Радио-мираж

В статье излагаются некоторые способы исследования беспроводных сетей на устойчивость ко взлому и предложены программные методы борьбы со злоумышленниками.

Александр Красоткин

Римляне первыми в известной истории поняли важность дорожных коммуникаций для военного и экономического развития государства. Более двух тысяч лет назад в древней империи на дорогах ставились мильные столбы, составлялись точные дорожные карты и продавались итинерарии, весьма напоминающие современные путеводители. Строительство новых дорог заблаговременно планировалось. Они редко проходили по болотистым местностям и строились в прямом направлении на максимально возможную длину. В пересеченной местности на дорогах уменьшали уклон для безопасности и удобства передвижения путников. На поворотах полотно дороги делалось шире, чтобы едущие навстречу повозки могли разминуться, не сцепившись бортами.

Прошло более двадцати веков, но некоторые дороги и мосты Римской империи используются до сих пор. Что же касается планирования строительства новых магистралей, современные технологии отнюдь не отменяют сформулированный римскими инженерами постулат: дорога должна быть удобной для путников и минимизировать время прохождения по данному маршруту. А асфальт и бетон — это всего лишь строительные материалы.

Подобная ситуация наблюдается и в иных сферах. Новая технология ничуть не перечеркивает опыт, наработанный ранее, а скорее добавляет новые задачи в список проблем. Аналогично и с беспроводными сетями. Удобство развертывания и мобильность клиентов оборачиваются легкостью несанкционированного перехвата трафика. Методики криптозащиты передаваемых данных уязвимы в случае длительного прослушивания трафика, что демонстрируется утилитой Aircrack-ng, справляющейся с криптозащитой протокола 802.11 WEP и WPA/WPA2-PSK. В конечном итоге время преодоления криптозащиты зависит от вычислительной мощности атакующей системы. На практике этот процесс занимает от нескольких часов до нескольких дней. К тому же не стоит забывать о требованиях законодательства США к разработчикам криптографического программного обеспечения о необходимости «черного хода», позволяющего дешифровать закодированную информацию. Аналогичные требования есть и в нашей стране. И хотя вероятность, что внутрисетевым трафиком заинтересуются спецслужбы, намного меньше вероятности хакерского интереса, следует признать факт: рано или поздно криптозащита беспроводной сети будет преодолена. Возможность взлома — это не приближающийся крах, а повод обратиться к богатому опыту борьбы с сетевыми злоумышленниками, наработанному еще до того, как беспроводные сети вышли за статус опытов в экспериментальных лабораториях.

Если при пассивном перехвате трафика злоумышленника вычислить нельзя, то, решившись на активные действия, он дает шанс себя обнаружить. Изучение журналов регистрации доступа к сетевым ресурсам и отчетов систем обнаружения вторжений (Snort, к примеру) занятие настолько же скучное, насколько и эффективное для выявления нестандартной активности. Но предоставлять промышленные ресурсы для свободного изучения взломщикам сети, пожалуй, несколько рискованно. Лучше подкинуть «аппетитно» выглядящую приманку, атака на которую не повлияет на работоспособность реальной сети. Значительную помощь в «ловле на живца» окажет применение методики систем ловушек — Honeypot. Их основная цель — вызывать «огонь на себя». Имитируя уязвимые сетевые системы, они отвлекают внимание злоумышленников от рабочих систем. А будучи атакованными, собирают доступную информацию о взломщиках и примененных ими методах.

Главное из достоинств данной методики в том, что системы Honeypot не дают ложных срабатываний. Это объясняется тем, что, если использованные для ловушек сетевые адреса не рекламируются (нет объявлений о предоставлении ресурсов к публичному доступу), любая активность, направленная на них, априори

не является санкционированной владельцами сети. Кстати, из этого факта не стоит делать вывод, что ловушки лучше, чем системы обнаружения вторжений, ложные тревоги у которых бывают нередки. Просто у них разные задачи. И лучшим решением будет использовать эти технологии в связке.

Среди множества различных систем ловушек следует упомянуть одну из наиболее интересных на данный момент разработок — Honeyd. Эта программа дает возможность, базируясь на одном сетевом компьютере, создавать до 65535 уникальных хостов-фантомов. Для их описания используется несложный конфигурационный файл. Виртуальные хосты имитируют различные операционные системы на уровне сетевых протоколов. Что в результате позволяет серьезно озадачить злоумышленников и вычислить их еще на ранних этапах подготовки взлома.

Созданные системой Honeyd хосты можно объединять в виртуальную сеть. Задав топологию такой сети, схему маршрутизации и определив процент потерь пакетов, можно обеспечить взломщику ощущение исследования настоящей рабочей сети. Имитация работы сервисов хостов-фантомов достигается путем переброски соединений на рабочие сервисы или использованием специально разработанных интерактивных сценариев. Сценарии можно легко модифицировать и добавлять новые.

Примечательно, что для придания сетевым фантомам реалистичности взяты базы данных сетевых сканеров Nmap и Xprobe, в свою очередь предназначенных для определения доступных сервисов и типов операционных систем. Идея использовать инструментарий «сетевых исследователей» для их же мистификации оказалась удачной. Незаметно отличить сетевой фантом от реальной системы — задача, требующая времени. Большинство же взломщиков терпеливостью не отличаются, и не нужно это время им предоставлять.

Сообщения системы Honeyd о несанкционированной активности наряду со своей наглядностью отличаются некоторой лаконичностью. Если же стоит задача собрать детальную информацию о сетевых атаках, журнала сообщений Honeyd будет недостаточно. Следует подключать какую-либо сетевую систему обнаружения вторжений. Например, Snort. Как и Honeyd, это программное Open Source-решение, в свою очередь обносящееся к классу сетевых систем обнаружения вторжения (Network Intrusion Detection System, NIDS).

Сетевые системы обнаружения вторжения функционируют на сетевом уровне по модели OSI. Ими осуществляется контроль устанавливаемых соединений, анализ структуры и содержимого сетевых пакетов. NIDS может работать как на отдельном компьютере, контролируя свой собственный трафик, так и на выделенном сервере (шлюз, маршрутизатор, зонд), анализируя весь проходящий трафик. При обнаружении атаки NIDS включает механизм реагирования на данный тип угрозы. Спектр возможных действий довольно широк. От передачи предупредительных сообщений на рабочую консоль (e-mail, пейджер, телефон, факс, syslog-сервер, определенный пользовательский файл, UNIX-сокет или службу Windows WinPopup) до блокировки учетной записи, разрыва соединения, реконфигурации брандмауэра или маршрутизатора. Системы обнаружения вторжения имеют собственную базу знаний об известных типах сетевых атак, а также могут предоставлять возможность разработки и включения пользователем новых описаний сетевых инцидентов.

Система Snort позволяет в режиме реального времени осуществлять анализ сетевого трафика, проверяя корректность структуры сетевых пакетов, соответствие содержимого определенным правилам. Для описания сетевых инцидентов и определения реакции системы используется гибкий язык сценариев. Встроенная база знаний позволяет определить распространенные типы сетевых инцидентов, таких как: «скрытое» сканирование (использующее установленные в сетевых пакетах флаги FIN, ASK); сбор баннеров сетевых сервисов (Services & OS fingerprinting); атаки на переполнение буфера различных сервисов; атаки, использующие преднамеренное нарушение структуры сетевых пакетов (ping of death); атаки вида «отказ в обслуживании» (DoS/DDoS) или эксплуатирующие известную уязвимость сервисов.

При фиксировании системой Snort описанного сетевого инцидента можно, конфигурируя брандмауэр, прервать сетевую атаку, передать предупреждающее сообщение администратору по электронной почте, SMS или иным способом.

Snort, помимо работы в режиме сетевой системы обнаружения вторжения, может работать в двух основных конфигурациях: как пакетный сниффер (анализатор сетевого трафика, аналог tcpdump) и в режиме сбора и сохранения информации обо всех переданных/полученных пакетах (что удобно для диагностики сети).

В завершение отмечу, что убедиться, насколько беспроводная сеть недоступна для несанкционированного перехвата трафика и устойчива к вторжению, можно лишь проведением аудита. И хотя исследование сетевой безопасности — тема достаточно сложная, на должном уровне требующая профессионального подхода, первичный анализ вполне можно провести доступным в Интернете инструментарием. Например, Airmon-ng удобен для переключения сетевого интерфейса в режим прослушивания всего трафика, передаваемого на Wi-Fi-частотах. Для перехвата трафика можно использовать Kismet и Airodump-ng. Они также позволяют вычислить и «скрытые» сети, точки доступа которых не передают маячковых сигналов. С целью активного исследования выбранной беспроводной сети путем вброса определенным образом сформированных сетевых пакетов можно задействовать Aireplay-ng. А надежность криптозащиты трафика можно проверить с помощью Aircrack-ng. Все упомянутые утилиты доступны в Интернете в виде исходных кодов и хорошо задокументированы.

Если же проведенный анализ показал удовлетворительный результат — сеть устойчива к взлому, — все же забывать про угрозу вторжения не стоит. Преодоление защиты — это лишь вопрос времени и технологий.