Московский Физико-Технический Институт (ГУ МФТИ)
Кафедра Радиотехники

Эссе по курсу «Защита информации»

«Системы обнаружения вторжения»

Выполнил студент 114 группы Родкин Михаил Михайлович

http://www.re.mipt.ru/infsec

Москва, 11.04.05

Что такое IDS?

Система обнаружения вторжения (СОВ), она же в исходном, англоязычном варианте IDS (Intrusion Detection System), – это программный комплекс, который позволяет выявлять и блокировать попытки взлома LAN и оповещать об этом. Такие системы состоят из многих компонентов, но наиболее общо из можно разделить на три части. Сердце системы - модуль перехвата трафика, работающего в пределах сегмента сети, он применяется для сбора информации, которая впоследствии будет использована для диагностики. Для ее выполнения потребуется анализатор, а для ответных действий системы - модуль оповещения/блокировки. Нетрудно догадаться, что таких систем может быть великое множество. Кому-то требуется защитить весь сегмент сети, а кому-то только сервер, кого-то атакуют извне, а кого-то «свои», у кого-то есть деньги, чтобы развернуть систему, и нанять персонал, а у кого-то нет. Поэтому и системы бывают разные – сетевые и хостовые, для серверов и рабочих станций, для архитектур Fast Ethernet и Gigabit Ethernet, для обнаружения и предотвращения атак. Самыми популярными по праву считаются *сетевые решения* (Network Intrusion Detection Systems, NIDS), контролирующие сразу множество узлов в сети. Они анализируют трафик с целью обнаружения известных атак на основании имеющихся у них наборов правил. Исключением с точки зрения принципов анализа являются системы на базе нейросетей и искусственного интеллекта. Однако, это экзотика, требующая сложной (в том числе аппаратной) реализации, а, значит, предназначена на отдельных клиентов. На них мы останавливаться не будем. В противоположность сетевым решениям существуют так называемые *системы на уровне хоста* . В отличие от сетевых, они не работают трафиком, а проверяют регистрационные журналы операционной системы или приложения.

Какие бывают СОВ.

Любой процесс познания начинается с классификации. Попробуем разобраться, какие же существуют IDS (СОВ), и что каждая из них предлагает. Один из способов классификации СОВ основывается на уяснении того, что они, собственно, контролируют. Одни контролируют весь сетевой трафик и анализируют сетевые пакеты, другие разворачиваются на отдельных компьютерах и контролируют операционную систему на предмет выявления признаков вторжения, третьи, как правило, контролируют отдельные приложения. Другая классификация основана непосредственно на методах обнаружения подозрительной деятельности. Рассмотрим обе из них.

СОВ, защищающие сегменты сети.

Этот класс IDS (СОВ) в настоящее время наиболее распространен среди коммерческих продуктов. Система обычно состоит из нескольких специализированных серверов, которые анализируют сетевой трафик в различных сегментах сети и передают сообщения о возможном нападении на централизованную консоль управления. Никакие другие приложения не работают на серверах используемых СОВ, поэтому они могут быть хорошо защищены от нападения. В настоящий момент практикуется несколько вариантов развертывания (местоположения) СОВ на основе защиты сети: позади внешней системы сетевой защиты (межсетевых экранов) – обнаружение нападения, проникающего через оборонительный периметр сети из внешнего мира; впереди внешней системы сетевой защиты – доказывает, что нападения из Интернета против сети предпринимаются регулярно; на опорных сетевых каналах – обнаружение неправомочной деятельности в пределах сети и мониторинг большого объема сетевого трафика; и, наконец, в критической подсети – выявление атак на критические ресурсы. Сетевые СОВ обладают многими преимуществами. Во-первых, несколько удачно расположенных систем могут контролировать большую сеть. При этом их развертывание оказывает незначительное воздействие на существующую сеть т.к. подобные СОВ, как правило, пассивные

устройства, которые перехватывают сетевой трафик, не загружая сеть служебными потоками. Такая система может быть весьма защищенной от нападений на нее саму. Недостатков у нее тоже немало - система не в состоянии распознавать нападение, начатое в момент высокой загрузки сети. Некоторые разработчики пытаются решить эту проблему, реализуя СОВ на основе аппаратных средств, обладающих более высокой скоростью. Кроме того, необходимость быстро анализировать пакеты вынуждает разработчиков обнаруживать нападение с минимальными затратами вычислительных ресурсов, что серьезно снижает эффективность обнаружения. Несмотря на это, все современные коммерческие системы, хотя и анонсируют возможность работы в Fast Ethernet, на деле не могут работать в сетях с пропускной способностью выше 60 – 80 Мбит/с. Вторая серьезная проблема таких СОВ это то, что они не могут быть реализованы в современных коммутируемых сетях. Коммутаторы разделяют сеть на ряд небольших сегментов (обычно один высокоскоростной канал Ethernet на сервер) и обеспечивают выделенные каналы между серверами, обслуживаемыми тем же коммутатором. В таком случае, будучи подключенной к одному из каналов, СОВ не сможет контролировать трафик по другим каналам. В наихудшем варианте ей будет доступен лишь широковещательный трафик. Еще недостатки этой системы: неспособность анализировать зашифрованную информацию, и отсутствие анализа степени проникновения злоумышленника, снижают ее эффективность.

Расширением такой СОВ можно считать систему GrIDS (Graph-Based Intrusion Detection System в английском варианте). Не желая попадаться, злоумышленники научились тактике распределенного сбора информации. Применение нескольких машин, позволяет избежать сходства трафика с известным шаблоном, присущим той или иной тактике вторжения. В результате обычные сетевые СОВ (NIDS) удается обойти. Для предотвращения именно таких атак были созданы GrIds. Принцип их функционирования аналогичен технике сбора информации обычной сетевой СОВ, при этом в каждый сегмент LAN устанавливается свой сниффер (модуль перехвата траффика). Информация от них собирается вместе, анализируется и представляется в виде схемы информационных потоков. Благодаря такой методике удается распознавать сложные шаблоны. Последние, кстати, характерны и для сетевых червей, так что GrIDS вполне можно использовать и для их обнаружения.

СОВ, защищающие отдельный сервер.

Данные (Host-based IDS) системы обнаружения были созданы для работы под управлением конкретной операционной системы. Они собирают информацию о контролируемом ими сервере на основе анализа активности процессов. Это позволяет СОВ анализировать действия на сервере с высокой степенью детализации и точно определять, кто из пользователей выполняет злонамеренные действия в операционной системе сервера. Они способны обнаруживают нападения, которые не выявляют СОВ, защищающие сегмент сети. Стоит заметить существенное различие между этими типами СОВ. Как правило, сетевые системы работают в режиме реального времени, в то время как хостовые анализируют системные журналы, то есть обнаруживают злоумышленника постфактум. Некоторые хостовые СОВ имеют возможность управлять группой серверов, подготавливая централизованные отчеты о возможных нападениях, которые обобщаются на консоли администратора защиты. Другие генерируют сообщения, совместимые с системами управления сетью. СОВ такого типа способны работать в сетях, использующих шифрование данных, и функционируют в коммутируемых сетях. Благодаря тому, что СОВ работают на отдельном сервере, механизмы сбора информации должны устанавливаться и поддерживаться на каждом сервере. Это затрудняет обслуживание системы и увеличивает загруженность серверной машины. Они не способны контролировать ситуацию во всей сети, так как «видят» только сетевые пакеты,

получаемые сервером, на котором они установлены. Эти системы сильно загружают процессор и требуют больших объемов дискового пространства для хранения своих журналов. По сравнению с системами, контролирующими сегмент сети, они более уязвимы и могут быть атакованы и заблокированы подготовленным противником. К недостаткам стоит еще отнести трудности в обнаружении и противодействии нападению, связанному с отказом в обслуживании.

Одной из разновидностей хостовых СОВ являются OIDS (Operational Intrusion Detection Systems). Они призваны помочь в защите от внутреннего врага (несанкционированных действий), на долю которых приходится около 4/5 всех случаев взломов. Эти системы разработали на случай, если злоумышленнику удалось войти в систему от имени (логина) легального пользователя. Или, когда атака на сеть происходит изнутри нее самой. Система сравнивает действия конкретного пользователя в данный момент времени с его обычными, и в случае сильных расхождений - бьет тревогу. Проще говоря, оценивается типичность действий (операций) каждого пользователя; в то время как сетевые СОВ оценивают типичность трафика.

СОВ на основе защиты приложений.

Эти системы контролируют события, проявляющиеся в пределах отдельного приложения, и нередко обнаруживают нападения при анализе его системных журналов. Возможность связываться непосредственно с приложением посредством служебного интерфейса, а также большой запас прикладных о нем знаний позволяют СОВ данного класса обеспечивать более детальное представление о подозрительной деятельности внутри приложения. Они способны работать в зашифрованных средах за счет взаимодействия с программами, выполняющими шифрование. Такие системы наиболее уязвимы к атакам, в результате которых могут быть отключены противником, ибо работают как простые приложения на контролируемом ими сервере.

В настоящее время различия между системами на основе защиты приложений и системами на основе защиты отдельного сервера не всегда четко прослеживаются, и эти два класса систем нередко объединяют в один.

СОВ на основе сигнатуры.

До этого момента мы рассматривали СОВ с точки зрения возможной их архитектуры: где они будут размещены, и что они будут контролировать. Это, пожалуй, наиболее глобальная их классификация, ведь задавшись определенным типом, мы уже определили рамки функционирования системы и ее специфику. Однако такой подход не определяет саму способность системы адекватно реагировать на потенциальные угрозы, отличать «своих» от «чужих». Поэтому анализ событий – краеугольный камень их функционирования. На его основе существующие СОВ можно поделить на использующие обнаружение сигнатуры и обнаружение аномалии.

Подход к обнаружению вторжения на основе сигнатуры выявляет деятельность, которая соответствует предопределенному набору событий, уникально описывающих известное нападение. Как и антивирусные сканеры, NIDS работают с паттернами (в данном контексте - шаблонами характерных свойств). Здесь речь идет не о детектировании опасного кода, а об анализе трафика на предмет наличия подозрительных свойств, присущих тому или иному способу взлома. При обнаружении такового он блокируется, и сообщение об этом высылается администратору. При этом система не страдает недостатком генерирования большого числа ложных тревог. Обычно первый этап взлома LAN - это сбор информации о ней. Как правило, он осуществляется полупассивно. Но и в этом случае, когда на сеть только готовятся осуществить нападение, СОВ способны обнаружить характерные особенности трафика (при сканировании портов) и вовремя среагировать. Из вышесказанного следует, что системы на основе сигнатуры должны быть заранее запрограммированы, чтобы обнаружить каждое известное нападение. Эта

методика чрезвычайно эффективна и является основным методом, используемым в коммерческих программах. Как и всякие системы, она не лишена недостатков. Они проистекают из самой ее сути. А именно, сами сигнатуры во многих системах данного класса определены достаточно узко, что затрудняет обнаружение ими вариантов традиционных нападений, сигнатура которых незначительно отличается от имеющейся в их базе. Но главный недостаток в другом. Это задержка обновления. Поставщики IDS зачастую не успевают оперативно реагировать на новые виды атак и своевременно выпускать соответствующие сигнатуры. Поэтому возможность самостоятельного написания правил представляется весьма полезной. Однако при таком подходе велика вероятность, что написанное правило окажется неэффективным. В этом случае нужна его основательная проверка, к примеру, путем симуляции соответствующей уязвимости. К тому же защита от очередной появившейся атаки требует добавления новой сигнатуры в базу сигнатур IDS, что приводит к разрастанию базы и снижению производительности. Проблема может быть в какой-то степени решена путем описания группы уязвимостей одним правилом.

СОВ на основе аномалий.

Такие системы обнаруживают нападения, идентифицируя необычное поведение (аномалии) на сервере или в сети. Принцип их функционирования основан на том, что нападающие ведут себя не так, как «нормальные» пользователи, и могут быть обнаружены системами, идентифицирующими эти различия. Системы на основе выявления аномалии устанавливают базис нормального поведения, профилируя специфических пользователей или сетевые подключения, и выявляют случаи отклонения контролируемой деятельности от нормы. На сегодняшний день системы данного класса пока еще часто производят большое количество ложных срабатываний. Однако, несмотря на это, исследователи утверждают, что они способны обнаружить нападение, ранее незамеченное, в отличие от СОВ на основе сигнатуры, которые полагаются на результаты анализа прошлых нападений. Некоторые коммерческие СОВ реализуют ограниченные формы обнаружения аномалии, однако лишь единицы полагаются исключительно на эту технологию. Такие системы очень капризны и требуют обширных «обучающих выборок» на основе системных отчетов с результатами вторжений для выявления нормальных образцов поведения. Здесь мы рассмотрели основные типы СОВ, присутствующие на текущий момент. Однако на этом их многообразие и возможности не ограничиваются.

СОВ, автоматически отвечающие на нападения .

Человек-администратор не всегда доступен в момент нападений на систему, поэтому некоторые СОВ могут быть сконфигурированы так, чтобы автоматически отвечать на них. Самая простая форма автоматизированного ответа – уведомление администратора. После обнаружения нападения СОВ может послать по электронной почте или пейджеру письмо администратору с кратким описанием произошедшего события. Более активный ответ может остановить продвижение нападения и блокировать дальнейшие попытки нападающих. Как правило, СОВ не обладает способностью блокировать действия конкретного человека, но могут блокировать конкретные IP-адреса, с которых работает нападающий. Такие системы способны выполнить разрыв подключений TCP при введении пакетов сброса в подключения нападающего с адресатом нападения; реконфигурировать маршрутизаторы и систему сетевой защиты с целью блокировать пакеты от IP-адреса нападающего и протоколы, им используемые. В критических ситуациях, реконфигурируя маршрутизаторы и системы сетевой защиты, СОВ этого класса способны разъединить все текущие подключения, используя специфические сетевые интерфейсы. Более агрессивный способ ответить нападающему предусматривает возможность наступательных действий против нападающего, а также получение информации о сервере нападающего. Однако сам этот ответ может быть достаточно

опасен для организации, так как он, скорее всего, будет незаконным и принесет убытки невинным пользователям Интернета.

Инструментальные средства, дополняющие СОВ.

Существует несколько инструментальных средств, которые дополняют СОВ и часто обозначаются разработчиками как полноценные СОВ, потому что они исполняют аналогичные функции.

«Горшки меда» (Honey Pots) – системы-«приманки», которые пытаются «соблазнить» атакующего, прежде чем он достигнет критически важных приложений. Мониторы и регистраторы вторжения на «горшке меда» обнаруживают несанкционированные акции и собирают информацию о действиях нападающего. Системы «Психиатрическая палата» (Padded Cell) реализуют несколько иной подход. Не привлекая нападающих реальными данными, Padded Cell ждет, пока обычная СОВ обнаружит вторжение. После этого нападающий передается специальному серверу системы Padded Cell. Подобно «горшку меда», эта моделируемая среда может быть заполнена реальными данными, чтобы убедить нападающего, что нападение идет согласно плану. Благодаря таким системам, действия нападающего могут легко контролироваться, а результаты использоваться для совершенствования системы защиты. Система на основе Honey Pots может быть эффективна в выявлении злонамеренных лиц, работающих в качестве авторизованных пользователей, однако у них много недостатков. Во-первых, необходим высокий уровень подготовки администраторов и руководителей службы безопасности, а, во-вторых, юридические значения использования таких устройств еще недостаточно определены, а, значит, против использовавших такие системы вполне может начаться судебное преследование. За исключением отдельных исследовательских прототипов, Padded Cell в данное время недоступны. (см. [3])

Все рассмотренные выше типы IDS широко известны. Их принципы были заложены еще в середине 80-х, эти системы обладают широким спектром действия. Однако, мир не стоит на месте, и жаждущие проникнуть в закрытые от посторонних глаз хранилища всегда оказываются на один шаг впереди разработчиков защитного ПО. Как только появились первые СОВ, так сразу возникли средства борьбы с ней. Тут у потенциальных злоумышленников огромный выбор. Кроме обычных дыр в ПО, можно попытаться «завалить» систему лавиной трафика, можно заблокировать ответную реакцию системы или переконфигурировать сетевое оборудование. Например, злоумышленник может сначала атаковать маршрутизатор и изменить его настройки так, чтобы он направлял трафик через сегмент, который не контролируется и доступен атакующему. Известны и куда менее изощренные способы, вызванные самим ПО. Так, с появлением MS IIS Web Server возникла непредвиденная проблема Дело в том, что системы обнаружения вторжения в процессе своей работы декодируют формы HTTP-запросов типа hex и UTF. До недавнего времени это были два наиболее распространенных формата кодирования URL (Uniform Resource Locator). В MS IIS Web Server реализован и другой формат, предназначенный для представления истинных строк символа Unicode/wide. Поскольку IDS системы не умели обрабатывать HTTP запрос в таком формате, то они и не могли анализировать его. Это обстоятельство позволило использовать новый формат для обхода IDS. Простая атака на переполнение буфера оказалась фатальной для Microsoft SQL Server 2000 Resolution Service и Microsoft Desktop Engine (MSDE) 2000. Хотя она известна довольно давно и уже выпущены специальные программные заплатки, дебют 25 января 2003 г. сетевого вируса Slammer, использующего его, оказался успешным. (см. [1])

Как мы убедились, проблемы обнаружения несанкционированных вторжений чрезвычайно сложны. Для их решения крупные компании тратят десятки миллионов долларов в год. А что же делать тем, у кого таких денег нет, а защитить сеть от чужих глаз очень хочется? И здесь можно найти решение. Например, существует

небезызвестный сетевой проект Snort. В рамках этого проекта происходят разработка, распространение и поддержка одноименной сетевой системы обнаружения вторжений, предназначенной для мониторинга небольших сетей. Система Snort распространяется свободно в исходных текстах или в откомпилированном двоичном формате при условии соблюдения лицензии GNU GPL (General Public License). Snort позволяет в режиме реального времени анализировать сетевой трафик, проверяя корректность структуры сетевых пакетов и соответствие содержимого определенным правилам. Для описания сетевых инцидентов и определения реакции системы используется гибкий язык сценариев. При фиксировании системой Snort сетевого инцидента можно, конфигурируя брандмауэр, предотвратить сетевую атаку или передать предупреждающее сообщение через syslog-сервер, определенный пользовательский файл, Unix-сокет или службу Windows WinPopup. Существуют множество вариантов этой системы для различных операционных систем: от Windows до Solaris и различных архитектур: i386, Sparc, Alpha. Для тех, кто не желает связываться со сложными и дорогостоящими программными средствами, существуют и вовсе тривиальные решения – воспользоваться встроенными средствами W2000. Как можно узнать, что на вашу сеть предпринято нападение? Например, проще всего отловить злоумышленника в момент сканирования портов. Также можно заметить внезапное увеличение сетевого трафика. Для этого можно использовать специальные инструменты, но в Windows 2000 вы можете просто добавить предупреждение в мониторе производительности (performance monitor), когда превышен определенный предел. Хорошими индикаторами сетевого трафика являются счетчики TCP-Segments/Sec. или Network Interface-Packets/Sec. Сканирование портов обычно проявляется как устойчивое увеличение трафика в течение нескольких минут, в зависимости от количества просмотренных портов. Вдобавок, есть встроенный инструмент командной строки netstat. С его помощью можно просмотреть статистику по протоколам, по попыткам подключения, по задействованным для этого портам. Другой очень важный счетчик - Web Service-Not Found Errors/sec. Так как любой Web-сканер проверяет, существуют ли определенные URL, счетчик покажет резкое увеличение 404 ошибки. Вы можете заранее установить предупреждения, которые указали бы, что против вас используется cgi сканер. Параллельно, другие счетчики должны поднять тревогу, что против компьютеров вашей сети начато нападение грубой силы. Здесь вам помогут два счетчика - Server-Logon/sec и Server-Errors Logon. Оба они покажут вам, если злоумышленник пытается подобрать пароль к системе. Отслеживая состояние этих компонентов, вы сможете помешать множеству попыток взлома, без использования каких либо сторонних продуктов обнаружения вторжения. Нереально постоянно наблюдать регистрируемые данные целый день, но можно настроить систему таким образом, чтобы предупреждения посылались вам по электронной почте. Можно использовать службу планировщика, чтобы регулярно регистрировать все процессы или сетевые подключения, выполняющиеся в настоящее время. Создавая небольшой сценарий и используя несколько бесплатных инструментов, вы можете построить систему обнаружения вторжения, которая может выиграть у любой коммерческой IDS системы. Для определения вторжения не обязательно иметь более мощное программное обеспечение, чем стандартные средства Windows. (см. [5])

Будущее СОВ

Исследовательские работы в области создания СОВ активизировались после 1985 года, но крупномасштабное коммерческое использование СОВ не начиналось вплоть до 1996-го. Некоторые СОВ получили отрицательную рекламу из-за большого количества ложных срабатываний, недостатка универсальности и недостаточной интеграции с системами управления сетью предприятия. Вместе с тем анализ тенденций их развития позволяет предположить, что в недалекой перспективе большинство проблем, связанных с

функциональностью СОВ, будут разрешены, а, значит, у этих систем есть большое будущее, и оно не за горами.

Ссылки на тему:

Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК-Пресс, 2002г.

www.computerra.ru/offline/2002/444/17907/ - сайт журнала «Компьютера».

www.compdoc.ru/network/local/snort/ - о проекте Snort

www.connect.ru/article.asp?id=3884 – обзорная статья

www.softportal.com/articles/item.php?id=107 – методы защиты, встроенные в Win2k

http://security.to.kg/comp/taksonom.htm - сайт SecurityLab.

www.osp.ru/lan/2003/06/038_print.htm - журнал «LAN»/