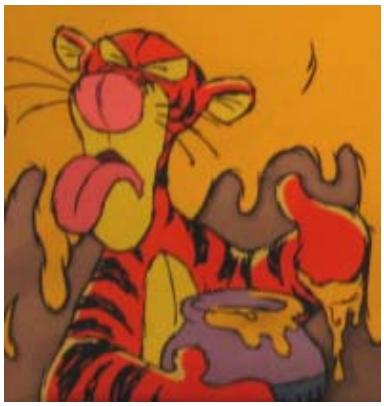
Honeypots – приманка на хакера



Эссе на тему «Honeypots»
Студента 015 группы
Заслонко М.А.

Введение

Каждый день информационные технологии становятся всё более и более важным элементом в любой компании. В то же время число компьютерных преступлений неизбежно возрастает. В настоящее время множество компаний и фирм страдают от действий различных компьютерных преступников(так называемых *хакеров*). В связи с этим были предприняты многочисленные попытки защитить и обезопасить себя в информационном плане. Но к сожалению злоумышленники изобретают всё новые и новые пути атак, когда как большинство защитных систем направлено на отлавливание наиболее распространённых видов взлома. В связи с этим встаёт серъёзный вопрос информационной безопасности внутри сети Internet а так же внутри локальных сетей. Технология Honeypots была изобретена именно для отслеживания и изучения новых способов взлома, сбора информации и специфической защиты от компьютерных злоумышленников.

Основные понятия

1. Предыстория

Сама идея создания специальной среды для отслеживания и изучения действий злоумышленников не нова, но технология Honeypots была разработана относительно недавно. Одним из тех кто воплотил её в жизнь был Лэнс Спицнер (Lance Spitzner), специалист по информационной безопасности компании Sun Microsystems. До того как заняться гражданской деятельностью, он служил офицером в танковых частях Сил Быстрого Развертывания США, откуда и взялся военный подход к обеспечению информационной безопасности и применение специфичных терминов: "противник", "тактика", "разведка".

Honeypots являются новой интересной технологией. Они позволяют нам брать инициативу в свои руки и изучать работу хакеров. Первый шаг к пониманию технологии Honeypots состоит в том, чтобы определить, что же такое на самом деле Honeypot. Это может быть сложнее чем кажется на первый взгляд. Существует множество различных определений Honeypot, и мнений по поводу того, что же он должен делать. Одни считают что это - средство для соблазнения и обмана взломщиков, другие полагают, что это - не что иное, как технология для обнаружения атак, а третьи думают, что honeypots являются реальными компьютерами, созданными для взлома и последующего изучения. По большому счёту, все эти определения верны.

В отличие от систем firewall или IDE(Intrusion Detection Systems), Honeypots не решают определённой задачи. Это очень гибкий инструмент, с помощью которого можно делать всё, от обнаружения зашифрованных атак в сетях, до предотвращения мошенничества с кредитными картами. Эта самая гибкость и придаёт данной технологии такую силу. Как сказал Лэнс Спицнер: «Honeypot – это информационный системный ресурс, чья польза состоит в его несанкционированном и незаконном использовании»

2. Технология

Honeypot(дословно – горшочек с мёдом) по сути, является компьютером – приманкой для атак. Он не предназначен для того чтобы напрямую увеличивать безопасность сетей. Наоборот, Honeypot привлекает внимание нарушителей и соответственно может привлечь внимание злоумышленника внутри сети, где тот расположен. Традиционным механизмом провокации потенциального взломщика является создание мнимого хоста – т.е. системы, имитирующей работу некоторых, потенциально интересных для взломщика сервисов. Простым примером может быть установка операционной системы в стандартной конфигурации без установки критических обновлений. Эта система устанавливается на сервер, не содержащий никакой полезной информации. Базовые версии (без установленных обновлений и исправлений (patches)) операционных систем общего назначения обычно имеют значительное количество широко известных уязвимостей.

Так как сам по себе Honeypot относительно пуст, то есть в ресурсе не расположено каких либо продуктивных систем, то любой входящий либо исходящий трафик считается подозрительным и вся полученная информация считается «интересной». Опять же из-за «пустоты» нашего Honeypot’а анализ полученной информации получается довольно простым(не создаётся каких либо лишних логов). Эта информация является довольно ценной, так как из неё можно почерпнуть новые знания о методах взлома и соответственно усилить общую безопасность сети.

Можно подумать что Honeypot так же помогает предотвращать атаки, так как долгое время удерживает взломщиков на ложной цели и отнимает их ресурсы. Но так как большинство современных атак основывается на автоматических скриптах, то Honeypot соответственно не может сдерживать конкретного злоумышленника, так как такового просто нет.

Типы Honeypots

Для лучшего понимания Honeypot'ов их принято разбивать на две категории. Это так называемые пассивные - анализирующие(research honeypots) и активные - производственные (production honeypots)

Активные Honeypot'ы предназначены для того чтобы уменьшить риск организации быть подверженным атаке(несут собой ложные цели). Кроме того, они могут быть использованы для ответной атаки. Production honeypots могут также использоваться для разоблачения и идентификации нападавшего после того, как он однажды побывал в вашей организации.

Пассивные Honeypot'ы занимаются тем, что собирают ценную информацию об атаках, когда как сами по себе не являются мерами защиты для конкретной организации.
Эта информация затем может быть использована для различных целей, таких как раннее предупреждение и предсказание атак.

Так же существует ещё две большие категории на которые подразделяют Honeypots. Это Honeypots низкого взаимодействия(low-interaction) и высокого взаимодействия(high-interaction). Взаимодействие определяет уровень активности, который Honeypot позволяет атакующему(взломщику).

1. Low-interaction honeypots

Этот вид Honeypots ограничен во взаимодействии. Он обычно предназначен для эмуляции сервисов и операционных систем. Соответственно активность атакующего будет ограничена уровнем эмуляции, который воспроизводит данный Honeypot.

Преимущество Low-interaction honeypots – это их простота. Они могут быть легко размещены и так же легко осуществляется их поддержка. Обычно они включают в себя установку программного обеспечения, выбор операционной системы и сервисов для эмуляции и мониторинга. Поэтому их размещение представляется довольно лёгким. Так же эмулируемые сервисы уменьшают риск охватывая всю активность атакующего(взломщика). Злоумышленник никогда не получит доступ к операционной системе, чтобы атаковать или навредить другим.

Основным недостатком Low-interaction honeypots является то, что они получают лишь ограниченный объём информации и созданы для того чтобы обнаруживать известные виды активности злоумышленников. Так же атакующему проще засечь присутствие honeypot'а низкого взаимодействия. Насколько бы хорошо ни была выполнена эмуляция, опытный хакер всегда сможет распознать наличие honeypot'а.

2. High-interaction honeypots

Honeypots высокого взаимодействия отличаются от предыдущей группы тем, что они сами по себе довольно сложны. Они включают в себя настоящие операционные системы и приложения. Эмуляции не происходит и атакующий получает «натуральный продукт». Если, к примеру, надо запустить FTP сервер под Linux, то мы создаём реальную систему Linux и запускаем реальный FTP сервер. Преимущества такого решения состоят в следующем:

Во-первых, можно получить исчерпывающее количество информации. Предоставив злоумышленнику настоящую систему можно изучить в полном объёме его поведение.

Во-вторых, в honeypots высокого взаимодействия не производится каких либо предположений по поводу того, как себя поведёт «противник». Вместо этого предоставляется открытая среда и вся активность фиксируется. Это позволяет изучать поведение, которое не было ожидаемо от атакующего.

Однако недостаток такого вида honeypots заключается в том, что злоумышленник может использовать реальную систему чтобы атаковать другие системы(не являющиеся приманками). Соответственно надо применять дополнительные технологии чтобы избежать этого.

Итого honeypots высокого взаимодействия могут делать всё то, что могут honeypots низкого взаимодействия, и многое другое. Однако их намного сложнее размещать и поддерживать.

3. Примеры некоторых известных Honeypots программ.

Что касается Low-interaction honeypots – хорошими примерами будут такие технологии как **Specter**(Netsec) и **Honeyd**(Niels Provos). **Honeyd** разработан для использования в Unix'овых операционных системах, таких как OpenBSD или Linux; однако вскоре будет адаптирован и к Windows. **Specter** – это коммерческий продукт, разработанный и продаваемый швейцарской компанией Netsec. **Specter** – одно из немногих honeypot-решений для сред Windows2000 и WindowsXP

В качестве примера High-interaction honeypots можно привести относительно недавно появившуюся технологию **Honeynets**, в разработке которой принимал участие сам Лэнс Спицнер. В следующей главе мы остановимся подробней на этом виде High-interaction honeypot и рассмотрим некоторые аспекты этой технологии.

Honeynets

Если использовать не отдельно стоящую систему (honeypot), а построить специализированный сетевой комплекс(объединение honeypots в сеть), то это может вывести исследование на качественно новый уровень. Такая технология объединения honeypots в сеть носит название Honeynets. Некоторые злоумышленники ищут для атаки цель с какой-то определенной уязвимостью. В honeynet может использоваться несколько различных систем одновременно и, следовательно, мы сможем наблюдать за разными категориями злоумышленников.

Рассмотрим пример типовой системы Honeynet. Она состоит из межсетевого экрана (firewall), подсистемы регистрации и собственно приманки (honeypots). На рисунке 1 изображена типовая Honeynet, в которой honeypots представлены в виде различных

операционных систем.

Honeynet может функционировать как параллельно с рабочей сетью, так и независимо от нее. Подключение к Интернет может осуществляться либо по отдельному каналу(на honeynet зарегистрирован отдельный диапазон IP-адресов), либо посредством использования маршрутизатора компании для общения с внешним миром основного - все зависит от данной ситуации.

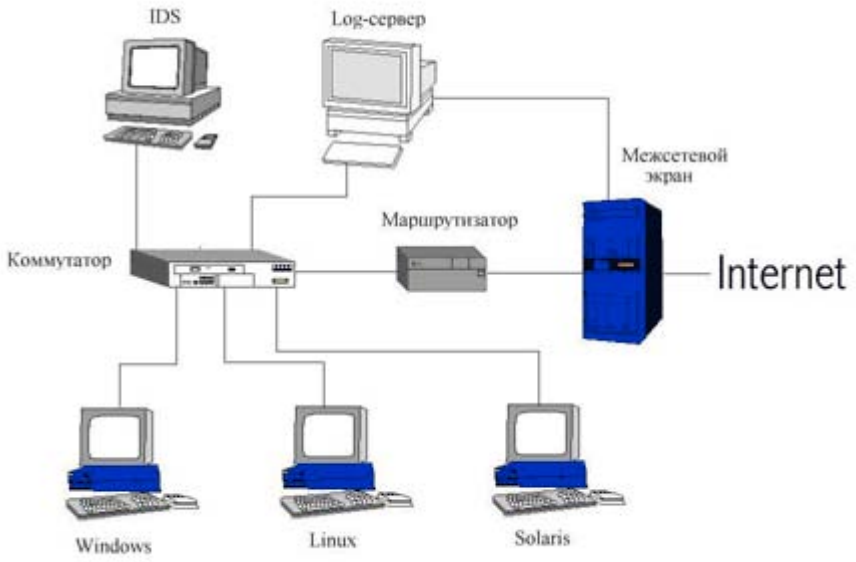


рисунок 1

В данном примере с помощью межсетевого экрана можно достаточно надежно контролировать ситуацию. Изменяя логику своего поведения (динамически менять правила фильтрации) можно исключить возможность использования какой-либо из систем, входящих в honeynet, в качестве базы для злоумышленных действий. Кроме того, большинство современных межсетевых экранов обладают также и мощной подсистемой регистрации событий. Таким образом, при помощи межсетевого экрана можно так же решать и задачу сбора данных, делая ее многоуровневой.

Использование системы обнаружения атак(IDS), а так же сервера регистрации помогает выполнять основную часть работы по регистрации и накоплению информации. При этом сервер регистрации должен получать от систем-приманок информацию о происходящих на них событиях, а компьютер на котором установлена система IDS «прослушивать» весь сетевой трафик, включая набираемые злоумышленником команды, а так же направляемый ему вывод программ.

Что касается назначения систем-приманок (honeypots), то оно очевидно. Предполагается, что эти «приманки» будут вести себя как можно более естественно, поэтому в них специально не вносят никаких серьезных изменений, например эмуляций уязвимостей или искусственного уменьшения степени защиты.

Рассмотрим функцию выполняемую маршрутизатором. Он предназначен для того чтобы скрыть от взломщика наличие межсетевого экрана. Допустим, что хакеру удалось проникнуть в одну из honeypot систем. Тогда он будет думать, что между этой системой и всемирной сетью находится обыкновенный маршрутизатор, так как довольно сложно обнаружить "прозрачно" работающий межсетевой экран.

По мере того как происходит установка, настройка и работа с honeynet, пользователь

получает драгоценный опыт по обнаружению атак, так же это помогает надлежащим образом реагировать на тот или иной инцидент с информационной безопасностью и что самое главное способствует восстановлению систем после нападения(взлома). Так же несомненным плюсом является тот факт, что данный опыт приобретается как бы на тренажере, а не на задействованной реальной системе, что в свою очередь помогает избавиться от неизбежных финансовых либо моральных потерь в процессе приобретения такого опыта традиционным способом.

Преимущества и недостатки

О преимуществах honeypots уже многое было сказано. В частности то что они просты в использовании(не требуется составления каких-либо замысловатых алгоритмов), предоставляют небольшой объём информации, которая преимущественно является очень ценной(не регистрируются большие объёмы информации)и что они могут использоваться для выявления не только известных но и новых методик взлома – всё это несомненно является большим плюсом. Но существует так же и ряд недостатков, о которых нельзя не упомянуть.

Как и любая другая технология, honeypots не лишены слабостей. Основным из недостатков данной технологии является ограниченное поле зрения. То есть honeypot может отслеживать и исследовать только ту активность, которая напрямую направлена на него. Они не смогут отслеживать атаки на другие системы, даже если находятся с ними в одной сети. При использовании более сложных видов honeypots(таких как honeynets), появляются проблемы с поддержкой таких систем, так как администрирование таких «сетей-приманок» может быть довольно ресурсоёмким. Ну и кроме всего прочего, конечно же, присутствует фактор риска, так как honeypot как и любая другая программа может быть взломан и использован против его создателей. Следующая глава как раз будет посвящена этой проблеме, в ней мы рассмотрим вопросы, связанные с безопасностью honeypots.

Безопасность Honeypots

Как видно из вышесказанного, разные типы Honeypots могут решать различные задачи. Что же касается эффективности honeypot, то при обнаружении системы-приманки она резко уменьшается. Последствия обнаружения хакером honeypot систем могут быть различными. Во-первых, он будет иметь возможность обходить их стороной в будущем и во-вторых, у него будет возможность давать системе-приманке ложную информацию, что, несомненно, запутает пользователя. Соответственно в большинстве случаев выгодно, чтобы honeypot системы оставались необнаруженными.

Не принципиально, каким типом honeypot пользоваться, так как практически любая из систем honeypot может быть обнаружена. Если хакер обладает определенными знаниями и навыками, а так же имеет доступ к необходимому ПО, то факт обнаружения honeypot становится лишь вопросом времени. При появлении новых версий honeypot или обновлении старых версий, хакеры некоторое время остаются бессильны, но по прошествии некоторого времени появляются новые методы и средства обнаружения honeypot.

Эту проблему можно попытаться решить в два этапа. Во-первых, следует понять, насколько критично обнаружение honeypot. Так как если honeypot и был обнаружен, но до этого успел собрать и передать какую то информацию, то можно считать, что он выполнил свою работу, так как обнаружил угрозу и оповестил пользователя. Если же honeypot

требуется для сбора информации, то для этого необходимо чтобы honeypot - системы работали без обнаружения довольно длительные сроки - недели или даже месяцы. В этом случае следует отказаться от использования стандартного honeypot, так как если взломщик сможет скачать такую же копию honeypot, то он сможет изучить коды что поможет ему легко обнаружить данный тип «приманки». Следует изменить поведение honeypot, так чтобы ваша приманка не была похожа ни на один из других honeypot в Интернете. В любом случае можно очень сильно усложнить жизнь злоумышленнику, если ваша honeypot система будет вести себя по-новому для него.

Что касается honeypot низкого взаимодействия, то риск немного ниже из-за того, что настоящие приложения или системы не доступны для эксплуатации. Происходит лишь имитация приложений. Однако пользователю следует осознавать то, что хакер может обойти имитируемые приложения и, следовательно, должны быть применены все мерв предосторожности по защите этих самых honeypot приложений.

Для honeypot высокого взаимодействия проблема является более актуальной. Дело в том, что в них используются реальные ОС и приложения и, соответственно, при контакте с хакером, последний имеет возможность получения полного контроля над honeypot системой. Как следствие - доля риска более высока. В случае с high-interaction honeypot следует предпринять два шага. Первый – это использование нескольких этапов контроля. В качестве второго шага можно предложить вмешательство пользователя. Следует вести пристальное наблюдение за honeypot. Следует незамедлительно проверять любую неопознанную активность(создание каких-либо процессов, скачивание информации ит.д…). Если же взломщику таки удалось внедриться в систему, то человек всегда имеет возможность разорвать соединение.

Honeypots имеют огромный потенциал, но, как и любая другая новая технология, в них встречаются некоторые недоработки. Наверняка в ближайшем будущем этим технологиям будет уделено более пристальное внимание. Ведь если бы данная технология была более распространена в сети, чем это есть сейчас, то злоумышленник бы лишний раз задумался, стоит ли атаковать подвернувшуюся систему, ведь она может оказаться не легкой добычей, а аквариумом, в котором он сам станет объектом изучения.

Использованные источники:

Lance Spitzner: Definitions and Value of Honeypots
Lance Spitzner: Problems and Challenges with Honeypots

http://www.tracking-hackers.com/

Серия статей «Know Your Enemy»
http://project.honeynet.org

Обзорная статья о системах Honeynets
http://www.bugtraq.ru/library/security/honey.html

Reto Baumann, Christian Plattner - White Paper: Honeypots