хакеры любят мед

крис касперски ака мыщъх, no-email

последнее время появляются все более и более изощренные системы борьбы с хакерами, одним из которых является honeypot – своеобразный капан для атакующих. сколько молодых парней отправились за решетку с его помощью! даже в нашей, традиционно лояльной к хакерам стране, имеется несколько случаев условных осуждений. если так пойдет и дальше, то хакерствовать станет просто невозможно, если, конечно, не задавить идею honeypot'ов в зародыше, доказав ее неэффективность.

введение

Как ни защищай свой курятник, хитрая лисица все равно найдет дыру и утащит самую жирную курицу. Всех дыр ведь не заткнешь… Но можно попробовать поймать лису в капкан, подложив ей соблазнительную приманку и потом – бабах! – выстрелить в упор из ружья. С компьютерами – та же история. Программное обеспечение уязвимо. Своевременная установка заплаток отсекает лишь наиболее тупых из хакеров, использующих для атаки готовые программы и не привыкших думать головой. Профессиональных же взломщиков, занимающихся самостоятельным поиском новых дыр, заплатки не останавливают.

Рассказывают, что один джентльмен однажды приобрел супер-навороченный сейф и долго хвастался какой он надежный и прочный. Дело кончилось тем, что забравшиеся к нему грабители прожгли какой-то хитрой кислотой в сейфе дыру и… не обнажили ничего! Деньги и драгоценности хранились совсем в другом месте.

Подобная тактика широко используется и для обнаружения компьютерных атак. На видном месте сети устанавливается заведомо уязвимый сервер, надежно изолированный ото всех остальных узлов, и отслеживающий попытки несанкционированного проникновения в реальном времени с передачей IP-адреса атакующего в ФСБ или подобные ему органы. Даже если хакер спрячется за хитрой прописью (proxy), Большой Брат все равно найдет его и в слетающую с петель дверь ворвутся не дружелюбно настроенные маски-шоу.

Сервер, выполняющий роль приманки, на хакерском жаргоне называется "***горшком с медом***" (или по-английски ***honeypot***), а сеть из таких серверов, соответственно, ***honeynet***. Этимология этого названия восходит к английскому поверью, что если оставить горшок с медом, на него слетятся пчелы (хакеры). И кому только могло прийти в голову назвать хакеров пчелами? Хакеры – это мыши, хомяки и крысы! Но мед они все-таки любят. И доверчиво ловятся на него.

Противостоять honeypot'ам чрезвычайно сложно. Внешне они ничем не отличаются от обычных серверов, но в действительности представляют собой хорошо замаскированный капан. Один неверный шаг и хакеру уже ничто не поможет. Утверждают, что опытная лиса ухитряется съесть приманку, не попавши в капкан. Так чем же мы – хакеры – хуже?

внутри горшка

Типичный honeypot представляет собой грандиозный программно-аппаратный комплекс, состоящих из следующих компонентов: узла-приманки, сетевого сенсора и коллектора (накопителя информации).

Приманкой может служить любой север, запущенный под управлением произвольной операционной системы и сконфигурированный на тот или иной уровень безопасности. Изолированность от остальных участков сети препятствует использованию сервера-приманки как плацдарма для атак на основные узлы, однако, дает хакеру быстро понять, что он на полпути к ловушке и отсюда следует немедленно ретироваться заметая следы. Теоретически, администратор может организовать подложную локальную сеть, практически же это оказывается неподъемно дорогостоящим решением и приходится искать компромисс – либо ослабленная изоляция, ограждающая только критически важные узлы, либо эмулятор локальной сети, запущенный на одном компьютере. Чаще всего узлов с приманкой бывает несколько. Одни из них содержат давно известные дыры и рассчитаны на начинающих хакеров, только-только осваивающих командую строку и читающих книги десятилетней давности. Другие – защищены по самые помидоры и ориентированы на выявление еще неизвестных атак, совершающихся опытными взломщиками. Поэтому, даже обнаружив новую дыру, не спешите

ломиться на первый же попавшийся сервер. Ведь, если атака завершиться неудачно, информация об уязвимости попадет в загребущие лапы специалистов по информационной безопасности, а вы – на скамью подсудимых или (что еще хуже) больничную койку – пересчитывать перебитые ребра. Кстати говоря, очень многие узлы-приманки построены на оси с настройками по умолчанию. И в этом есть свой резон. Дыры умолчаннных конфигураций хорошо известны, что обеспечивает максимальный приток атакующих – это раз. У атакующего создается обманчивое впечатление, что он имеет дело с администратором-недоучкой, поставившим стандартный дистрибьютив не первой свежести и ни хрена не смыслящего в вопросах безопасности. Действительно, большинство начинающих администраторов именно так и поступают, однако, риск попасться в капан honeypot'a слишком велик и от атаки лучше всего воздержаться.

Сетевой сенсор чаще всего реализуется на базе UNIX-подобной ОС, а для мониторинга информации используется утилита tcpdump или ее аналоги. В зависимости от конфигурации сети, сенсор может находится как на одном из узлов данного сегмента локальной сети, так и являться маршрутизатором, расположенным перед приманкой. Иногда сетевой сенсор совмещается непосредственно с самой приманкой. Это существенно упрощает и удешевляет систему honeypot'a, однако, ослабляет ее иммунитет (захватив управление приманкой, атакующий быстро обнаружит сенсор и сделает ему харакири). Размещение сенсора внутри широковещательного сегмента обеспечивает ему наибольшую скрытность. Сетевой интерфейс сенсора может и не иметь собственного IP-адреса, прослушивая трафик в Stealth-режиме, что достигается путем физического обрезания передающего провода на сетевой карте (подробнее см. статью о снифферах). Маршрутизатор в этом смысле намного более заметен, однако, определить работает ли на нем сетевой сенсор или нет, в общем случае невозможно.

Дампы tcpdump'a обрабатываются различными анализаторами (например, системами обнаружения вторжений), во-первых, распознающими сам факт атаки, а, во-вторых, определяющими IP-адрес нарушителя. Накапываемая информация оседает в коллекторе, сердцем которого является база данных. Это самое уязвимое место honeypot'a. Необходимо заранее выбрать четкий набор критериев, позволяющих однозначно определить какие действия являются нормальными, а какие нет. В противном случае, администратор будет либо постоянно дергаться, вздрагивая от каждого сканирования портов, либо пропустит слегка видоизмененный вариант известной атаки. Есть и другая проблема. Если приманка не имеет никакого другого трафика, кроме хакерского (что легко определить по характеру изменения поля ID в заголовках IP-пакетов, подробнее о котором рассказывалась в статье о брандмауэрах), то атакующий немедленно распознает ловушку и не станет ее атаковать. Если же приманка обслуживает пользователей внешней сети, непосредственный анализ дампа трафика становится невозможным и хакеру ничего не стоит затеряться на фоне легальных запросов. Достаточно эффективной приманкой являются базы данных с номерами кредитных карт или другой конфиденциальной информацией (естественно, подложной). Всякая попытка обращения к такому файлу, равно как и использование похищенной информации на практике, недвусмысленно свидетельствует о взломе. Существуют и другие способы поимки нарушителей, но все они так или иначе сводятся к жестким шаблонам, а значит, в принципе неспособны распознать хакеров с нетривиальным мышлением.

Короче говоря, возможности honeypot'ов сильно преувеличены и опытный взломщик может их обойти. Попробуем разобраться как.

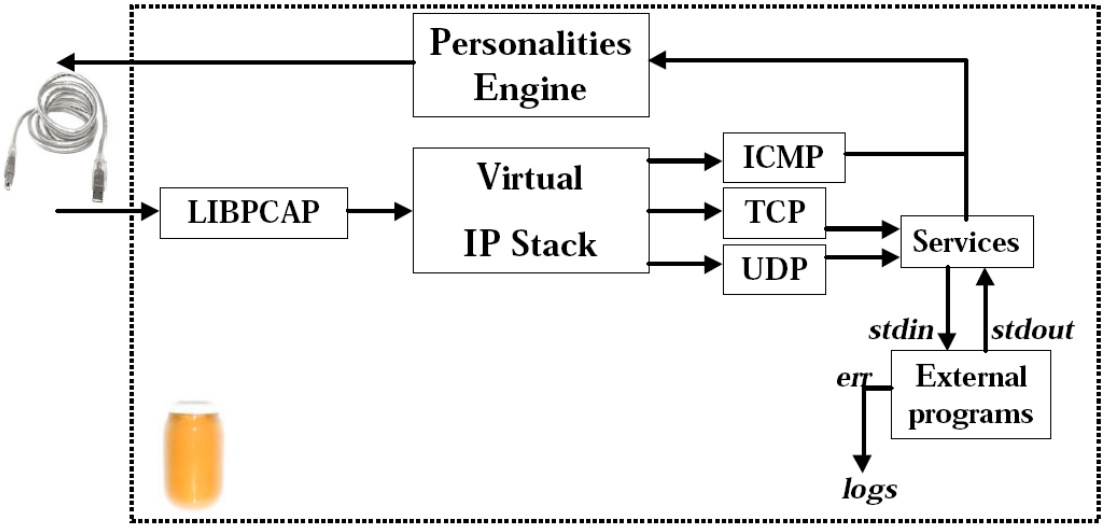

Рисунок 1 блок-схема простейшего honeypot'а

подготовка к атаке

Для начала хакеру потребуется надежный канал связи, чтобы дяди из органов не могли его отследить. Строго говоря, отслеживаются все каналы, однако, степень защищенности каждого из них различна. Если вы находитесь в широковещательной сети, для успешной маскировки можно ограничиться клонированием чужого IP и MAC-адреса (естественно, клонируемая машина в момент атаки должна быть неактивна). При условии, что в локальной сети не установлено никакого дополнительно оборудования для определения нарушителей, идентифицировать хакера практически невозможно, хотя здесь есть одно "но". Если машина хакера уязвима, honeypot может незаметно забросить на его компьютер "жучка" со всеми вытекающими отсюда последствиями. Многие начинающие злоумышленники ловятся на cookie, переданные через браузер (вот ламеры!).

Для надежности, лучше атаковать жертву не напрямую, а через цепочку из трех-пяти хакнутых компьютеров, а в Интернет выходить по протоколу GPRS через чужой сотовый телефон, как можно дальше отъехав от своего основного места жительства, чтобы вас не смогли запеленговать. Выходить в сеть по коммутируемому доступу – равносильно самоубийству, в особенности со своего домашнего номера. Не надейтесь ни на какие proxy – они вас не спасут, точнее могут не спасти, поскольку никогда заранее неизвестно: протоколирует ли данный proxy-сервер все подключения или нет. Многие бесплатные proxy в действительности являются приманками, установленными спецслужбами и существенно помогающим им в отлове хакеров.

срывая вуаль тьмы

Прежде чем, бросаться в бой, необходимо тщательно изучить своего противника: реконструировать топологию сети, определить места наибольшего скопления противодействующих сил и, естественно, попытаться выявить все honeypot'ы. Основным оружием хакера на этой стадии атаки будет сканнер портов, работающий через "немой" узел и потому надежно скрывающий IP-атакующего (подробнее см. статью о брандмауэрах).

Явно уязвимые сервера лучше сразу отбросить – с высокой степенью вероятности среди них присутствуют honeypot'ы, дотрагиваться до которых категорически небезопасно. Исключение составляют, пожалуй, лишь основные публичные сервера компании, расположенные в DMZ-зоне – совмещать их honeypot'ом никому не придет в голову, правда, на них вполне может работать система обнаружения вторжений.

Безопаснее всего атаковать рабочие станции, корпоративной сети, распложенные за брандмауэром (если такой действительно есть). Вероятность нарваться на honeypot минимальна. К несчастью, для атакующего, рабочие станции содержат намного меньше дыр, чем серверные приложения, а потому атаковать здесь особенно и нечего.

артобстрел отвлекающих маневров

Выбрав жертву, не торопитесь приступать к атаке. Прежде убедитесь, что основные признаки honeypot'a отсутствуют (узел обслуживает внешний трафик, имеет конфигурацию отличную от конфигурации по умолчанию, легально используется остальными участниками сети и т. д.). Теперь, для нагнетания психологического напряжения, несколько дней интенсивно сканируйте порты, засылая на некоторые из них различные бессмысленные, но внешне угрожающие строки, имитируя атаку на переполнение буфера. Тогда администратору будет не так-то просто разобраться имело ли место реальное переполнение буфера или нет, а если имело – то каким именно запросом осуществлялось.

Естественно, артобстрел необходимо вести через защищенный канал, в противном случае вас выдерут так, что мало не покажется (хотя с юридической точки зрения сканирование портов, не приводящее к несанкционированному доступу, вполне законно, на практике действует закон диких джунглей, гласящий – не дергай за хвост ближнего своего).

атака на honeypot

Будучи по своей природе обычным узлом сети, honeypot подвержен различным DoS-атакам. Наиболее уязвим сетевой сенсор, обязанный прослушивать весь проходящий трафик. Если хакеру удастся вывести его из игры, то факт вторжения в систему на некоторое время останется незамеченным. Естественно, атакуемый узел должен остаться жив, иначе будет некого атаковать. Будем исходить из того, что сенсор принимать все пакеты, тогда послав пакет на несуществующий узел или адресованный любому другому ненужному узлу, мы завалим вражину наповал.

Как вариант, можно наводнить сеть SYN-пакетами (ищите в Интернете описание SYN-атаки) или вызвать ECHO-death (шторм ICMP пакетов, направленный на жертву с нескольких десятков мощных серверов, что достигается спуфингом IP-адресов – т.е. посылкой эхо запросов от имени жертвы),

Саму же атаку лучше всего осуществлять поверх протоколов, устойчивых к перехвату трафика и поддерживающих прозрачное шифрование, ослепляющее сетевой сенсор. Чаще всего для этой цели используется SSH (Secure Shell), однако, он ограничивает выбор атакующего только явно поддерживающими его узлами, что сводит на нет весь выигрыш от шифрования.

утонувшие в меде

Если атакуемый узел все-таки оказался honeypot'ом, то все действия атакующего либо вообще не возымеют никакого успеха (уязвимый сервер молча "съедает" заброшенный shell-код, исправно продолжая работать), либо покажут пусто ресурс, не содержащий практически ничего интересного. В этой ситуации главное не запаниковать и не растеряться. Первым делом необходимо избавится от компрометирующего вас сотового телефона (ни в коем случае не ограничивайтесь одной лишь выемкой SIM-карты, поскольку телефон так же содержит свой собственный идентификационный номер). Затем следует смотаться с места преступления, по возможности не привлекая ни чьего внимания. Если же вы атаковали жертву из локальной сети – просто уничтожьте все относящиеся к атаке программное обеспечение и связанные с этим файлы, включая временные.

Естественно, сказанное выше, относится только к атакам на действительно серьезные ресурсы (государственные сайты, банковские учреждения и т.д.). Ожидать, что после взлома чей-то домашней странички за вас возьмутся всерьез, несколько наивно.

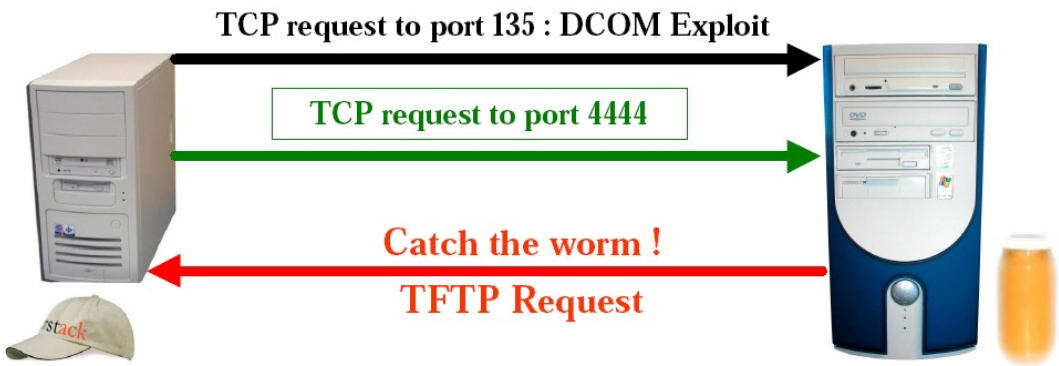

Рисунок 2 атакующий думает, что он атакует уязвимый сервис, в действительности он упал в горшок (с медом).

заключение

Сила honeypot'ов – в их новизне и неизученности. У хакеров еще нет адекватных методик противостояния, однако, не стоит надеяться, что такая расстановка сил сохранится и в дальнейшем. Архитектура honeypot'ов плохо проработана и уязвима. Уже сегодня опытному взломщику ничего стоит обойти их, завтра же это будет уметь каждый подросток, установивший UNIX, и презревши мышь, взявшийся за клавиатуру.

Рисунок 3 айда все есть мед