ШИРОКО ОТКРЫТЫЕ ДВЕРИ БЕСПРОВОДНЫХ СЕТЕЙ[1]

Николай Петров, CISSP
npetrov@kerberus.ru

Последние несколько лет технологии беспроводных сетей настолько стремительно развиваются, что сегодня никого не удивишь наличием карты беспроводного доступа в стандартной конфигурации переносного компьютера.

О преимуществах беспроводных сетей написаны тысячи статей, и сотни о том, как сделать их безопасными. В статьях по безопасности, как правило, идет речь об уязвимых местах реализации алгоритма шифрования WEP (Wired Equivalent Privacy), и в качестве решения предлагается использовать протоколы VPN (Virtual Private Network), WPA(Wi-Fi Protected Access), 802.1x (IEEE стандарт доступа и авторизации для 2-го уровня модели OSI) и RADIUS для аутентификации. В качестве дополнительной меры также можно установить Систему Обнаружения Вторжений (Intrusion Detection Sytem) для беспроводных сетей. Но так ли все просто?

В этой статье автор не претендует на полное описание всех возможных уязвимых мест присущих беспроводным сетям. Факты и рекомендации, изложенные в статье, основаны на многолетнем опыте автора по диагностике и построению защиты корпоративных сетей десятков крупнейших российских и зарубежных компаний.

В ЧЕМ ЖЕ ОПАСНОСТЬ?

Готовя эту статью, автор проехал по центру Москвы со специально оборудованным переносным компьютером с целью обнаружения беспроводных сетей и идентификации их параметров. Для сохранения чистоты эксперимента, идентификацию параметров беспроводных сетей была прекращена, как только их количество превысило 100. Полученные результаты просто шокируют. Из более ста обнаруженных сетей, в 32% случаев WEP был обнаружен выключенным, а в 37% в качестве настроек ESSID (Extended Service Set ID) использовались установленные по умолчанию параметры оборудования или имя компании! Многие из Вас наверно подумали, что приведенные проценты скорее всего относятся к домашним беспроводным сетям или сетям открытого (публичного) доступа?

К сожалению, большинство обнаруженных сетей принадлежат крупным известным компаниям. Безусловно, сетевые администраторы таких компаний должны знать о способах обхода фильтрации MAC адресов, получения закрытых ESSID и уязвимостях WEP. Но готовы ли они к атакам MITM для 1-го и 2-го

[1] Статья опубликована в журнале «Мобильные Системы» №1, январь 2005

уровней модели OSI, атакам на 802.1x, аутентификацию RADIUS и VPN? Давайте рассмотрим все по порядку.

Опытного хакера беспроводных сетей практически невозможно обнаружить, и даже обнаружив, что Вы будете делать, если он сидит с включенным компьютером в машине, пусть даже прямо под окнами офиса вашей компании?

Традиционно, хакер старается нигде не оставлять следов. В обычных сетях для атак ему приходиться использовать скомпрометированные ранее хосты, в то время как с помощью беспроводных сетей, он и так достаточно скрыт. Причем в проводных сетях, хакер так или иначе оставляет следы, пользуясь определенным IP адресом. Безусловно, опытный хакер использует различные механизмы подмены и сокрытия своего настоящего IP адреса. В нашей практики не раз возникали случаи, когда руководство компании заказывало проекты оценки защищенности в тайне от своих сотрудников отделов ИТ и компьютерной безопасности с целью проверки не только надежности имеющихся мер компьютерной безопасности, но и своевременности и адекватности реагирования указанных служб на инциденты.

Скрыть атаку со стороны Интернет довольно просто, например, используя для сканирования и атаки цепочку прокси-серверов. В офис же компании, нас приводили просто как консультантов в области бизнеса и сажали в заранее подготовленную комнату. В таких случаях мы всегда настаивали на наличии лазерного принтера. Придя в отведенную комнату, мы первым делом «печатали страницу конфигурации» принтера, получая IP адреса DNS серверов, адреса маршрутизации по умолчанию, маску сети, IP и MAC адреса самого принтера. После этого, подставив IP и MAC адрес принтера в настройки одного из наших компьютеров, мы принимались за прослушивание(sniffing) сетевого трафика, тем самым избегая возможности быть обнаруженными, например, программой arpwatch, которая сразу оповестит о появлении в локальной сети нового устройства с неизвестным ранее MAC адресом. Да, мы обошли одну из защит, но что если в компании используется система обнаружения вторжений, специальный защищенный сервер для хранения и анализа журналов безопасности, шифрование сетевого трафика, сегментация сети, внутренние межсетевые экраны, программы, следящие за изменениями файловой системы на критичных серверах и рабочих станциях? При такой защите любой хакер рано или поздно оставит следы своего присутствия.

Но зачем хакеру идти таким длинным и опасным путем? Гораздо проще попытаться проникнуть в корпоративную сеть сидя в машине, недалеко от вашего офиса, что-то делая на своем компьютере. Используя же специальную антенну и карту беспроводного доступа, он может находиться и во дворе соседнего с вашим офисом жилого дома. А если он еще изменил MAC адрес и зашифровал диск компьютера с помощью Drive Crypt Plus Pack или PGP, то Вам будет очень сложно доказать его виновность. Такой хакер практически недосягаем. Если вы не уделили достаточного внимания защите вашей беспроводной сети, то стандартные механизмы защиты остановят его лишь на несколько часов.

Стандартные средства защиты, такие как закрытые ESSID, фильтрация MAC адресов и протоколов не сделают вашу беспроводную сеть безопасной, а могут лишь задержать хакера на короткое время.

Дело в том, что ESSID в явном виде присутствует во фреймах повторной аутентификации(reauthentication) и установления соединения(reassociate). Таким образом, посылая пакеты деаутентификации(deauthentication) можно получить ESSID. Так же просто обойти фильтрацию MAC адресов. Для этого достаточно некоторое время прослушивать сетевой трафик, в котором передаются MAC адреса клиентов сети. После получения MAC адреса возможны два варианта: дождаться окончания работы клиента и попробовать войти в сеть с его MAC и IP адресом, либо войти в сеть сразу, не дожидаясь окончания его работы. Во втором случае, рекомендуется отключить ARP на беспроводном интерфейсе и по возможности посылать минимум пакетов с этого интерфейса. Существуют еще несколько технических деталей направленных на то, как не оказаться замеченным беспроводной системой обнаружения вторжений. В результате наших действий, мы превратились в сетевого близнеца санкционированного пользователя беспроводной сети. Также можно послать беспроводной точке доступа фрейм деаутентификации от имени интересного нам клиента, и попробовать самим аутентифицироваться вместо него. Фильтрацию протоколов обойти сложнее. К счастью для хакеров и несчастью для сетевых администраторов, очень немногие точки доступа могут правильно определить правила фильтрации протоколов. А там, где они определены правильно, на помощь хакеру приходят MITM (Man-In-The-Middle) атаки для SSH, HTTPS, DNS протоколов. Не стоит забывать, что если хакеру удалось подключиться к беспроводной сети, то этого вполне достаточно для поиска открытых портов хостов беспроводной сети, определения сервисов, поиск уязвимостей и проникновение через уязвимые места. Поэтому автор надеется, что клиенты вашей сети защищены персональными межсетевыми экранами, и для аутентификации используется по меньшей мере 802.1x/EAP-TLS(Extensible Authentication Protocol-Transport Layer Security).

Следующий этап действий хакера это преодолеть шифрование WEP, если, конечно, оно используется. Насколько легко ему это сделать?

Здесь хакеру придется воспользоваться программой, реализующей одну из следующих атак:

- Атака последовательным перебором;
- FMS атака или улучшенная FMS атака;
- Внедрение специального сгенерированного трафика для ускорения взлома WEP.

Атака последовательным перебором эффективна только для 40-битных ключей WEP и не подходит для 108-битных ключей. К сожалению, многие производители оборудования беспроводного доступа допустили существенные ошибки приняв «де факто» 40-битный WEP алгоритм. Его недостатки существенно снижают количество возможных WEP ключей с 2^{40} до 2^{21}, и тем самым необходимое для перебора время (например, до 15 с на 1600 MHz Pentium® M автора).

Одной из наиболее известных атак на WEP является так называемая Флухрер, Мантин, Шамир (Fluhrer, Mantin, Shamir - FMS) атака. После опубликования ими статьи «Weaknesses in the Key Scheduling Algorithm of RC4», атака была реализована в таких известных программах, как Wep_crack и AirSnort. Однако, через некоторое время H1kari из Dasb0den Labs предложил улучшенный вариант этой атаки в статье «Practical Exploitation of RC4 Weaknesses in WEP Environments». Если раньше для взлома WEP требовались 6 миллионов пакетов, то при использовании улучшенной атаки FMS, достаточно 500 тысяч. Интересую-

щиеся технические специалисты могут более подробно познакомится с программой dwepcrack из комплекта BSD-airtools написанного H1kari. Эта программа реализует улучшенную FMS атаку.

Закономерность успешного взлома WEP такова, что чем больше хакер собрал пакетов беспроводного трафика, тем больше вероятность удачного взлома. Так как WEP не содержит элементов проверки целостности, ничего не мешает хакеру внедрить специально сгенерированный трафик, который впоследствии поможет ему значительно сократить время взлома. Для этого ему потребуется перевести свою беспроводную карту в режим RFMON для прослушивания трафика. Существует определенное заблуждение, которое автор слышал от технических специалистов, о том, что беспроводная карта не может ничего передавать, если находится в режиме RFMON. Это не соответствует действительности. Карта в этом режиме может передавать, однако не может подтверждать успешную передачу, посылая ACK пакеты. Для целей внедрения специально сгенерированного трафика, автор пользуется программами Wepwedgie и reinj. Необходимо отметить, что использование одной из вышеназванных программ позволяет проводить обнаружение и сканирование хостов, даже при отсутствии знания ключа WEP.

В зависимости от уровня безопасности атакуемой сети, хакер может перейти к атакам MITM и использованию подставных точек доступа.

В этом случае, обычно применяется основанная на одном из компьютеров хакера, точка доступа, в то время как его второй компьютер используется для создания помех для физического уровня модели OSI. Создание помех приводит к отказу в обслуживании настоящей точки беспроводного доступа и возможности представить подставную точку доступа клиентам беспроводной сети. Атака MITM совсем не обязательно должна быть только одного 1-го или 2-го уровня. Комбинирование атак двух уровней доказало свою высокую эффективность на практике.

Последнее, с чем обычно сталкивается хакер, это преодоление защиты, построенной с помощью 802.1x и/или VPN.

Если защита, построенная на основе 802.1x, поддерживает EAP-TLS, EAP-TTLS, EAP-PEAP, то в этом случае, хакеру ничего не остается делать, кроме как направить свои силы на преодоление защиты сервера сертификатов, если, конечно, он сможет получить к нему доступ. Однако, в Москве, по опыту автора, наиболее часто используется EAP-LEAP. EAP-LEAP, также как и EAP-MD5 проводят аутентификацию по паролю, не используя сертификаты. Таким образом, атака на EAP-LEAP, на самом деле, представляет собой атаку на MS-CHAPv2. Технические специалисты могут поэкспериментировать с утилитами «Leapcrack» и «Asleap-imp». EAP-MD5 подвержен атаке MITM, так как в этом случае, аутентификация между точкой доступа и клиентом является однонаправленной. Подставная точка доступа и сервер RADIUS, установленные на компьютере хакера, могут перенаправить трафик пользователей на подставной RADIUS сервер, который на запросы аутентификации пользователей всегда будет отвечать положительно.

Атаки, направленные на VPN заслуживают отдельной статьи, поэтому автор ограничится констатацией общеизвестных фактов. Из VPN решений наиболее часто используются следующие: PPTP(Point-to-Point Tunneling Protocol), IPsec и VPN, основанные на использовании SSL. Существует бесчисленное множество утилит для атак PPTP. Автор, в своей профессиональной деятельности, ис-

пользует anger и ettercap. Относительно атак IPsec, необходимо отметить, что, на самом деле все такие атаки направлены на определенные варианты его реализации, а не на сам алгоритм. Например, следующие варианты реализации были подвержены атакам переполнения буфера или MITM:

- PGPFreeware 7.03 – PGPNet
- WAVEsec
- SafeNet
- Cisco VPN Client
- CheckPoint VPN-1/SecureClient

Если хакеру не удалось преодолеть меры защиты вашей беспроводной сети, то почему бы ему не провести атаку в обслуживании (DoS – Denial of Service)?

К сожалению, особенностью существующих беспроводных сетей является невозможность из защиты от атак в обслуживании 1-го и 2-го уровня модели OSI. Наиболее часто используются следующие атаки:

1. Помехи для физического уровня. Представьте, что хакер для того, чтобы создать помехи вашей беспроводной сети, вооружился беспроводной картой с повышенной мощностью передаваемого сигнала, например 23 dBm (200-mW), и направленной антенной (24 dBm). В этом случае, EIRP(effective isotropic radiated power) будет примерно 45 dBm (2 dBm составляют потери соединений антенны с картой). Переведя эту цифру в Ватты, мы получим 31 Вт, тогда как разрешенная мощность составляет 1 Вт! Но разве хакер заботится о разрешениях? Он просто запускает на своем компьютере программу создающую беспорядочный трафик для вашей беспроводной сети с помощью FakeAP, Void11 или File2air.

2. Помехи, вызываемые пакетами прекращения соединения и аутентификации. Это наиболее известная и широко используемая атака, поддерживаемая программами dinject, omerta, void11, wlan_jack, File2ir.

3. Атака с помощью неправильно сформированного пакета аутентификации. В результате этой атаки, точка доступа посылает клиенту сообщение с информацией о получении пакета аутентификации в неправильной последовательности. Это приводит к деаутентификации клиента. Атака может быть выполнена с помощью fata_jack.

4. Атака, вызывающая заполнение буферов соединения и аутентификации беспроводной точки доступа. Многие беспроводные точки доступа никак не защищены от этой атаки и получение ими определенного количества пакетов аутентификации и установления соединения приводит к невозможности принятия новых запросов. Один из вариантов такой атаки выполнен в виде программы на языке Perl: macfld.pl.

НОВЫЕ СТАНДАРТЫ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ 802.11I И WPA.

Пока проходил очередной этап обсуждения нового стандарта безопасности беспроводных сетей 802.11i, Wi-Fi альянс(http://www.wi-fialliance.org) предложил использование WPA(Wireless Protected Access). В свою очередь, WPA предложил реализацию практически того же, что обсуждалось в стандарте 802.11i. Применение, как вышеназванных стандартов, так и своих собственных разработок ведущими поставщиками оборудования, предотвратило использование широко известных уязвимостей, связанных, например, с WEP, в тоже время принесло новые опасности. Например, при использовании

802.11i/WPA/WPA2 внедрение специальных пакетов в трафик, стало практически невозможным из-за использования механизмов обеспечения целостности: TKIP(Temporal Key Integrity Protocol) и CCMP(Counter Mode with CBC-MAC).

Однако эти стандарты существенно упростили задачу хакера по проведению атак, вызывающих отказ в обслуживании. Что будет, если при использовании TKIP, хакер нарушит целостность пакетов трафика? В соответствии со стандартом, если обнаружен один и более пакет с нарушенной целостностью, точка доступа разрывает соединение на одну минуту и генерирует новый ключ сеанса. Таким образом, хакер, вставляющий пакет в трафик между клиентом и точкой беспроводного доступа каждую минуту, способен вывести соединение из строя на продолжительное время. Теперь представьте действия ИТ службы, не понимающей, что происходит, и пользователей, отрезанных от информационных систем предприятия. Да, в статьях и специализированной литературе о безопасности беспроводных сетей, подчеркиваются опасности атак, вызывающих отказ в обслуживании, и, как правило, не рекомендуется применять беспроводные сети для организации работы критичных Бизнес-Приложений. Но ведь беспроводные сети – это так удобно, ведь пользователи могут работать вне зависимости от наличия определенных мест офиса, оборудованных точками проводного доступа. А учитывая существенные затраты на кабельные работы, очень многие компании в Москве оборудовали свои новые офисы беспроводными сетями, не уделив должного внимания их безопасности.

ПРОВЕРКА БЕЗОПАСНОСТИ ВАШЕЙ БЕСПРОВОДНОЙ СЕТИ.

Если, прочитав эту статью, у Вас пропала уверенность относительно безопасности вашей беспроводной сети, то единственное, что можно и нужно сделать – это проверить можно ли действительно попасть в вашу беспроводную сеть, заказав тест на проникновение (penetration test).Возможно, результаты теста укажут на необходимость изменить применяемые правила доступа к сети, использовать специальные VPN решения, аутентификацию на основе сертификатов и внедрить одну из беспроводных систем обнаружения вторжений.

Системы обнаружения вторжений для беспроводных сетей развиваются очень стремительно, и хотя ни одна из коммерческих и бесплатных версий представленных на рынке не гарантирует 100% обнаружения хакера, с точки зрения безопасности, лучше ее иметь. Даже если такая система обнаруживает новые ESSID и MAC адреса, это может позволить вовремя обнаружить попытки получения доступа, предпринятого юным читателем журнала «Хакер». Обращаясь к консультантам в области информационной безопасности, выясните у них, какую методологию и что за инструменты они будут использовать. Если окажется, что из оборудования и программного обеспечения, необходимого для тестирования, у них есть встроенная в компьютер карта беспроводного доступа и один из следующих коммерческих продуктов: NAI Sniffer Wireless, WildPacket's AiroPeek, AirMagnet и бесплатный Netstambler, то вам следует проявить осторожность при заказе услуг у таких консультантов. Так как этих продуктов явно недостаточно для проведения тестирования. Также, вы можете поинтересоваться, по какому принципу работает Netstambler. Если Вам скажут, что это сниффер, анализирующий беспроводной трафик, то это укажет на некомпетентность консультанта в данном вопросе. На самом деле Netstumbler (или более расширенная Unix версия dstumbler из комплекта BSD airtools), представляет собой обычный сканер, посылающий специально сформирован-

ный пакет, в ответ на который точка беспроводного доступа отвечает номером канала, ESSID, признаком наличия WEP и уровнем сигнала. Проблема заключается в том, что, во-первых, так называемые «закрытые сети» не отвечают на такие фреймы. А во-вторых, грамотный сетевой администратор должен поставить фильтр на такие запросы. Поэтому, использование Netstambler не позволит обнаружить все беспроводные сети. Более того, так как процесс Netstambler'a двухсторонний, это означает, что с его помощью можно обнаружить беспроводные сети, находящиеся в пределах области передачи вашей беспроводной карты, которая, безусловно, проигрывает самой себе оборудованной специальной антенной в области приема. Но хакеры не только поэтому не пользуются Netstambler'ом. Беспроводным системам обнаружения вторжений очень легко обнаружить такие фреймы. Зачем же им будут пользоваться профессиональные консультанты в области информационной безопасности? Хотя автору попадались на глаза курсы по безопасности беспроводных сетей, в программе которых присутствует демонстрация возможностей и обучение работе с Netstambler.

Несмотря на постоянные утверждения поставщиков оборудования беспроводного доступа, о новых механизмах защиты, начиная с версии 10.X, основной проблемой обеспечения безопасности будут оставаться как технические, так и организационные факторы. Отсутствие программы повышения информированности пользователей в области безопасности будет способствовать успешному проведению хакером атак, направленных на получение информации и паролей, необходимых для проникновения в защищенную сеть(social engineering). Отсутствие необходимого обучения администраторов будет приводить к неправильной, с точки зрения безопасности, организации правил доступа и контроля вашей беспроводной сети. Причем в последнем случае, обучение администраторов, как правило, заключается в демонстрации возможностей программы AirMagnet специалистами системного интегратора, установившего оборудование беспроводной сети.

В феврале-мае 2005 года автор планирует прочитать курс, посвященный особенностям получения несанкционированного доступа и построению защиты беспроводных сетей, в учебном центре «Микроинформ».