например, при использовании программных точек доступа на основе драйвера madwifi, а не HostAP и «зашумлении» с их помощью эфира ложными фреймами beacon атака может быть не обнаружена.

Механизмы реагирования

Основной задачей системы обнаружения атак является своевременное уведомление администратора о потенциальных проблемах. В беспроводных IDS используются традиционные для систем подобного класса механизмы оповещения, такие как:

- отправка сообщения по электронной почте;
- уведомление через службу Messenger;
- отправка SMS или сообщения на пейджер;
- уведомление через систему мгновенного обмена сообщениями;
- передача POST ли GET запроса Web-серверу;
- передача управляющих сообщений SNMP;
- запись сообщений в журнал событий Windows или на сервер Syslog;
- печать сообщений на принтере.

Как и проводные системы обнаружения атак, беспроводные IDS могут использовать механизмы, направленные на снижение возможных последствий обнаруженной атаки. И точно так же, как и в проводных сетях, таких механизмов два:

- реализация DoS-атаки на узел возможного злоумышленника;
- блокирование атакующего средствами активного сетевого оборудования.

Кроме того, беспроводные системы обнаружения атак, как правило, реализуют функции определения координат источника сигнала и блокирования попыток соединения из точек, находящихся за пределами периметра.

В беспроводных сетях роль поддельных TCP-RST пакетов, применяемых проводными IDS, выполняют управляющие фреймы Disassociate или Deauthentication, по сути система обнаружения атак сама проводит атаку, описанную ранее в этой главе, причем эта атака может быть направлена как на точку доступа (Disassociate All), так и на конкретного клиента беспроводной сети.

При настройке этого механизма необходимо соблюдать осторожность, поскольку Вы наверняка являетесь не единственным пользователем радиоэфира в округе. Если WIDS настроена на блокировку всех клиентов и точек доступа, отсутствующих в "белом списке" беспроводной сети компании, вашим соседям просто не дадут нормально работать.

Некоторые из продуктов данного класса, особе те, которые интегрированы с точками доступа, могут включать MAC-адрес потенциального злоумышленника в черный список на точке доступа, предотвращая попытки повторного соединения. Эту возможность тоже желательно использовать аккуратно. Например, при тестировании защищенности одной из беспроводных сетей авторам удалось вывести ее из строя, потратив буквально несколько десятков пакетов на каждого клиента. Просто WIDS надолго блокировала на точке доступа MAC-адрес машины, осуществляющей атаку. Естественно многие атаки проводились от адреса клиента сети или точки доступа. Хотя в этой ситуации попытки провести атаки типа "человек посередине" обречены на провал, вывод сети из строя сам по себе может причинить довольно серьезный ущерб.

При блокировке подключений несанкционированных точек доступа к корпоративной сети системы обнаружения беспроводных атак могут взаимодействовать с коммутаторами локальной сети. Как правило, на WIDS существует возможность задать список адресов коммутаторов или строить его динамически на основе опроса устройств по протоколу SNMP. При обнаружении несанкционированной точки доступа, нарушающей политику беспроводной безопасности, система по протоколу SNMP опрашивает известные устройства на предмет наличия ее MAC- адреса в таблице коммутации. Если поиск успешен, то система посылает коммутатору команду на блокировку порта, к

которому подключена точка доступа. К сожалению, этот механизм не может быть применен для блокировки клиентов с ненастроенными беспроводными адаптерами, поскольку установить адрес проводного интерфейса по MAC-адресу беспроводного интерфейса достаточно трудно.

Проверить тот факта, что точка доступа подключена к проводной сети компании, можно отправив контрольный ARP-запрос, который будет ретранслирован в беспроводную сеть. Поскольку MAC-адрес отправителя передается в открытом виде даже при использовании протоколов шифрования трафика, он может быть использован для контроля появления пакета в беспроводной сети. Справедливо и обратное – перехватив и повторно послав зашифрованный ARP-пакет в локальную сеть через несанкционированную точку доступа, можно по наличию его в проводном сегменте определить место подключения устройства.

Одной из полезных функций систем обнаружения беспроводных атак является возможность определения координат устройства, нарушившего политику безопасности. В случае, если система использует один мобильный сенсор, то для позиционирования понадобятся направленная антенна, план здания и некоторая физкультурная подготовка.

Сделав замеры уровня сигнала от искомого объекта с трех точек, определяются векторы, по которым наблюдается максимальный уровень. Точкой пересечения этих линий является место положения источника радиосигнала. В большинстве случаев, векторы не пересекутся в одной точке, а образуют так называемый «треугольник ошибок», размеры которого при небольших расстояниях, будут очень велики. Этот метод пеленгации, или триангуляции хорошо известен всем по военным фильмам и «охоте на лис».

Триангуляция с направленной антенной

Очень похожая технология используются в распределенных системах обнаружения беспроводных атак. При обнаружении сигнала искомого объекта несколькими сенсорами по уровню сигнала определяется примерное расстояние до его источника. Вокруг каждого

сенсора строится окружность, радиус которой обратно пропорционален уровню принимаемого сигнала. Место расположения источника сигнала будет находиться в районе пересечения окружностей.

Позиционирование устройств

В реальных условиях для повышения точности работы этого метода требуется учет особенностей помещения, поскольку в большинстве случаев отражение и рассеяние сигнала уменьшает точность определения его мощности. Для этого проводят предварительные замеры уровня сигнала от источников, находящихся в различных точках помещения, и на основании этих данных рассчитывают соответствующие поправки. Естественно, в современных системах все расчеты проводятся автоматически. Некоторые системы автоматически вносят корректировки, связанные с затуханием и отражением сигнала, на основе текущей ситуации в эфире. Для корректного выполнения этой функции администратор указывает расположение сенсоров WIDS и точек доступа на плане здания, что позволяет системе определять расстояния от сенсоров до источников сигнала и вычислять дополнительно затухание, вносимое за счет особенностей помещения.

С функцией определения местоположения источника сигнала связан еще один интересный механизм, в настоящее время широко внедряемый многими производителями WIDS. Суть его заключается в том, что система обнаружения атак блокирует попытки подключения с территорий, находящихся за пределами физического периметра, даже если подключается вполне легальный клиент. Это позволяет ограничить соединения к сети только пределами физического периметра. Однако не стоит считать этот механизм очередной панацеей. Грамотное использование антенн и физических особенностей здания, и некоторая толика удачи вполне позволяют квалифицированному злоумышленнику создать видимость, что соединение происходит с разрешенной территории.

Реализация атаки

Исходная сеть:

Имеется обычный роутер, который раздает интернет своим клиентам, образуя беспроводную сеть Wi-Fi.

Вы выступаете в роли злоумышленника, который, как и все является обычным клиентом с обычным ПК. Для реализации данной атаки вам понадобится сетевой sniffер (анализатор сетевого трафика) WireShark.

Итак, цель: Организовать «прослушку» трафика от клиентов в сети. Для этого нужно «встать посередине».

Задачи сводятся в четыре шага:

1. Подготовка двойника настоящей точки доступа.
2. Разрешение доступа в интернет на созданный беспроводной сетевой интерфейс.
3. Перезагрузка роутера на правах администратора, или DDOS-атака на роутер.
4. В момент провисания настоящего роутера задействовать двойника.

Первый шаг. Необходимо подготовить точку доступа. Для этого воспользуемся встроенной в Windows программой netsh.

В данном примере SSID настоящей точки доступа Rostelecom_16 и, так как вы являетесь клиентом сети, то вам известен пароль к настоящей точке доступа. Создаем с таким же названием и таким же паролем точку доступа:

netsh wlan set hostednetwork mode = allow ssid = «Rostelecom_16» key = «пароль настоящей ТД» keyUsage = persistent

В сетевых подключениях появится новый беспроводной интерфейс (Рис 1.).

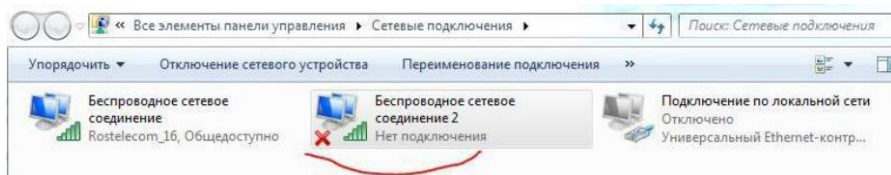


Рис. 1. Сетевые подключения

Не торопитесь запускать данное подключение!

Примечание: если ничего не появилось в сетевых подключениях, то поможет перезапуск Wi-Fi адаптера.

Второй шаг. Делаем интернет общим для созданного (но еще не запущенного!) подключения (Рис. 2).

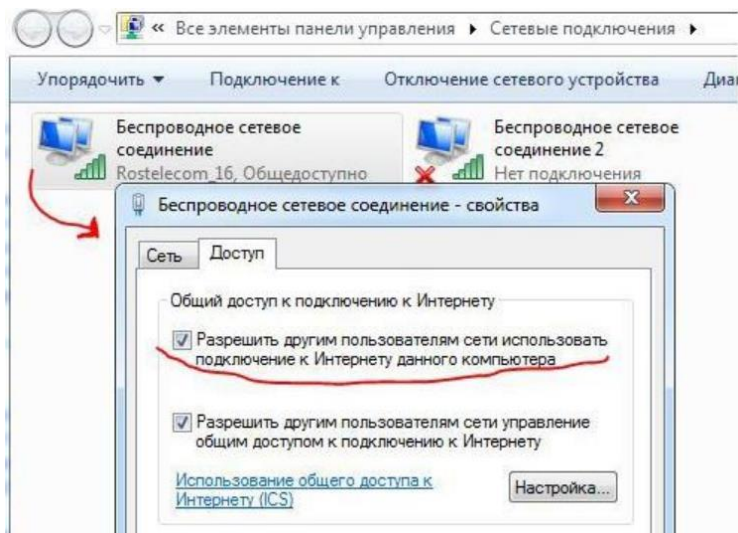


Рис. 2. Второй шаг

Третий шаг. Как уже отмечалось, в данном примере есть возможность администрирования роутера. Кстати, не секрет, что одной из самых распространенных уязвимостей являются пароли и настройки по умолчанию. В настройках маршрутизатора всегда есть кнопка «перезагрузить». Ею мы и воспользуемся, чтобы временно сбросить всех клиентов.

Четвертый шаг. Когда начнется сброс (именно в этот момент!), нужно активировать точку доступа двойника.

Команда: `netsh wlan start hostednetwork`

Чтобы убедиться, что «вы стали посередине», смотрим своих клиентов командой: **netsh wlan show hostednetwork**

```
Параметры размещенной сети
-----
Режим                : разрешен
Имя идентификатора SSID : "Rostelecom_16"
Максимальное количество клиентов : 100
Проверка подлинности: WPA2-Personal
Шифр:                CCMP

Состояние размещенной сети
-----
Состояние            : Запущено
BSSID                : 2a:f4:6a:ae:63:7a
Тип радиомодуля      : 802.11n
Канал                : 10
Число клиентов       : 2
                    54:35:30:08:50:bf
                    00:16:e3:e0:a4:1d
                    Проверка подлинности выполнена
                    Проверка подлинности выполнена
```

Рис. 3. Просмотр клиентов

Всё! Что произошло? Нетрудно, догадаться, что, воспользовавшись моментом простоя, мы совершили подмену настоящего сервера, сдвинув настоящий сервер на второй план.

Вовремя сброса (перезагрузки) роутера, он пропадает из поля видимости, поэтому в начале сброса все клиенты отцепились от сети, но когда обнаружили такой же SSID (наш двойник), то сразу же подцепились, казалось бы, обратно. А на самом деле к серверу двойнику, который также раздает интернет.

В завершении, чтобы окончательно добиться поставленной цели, запускаем так называемую программу акулу WireShark и слушаем трафик от клиентов..

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Ознакомиться с предложенным теоретическим материалом для получения информации о методах анализа и перехвата передаваемых данных.
2. Применить на практике полученные знания в виде проведения «атаки по середине» на настроенную беспроводную сеть.
3. Подготовить ответы на контрольные вопросы.

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ

1. Дайте определение термину «атака по середине». Изложите принцип атаки. Приведите пример такой атаки.
2. Изложите как обнаружить MITM-атаку.
3. Перечислите системы обнаружения беспроводных атак и основные задачи, решаемые с их помощью.
4. Изложите в чем заключается функция инвентаризации беспроводных устройств.
5. Перечислите ситуации, приводящие к срабатыванию системы контроля состояния физического и канального уровней сети 802.11.
6. Перечислите ошибки настройки различных компонентов в беспроводной сети.
7. Перечислите механизмы оповещения атак в беспроводных IDS.
8. Изложите, что такое «технология триангуляции», «позиционирование устройств».
9. Опишите как реализуется атака.

ФОРМА ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ

На выполнение лабораторной работы отводится 2 занятия (4 академических часа: 3 часа на выполнение и сдачу лабораторной работы и 1 час на подготовку отчета).

Отчет на защиту предоставляется в печатном виде.

Структура отчета (на отдельном листе(-ах)): титульный лист, формулировка задания (вариант), этапы выполнения работы (со скриншотами), результаты выполнения работы. выводы.

ОСНОВНАЯ ЛИТЕРАТУРА

1. Смелянский Р.Л. Компьютерные сети. 2 т. Т.1. Системы передачи данных [Текст] / Р.Л. Смелянский. –М.: Изд. Центр «Академия», 2011.- 304 с.
2. Смелянский Р.Л. Компьютерные сети. В 2 т. Т.2. Сети ЭВМ [Текст]: учебник для вузов / Р.Л. Смелянский. –М.: Изд. Центр «Академия», 2011.- 240 с.
3. Власов Ю.В. Администрирование сетей на платформе MS Windows Server [Электронный ресурс] / Ю.В. Власов, Т.И. Рицкова. —М.: Интернет-Университет Информационных технологий (ИНТУИТ), 2016. — 622 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52219.html>

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

4. Технологии коммутации и маршрутизации в локальных компьютерных сетях. [Текст]: учеб. пособие для вузов / Е.В. Смирнова, А.В. Пролетарский [и др.]; под. ред. А.В. Пролетарского. -М.: Изд-во МГТУ им. Н.Э. Баумана, 2013. - 389 с.: ил.
5. Таненбаум Э. Компьютерные сети [Текст] / Э. Таненбаум. – 4-е изд. – СПб.: Питер, 2010. — 992 с.
6. Ачилов Р.Н. Построение защищенных корпоративных сетей [Электронный ресурс]: учеб. пособие / Р.Н. Ачилов. — Москва: ДМК Пресс, 2013. — 250 с. — 2227-8397. — Режим доступа: <http://e.lanbook.com/book/66472>

Электронные ресурсы:

7. Электронно-библиотечная система «Лань»
8. Электронно-библиотечная система «Университетская библиотека ONLINE»
9. Электронно-библиотечная система «IPRbooks»
10. Электронно-библиотечная система «Юрайт»