Обнаружение неавторизованных беспроводных точек доступа

Несанкционированная точка доступа может поставить под угрозу безопасность всей сети, поскольку она открывает доступ к корпоративной сети для посторонних. Чтобы устранить эту уязвимость системы безопасности, сетевой администратор должен сначала выявить присутствие неавторизованной ТД в сети, а затем определить ее местонахождение.

Существует два метода поиска, наиболее широко используемых для обнаружения неавторизованных ТД: метод конвергенции и векторный метод. У каждого из них есть свои преимущества и соответствующий набор инструментов. Понимание этих методов поможет сетевому администратору обеспечить безопасность беспроводной сети.

Содержание

FLUKE networks

Обнаружение неавторизованных беспроводных точек доступа

Неавторизованная точка доступа может поставить под угрозу безопасность беспроводной сети. Мы называем неавторизованной такую точку доступа (ТД), которая установлена без ведома или согласия системного администратора компании. Бывает, что сотрудник просто берет из дома на работу беспроводный маршрутизатор, чтобы иметь временный доступ к беспроводной сети во время совещания. Гораздо более опасна ситуация, когда посторонние устанавливают точку доступа, чтобы воспользоваться возможностью бесплатного доступа к Интернет или взломать сеть, чтобы узнать, что в ней хранится. И в том, и в другом случае в отношение несанкционированной ТД преднамеренно или из-за неведения не применяются адекватные настройки безопасности. Эти ТД открывают доступ к корпоративной сети для посторонних.

Разработаны решения, помогающие администратору сети обнаружить наличие неавторизованных точек доступа. Однако, это еще полдела. Администратору сети требуется, кроме того, выявить местонахождение этой точки доступа. Локализовав точку доступа, ее можно удалить из сети или изменить конфигурацию с учетом необходимых требований безопасности.

Существует два метода поиска, наиболее широко используемых для обнаружения неавторизованной ТД: метод конвергенции и векторный метод. Выбор метода зависит от инструментов, которые имеются в Вашем распоряжении.

Метод конвергенции

Этот метод применяется тогда, когда для обнаружения ТД используется беспроводная сетевая карта с антенной с круговой диаграммой направленности и индикатор уровня сигнала. Антенна с круговой диаграммой направленности направляет и получает сигналы одинаково хорошо по всем направлениям. Ее иногда называют «ненаправленной», потому что ни одно из направлений не является предпочтительным. На рисунке 1 показана схема действия антенны с круговой диаграммой направленности.

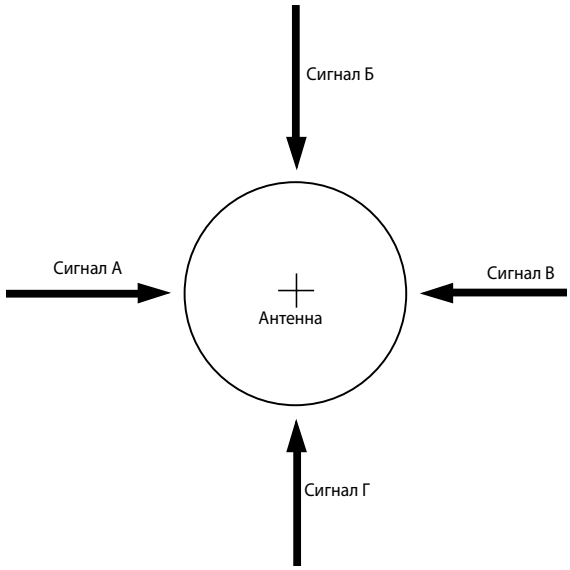

Рисунок 1 Схема действия антенны с круговой диаграммой направленности

Эта антенна применяется в стандартных беспроводных сетевых картах доступа для ноутбуков. В данном случае антенна с круговой диаграммой удобна, поскольку мощность сигнала остается на одном и том же уровне и не зависит от положения компьютера.

Рисунок 2 Стандартная беспроводная сетевая карта с антенной с круговой диаграммой направленности

Метод конвергенции предполагает также применение индикатора уровня сигнала. Он используется для измерения мощности сигнала, поступающего от неавторизованной ТД. Чем сильнее сигнал, тем ближе точка доступа. Существуют индикаторы нескольких типов. Чаще всего применяется служебная программа, которая обычно входит в комплект поставки беспроводной сетевой карты, устанавливаемой в ноутбук. Разные производители создают различные версии этих простых программ. Однако, как правило, они позволяют получить наглядное представление о мощности сигнала. Проблема заключается в том, что с их помощью сложно заметить небольшие изменения мощности на упрощенной графической диаграмме.

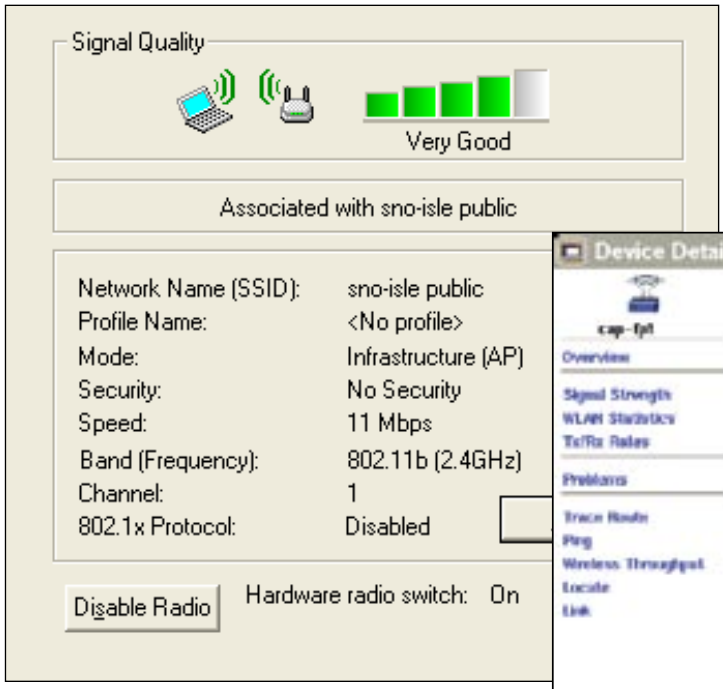

Рисунок 3 Программный индикатор уровня сигнала

Рисунок 4 График мощности сигнала, оптимизированный для охоты за неавторизованными беспроводными устройствами

Можно также установить на ноутбук программное обеспечение независимых производителей, обеспечивающее повышенное качество измерения мощности сигнала. Эти приложения позволяют измерять большее количество параметров и представлять результаты измерений в виде более крупных и удобных графиков. Если необходимо избежать применения для этой цели компьютера, можно воспользоваться ручными индикаторами уровня радиосигнала. Эти инструменты часто разрабатываются специально для обнаружения неавторизованных точек доступа. Удобная организация информации позволяет ускорить процесс обнаружения ТД (см. рисунок 4).

Чтобы выполнить поиск неавторизованной ТД по методу конвергенции, вооружитесь беспроводной сетевой картой с антенной с круговой диаграммой направленности и индикатором уровня сигнала. Выберите в качестве целевой ТД свою карту. Походите по помещению, отмечая уровень сигнала, до тех пор, пока не поймете, откуда примерно следует начать охоту за неавторизованными беспроводными устройствами. Представьте, что область поиска – это большой прямоугольник, разделенный на четыре квадранта. См. рисунок 5. Перейдите в один из углов области поиска. Запишите уровень мощности сигнала. Перейдите во второй угол. Запишите уровень мощности сигнала. Перейдите в третий угол и снова зафиксируйте мощность. Перейдите в третий угол и снова зафиксируйте мощность. Сравнив полученные результаты, можно узнать, где находится искомая ТД. Она будет расположена в том квадранте, где отмечается самый высокий уровень сигнала. В нашем примере это нижний правый квадрант. Теперь представьте этот квадрант в виде новой области поиска, разделенной на четыре меньших квадранта. Повторите серию измерений в этой области поиска, перемещаясь из угла в угол и отмечая уровень сигнала. В данном случае самый сильный сигнал зафиксирован в верхнем правом квадранте. Обойдите эту территорию, поделив ее на четыре части, и снова измерьте мощность. В нашем примере для обнаружения искомой ТД хватило 3 сегментаций (12 измерений). Если исходная область поиска больше, может потребоваться дополнительная сегментация и измерения.

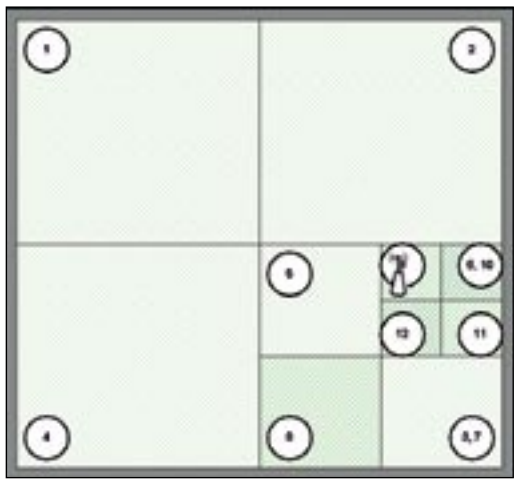

Рисунок 5 Алгоритм поиска методом конвергенции

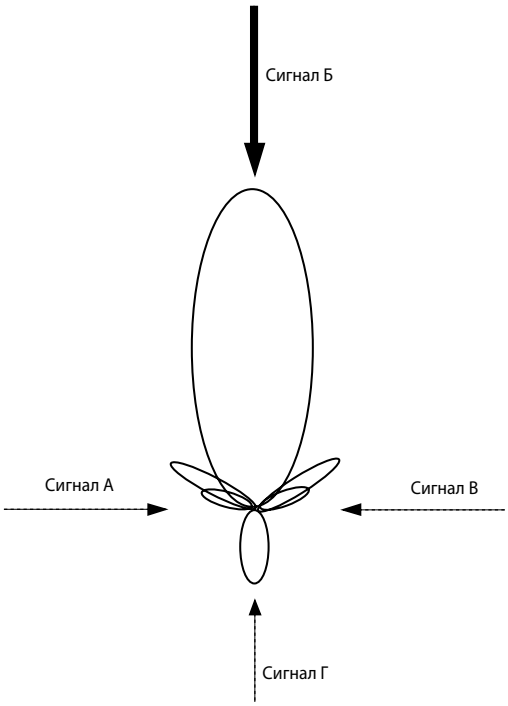

Рисунок 6 Алгоритм поиска методом конвергенции

Векторный метод

Второй метод поиска местонахождения неавторизованной точки доступа называется «векторным». Этот метод применяется тогда, когда для обнаружения ТД используется беспроводная сетевая карта с направленной антенной и индикатор уровня сигнала. Направленная антенна позволяет обмениваться сигналами максимальной мощности в одном направлении. При этом сигнал, поступающий по другим направлениям, подавляется. На рисунке 6 показана схема действия антенны с круговой диаграммой направленности.

Существует несколько модификаций направленных антенн. Локализация неавторизованной точки доступа упрощается, если применять внешнюю антенну, подключенную к беспроводной сетевой карте. Для этой антенны требуется специальная беспроводная сетевая карта. Обычно на них имеется гнездо для антенного разъема. При подключении внешней направленной антенны внутренняя антенна с круговой диаграммой направленности выключается.

Как и в случае метода конвергенции, векторный метод предполагает применение индикатора уровня сигнала. Рекомендуется использовать портативный инструмент, созданный специально для поиска неавторизованных ТД. Указанные методы поиска основаны на разных алгоритмах.

Чтобы выполнить поиск неавторизованной ТД по «векторному» методу, потребуется беспроводная сетевая карта с направленной антенной и индикатор мощности сигнала. Выберите в качестве целевой ТД свою карту. Походите по помещению, отмечая уровень сигнала, до тех пор, пока не поймете, откуда примерно следует начать охоту за неавторизованными беспроводными устройствами. Представьте, что область поиска – это большой прямоугольник, разделенный на четыре части. См. рисунок 8. Теперь перейдите в центр области поиска и нацельте антенну в угол области поиска. Запишите уровень мощности сигнала. Повернитесь на 90°, не сходя с места, и направьте антенну во второй угол. Запишите уровень мощности сигнала. Направьте антенну в третий угол и зафиксируйте мощность. Направьте антенну в четвертый угол и запишите уровень сигнала. Сравнив полученные результаты, можно узнать, где находится искомая ТД. Она будет расположена там, где отмечается самый высокий уровень сигнала.

Рисунок 7 Карта с внешней направленной антенной

В нашем примере это нижняя правая часть области поиска. Теперь представьте, что новая область поиска делится на четыре меньших подобласти. Повторите серию измерений в этой области. Встаньте в центре, направьте антенну в каждый из углов и зафиксируйте мощность сигнала. В данном случае самый сильный сигнал зафиксирован в верхней правой подобласти. Обойдите эту территорию, проведите измерения и поделите ее на четыре части. В нашем примере для обнаружения искомой ТД хватило 3 сегментаций (12 измерений). Если исходная область поиска больше, может потребоваться дополнительная сегментация и измерения.

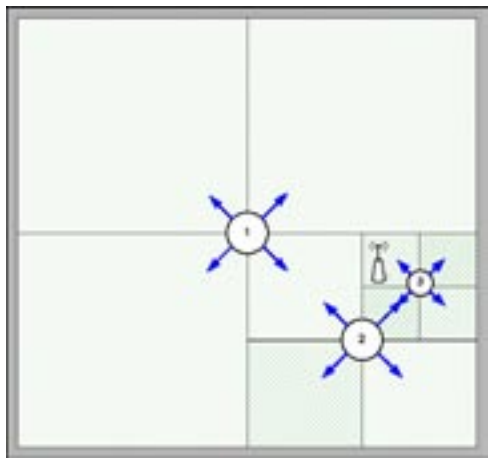

Рисунок 8 Алгоритм поиска векторным методом

Сравнение методов

В нашем примере количество операций сегментирования и измерения одинаково для обоих методов. Очевидно, что измеряя уровень сигнала методом конвергенции, приходится гораздо больше ходить с индикатором из угла в угол. Это приводит к тому, что поиск неавторизованных точек доступа отнимает больше времени. Более тонкое различие между этими методами можно отметить при необходимости локализовать точку доступа в многоэтажном здании. Допустим, Вы предполагаете, что неавторизованная точка доступа находится на третьем этаже пятиэтажного бизнес-центра. С помощью метода конвергенции можно обнаружить местонахождение комнаты с самым высоким уровнем сигнала. Однако это не дает возможности обнаружить ТД. Точность измерений тут не при чем – точка доступа может располагаться на другом этаже. С другой стороны, если прибегнуть к векторному методу, то антенну можно поворачивать на 180° по вертикали, чтобы понять на каком этаже находится неавторизованная ТД.

	Поиск по методу конвергенции	Поиск по векторному методу
Необходимые инструменты	Беспроводная сетевая карта WLAN со встроенной антенной с круговой диаграммой направленности, индикатор уровня радиосигнала	Направленная (внешняя) антенна, беспроводная сетевая карта WLAN с разъемом для подключения антенны, индикатор уровня радиосигнала
Преимущества	Используются наиболее распространенные типы карт и антенн	Можно меньше ходить в поисках ТД и выполнять трехмерный поиск за счет перемещения антенны в вертикальном и горизонтальном направлениях.
Недостатки	Приходится много ходить, и это приводит к тому, что поиск занимает больше времени. Этот метод плохо подходит для многоэтажных зданий.	Требуется специальная беспроводная сетевая карта и антенна. Как правило, они стоят дороже.

Практические соображения

На практике бывает необходимо изменить схему поиска с учетом наличия помещений непрямоугольной формы, стен, перегородок и других препятствий. Во время измерений необходимо держать антенну на одной и той же высоте. Точность измерений можно повысить, если держать антенну над уровнем перегородок. В поисках точек доступа не забывайте о третьем измерении. Если в наличии имеется только антенна с круговой диаграммой направленности, определить, на каком этаже находится неавторизованная точка доступа можно путем замеров мощности сигнала на нескольких этажах. При проведении измерений векторным методом, постарайтесь сделать так, чтобы во время изменения ориентации антенны близлежащие объекты (прибор, корпус тела, руки) не двигались. Обычно проще всего подключить направленную антенну к ручному или программному индикатору уровня сигнала и перемещать по кругу измерительный прибор целиком вместо того, чтобы вращать только антенну. Попрактикуйтесь в обнаружении тестовых точек доступа, местоположение которых известно заранее. Это поможет определить, насколько чувствительно оборудование к изменениям расстояния до ТД, высоты антенны и ее направления (если это направленная антенна). Обратите внимание, что металлические предметы (стены с содержанием металла, перегородки в металлических рамах, вертикальные жалюзи) могут влиять на точность обнаружения источника сигнала, особенно если тот слаб. Знакомство с особенностями помещений помогает в случае необходимости быстрее выявлять неавторизованные ТД.

Сохраняйте бдительность

В целях сохранения безопасности сети, проинформируйте сотрудников об опасности, связанной с установкой несанкционированных точек доступа. Внесите соответствующую информацию в свод корпоративных правил. Используйте защищенный механизм доступа к сети (например, IEEE 802.1X). Выполните обычную проверку безопасности, попробовав найти неавторизованные и незащищенные беспроводные устройства, чтобы выявить источники угрозы. Найдя неавторизованную ТД, быстро локализуйте ее, чтобы избавиться от этой причины нарушения политики сетевой безопасности. Воспользовавшись проверенными методами обеспечения защиты беспроводных сетей, можно свести риск к минимуму.

О компании Fluke Networks

Fluke Networks предоставляет инновационные решения по установке и сертификации, а также тестированию, мониторингу и анализу медных и волоконно-оптических линий и беспроводных сетей, используемых предприятиями и телекоммуникационными компаниями. Универсальная линия решений Network SuperVision™ предлагает специалистам по установке и обслуживанию, а так же владельцам сетей все необходимое для быстрой, точной и легкой оптимизации работы сети. Получить дополнительную информацию об устройстве EtherScope Series II Network Assistant, поддерживающем функции анализа беспроводных сетей 802.11a/b/g и поиска неавторизованных точек доступа можно на сайте **www.flukenetworks.com/etherscope**.

Ссылки

Carr, Joseph J. Directional or Omnidirectional Antenna? Universal Radio Research.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks работает более чем в 50 странах мира. За информацией о региональных дистрибьюторах и представительствах обращайтесь на сайт **www.flukenetworks.com/contact**.

Напечатано в США. 11/2006 2804968 H-RUS-N Ред. A