Эссе по курсу «Защита информации»,
кафедра радиотехники,
Московский Физико-Технический институт (ГУ МФТИ),
http://www.re.mipt.ru/infsec

«Определение Honeypots и Honeynets» («Definitions of Honeypots and Honeynets»)

Подготовлено студентом 115 группы
ФРТК МФТИ (ГУ)
Криштальским Павлом Андреевичем

0. Введение.

Большинство разделяют процесс защиту информации на три основных этапа: *предупреждение* атаки, *обнаружение* атаки и *ответную реакцию* на атаку.

Предупреждение атаки – это процесс, направленный на то, чтобы не допустить злоумышленника (здесь и далее под злоумышленником мы будем понимать лицо, либо группу лиц, пытающихся получить доступ и каким-либо образом воспользоваться информацией, к которой у них нет прав доступа) к информации.

Обнаружение – это обнаружение того, что в работе системы есть некий «сбой», предупреждение атаки и немедленное оповещение администраторов об этом.

И, наконец, ответная реакция – ответные действия на действия злоумышленника – от запрета подключения к системе (например, путем запрета соединения с определенного адреса) до отслеживания местонахождения и задержания его.

Из этих вышеперечисленных этапов, *обнаружение*, наверное, наиболее критичный фактор. Не важно, какое оборудование, ПО и методы защиты используются в нашей системе – рано или поздно они дадут сбой. Причина элементарна – это человеческий фактор: любая система безопасности создаётся людьми, а люди не застрахованы от ошибок, какими профессионалами бы они не были.

На первый взгляд может показаться, что обнаружение неавторизованных действий не представляет из себя ничего сложного. На самом деле это не так – при работе системы в сети (например, сервера) через него проходит огромный поток информации, среди которой действия злоумышленника (в случае наличия таковых) попросту теряются, как иголка в стоге сена. Это всегда чрезмерно усложняло задачу обнаружения атаки, и, как следствия, защиту информации.

В конце 90-х годов Лэнсом Спицнером (Lance Spitzner), специалистом по компьютерной безопасности компании Sun Microsystems был предложен новый подход обеспечения информационной безопасности, который основан на изучении поведения злоумышленников, используемых ими средствах и инструментов, их тактики и мотивов – это создание некой среды, направленной на то, чтобы быть атакованной и отслеживать, как это было сделано. (Вообще говоря, идея создания специальной среды для изучения действий злоумышленников не нова, её описание встречается, в частности, в публикациях Билла Чесвика (Bill Cheswick) “An evening with Berferd”. В той ситуации создана среда для отслеживания действий злоумышленника.).

1. Что такое Honeypots?

Такая среда называется Honeypot (дословно в переводе с английского – «горшок меда»).

Суть системы в том, чтобы быть подключенной к сети Интернет в качестве ловушки, которой рано или поздно заинтересуются злоумышленники. В процессе взлома этой системы установленные не ней средства слежения и регистрации должны зафиксировать все подробности этого процесса.

Первичная цель – сбор данных о противнике, его тактике и мотивов (всё-таки самое главное в изучении противника – это понять его цель, чтобы лучше понять, что нам угрожает, и как лучше защититься от этих угроз). Наверное, здесь ещё стоит упомянуть о том, что Лэнс Спицнер – бывший военный. Отсюда появляется такой подход к защите информации – здесь мы берем в руки всю инициативу. Мы не обороняемся, как в «стандартных» методах защиты, например межсетевые экраны (firewalls), системы обнаружения вторжений (IDS - Intrusion Detection Systems), криптографические методы, а «нападаем», и делаем ответный ход раньше, чем противник сможет нанести удар.

Honeynet может состоять из тех же самых систем и приложений, которые организация использует в своей повседневной деятельности. Уязвимости,

существующие в honeypot (где они могут быть тщательно изучены и проанализированы), полностью отображают риски и уязвимости рабочих систем организации.

Они способны на многое – от обнаружения зашифрованной атаки по сетям IPv6 до отслеживания последнего использования кредитной карты. Это очень гибкий инструмент и он может представать во многих видах. (Лэнс Спицнер)

Сам Лэнс Спицнер определяет honeypot как “ресурс информационной системы, чья ценность заключается в несанкционированно использовании” (“A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.”). Это определение полностью охватывает всевозможные типы honeypots. Это ресурсы, у которых нет, и не может быть санкционированной деятельности извне, соответственно, любая деятельность - скорее всего деятельность злоумышленника.

Именно это и делает honeypots такими удобными для использования:

2. Преимущества honeypots.

- *Малый объем данных высокой ценности:* Honeypots собирают мало информации, т.к., в отличии от серверов, ведущих полные логи трафика, достигающие порой больше гигабайта в день, honeypots сохраняют только информацию, которая наверняка является нужной нам. Она может составляет всего 1 мегабайт в день, но без лишних данных – только данные по факту взломов и попыток несанкционированного доступа.
- *Минимум ресурсов:* для обнаружения «плохой» активности не требуется больших вычислительных ресурсов – это не сервер, а лишь «муляж» некой системы. Для создания ловушки достаточно компьютера на базе первого пентиума, который в то же время может эмулировать новейшее оборудование.
- *Новые инструменты и тактики:* honeypots сохраняют любой поток информации, проходящий через них, включая инструменты и способы, которые возможно ранее не были известны.
- *И, наконец, простота:* honeypots очень просты: нет никаких алгоритмов, как разрабатывать или поддерживать их. Чем проще технология, тем меньше вероятность ошибки.

3. Минусы honeypots.

Разумеется, ни одна система не бывает без недостатков. Среди них в технологии honeypots стоит выделить в первую очередь:

- *Ограниченность использования:* Они способны отслеживать только ту активность, на которую они настроены, и не способны заметить атаку на другую систему. Т.е. если будет производиться попытка взлома, о которой honeypot «не знает заранее» - он ничего нам об этом не сообщит.
- *Риск:* Всегда есть опасность того, что система защиты будет нарушена. Так же и здесь: никто не страхует нас от того, что злоумышленник не возьмет honeypot под свой контроль и не проникнет в систему.

4. Типы honeypots.

Honeypots могут быть воплощены в многочисленных вариантах, создавая сложность в их описании. Для упрощения, их разделяют на две большие группы – honeypots высокого и низкого взаимодействия (high-interaction and low-interaction honeypot). Взаимодействие определяет уровень активности, которую honeypot позволяет атакующему.

Honeypots низкого взаимодействия имеют ограниченное взаимодействие, они нормально работают, эмулируя сервисы и операционные системы. Деятельность атакующего ограниченна уровнем эмуляции honeypot. Преимущества такого типа honeypots – их простота. Они оказывается очень легкими в настройке и поддержке, при минимуме риска.

Honeypots высокого взаимодействия – как правило комплексные решения, поскольку они основаны на реальных ОС и приложениях. В данном случае ничего не эмулируется – всё реально. У таких honeypots два плюса. Первый – это то, что предоставляя атакующему настоящую систему, можно собрать более полную информацию по атаке. Второе – не нужно предугадывать поведение атакующего для более грамотной эмуляции. Мы просто предоставляем злоумышленнику реальную систему. И мы сможем уловить действия. О которых даже могли и не догадываться. Если в первом случае злоумышленник очень быстро может заметить подставу, как только попытаемся произвести действие, выходящие за границы эмуляции, то в данном случае такого не произойдет. Но не стоит забывать о безопасности – реальные системы подразумевают реальные данные и реальную возможность проникновения в систему.

Honeypots высокого со временем развились в более совершенную систему обнаружения атаки – honeynets (под руководством Лэнса Спицнера был создан проект – honeynet, который существует и развивается до сих пор).

5. Honeynets.

Идея honeynets та же, что и у honeypots, но здесь имеется несколько различий.

- Это не единая система, а сеть, состоящая из многих компьютеров. Эта сеть располагается за межсетевым экраном, на котором все входящие и исходящие данные фильтруются, фиксируются и контролируются. Полученная информация далее анализируется с целью изучения средств, тактики и мотивов злоумышленников. При этом в honeynet могут использоваться одновременно множество различных систем: Windows, Solaris, UNIX, Cisco и т.п. Эта среда уже более полно моделирует реальную сеть.
- Во-вторых – все используемые в honeynet системы реальны. Это не эмуляция ошибки или системы, созданной для того, чтобы быть атакованной, – это реальная система, со всеми уязвимостями. Ничего также не сделано для искусственного ослабления защиты. Практически, можно брать систему из рабочее сети и включать её в honeynet.

Использование реальных систем в honeynet делает эту систему уникальной. Например, проект Honeynet использовал часто встречающиеся в Internet системы с конфигурацией по умолчанию: Linux, Solaris, Windows98 и Windows NT. Поскольку используются наиболее распространенные операционные системы, уязвимости, обнаруженные в этих исследованиях, могут быть отнесены и к большей части систем в Internet.

6. Как работают honeynets.

Первичная цель Honeynet состоит в изучении поведения злоумышленников.

Первичная цель Honeynet состоит в изучении поведения злоумышленников. Этого добиваются путем отслеживания каждого шага злоумышленника, создавая для него специальную среду, в которой контролируется любая деятельность атакующего. При этом основной проблемой, как уже упоминалось ранее, является информационная перегрузка системы. Выявление активности злоумышленника среди остальной активности – настоящее искусство. Но, поскольку honeynets построены на базе honeypots, эта проблема решена ещё при определении рассматриваемой системы –

никакой «официальной» деятельности в системе honeynets нет. Т.е. все данные, которые мы получаем, - скорее всего попытка атаки, а исходящий трафик практически на стопроцентно говорит нам, что система атакована. Это ключевые моменты honeynets.

В построении системы honeynets можно отметить два критических момента – это управление данными и сбор данных. Основной смысл сбора данных интуитивно понятен – это сбор и анализ данных, пришедших/ушедших из нашей системы. Управление данными – это необходимость контролировать все входящие и исходящие потоки. Основная идея этого контроля – быть уверенным, что при удачной атаке honeypot, она не будет использована для атаки другого honeypot в нашей системе.

7. Управление данными.

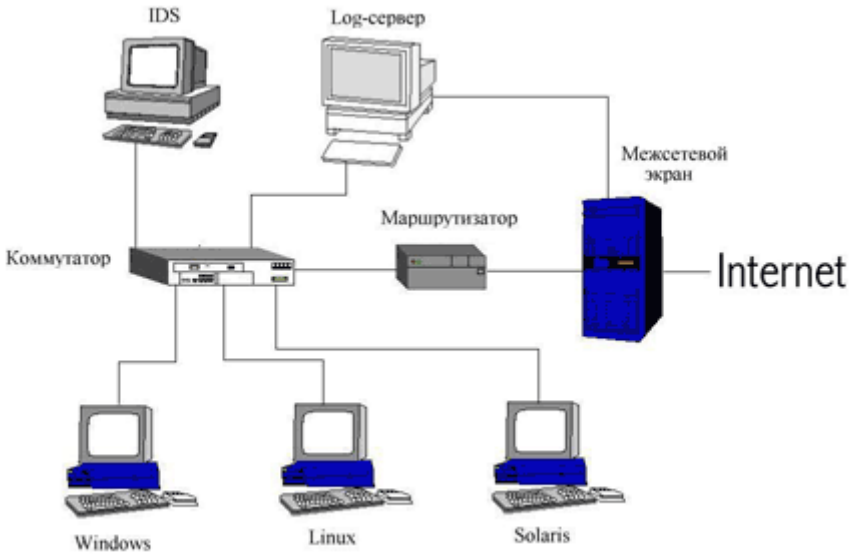
Типовой honeynet условно можно разделить на три части (см. рисунок): межсетевой экран (firewall), подсистему регистрации (маршрутизаторы/коммутаторы) и собственно приманки (honeypots).

Honeynet функционирует параллельно с рабочей сетью и независимо от нее. Эта сеть может быть подключена к Интернет по отдельному каналу, на нее может быть зарегистрирован отдельный диапазон IP-адресов, а может использовать для общения с внешним миром основной маршрутизатор компании - все зависит от конкретной ситуации.

Рассмотрим, каким образом данные функциональные элементы участвуют в выполнении перечисленных задач.

Межсетевой экран позволяет контролировать ситуацию: в процессе работы он может линамически менять логику своего поведения, в зависимости от внешних событий. На межсетевой экран ложится ответственность контроля исходящего трафика. С одной стороны – нельзя разрешать делать неограниченное количество исходящих соединений, иначе есть риск успешной атаки на другие honeypots системы, в случае взлома рассматриваемой. С другой стороны – если запретить исходящие соединения, злоумышленник очень быстро заподозрит ловушку и прекратит попытки атаки (со слов Лэнса Спицнера, в начале проекта Honeynets так и было – часто атакующие очень быстро сворачивали свою деятельность, как только обнаруживали, что не могут создать исходящее соединение). Выход из этой ситуации только один – ограничение числа соединений. Опытным путем командой Honeynets было установлено, что 5-10 исходящих соединений – вполне достаточно, чтобы атакующий ничего не заподозрил.

Большинство современных межсетевых экранов имеют также и мощную подсистему регистрации событий. Таким образом, межсетевой экран помогает решать и задачу сбора данных, делая ее многоуровневой.



Вторая часть – маршрутизатор, основная идея которого скрыть присутствие межсетевого экрана. Наличие маршрутизатора в системе – обычное дело и не вызывает никаких подозрений.

Третья часть – ловушки-honeynets.

8. Сбор данных.

Сбор данных – это запись всех действий всех злоумышленников. Именно эти действия в последствии анализируются с целью изучения средств, их тактики и мотивов. Основная задача – это не дать атакующему понять, что за ним не просто следят, а он, фактически, под контролем. Т.е., мы одновременно должны внести в систему изменения, но при этом – сделать это по-минимуму. Помимо этого, нам нужно вести логии, иначе honeynet теряет всю свою идею. Очевидно, что сохранять логии на той машине, на которой установлен honeynet, нельзя – злоумышленник, в случае благополучного для него исхода, наверняка сотрет всю эту информацию, и очень важные данные о том, как ему удалось взломать систему, будет утеряна. То есть, нам необходимо хранилище, на которое будет вестись запись всех логов, возможно даже не одно (при этом, можно также сохранять логии и на самой машине, которая, как предполагается, будет атакована – в данном случае все нормально и злоумышленник не будет «напуган», т.к. ведение логов на машине – вполне типичная ситуация). Наиболее оптимальным решением является многоуровневая фиксация действий атакующего.

В качестве первого уровня выступает межсетевой экран. Помимо контроля за данными, о котором говорилось выше, на него элементарно можно повесить запись всех проходящих (как входящих, так и исходящих) пакетов. К тому же, в случае попытки установления исходящего соединения, межсетевой экран может смело нас об этом оповещать – это атака.

Второй уровень – это система обнаружения атак (IDS), имеющая два предназначения. Первое(и основное) – это фиксация всей сетевой активности, проходящей через сетевой кабель. А, поскольку, IDS подключена к коммутатору, ей доступен весь сетевой трафик. Второе предназначение – собственно, основное предназначение IDS – оповещение о подозрительной деятельности (IDS имеет базы сигнатур, и если перехваченный пакет совпадает с одной из сигнатур, это ещё один звоночек об атаке). Но в целом это назначение не столь важно – так как в рассматриваемой нами системе любое соединение подозрительно по определению.

Третий уровень, сами системы (honeypots, входящие в honeynet). Как упоминалось ранее, хранить какие-либо данные только локально – глупо и нецелесообразно. Для записи данных нужно использовать специально предназначенный для этого syslog-сервер, поломать который будет значительно сложнее, чем honeypot. При этом, мы даже и не пытаемся скрыть факт записи данных на лог-сервер. Если злоумышленник это обнаружит факт записи, он просто отключит syslog. Это вполне нормально. По крайней мере, мы точно будем знать, как был получен доступ к системе.

Более продвинутые атакующие захотят стереть уже записанное с сервера, и это именно то – что нужно. В силу большей защищенности сервера, чем honeypot, понадобятся более продвинутые средства и методы взлома, которые фиксируются и обрабатываются в дальнейшем.

9. Сопровождение.

Honeynet - не отлитое в бронзе решение, которое можно поставить и забыть о нем, оно требует постоянного внимания и бессонных ночей. Для достижения максимального эффекта нужно обнаруживать деятельность злоумышленников, и как можно быстрее обрабатывать и анализировать данные. Только в этом случае honeynets способны нам помочь. Но здесь нельзя забывать – что зачастую анализируется не результат атаки, а лишь её попытка. И чтобы выудить из этих данных полезную информацию, необходимо обладать хорошими аналитическими способностями.

Существует также потенциальная возможность того, что злоумышленник сможет обойти систему сбора данных.

Наконец, Honeynet не решает проблемы безопасности. Они остаются такими же, соответствующими реальной системе.

a. Заключение.

Honeynet - специальное средство, предназначенное для сбора разведывательных данных об инструментальных средствах, тактике и мотивах злоумышленников. Оно включает в себя все положительные стороны honeypot, в частности работу в качестве ложной цели и системы оповещения, однако ее основное предназначение - изучение. Между honeypot и Honeynet есть два принципиальных различия. Первое различие состоит в том, что Honeynet не одиночная система, а сеть, состоящая из нескольких систем и приложений. Второе различие в том, что в состав Honeynet входят самые обычные системы, которые можно повсюду встретить в Internet; т.е. мы не эмулируем ни системы, ни уязвимости. Это делает Honeynet превосходным средством для обучения. Однако, Honeynet требует огромного количества административных затрат. Администратор Honeynet несет ответственность за то, чтобы другие системы не были атакованы с использованием атакованной Honeynet. Без надлежащего администрирования риск взлома может превышать получаемую выгоду. Этот средство не является идеальным средством в области безопасности и не является подходящим решением для каждой организации. Проект Honeynet настойчиво рекомендует сначала предпринять все стандартные меры обеспечения безопасности, типа своевременного внесения изменений в системы и отключения ненужных сервисов. Лишь после этого можно задумываться о построении и использовании Honeynet для сбора информации и изучения противника.

b. Используемая литература (ссылки).

1. *http://www.honeynet.org (различные статьи, автор – Лэнс Спицнер)*
2. *http://project.honeynet.org/ (различные статьи, автор – Лэнс Спицнер)*
3. *http://www.tracking-hackers.com (различные статьи, автор – Лэнс Спицнер)*
4. *http://bugtraq.ru/library/security/honeynet.html*
5. *http://www.i2r.ru/static/452/out_17527.shtml*