Пашкова Анна Сергеевна
студентка
Бурдастых Юлия Николаевна
студентка
Вихарева Анна Валерьевна
студентка
Кононов Алексей Сергеевич
студент
ФГБОУ ВО «Юго-Западный
государственный университет»
г. Курск, Курская область

АНАЛИЗ ЭФФЕКТИВНОСТИ СРЕДСТВ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

***Аннотация**: в данной статье рассмотрены технологии обнаружения сетевых атак, а также проведен анализ эффективности этих средств, изучение аппаратно-программных средств, специализированное с целью выявления и устранения сетевых угроз. Статья должна послужить руководством по защите персонального компьютера, подключенного к сети и личных данных пользователя этого компьютера.*

***Ключевые слова**: сетевые атаки, информационная безопасность, программные средства, сетевые угрозы, узел сети, IDS, IPS, сервер, сеть, несанкционированное вторжение.*

В двадцать первом веке движущей силой и основным предметом всех сфер человеческой работы делается информация, и статус каналов, сетей и защищенность серверов будут базой экономического формирования. К сожалению, сложные сетевые технологии довольно уязвимы для целенаправленных атак. При этом подобные атаки могут производиться удаленно, в том количестве и из-за пределов национальных границ. Целиком это устанавливает новые трудности

перед разработчиками и строителями информационной инфраструктуры. Многие нынешние формы бизнеса целиком основываются на сетевых технологиях (электронная торговля, IP-телефония и т. д.) и согласно этой причине особенно уязвимы. Понадобится тут и международное сотрудничество в сфере законодательства и установления барьеров для сетевых террористов. Никак не исключается, что будет необходимо со временем изменить с учетом условий безопасности некоторые протоколы и программы.

Средство IDS/IPS – программное или аппаратно-программное средство, специализированное с целью выявления и устранения сетевого несанкционированного вторжения или атак, нарушения безопасности. В функции средств IDS/IPS вступают: анализ сетевого трафика (входящего и/или исходящего) и выявление сетевых вторжений и атак, а также вредоносных программ; предотвращение сетевых вторжений, атак и защита от вредоносных программ в сетевом трафике; обнаружение уязвимостей, как дополнительная функция для выявления атак на них.

Средства IDS/IPS классифицируются:

1. Согласно способу реагирования (режиму функционирования):

– режим обнаружения вторжений (IDS) – пассивные, обнаруживают и регистрируют данные сетевых вторжений, атак и вредоносных программ, выдают предупреждения при выявлении и/или вносят сведения в журнал;

– режим предотвращения вторжений (IPS) – активные, кроме функции выявления, кроме того мешают сетевым обнаружениям, атакам и вредным программам. Главные методы противодействия: блокирование сочетаний, окончание сессий с нападающим узлом и фильтрование сетного трафика с вредных проектов.

2. Согласно области использования: сетевые (network-based IDS, NIDS) – отслеживают вторжения и атаки, контролируя сетевой трафик, и ведут наблюдение за несколькими хостами; узловые (персональные) (host-based IDS, HIDS) – формируются на узлах (рабочих станциях, серверах), отслеживают вторжения и атаки, нацеленные на определенный узел, применяя анализ системных вызовов,

логов приложений, модификаций файлов (исполняемых, файлов паролей, системных баз данных), состояния узла и других источников; согласно определенным протоколам (protocol-based IDS, PIDS) – отслеживают проникновения и атаки, контролируя общесетевой трафик по конкретным сетевым протоколам; на уровне приложения (application protocol-based IDS, APIDS) – отслеживают вторжения и атаки на определенные приложения (к примеру, на интернет-приложения); на уровне операционных систем (operation system IDS, OSIDS) – отслеживают вторжения и атаки в определенные операционные системы; на уровне системы управления базами данных (data baces managment system (DBMS)-based IDS, DBMSIDS) – отслеживают вторжения и атаки на конкретные СУБД. Согласно способу выявления проникновения и атаки: обнаружение аномального поведения (anomaly-based) – оценка ведется с целью выявления отклонений в работе сети или статистически важных отличий трафика от стандартного в данной сети. Этот способ ориентирован на обнаружение новых типов атак. Минусом такого подхода считается затруднительность в настройке и огромное число ложных тревог в случае неправильно установленных правил; выявление по сигнатуре (signature-based) – при рассмотрении трафика сравниваются пакеты с базой данных сигнатур (известных атрибутов атак). Подобный аспект позволяет обнаружить известные сетевые угрозы. Главной проблемой подобного подхода считается устаревание баз сигнатур – появлениями новых типов атак и обновлением баз сигнатур способен пройти довольное количество времени, в протяжение которого станет нельзя выявить подобную угрозу. Задача выполнения тестовых испытаний – анализ возможности и производительности защиты средств IDS/IPS от различных сетевых атак и угроз.

Классификация систем обнаружения атак

Существует большое число классификаций систем выявления атак, но наиболее лучшей является классификация по принципу реализации:

1) host-based – система ориентирована на определенный узел сети;

2) network-based – система ориентирована на целую сеть или сегмент сети.

Имеется немало способов перехитрить IDS, к примеру, перегрузив его. Многие IDS обладают механизмы усовершенствования эффективности и это может являться применено хакером, к примеру, многие IDS игнорируют параметры, передаваемые в запросе GET. Возможно обмануть IDS, используя медленное сканирование. Есть известная сигнатура атаки, содержащая в себе конкретную строку в URL-запросе. В случае если показать ее в альтернативной кодировке с применением символов %, IDS данную строку никак не распознает. Настройка IDS обязана осуществляться с учетом реальных угроз конкретной сети. Рассчитывать на то, что сервис провайдер содержит собственную систему IDS, ни в коем случае нельзя. Необходимо также учесть, что поставляемые совместно с IDS программы анализа журнальных файлов, требуют оптимальной настройки. Настройка IDS основательно зависит от используемой ОС. Одним из приемов атак считается шестнадцатеричное кодирование параметров HTTP-запросов или применение для этих целей уникодов. Концепция атаки состоит в том, что дешифровка такого представления параметров может в конкретных случаях выполняется неправильно, что показывает хакерам дополнительные возможности. Еще один минус IDS считаются ложные тревоги, которые при достаточно высокой частоте могут, в конце концов, приглушить внимание админа к реальным угрозам.

IDS предоставляет данные для сетевого администратора, для того чтобы он, в случае если посчитает необходимым, сделал конкретные меры. В некоторых случаях в действительности, что действия администратора уже запоздали. Исследования показывают, что задержка в 10 часов предоставляет 80% для успеха взломщика, а при 20 часах возможность проникновения оказывается равной 95%, при 30 часах задержки – удача хакера гарантирован, каким бы опытным ни был админ. При нулевой задержке взаимодействия на подготовку атаки неплохой администратор не оставляет практически никаких шансов хакеру. Стремительная реакция на угрозу уменьшает осуществимый ущерб не только для атакуемого объекта, но иногда и для всего Интернет сообщества (способен сократиться число пораженных сетевых объектов.

IDS пригодна для того, чтобы понять, насколько ситуация тревожна. С целью усовершенствования положения необходимы вспомогательные действия. Положение IDS на рынке услуг показывает рис. 1, из него видно, что интерес к IDS становится ограниченным.

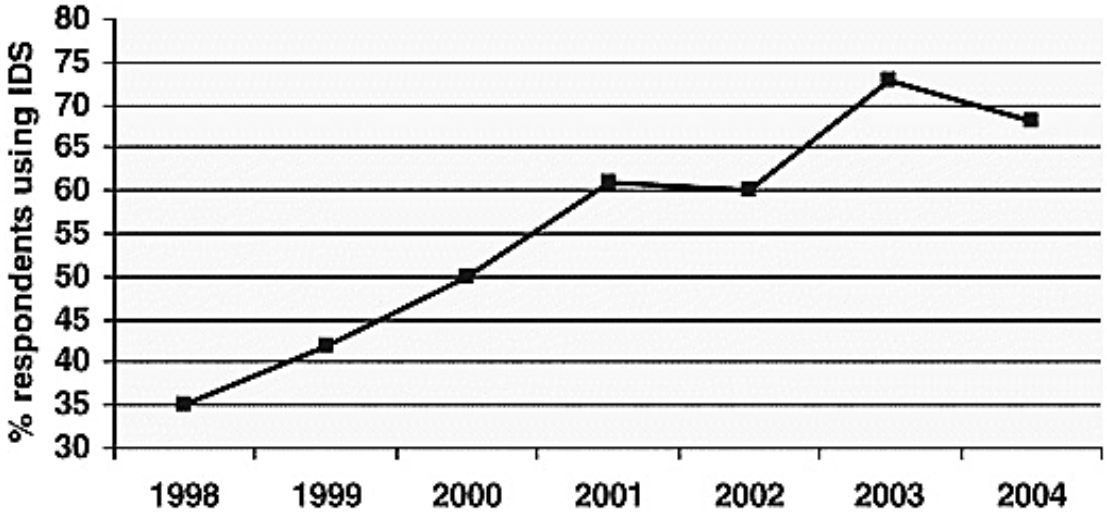

Рис. 1. Вариация числа используемых IDS по годам

Так как IPS/IMS основываются на IDS, они наследуют все ее минусы (нечувствительны к неизвестным сигнатурам атак, дают ложные тревоги и пр.). Данные системы блокируют только атаки, которые детектируются с большой степенью достоверности. Помимо этого, они требуют тонкой настройки высоко квалифицированными администраторами. В случае отказа IPS (или успешной атаки) сеть или компьютер, которую она защищает, потеряет доступа к внешней сети.

Технология обнаружения атак должна преодолевать со следующим:

1. Распознавание известных атак и предупреждение о них определенных лиц.

2. Понимание непонятных источников сведений об атаках.

3. Возможность управления способами защиты неспециалистами в области безопасности.

4. Контроль всех действий субъектов информационной сети (программ, пользователей и т. д.).

5. Освобождение или снижение функций персонала, который отвечает за безопасность, нынешни*х* рутинных операций согласно контролю.

Зачастую системы выявления атак могут осуществлять функции, которые расширяют диапазон их использования. К примеру:

Контроль эффективность межсетевых экранов. Возможно разместить систему обнаружения после межсетевого экрана, чтобы установить недостающих правил на межсетевом экране.

Контроль узлов сети с устаревшим ПО

Блокирование и контроль доступа к некоторым ресурсам Internet. Хоть они отдалены от возможностей подобных как сетевых экранов, однако если нет денег на приобретение сетевого экрана, можно расширить функции системы обнаружения атак

Контроль электронной почты. Системы могут отслеживать вирусы в письмах, а вдобавок подвергать анализу содержимое входящих и исходящих писем

Системы обнаружения атак, которые стоят на определенных пк, как правило, исследуют сведений из журналов регистрации ОС и разных приложений. Но в последнее время выпускаются программы, которые непосредственно интегрированные с ядром ОС.

Плюсы систем обнаружения атак

Коммутация позволяет распоряжаться большими сетями, как несколькими небольшими сетевыми сегментами. Выявление атак на уровне определенного узла предоставляет более успешную работу в коммутируемых сетях, так как позволяет поставить системы обнаружения на тех узлах, где это необходимо. Системы сетевого уровня никак не нуждаются, что бы на хосте ставилось ПО системы выявления атак. Для контролирования сетевого сегмента, необходим только один сенсор, независимо от количества узлов в этом сегменте.

Пакет отправленный от злоумышленника, не будет возвращен назад. Системы, которые функционируют на сетевом уровне, осуществят обнаружение атак при живом трафике, то есть в масштабе реального времени. Рассматриваемая информация содержит сведения, которые будут доказательством в суде.

Системы обнаружения, которые функционируют на сетевом уровне, не зависят от ОС. Для подобных систем все равно, какая именно ОС создала пакет. Рассмотрим наиболее популярные средства IDS.

Таблица 1

Общая информация по средствам IDS/IPS

Наименование	Snort	Suricata	Bro Network Security Monitor	AlienVault OSSIM
Тип средств IDS/IPS	Сетевая	Сетевая	Сетевая	Сетевая
Назначение (способы реагирования)	IDS и IPS	IDS и IPS	IDS и IPS	IDS и IPS
Разработчик	Sourcefire	OISF	Vern Paxson	AlienVault
Способ реализации	Программный	Программный	Программный	Программный
Поддерживаемые операционные системы	Linux, FreeBSD, Windows	BSD, Mac OS X, Solaris, Windows/Cygwin. Linux, UNIX	Linux, BSD UNIX (FreeBSD, NetBSD, OpenBSD)	Linux
Лицензия	Бесплатная (GNU GPL)	Бесплатная (GNU GPL)	Бесплатная (GNU GPL)	Бесплатная (GNU GPL)
Версия	39693	3.0.1	42402	5.0.3

Таблица 2

Основные функциональные возможности средств IDS/IPS

Наименование	Snort	Suricata	Bro Network Security Monitor	AlienVault OSSIM
Контролируемые сетевые протоколы	TCP, UDP, ICMP, HTTP/S, FTP, Telnet, SSH, SMB, SMNP, SMTP, IMAP, NetBios	TCP, UDP, ICMP, HTTP/S, FTP, Telnet, SSH, SMB, SMTP, SMNP, IMAP, NetBios	TCP, UDP, ICMP, HTTP/S, FTP, Telnet, SSH, SMB, SMNP, SMTP, IMAP, NetBios	TCP, UDP, ICMP, HTTP/S, FTP, Telnet, SSH, SMB, SMTP, SMNP, IMAP, NetBios
Сигнатурный метод обнаружения угроз	+	+	+	+
Аномальный метод обнаружения угроз	–	–	+	+
Реагирование на сетевые	+	+	+	+

атаки в режиме реального времени				
Формирование отчетов	+	+	+	+
Тип аудита (логирование и запись событий)	Лог-файлы, базы данных и веб-интерфейс (Snoby, Squil, Squert и др)	Лог-файлы, базы данных и веб-интерфейс (Snoby, Squil, Squert и др)	Лог-файлы	Лог-файлы, базы данных и веб-интерфейс (Snoby, Squil, Squert и др)
Возможность работы с другими сетевыми устройствами	–	–	–	+
Наличие многопоточного режима работы	–	+	+	+
Анализ туннелированных протоколов	+	+	+	+
Формирования чёрного и белого списка IP адресов	+	+	+	+

Таким образом, средства обнаружения вторжений являются одним из важнейших факторов, обеспечивающих защиту информации в сетях. В данной статье мы рассмотрели классификацию средств обнаружения сетевых атак, указали основные функции, выделили плюсы использования этих средств и варианты реакции на обнаружение атак. Так же мы провели сравнительный анализ наиболее популярных средств IDS и записали данные в таблицы. По приведенной нами информации видно, что средства, описываемые в данной статье, не имеют существенных отличий, все они являются бесплатными, что делает их общедоступными. Кроме того, большинство из них поддерживается на многих известных операционных системах, таких как Windows, Linux и т. д., что немаловажно. Грамотное применение средств обнаружения сетевых атак в совокупности с постоянным контролем может уберечь информационную систему от многих неприятностей.

Список литературы

1. Защита информации [Электронный ресурс]. – Режим доступа: http://infoprotect.net/

2. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org

3. CITForum.ru [Электронный ресурс]. – Режим доступа: http://citforum.ck.ua/

4. Лаборатория центра обеспечения информационной безопасности [Электронный ресурс]. – Режим доступа: http://lab.infosec.uz/site/index