УДК 681.323

А.А. ЗАМУЛА, канд. техн. наук, В.Л. МОРОЗОВ

СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЯ

Введение

Под вторжением понимаются любые действия злоумышленника, направленные на получение доступа к информации, а также внесение изменений в обычный ход работы системы. Даже если атака на систему является лишь способом самоутверждения, чаще всего общей целью злоумышленника является нанесения ущерба компании.

Предупреждение вторжений предполагает реализацию мер, направленных на снижение вероятности успешного проникновения в систему. К важным мерам предотвращения вторжений стоит отнести: разработка и внедрение адекватной угрозам политики безопасности; планирование, внедрение и эффективное использование мер и средств информационной безопасности (фаерволы, системы обнаружения вторжений и другие); обнаружение источника и метода проникновения; обучение персонала особенностям работы по обнаружению и предотвращению угроз безопасности в информационной системе. Данные меры направлены на минимизацию ущерба, который может быть нанесен организации, и восстановление нормальной работы системы.

Необходимость создания систем обнаружения атак

Системы обнаружения атак (СОА) стали доступными с коммерческой точки зрения еще в 90-х годах XX века. СОА работает по принципу сигнализации: при обнаружении проникновения в систему подается сигнал тревоги. Сигнализация может представлять собой как аудио- и/или видеооповещение в виде, например, звуковых сигналов и/или мигающего света. Также можно настроить «тихое» оповещение: текстовое сообщение, присылаемое на мобильный телефон. Большинство СОА позволяет администраторам реализовать множество видов реакций на ту или иную угрозу с соответствующим оповещением. Кроме информирования администратора системы с помощью текстового сообщения или электронной почты, есть возможность оповещения другой компании, если вопросы обеспечения информационной безопасности организации были переданы на аутсорс. В современных системах СОА является частью системы предотвращения вторжений (СПВ). СПВ не только способна обнаруживать вторжение, но и имеет возможность предотвратить вторжение, используя активные методы. Ввиду того что указанные системы часто устанавливаются совместно, то для описания современных систем информационной безопасности используют общий термин: система обнаружения и предотвращения вторжений (СОПВ).

В соответствии с документацией NIST [1] есть несколько причин для внедрения и использования СОПВ:

- предотвращение вторжений в систему;
- обнаружение злоумышленников (например, установление IP-адресса);
- необходимость обнаруживать атаки в начальные моменты ее реализации;
- необходимость документирования существующих угроз информационной безопасности (ИБ) организации;
- необходимость контроля качества администрирования ИБ в информационной системе;
- необходимость сбора информации о вторжениях для улучшения диагностики, восстановления и устранения причин вторжения.

СОПВ является сдерживающим фактором, снижающим возможности потенциальных злоумышленников по совершению атак. Еще одной причиной, по которой следует устанавливать СОПВ, является то, что сетевое оборудование не во всех случаях способно обеспечить защиту от известных уязвимостей и новых видов атак.

Существует множество факторов, из-за которых снижается уровень защищенности информационной системы организации. Например, несовершенство или ошибки программ, сканирующих сеть с целью обнаружения уязвимостей. К тому же, в случае правильной идентификации уязвимости не всегда есть возможность быстрого реагирования на угрозу. СОПВ способна распознать действия злоумышленника, направленные на сканирование как систем защиты, так и информационной сети организации.

Одним из предназначений СОПВ является документирование угроз, которые имели место в информационной системе организации. В этом случае СОПВ используется для сбора сведений о состоянии ИБ организации, что позволяет своевременно повышать степень защищенности системы как в целом, так и отдельных компонентов защиты.

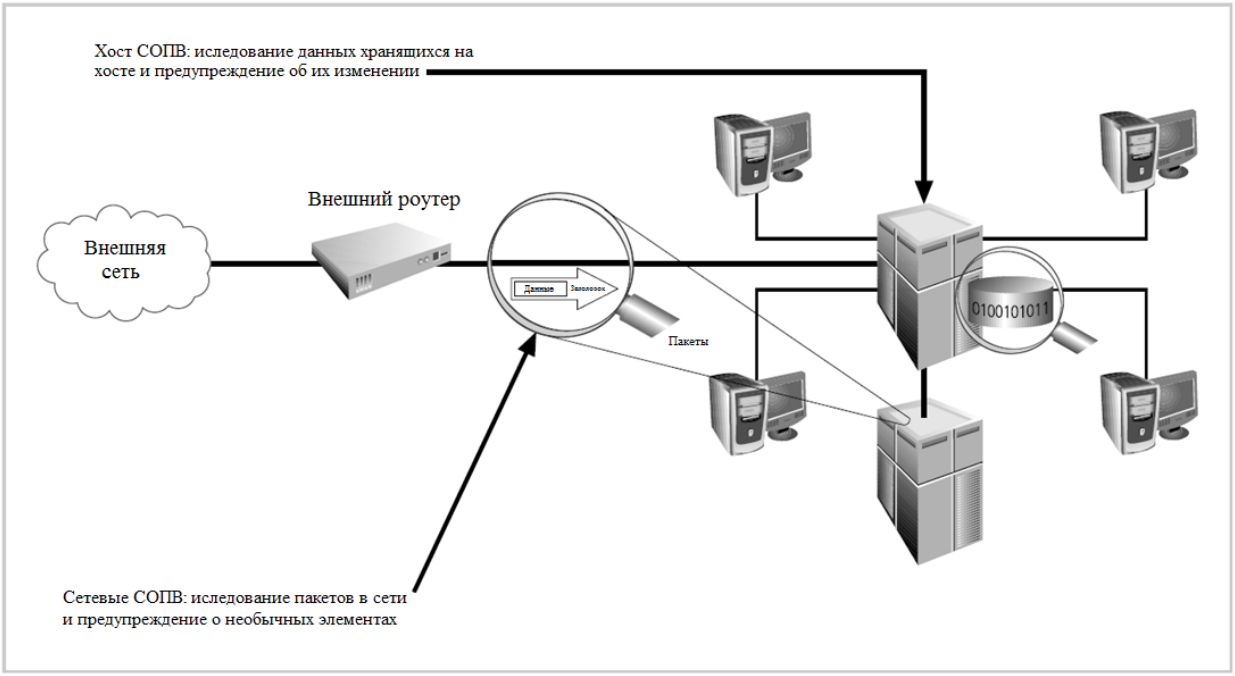
Наконец, СОПВ, если и не может предотвратить атаку, то она используется для анализа имевшей место атаки: как осуществлялась атака, результат, которого добился злоумышленник, какие методы он использовал. Данная информация важна для устранения уязвимостей и предупреждения последующих атак. Также полученная информация может быть использована для поиска злоумышленника и судебного разбирательства [2].

Варианты реализации СОПВ

В соответствии с NIST 800-94 [1], СПВ отличается от СОА лишь одной особенностью: СПВ способна обнаруживать и предотвращать реализацию угроз. При этом используются следующие методы защиты информационной системы:

- сброс сетевого соединения или сеанса, которые используются для атаки;
- блокирование доступа к объектам для пользовательского аккаунта, IP адреса и т.д.;
- блокирование доступа к выбранному хосту, сервису, приложению или ресурсу;
- изменение настройки политики безопасности, например, перенастройка сетевого устройства для блокирования доступа злоумышленника к вероятной цели и включение файервола для блокирования атак;
- установка необходимых обновлений в случае обнаружения уязвимости;
- изменение содержания атаки, например: удаление файла-вируса из письма, с возможностью чтения приложенных к нему не зараженных файлов [3].

СОПВ может работать как часть сетевой системы или только на выбранном компьютере (хосте). На рисунке изображены обе системы. Хост СОПВ (ХСОПВ) защищает сервер или данные, хранящиеся на хосте.



Системы обнаружения вторжений

Сетевые СОПВ (ССОПВ) направлены на защиту информационных сетей. ССОПВ можно разделить на две разновидности: беспроводные СОПВ и анализаторы поведения сети (АПС) СОПВ. Последние исследуют поток трафика в сети для обнаружения элементов свойственных DDoS атакам, действиям вредоносного программного обеспечения.

ССОПВ устанавливают на оборудовании, подключенном к сети. При этом система осуществляет функции проверки трафика на данном участке сети, осуществляя поиск элементов, относящихся к атакам. О факте обнаружения атаки уведомляется администратор. ССОПВ распознает значительно большее количество угроз, чем СОПВ, но. при этом является значительно более сложной в настройке и обслуживании.

Для верификации входящих пакетов и обнаружения атак ССОПВ сравнивает пакеты с базами сигнатур, которые хранятся в аппаратной части ССОПВ.

Пакет данных считается верифицированным, если он удовлетворяет условиям хотя бы одного из принятых стандартов интернет протоколов, которые объединены в стек протоколов в операционной системе или приложении. Многие виды атак, например DoS и DDoS, используют уязвимости протоколов, посылая неверно сформированные пакеты или же большое количество стандартных пакетов.

Важным преимуществом ССОПВ является тот факт, что малое количество оборудования способно обслуживать большие сети. Обычно ССОПВ использует пассивные методы обнаружения атак. Следовательно, внедрение в существующие сети не окажет существенного воздействия на нормальное функционирование сети. Безусловным преимуществом ССОПВ является то, что такую систему достаточно сложно обнаружить при внешних атаках.

К недостаткам ССОПВ следует отнести следующее:

- необходимо обрабатывать весь сетевой трафик, что возможно не во всех сетях;
- отсутствует возможность анализа зашифрованных пакетов;
- для определения ущерба от атаки необходимо участие администратора.

В то время как, сетевые СОПВ исследуют участки сети, ХСОПВ отслеживает активность на выбранном компьютере. ХСОПВ также известны как верификаторы целостности системы. Главным преимуществом ХСОПВ является возможность проверки шифрованного трафика и принятие решения о реализации актуальных атак. ХСОПВ инвариантна к смене сетевых протоколов. Также есть возможность детектирования неправомерного использования программ и приложений на основе анализа логов.

Однако ХСОПВ более сложна в настройке и обслуживании, чем ССОПВ и занимает больший объем дискового пространства. Также ХСОПВ неспособна отследить сетевое сканирование. А поскольку система отслеживает всю активность на выбранном компьютере, то снижается общая производительность.

Методы обнаружения СОПВ

СОПВ реализует различные подходы, при этом превалируют три основных: сигнатурный подход, статистический подход и метод анализа состояния пакетов.

СОПВ, основанная на сигнатурном подходе осуществляет исследование трафика сети в поисках элементов, которые находятся в базах сигнатур. Данный подход распространен ввиду того, что большинство атак имеют четко выраженные особенности. Такие особенности представлены в сигнатуре. Однако сигнатурные базы необходимо постоянно обновлять, иначе новые виды атак не будут распознаны. Атаки, распределённые по времени, сложнее распознать, поскольку сигнатурный подход рассматривает сетевую активность за небольшие интервалы времени. Преодоление этого недостатка состоит в том, что бы хранить и обрабатывать данные за большие промежутки времени. Но указанное потребует большого объема дискового пространства и вычислительных возможностей.

Статистический подход основан на сборе статистических данных о трафике во время нормальной работы сети. Полученная статистическая база при помощи статистических методов сравнивается с определенными временными промежутками текущего состояния

сети. О превышении активностью сети некоторого граничного значения уведомляется ответственный персонал. В статистические данные могут входить: данные о количестве используемой памяти и ресурсов процессора; типы принимаемых пакетов и их количество и другое. Достоинство данного подхода состоит в возможности определения новых типов атак. К сожалению, данный подход требует значительно больших объемов памяти и вычислительных мощностей. Кроме того, при использовании такого подхода не всегда удается обнаруживать атаки, приносящие малые статистические изменения. Если действия пользователей информационной системы невозможно предсказать, то данный метод мало эффективен, поскольку возможно большое количество ложных срабатываний.

Метод анализа состояния протоколов позволяет отслеживать все соединения между внешними и внутренними системами, записывая данные об источнике, получателе, времени отправки пакета. Согласно NIST SP 800-94 [1], метод анализа протоколов – это процесс сравнения априори известных профилей активности для каждого состояния протокола и событий для определения отклонений. Данный метод зависит от универсальных профилей производителя, определяющих как необходимо, и как не следует использовать протокол. Собранные во время работы системы данные используются для обнаружения атак, использующих большое количество запросов. Иногда этот процесс называют глубоким исследованием пакетов.

Также данный метод может исследовать сеансы аутентификации с точки зрения «подозрительной» активности.

Главный недостаток данного метода значительные затраты на отслеживание всех соединений. К тому же, если сетевой протокол (IP,UDP,TCP и другие) не противоречит стандарту, система не опознает вторжение.

Действия СОПВ зависят от выбранного метода обнаружения и выполненной настройки системы. В зависимости от настройки система может собирать дополнительную информацию о проникновении, изменять настройки сети, подать сигнал тревоги или даже противодействовать вторжению. При настройке СОПВ необходимо правильно рассчитывать реакцию системы на угрозу. Например, если реакция СОПВ на DoS атаки заключается в уменьшении количества активных сетевых подключений, то атака по сути достигла своей цели.

Реакцию на угрозы можно классифицировать как активную и пассивную. Активная реакция – это действия, выполняемые при обнаружении угрозы ИБ. Такая реакция может включать в себя: сбор дополнительной информации; изменение среды сети; действия, направленные против злоумышленников. Пассивная реакция заключается в информировании ответственного персонала о собранной информации и ожидании непосредственного участия администратора. В общем случае, администратор выбирает набор действий после анализа собранных данных. Пассивный вариант является более предпочтительным.

Выводы

Системы обнаружения и предотвращения вторжений являются важной составляющей в комплексе мер по организации защиты информации в информационной системе организации. В СОПВ имеет место уязвимости и их нужно компенсировать другими средствами. Таким образом, СОПВ может выполнять следующие функции:

- слежение и анализ системных событий и пользовательского поведения;
- тестирование настроек системы безопасности;
- создание основы нормального состояния системы, с последующим сравнением текущих состояний;
- распознавание элементов системных событий, относящихся к известным атакам;
- распознавание нормальной работы сети;
- управление аудитом операционных систем и ведение логов генерируемых данных;
- извещение персонала о обнаруженных атаках;

• выполнять внешними экспертам функции мониторинга информационной безопасности.

К сожалению, в СОПВ имеет место некоторые ограничения на использование. К таким ограничениям можно отнести:

• несвоевременное обнаружение, уведомление и реагирование на атаки при большом потоке входящей информации;

• сложность обнаружения новых видов или вариантов уже известных атак;

• невозможность эффективно реагировать на атаки злоумышленников, обладающих высокой квалификацией;

• отсутствие возможности исследовать атаки без участия человека;

• не обеспечивает надежную защиту от атак, направленных на уничтожение СОПВ.

Размещение и внедрение СОПВ не всегда является простой задачей. При установке СОПВ следует учитывать множество условий: настройка системы, особенности построения информационной сети организации. Одной из основных проблем внедрения СОПВ является управление системой.

Список литературы: 1. *Scarfone K., Mell P.* Guide to Intrusion Detection and Prevention Systems (IDPS) // NIST Special Publication 800-94. Gaithersburg, MD 20899-8930, 2007. – 127с. 2. *Fry C., Nystrom M.* Security monitoring. – Sebastopol: O'Reilly Media, Inc., 2009. – 248с. 3.*Scarfone K., Bace R.* NIST SP 800-31 // NIST, 2001. – 51с.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 14.02.2014