



Код безопасности
ГК «Информзащита»

Honeyrot Manager – проактивная защита от хакеров и инсайдеров

Статья содержит описание принципов работы и преимуществ Honeyrot-систем, их места в общей системе безопасности, а также описывает новый продукт компании – Security Studio Honeyrot Manager.

Honeyrot – приманка для нарушителя

Гонка вооружений

Информационная безопасность продолжает оставаться одной из наиболее динамично развивающихся областей. Основной движущей силой этого развития является столь же стремительное развитие средств нападения и постоянное появление новых угроз. Их количество постоянно растет вместе с внедрением новых технологий и новых продуктов. Угрозы становятся все более изощренными. Вполне очевидно, что развитие средств нападения и вредоносных программ всегда будет на шаг впереди, такова логика этого процесса.

Именно поэтому все большей популярностью пользуются системы раннего обнаружения и предотвращения атак, работающие на основе косвенных признаков (таких как поведение систем и пользователей), такие как системы обнаружения вторжений и корреляции событий. Эти системы способны противостоять не только известным, но и новым угрозам.

Одними из таких средств, позволяющих значительно повысить безопасность информационной сети, являются Honeyrot-системы.

Технология Honeyrot – приманка для нарушителя

Технология Honeyrot является одним из наиболее эффективных и доступных средств обнаружения и противодействия атакам на сетевые ресурсы.

Идея Honeyrot проста и известна с незапамятных времен – нарушителя ловят на приманку. В локальной сети размещается легкодоступная и привлекательная для нарушителя цель, внешне неотличимая от реальных ресурсов, единственное предназначение которой – попасться на глаза нарушителю, спровоцировать его на неправомерные действия и сообщить «куда следует» о факте «контакта».

Другими словами, Honeyrot – это система обнаружения попыток несанкционированного доступа к информационным ресурсам. Honeyrot имитирует работу реальной системы, являющейся потенциальной целью атак и несанкционированного доступа, отвлекает на себя внимание и ресурсы нарушителя, фиксирует все его действия и информирует службу безопасности о фактах нарушений. При этом, в зависимости от типа honeyrot, имитироваться могут любые системы, служащие потенциальными объектами для атак: сервера, базы данных, сетевые сервисы, файловые ресурсы и т.д.

Преимущества использования Honeyrot-систем

- **Предупрежден – значит вооружен**

Преимущества Honeyrot-систем определяются самим принципом их работы. Прежде всего, это практически полное отсутствие ложных срабатываний. Т.к. Honeyrot лишь имитирует реальную систему и к нему не обращаются ни реальные пользователи сети, ни легальные сетевые приложения, то любая активность на Honeyrot и любая попытка обращения к нему является несанкционированной и свидетельствует либо об атаке, либо об исследовании сети с целью найти уязвимые места в ее защите.

- **Возможность понять цели, методы и средства нарушителя**

Определение факта атаки является важнейшим моментом для администраторов, так как позволяет оперативно принять меры противодействия. Но помимо этого, Honeyrot позволяет также получить информацию, необходимую для изучения действий нарушителя. Дело в том, что Honeyrot позволяет сохранить следы воздействия для дальнейшего расследования. Атакованную Honeyrot-систему можно спокойно отключить и передать для анализа собственным или внешним специалистам по информационной безопасности, что обычно невозможно для реального сервера, например сервера баз данных корпоративных приложений или почтового сервера.

По оставленным нарушителем следам можно узнать об используемых им методах и средствах атаки, а также сделать выводы о ее целях. При этом важной особенностью Honeyrot-систем является сравнительно небольшое количество информации, которую нужно изучать при расследовании инцидента. Реальные системы сети протоколируют огромное количество информации и расследование инцидентов ИБ на основе логов многочисленных сетевых приложений и систем является довольно трудоемкой задачей. Honeyrot, напротив, содержит только нужную информацию, связанную с фактами нарушений, т.к. никакой легальной активности на нем не происходит.

Место Honeyrot в системе безопасности предприятия

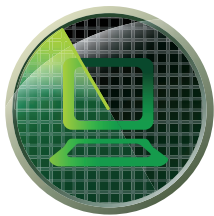
Как уже говорилось, технология Honeyrot является доступным и довольно эффективным методом раннего предупреждения и обнаружения вторжений. Из всего вышесказанного можно выделить два основных направления использования этой технологии.

Первое – это снижение риска сетевых атак на реальные системы. Honeyrot позволяет предупреждать, обнаруживать и протоколировать деятельность нарушителя. Установленный и грамотно настроен-

ный Honeyrot отвлечет внимание и ресурсы нарушителя от реальных систем, позволит выявить попытку атаки, предоставит информацию для ее изучения и даст дополнительное время для принятия адекватных мер защиты.

Второе направление – получение информации для изучения поведения, методов и инструментария нарушителей. Исследовательские Honeyrot-системы не уменьшают риск для организации, но полученная с их помощью информация может быть использована для построения более эффективных и надежных систем защиты реальных приложений и сетей.

Security Studio Honeyrot Manager



Security Studio Honeyrot Manager

Security Studio Honeyrot Manager (далее Honeyrot Manager) – новый продукт компании «Код Безопасности» – представляет собой готовую к использованию Honeyrot-систему, имитирующую СУБД Oracle с подставными данными бизнес-приложений. Honeyrot Manager позволяет обнаруживать вторжения нарушителей в локальную вычислительную сеть предприятия и анализировать их действия без снижения производительности реальных систем хранения и обработки данных, а так же без непосредственной угрозы потери ценной информации.

Honeyrot Manager регистрирует любые действия в контролируемой базе данных, которая фактически является специальным сенсором-ловушкой, проводит регулярный аудит собранных данных и анализирует их на соответствие настроенным правилам уведомлений. Результаты анализа активности регистрируются в журнале в виде сообщений о фактах НСД с указанием информации о компью-

тере и учетной записи потенциального нарушителя, времени и характере доступа, а также могут отправляться по электронной почте для уведомления заинтересованных лиц.

Все записи аудита хранятся в базе данных и доступны для последующего анализа даже в случае порчи сенсора нарушителем или краха системы. Настроенная система отчетов на основе Microsoft SQL Server Reporting Services позволяет производить анализ активности и видеть статистику работы системы.

Продукт позволяет имитировать работу как двух-, так и трехзвенных приложений. В случае имитации трехзвенного приложения полезной может быть утилита перемешивания данных, позволяющая модифицировать исходные реальные данные таким образом, чтобы они сохранили свою структуру и могли распознаваться приложением, но при этом перестали представлять какую-либо ценность для злоумышленников.



Рис.1 Схема работы Security Studio Honeyrot Manager

Почему СУБД Oracle?

Согласно исследованиям компании Gartner, Oracle является реляционной базой данных № 1 в мире с долей рынка около 50%. Большинство приложений корпоративного уровня используют в качестве хранилища данных СУБД Oracle. Таким образом, значительная часть критичной для организаций информации хранится и обрабатывается в этой СУБД, поэтому не удивительно, что именно базы данных Oracle являются наиболее привлекательной целью для атак, как со стороны внешних (хакеров) так и со стороны внутренних (инсайдеров) нарушителей.

Преимущества Honeyrot Manager

1. Применение Honeyrot Manager позволит своевременно выявить попытки несанкционированного доступа к критичным для организации базам данных и принять необходимые меры по устранению или снижению рисков потери или кражи конфиденциальной информации или выведения из строя бизнес-приложений.
2. Продукт прост в использовании, установке и настройке. Его применение позволит без больших временных и финансовых затрат значительно повысить уровень безопасности информационных систем и оценить активность нарушителей в корпоративной сети.



Код безопасности
ГК «Информзащита»

Тел.: +7 (495) 980-2345

E-mail: info@securitycode.ru

Вы можете узнать подробную информацию
о продуктах на сайте

www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. «Код Безопасности» входит в группу компаний «Информзащита» – признанного лидера в сфере информационной безопасности – и является преемником её многолетних наработок в области создания средств защиты информации для государственных и коммерческих заказчиков.