Подсистема оперативного информирования участников профессионального научного сообщества будет поддерживать следующие функциональные возможности: ведение списков рассылки; индивидуальное информирование о новых поступлениях в электронную библиотеку и другие подсистемы; информирование о размещении электронной публикации в закрытой зоне; информирование о мероприятиях определенной направленности и т.п.

Проект предполагает работу с тремя группами пользователей:

- авторы научных публикаций - инициаторы (модераторы) тем научных дискуссий, члены редколлегий, рецензенты и редакционные работники (зарегистрированные пользователи со специфическим набором прав доступа к материалам и разделам системы);
- научные работники и преподаватели, заявившие о заинтересованности участия в сетевых обсуждениях и публикациях своих материалов, потенциальные авторы получающие доступ к неопубликованным рабочим материалам системы (зарегистрированные пользователи со стандартными правами);
- незарегистрированные пользователи, имеющие возможность ознакомиться с материалами, находящимися в открытом доступе.

Работа выполняется поддержке Российского фонда фундаментальных исследований (грант 11-07-00555-а).

ИСПОЛЬЗОВАНИЕ ОБМАННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ЛОКАЛЬНОЙ СЕТИ ОРГАНИЗАЦИИ ОТ ВНЕШНИХ УГРОЗ

О.Ю. Пескова, В.М. Шериева
Таганрогский технологический институт Южного федерального университета (ТТИ ЮФУ)
Таганрог

ВВЕДЕНИЕ

Давно прошли времена, когда подключение организации к сети Интернет служило в основном для развлечения сотрудников, а в лучшем случае – для обмена электронной почтой. Сейчас многие предприятия используют глобальную сеть как часть своей технологической цепочки: Интернет используется не только для сбора информации, но и для работы с централизованными базами данных (например, для заказов у поставщиков), для работы с клиентами (например, через веб-сервера), для объединения филиалов и удаленных подразделений в единую сеть, и так далее. Поэтому сейчас остро стоят вопросы максимально эффективной и гибкой защиты ресурсов локальной сети организации при ее подключении к глобальной сети.

Наиболее эффективной считается стратегия (и она же является самой распространенной), которая состоит в том, чтобы обнаруживать любые недочеты в системе защиты и тут же их устранять. Но проблема этого подхода в том, что он пассивный: противник же всегда впереди и активно атакует. Практически всегда у хакера есть возможность адекватно отреагировать на защитные меры, и поэтому потенциально атакуемая сторона, чтобы минимизировать риск вторжения, просто обязана играть на опережение. [1]

Один из методов, позволяющий осуществить эту идею, называется HoneyPot (от англ. — «горшочек с медом»). HoneyPot представляет собой специальным образом доработанную систему, которая подключается к Интернет в качестве приманки, и злоумышленник будет атаковать приманку вместо того, чтобы атаковать реальную сеть. В процессе взлома системы-приманки установленные на ней средства слежения и регистрации должны зафиксировать все подробности этого процесса. Подобные системы-ловушки используются и в исследовательских целях как средство сбора информации о методах и средствах проведения атак (собранная информация, в частности, позволяет обнаруживать новые и уникальные уязвимости и эксплоиты), и для защиты организаций от взлома («промышленные» ловушки) [2]. Назначение промышленных ловушек - предотвращение атаки, обнаружение атаки и информационная поддержка в организации адекватных действий по блокированию атаки. Такие ловушки могут предотвращать нападения за счет замедления или эффекта увязания (tarring) автоматизированных атак. Ловушки могут более эффективно обнаруживать атаки, поскольку порождают меньшее количество тревог, как истинных, так и ложных. [3]

Однако, такому упрощенному подходу присущ целый ряд недостатков:

1. После взлома такой системы достоверность регистрационных журналов и другой информации из системы слежения становится сомнительной и по ней тяжело анализировать проведенные атаки, их источник и средства реализации.
2. Исследователям наиболее полезна для изучения методика проведения атак на стандартные системы, которые часто встречаются в Интернет; в систему HoneyPot же вносятся существенные изменения по сравнению со стандартными информационными системами. Кроме того, данные изменения - это демаскирующий признак, позволяющий определить наличие «подмены» - злоумышленник может обнаружить эти изменения и отказаться от своих планов либо продолжить изыскивать способы проведения успешной атаки на реальную сеть.
3. Проводя такие эксперименты, администратор должен осознавать ответственность и за других, т.к. его HoneyPot (особенно при ошибках в конфигурирования) может быть использован как промежуточное звено для сканирования или для организации атак на другие системы, например как часть blist (broadcast amplifier network)
4. Сфера действия HoneyPot ограничена: они работают только с теми атаками, которые направлены непосредственно против них, и пропускают те, которые проводятся на другие сервисы сети.

Эти недостатки можно ликвидировать или свести к минимуму, если использовать не отдельно стоящую систему (HoneyPot), а построить специализированный сетевой комплекс - HoneyNet, выводящий исследование на качественно новый уровень.

В нашем докладе рассматриваются особенности применения систем HoneyNet, а также описывается возможный механизм организации HoneyNet для локальных сетей с низкой и средней загрузкой.

КЛАССИФИКАЦИЯ СЕТЕЙ HONEYNET

Сеть HoneyNet – это высокотехнологичный комплекс, состоящий из отдельных HoneyPot, обеспечивающий высокую степень эмуляции реальных операционных систем и предназначенный для атак злоумышленника с целью изучения механизма атаки. Именно высокая степень идентичности и позволяет без вреда и риска узнать многое о злоумышленниках, их методах проникновения в реальные системы. В построенной сети HoneyNet весь трафик по всем направлениям управляется и фиксируется. Эмулирующие и анализирующие подсистемы в этом случае отделяются друг от друга. Каждый HoneyPot в сети HoneyNet является полностью функционирующей системой, схожей с теми, что работают в большинстве сетей. И когда любая из систем-приманок атакована, ловушка срабатывает, HoneyNet начинает централизованно фиксировать всю деятельность злоумышленника [4].

Сети HoneyNet могут быть реальными и виртуальными.

Реальная HoneyNet работает с производственным программным обеспечением (например, Windows Server 2003/2008, Microsoft Exchange Server, Microsoft Internet Information Service) на выделенном аппаратном оборудовании внутри существующей сети. Это потенциально максимально реалистичный и эффективный вариант. Она выглядит и ведет себя как настоящий производственный ресурс, и если данные на ней обновляются по аналогии с реальной сетью, то с достаточно большой вероятностью злоумышленник не сможет обнаружить подмену. Основной недостаток реальных HoneyNets заключается в том, что для организации и управления ими, как правило, требуется много усилий и времени, а также, возможно, средств: для установки качественной приманки иногда необходимо столько же времени, сколько для инсталляции настоящего производственного ресурса. Еще один серьезный недостаток состоит в том, что трудно помешать злоумышленнику, захватившему приманку, атаковать через нее другой производственный ресурс. Во многих реальных приманках UNIX/Linux используется механизм, который предотвращает захват производственных ресурсов (называемый иногда механизмом управления данными - data-control mechanism), но лишь немногие продукты семейства Microsoft Windows располагают такими функциями.

Подобные системы часто называют высокоинтерактивными HoneyNet. К высокоинтерактивным приманкам относится, в частности, система The HoneyNet Project [5]. The HoneyNet Project – это научная организация, занимающаяся исследованиями в области систем безопасности. В состав организации входят специалисты из разных стран, которые безвозмездно предоставляют свои ресурсы для развертывания и изучения обманных систем.

Другой класс приманок - виртуальные HoneyNets - представляют собой не программно-аппаратный комплекс, а среду эмуляции, программное обеспечение которой ограничивает возможности взломщика в соответствии с настройками. Как правило, при таком подходе потенциальный ущерб для производственных ресурсов существенно уменьшается или исключается полностью. Также к преимуществам использования виртуальных HoneyNets относятся существенное уменьшение стоимости

и более простое управление (но тем не менее от квалификации администратора во многом будет зависеть эффективность работы обманной системы).

Большинство виртуальных HoneyNets функционально примитивны: они имитируют открытые, закрытые порты или порты с отвечающей на запросы службой. Подобные системы называются низкоинтерактивными HoneyNets. Низкоинтерактивные HoneyNets представляют собой программу, реализующую один или несколько сетевых сервисов, предназначенных для взлома (например, FTP, HTTP, SMTP, DNS и т.д.). Основное ее назначение – вовремя узнать о совершении атаки. Для сбора информации о злоумышленнике, его инструментах и особенностях взлома этот вариант не подходит, но он волне может служить для отвлечения внимания хакера. Просканировав подобную систему сканером уязвимостей, злоумышленник обнаружит одну или несколько уязвимостей, которыми он сможет воспользоваться. К низкоинтерактивным приманкам относятся Honeyd, Honeyd-WIN32, KFSensor, SPECTER и другие.

Виртуальные приманки, которые только открывают порт и регистрируют начальный запрос злоумышленника, называются простыми слушателями порта (simple port listener). Более развитые слушатели порта могут отвечать на запросы несложными пакетами открытия или закрытия, что выглядит более реалистично и привлекает взломщика. Эти приманки фиксируют информацию, посылаемую злоумышленником, и отвечают в соответствии с сетевым протоколом, который использовался для запросов (например, посылают пакет SYN). Но даже такой примитивный обмен пакетами может быть полезен сетевому администратору, так как свидетельствует о несанкционированной активности внутри периметра сети и позволяет обнаружить источник атаки (а иногда и используемые методы и средства атаки). Многие виртуальные HoneyNets не ограничиваются начальным обменом сообщениями по протоколу, эмулируемая служба будет отвечать злоумышленнику так же, как ответила бы реальная система, передавая так называемые баннеры (например, выводя соответствующую текстовую информацию – текстовый баннер). Эмулируемая служба, которая передает имитированный баннер, называется баннерной службой (banner service). Эмулируемая служба, которая дает минимальный отклик на запрос, называется простой (simple) или стандартной (standard) службой.

Виртуальные сети HoneyNet имеют и существенные недостатки. Первое ограничение заключается в ограничении на возможные типы операционных систем – пользовательской и развернутой программным обеспечением виртуализации (хотя спектр возможностей здесь достаточно широк, и можно подобрать комплекс ПО практически под любую задачу). Кроме того, виртуальные HoneyNets также сопряжены с определенным риском, что злоумышлений сможет выйти из виртуального программного обеспечения и проникнуть в реальную систему, преодолев защитные механизмы контроля, управления данными и механизмы сбора данных. Хотя пока не было зафиксировано ни одного случая выхода хакера из виртуальной ловушки, но теоретически такая возможность может существовать.

ПРОЕКТ РАЗВЕРТЫВАНИЯ HONEYNET В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ОРГАНИЗАЦИИ

Главная сложность, возникающая при развертывании сети-приманки, — отсутствие готового решения. Администраторы сетей (особенно небольших) оказываются не готовы подбирать программное обеспечение, решающее все поставленные задачи и эффективно работающее в комплексе.

В рамках доклада будет предложен проект развертывания HoneyNet, который является достаточно универсальным. Проект может быть реализован как чисто программным, так и программно-аппаратным способом.

Рассмотрим программную реализацию HoneyNet, которая фактически представляет собой реализацию механизма «переключения» сервисов, подвергшихся сканированию, на «приманку».

Про результатам анализа для построения системы было выбрано следующее ПО:

- в качестве системы обнаружения атак была выбрана IDS Snort - облегченная система обнаружения вторжения, анализирующая протокол передачи и выявляющая различные атаки; цель ее применения в общей структуре NoneyNet- детектирование подозрительной сетевой активности и запись об этой активности в своем журнале – логе;
- для блокирования доступа подозрительного трафика, выявленного с помощью Snort, к локальной сети и его перенаправления на виртуальную сеть honeynet будет использоваться программа Iptables;
- в качестве сети-приманки будет применяться низкоинтерактивная honeynet KFSensor, которая точно воспроизводит поведение сетевого узла Windows и именно на нее будут перенаправляться подозрительные пакеты.

Snort – современное приложение защиты с тремя основными функциями, которые мы будем использовать:

1. Анализатор пакетов (packet sniffer) - читает пакеты из сети и отображает их в консоли (на экране).
2. Регистратор пакетов (packet logger) - записывает сетевые пакеты на диск.
3. Сетевая система обнаружения вторжений – позволяет Snort анализировать весь сетевой трафик для сопоставления с набором правил, установленным пользователем, и предоставления некоторых операций, основанных на наблюдениях.

Для наших целей достаточно бесплатной версии программы Snort для зарегистрированных пользователй, предполагающей доступ к набору правил с 30-дневной задержкой (Sourcefire VDB signatures) и к «любительским» наборам (community signatures), но для организаций с высоким риском проведения сетевых атак имеет смысл оформить подписку для наиболее оперативного реагирования на новейшие виды атак.

Система Snort предоставляет возможность выявить:

- использование эксплоитов (выявление Shellcode),
- сканирование системы (порты, ОС, пользователи и т.д.),
- атаки на сетевые службы Telnet, FTP, DNS и т.д.,
- атаки, связанные с Web-серверами (cgi, php, frontpage, iss и т.д.),
- атаки на базы данных SQL, Oracle и т.д.,
- атаки по протоколам SNMP, NetBios, ICMP, атаки на SMTP, imap, pop3,
- атаки DoS/DDoS,
- различные Backdoors,
- и так далее.

Snort является переносимой, работает на многих современных операционных системах (Linux, FreeBSD, NetBSD, OpenBSD и Windows). Благодаря возможности написания собственных правил, расширению функциональности за счет использования возможности подключения модулей и гибкой системе оповещения об атаках Snort представляет собой мощную систему в борьбе против злоумышленников [7].

Определение конфигурации аппаратных и программных средств, необходимых для оптимальной установки Snort, в основном зависит от характеристик сети организации: чем больше и чем более загружена сеть, тем более мощные компьютеры нужно использовать в качестве Snort-сенсора(ов). Система Snort должна соответствовать сети: иметь достаточный объем дискового пространства для записи пакетов; достаточно быстрый процессор и достаточный объем памяти для обработки обычно наблюдаемого в сети объема трафика, с некоторым запасом прочности на случай интенсивных атак и пиковых объемов. Для подбора необходимой конфигурации желательно провести ряд экспериментов в локальной сети организации, для которой будет настраиваться предлагаемая система.

IPTables позволяет назначить правила фильтрации, в соответствии с которыми будет определяться «судьба» сетевых пакетов. Каждое правило в IPTables - это строка, содержащая в себе критерии, определяющие, попадает ли пакет под заданное правило, и действие, которое необходимо выполнить в случае выполнения критерия. Могут использоваться различные критерии, по которым будут обрабатываться пакеты, - IP-адрес источника пакета или сети, IP-адрес места назначения, порт, протокол, сетевой интерфейс и т.д., а также различные виды действий: можно заставить ядро передать пакет в другую цепочку правил, «сбросить» пакет без отправки сообщения об ошибке, выдать на источник сообщение об ошибке и т.п. Были разработаны правила, перенаправляющие подозрительный сетевой трафик на виртуальную приманку KFSensor и препятствующие его проникновению в локальную сеть

KFSensor – низкоинтерактивная виртуальная приманка, которая точно воспроизводит поведение сетевого узла Windows. Стоимость стандартной редакции – $199. Она поставляется с 77 заранее настроенными портами (58 портов TCP и 19 портов UDP). Большинство этих портов задействованы в типичных средах Windows, хотя KeyFocus использует и несколько произвольных портов для «троянских коней», которые привлекают злоумышленников, отыскивающих уязвимые машины. [8]

KFSensor обеспечивает простую эмуляцию служб IIS, FTP, Telnet и Exchange. Соединения с IIS приводят к стандартной странице с надписью «Under construction». При обращении к порту 25 выдается реалистичный текстовый баннер Exchange, и программа эмуляции службы воспринимает ограниченное число базовых команд SMTP. Кроме того, KFSensor обеспечивает базовую эмуляцию Terminal Services для соединений RDP, Symantec pcAnywhere, Citrix MetaFrame, Virtual Network Computing (VNC), WinGate и других продуктов. С помощью кодов управления и сценариев можно настроить каждый порт и имитируемую службу.

KFSensor достаточно точно имитирует открытые порты NetBIOS и Windows RPC, т.е. дает отклик, характерный для операционных систем семейства Microsoft Windows, что важно, поскольку на первом этапе проведения атаки злоумышленник, как правило, с их помощью пытается определить, какая версия ОС установлена на атакуемой системе.

Приманка KFSensor работает на прикладном уровне, поэтому она не может имитировать набор протоколов IP и, в частности, не позволяет имитировать маршруты прохождения трафика, но для большинства атак этот сервис избыточен.

В том случае, если сетевой трафик велик и программные анализаторы пакетов не справляются с потоком, рекомендуется использовать в качестве средств анализа пакетов и обнаружения атак аппаратные средства – либо специализированные аппаратные IDS, либо функции анализа трафика, встроенные в коммутационное оборудование.

ЛИТЕРАТУРА

1. Узнай своего врага: Honeynets. Проект Honeynet / перевод В.В. Мяснянкина // Bugtraq.ru Информационная безопасность [Электронный ресурс]. — Режим доступа: http://bugtraq.ru/library/security/honeynet.html?k=9.
2. Первое описание концепции honeypot // Security Lab by Positive Technologies [Электронный ресурс]. — Режим доступа: http://www.securitylab.ru/informer/240663.php.
3. *Спитцнер, Л.* Honeynet Project: ловушка для хакеров. // CIT Forum [Электронный ресурс]. — Режим доступа: http://citforum.edunet.kz/security/internet/honeynet/.
4. *Мяснянкин, В.* Все любят мед //Bugtraq.ru Информационная безопасность [Электронный ресурс]. — Режим доступа: http://www.bugtraq.ru/library/security/honey.html.
5. *Глушко, С.* Ловушка для хищника // Xaker.Ru [Электронный ресурс]. — Режим доступа: http://www.xakep.ru/magazine/xa/106/066/1.asp.
6. Построение виртуальных ловушек // Security Lab by Positive Technologies [Электронный ресурс]. — Режим доступа: http://www.securitylab.ru/analytics/216223.php.
7. Система обнаружения вторжений на базе IDS Snort (snort ids). // The OpenNET Project [Электронный ресурс]. — Режим доступа: http://www.opennet.ru/base/sec/snort_ids.txt.html.
8. *Граймз, Р.* Использование приманок на базе Windows // Windows IT Pro. 2004. №4. (электронная версия: [Электронный ресурс]. — Режим доступа: http://www.osp.ru/win2000/2004/04/176949/).

ОРГАНИЗАЦИОННО-ПРАВОВАЯ СПЕЦИФИКА РАЗВИТИЯ СОСТАВЛЯЮЩИХ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

И.В. Поночевная

Санкт-Петербургский государственный инженерно-экономический университет
Санкт-Петербург

В настоящее время во всем мире резко повысилось внимание к проблеме системе информационной безопасности (СИБ). Это обусловлено процессами стремительного расширения потоков развития информационных ресурсов в глобальной компьютерной сети Internet , пронизывающих все сферы жизни общества и государства. К значительной части информационных ресурсов глобальной компьютерной сети Internet предъявляются требования по обеспечению определенной степени конфиденциальности.

Отличительной особенностью информационных объектов является комплексное использование на них информационных и телекоммуникационных систем, то есть инфокоммуникационных систем, что вызывает необходимость применения более широкого спектра составляющих для защиты информационного ресурса в информационном пространстве.

Рассматриваемые в работе декомпозиции составляющих СИБ могут оказаться совершенно бесполезными, если не будет соблюден надлежащий действующий пакет политик.

Действующий пакет политик включает в себя концепцию пакета политик безопасности (КППБ) и является в совокупности с составляющими СИБ основным документом, определяющим защищенность информационного пространства от внутренних, внешних и комбинированных «субъектов угроз» (Рис.2).

Полезные рекомендации на этот счет содержаться в международных стандартах, в частности в международном стандарте безопасности информационных систем ISO 17799-2005 (стандарт построения эффективной системы безопасности разработан в 2000 году Международной организацией по стандартизации и является официальным документом, описывающим комплексный подход к вопросам безопасности и рассматривающим в качестве элементов управления как технические, так и организационно-административные меры, обеспечивающие конфиденциальность, целостность, доступность и достоверность информации).