Содержание:

ВВЕДЕНИЕ

Система обнаружения вторжений (СОВ) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет [1]. Соответствующий английский термин — Intrusion Detection System(IDS). Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атакипротив уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей)

Первая концепция СОВ появилась благодаря Джеймсу Андерсону и статье. В 1984 Фред Коэн (см. Обнаружение вторжений) сделал заявление о том, что каждое вторжение обнаружить невозможно и ресурсы, необходимые для обнаружения вторжений, будут расти вместе с степенью использования компьютерных технологий.

Системы обнаружения вторжений

Системами обнаружения вторжений (Intrusion Detection Systems) называют множество различных программных и аппаратных средств, объединяемых одним общим свойством - они занимаются анализом использования вверенных им ресурсов и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способны предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин. [2]

Типичный план действий при вторжениях [3]

Возможный способ вторжения может состоять из 5 шагов:

Шаг 1: **внешняя разведка.** Злоумышленник собирает как можно больше информации, не выдавая себя. Это делается посредством получения общедоступных данных, действуя, как обычный пользователь. На этом этапе злоумышленника никак нельзя определить. Например, он может запрашивать информацию с сервиса whois для получения как можно большей информации, насколько это возможно, о доменном имени жертвы. Злоумышленник может просматривать веб-сайты. Он может читать новости, статьи о компании.

Шаг 2: **внутренняя разведка.** Злоумышленник использует более враждебные способы для сканирования информации, но пока еще не выполняет ничего вредного. Он может просматривать веб-страницы в поисках CGI-скриптов, которые легко взломать. Он также может использовать 'ping' для выяснения, какие машины включены. Он может сканировать порты, чтобы узнать, какие сервисы доступны. Для этого можно использовать утилиты такие, как 'rcpinfo', 'showmount', 'snmpwalk' и другие. На этом этапе злоумышленник выполняет нормальные действия и это нельзя назвать вторжением. В это время сетевые IDS могут заметить эти действия и сказать, что кое-кто «проверяет ручки дверей», но никто пока еще не пытается «открывать двери».

Шаг 3: **эксплойт.** Здесь злоумышленник переходит границу и начинает использовать различные «дырки» на машине-жертве. Он может попытаться скомпрометировать CGIскрипт, передавая команды shell в параметрах запроса. Он также может попытаться воспользоваться ошибкой переполнения, передавая большие данные. Злоумышленник может начать подбирать легкие пароли пользователей. Он может проходить различные этапы. Например, если удалось получить войти в систему как обычный пользователь, далее пытается получить командную строку администратора.

Шаг 4: **получение точки опоры.** Теперь, когда у хакера есть доступ к системе, пора спрятать доказательства атаки. Ему нужно подправить контрольный след, файлы логов и убедиться, что он сможет проникнуть сюда заново. Он может установить свою программу, которая разрешит в следующий раз проникнуть в систему без особого труда. Также есть возможность заменить существующие сервисы своими троянскими конями или создать своего пользователя. На этом

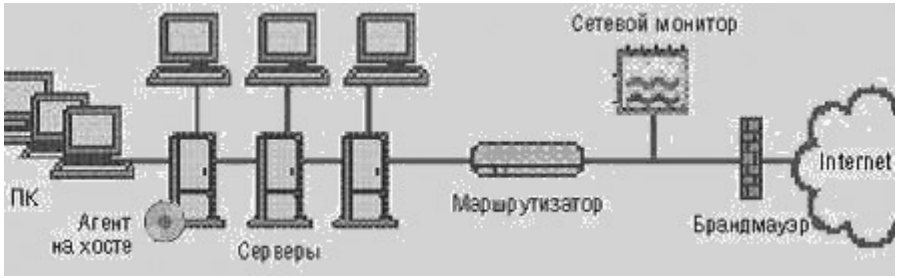
этапе по изменениям системных файлов верификатор целостности системы может заметить злоумышленника. Далее хакер будет использовать систему как точку опоры для остальных систем, так как многие сети меньше защищены от внутренних атак.

Шаг 5: **извлечение пользы.** Злоумышленник, пользуясь своим положением, похищает конфиденциальную информацию, злоупотребляет системными ресурсами (например, устраивает атаки на другие сайты с сервера-жертвы), или портит веб-страницы.

Также существует другой план действий злоумышленника. Вместо того чтобы подвергнуть атаке какой-то определенный сайт, злоумышленник может просто сканировать случайные адреса в интернете в поиске определенной дыры в системе. Например, он может искать во всем интернете машины с дырой SendMail DEBUG. Потом он просто использует найденную машину. Для него неважно, кем является жертва. Это называется «атака дня рождения»: по списку хорошо известных дыр в безопасности и по списку IP адресов – потенциальных жертв можно найти машину, на которой находится система с одной из тех дыр.

Что такое IDS

Системы обнаружения вторжений (IDS) можно представить, как гибрид сниффера (модуля перехвата трафика, работающего в пределах сегмента сети), анализатора и системы оповещения/блокировки. В их основу положена одна простая идея: агент осуществляет мониторинг манипуляций с файлами на хосте или анализ сетевого трафика и сообщает администратору обо всех отклонениях от нормального поведения.



Host based & Network IDS

Рынок систем обнаружения вторжений разделен на две

- основные группы: - системы, диагностирующие вторжение на основе анализа событий на хосте;

- системы, делающие это путем анализа трафика в сети.

Основной принцип систем выявления вторжений на базе хоста — добавление специального уровня обеспечения безопасности на наиболее важных или наиболее уязвимых вычислительных системах, т. е. на хостах. Агент располагается в определенной системе — например на сервере баз данных — и отслеживает результаты аудита и данные системного журнала этого хоста на предмет нетипичного поведения, такого, как повторные попытки входа в систему или изменение прав доступа к файлам. Кроме того, через определенные интервалы времени агент может выполнять контрольное суммирование для установления факта изменений системных файлов. В некоторых случаях агент способен даже остановить атаку на систему, но его основная функция — вести протокол событий и рассылать предупредительные сообщения.

Сетевые системы выявления вторжений располагаются в локальной сети (или в ее сегменте) и осуществляют мониторинг сетевого трафика, пакет за пакетом, в реальном времени (или настолько близко к реальному времени, насколько это возможно). Их задача — своевременно распознать, что характер трафика соответствует заранее определенным сценариям, или сигнатурам вторжений. Сценарии вторжений — это последовательность действий, совпадающая с известными шаблонами атак. Например, при атаке TearDrop по типу «отказ в обслуживании» (Denial of Service, DoS) рассылаемые пакеты фрагментированы таким образом, что это вызывает крах атакуемой системы. Сетевой монитор должен распознать пакеты, соответствующие сценарию TearDrop, и принять необходимые меры.

Основное преимущество системы на базе хоста состоит в том, что она может обнаружить некорректное использование ресурсов как внешними, так и внутренними пользователями, чего не в состоянии сделать ни сетевые мониторы, ни межсетевые экраны. Очевидно, что подобный инструмент следует применять в том случае, когда угроза изнутри более вероятна, чем вторжение хакера извне. Агенты на хостах — это мощные инструменты, им по силам решать такие задачи, как авторизация и доступ, являющиеся наиболее сложными при обеспечении защиты от внутренних пользователей.

Сетевой монитор обладает двумя основными преимуществами. Первое — это выдача предупреждений в реальном времени, что дает администратору возможность остановить или локализовать атаку до того, как она причинит ощутимый ущерб. Это особенно важно в случае атак DoS, когда для уменьшения размера ущерба нужно действовать как можно быстрее. Второе преимущество — накопление «вещественных доказательств». Администраторы не только могут проанализировать атаку для определения возможного причиненного ущерба, но и запись соответствующего сеанса способна сама по себе указать на требующие устранения изъяны в безопасности. (Это верно и для систем на базе хоста.) Так как большинство хакеров прежде всего сканируют намеченную сеть для выявления уязвимых мест, выбор хакером способа атаки сам по себе может указать на эти самые уязвимые места сети. В качестве простейшего примера можно привести операционную систему, на которую еще не была поставлена последняя «заплатка» ее разработчика.

Трудность для сетевых IDS представляют участки сети, в которых трафик шифруется. Ясно, что выявлять какие-либо особенности в трафике невозможно, если он зашифрован. Поэтому в пределах сегмента сети NIDS и криптосредства несовместимы. Такого недостатка лишены Host Based IDS, так как прежде чем попасть на хост, информация дешифруется и в дальнейшем может быть подвергнута полноценному анализу по привычному алгоритму.

Методы обнаружения

Различные IDS используют один из двух методов обнаружения вторжений: обнаружение аномалий и опознавание сигнатуры.

Способ обнаружение аномалий находит необычные явления в статистике. Вначале определяется типичные значения для таких параметров, как загруженность ЦПУ, активность работы диска, частота входа пользователей в систему и другие. Потом при возникновении значительных отклонений от этих значений система сигнализирует о возникшей ситуации. Преимущество этого способа заключается в том, что определяются аномалия независимо от того, чем порождены они. Например, при контроле трафика в сети было обнаружено, что в 14 часов многие рабочие станции подключаются к серверу и начинают выполнять некоторые операции. Это пример явления, которым стоит поинтересоваться и выяснить причину.

Способ опознавания сигнатуры основывается на исследовании трафика на предмет распознавания хорошо известных шаблонов атак. Это могут быть любые действия. Например, нужно проверять любой пакет, передаваемый по сети на наличие строки "/cgibin/phf?", который означает, что кое-кто пытается обратиться к уязвимому CGI-скрипту на веб-сервере. У некоторых IDS-систем огромная база таких строк. Их подключают к сети, и они начинают сканировать каждый пакет.

Внешние и внутренние вторжения

Лица, выполняющие злоумышленные действия, могут быть классифицированы в две группы:

- Внешние: злоумышленники – извне сети. Они могут выполнить различные атаки (ухудшение качества обслуживания веб-серверов, отправка спама на почтовые сервера и др.) они также могут пытаться обходить брандмауэр (firewall) для того, чтобы атаковать рабочие станции внутри сети. Внешние злоумышленники могут быть из интернета, dial-up линий, от физического проникновения в сеть.
- Внутренние: лица, которые законно используют локальную сеть. Они злоупотребляют своими правами (например, служащий социального обеспечения ставит галочку о том, что человек не живой только из-за того, что тот ему не понравился) или выдают себя за другого пользователя (используя его терминал).

По статистике 80% вторжений соответствуют внутренним вторжениям, а остальные 20% - внешним.

Уровни обнаружения

По уровню обнаружения атак IDS делят на следующие:

- NIDS (Network Intrusion Detection Systems)
- GrIDS (Graph-Based Intrusion Detection System)
- OIDS (Operational Intrusion Detection Systems)
- Host Based IDS
- ERIDS (External Routing Intrusion Detection System).

NIDS (Network Intrusion Detection Systems) работает на сетевом уровне, а механизм частично заимствован у снифферов. Они точно также осуществляют перехват данных, их анализ и протоколирование, вот только делают это в автономном режиме и совсем с другими целями. Как и антивирусные сканеры, NIDS работают с 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. 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, NIDS способны обнаружить характерные особенности трафика (при сканировании портов, к примеру) и вовремя среагировать. Все NIDS не зависят от типа используемой в сети ОС. Для работы им необходим выделенный узел в контролируемом(-ых) сегменте(-ах) и сетевой адаптер, умеющий принимать все типы пакетов.

GrIDS (Graph-Based Intrusion Detection System) по своей сути являются усовершенствованными NIDS. Настолько, что приобретают ценные свойства, не присущие простым NIDS. В каждый сегмент LAN устанавливается свой сниффер. Информация от них собирается вместе, анализируется и представляется в виде графа (схемы информационных потоков). Хорошо работает против тактики распределенного (распараллеленного) сбора информации, которая позволяет обойти обычные NIDS. Благодаря такой методике удается распознавать сложные шаблоны. Последние, кстати, характерны и для I-Worms. Поэтому GrIDS можно рассматривать и как способ обнаружения сетевых червей.

OIDS (Operational Intrusion Detection Systems) предназначены для защиты от внутренних 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 NIDS оценивают типичность трафика.

Host Based IDS - IDS на базе хоста, цель создания которых - защита наиболее важных, или наиболее уязвимых участков LAN. Модуль анализа устанавливается непосредственно на то, что собираются защищать. Далее, Host Based IDS анализирует обращения к этому объекту, опять же пытаясь распознать в трафике

характерные сигнатуры. Возможно использование других методов, например - проверки контрольных сумм файлов, размещенных на объекте, с целью выявить их несанкционированную модификацию. К достоинствам такой системы можно отнести тот факт, что она способна эффективно противостоять как вторжениям извне, так и изнутри. В то же время важно, чтобы Host Based IDS была совместима с используемой на защищаемом хосте ОС.

ERIDS (External Routing Intrusion Detection System) – пример инновационной и узкоспециализированной системы. Необходимость ее создания была продиктована тем фактом, что помимо простого и распределенного способа сбора данных о сети существуют менее тривиальные. Например, злоумышленник сначала осуществляет атаку на маршрутизатор, изменяет его настройки так, что он направляет трафик через сегмент, который не контролируется и доступен атакующему. Анализ перехваченного трафика проводится уже в этом сегменте, в спокойной обстановке.

IDS используют сигнатуры, которые объединены в базу данных сценариев атак (БДСА); кроме того, администраторы могут добавить в нее свои собственные сценарии или модифицировать существующие. Если система распознает атаку, она посылает предупреждение администратору. В некоторых случаях система выявления вторжений может и ответить на атаку, например, разрывая соединение. Кроме мониторинга и рассылки предупреждений система ведет запись действия во время атаки для пос4ледующего анализа. Сетевые системы обнаружения вторжений могут взаимодействовать с другими системами безопасности, такими, как межсетевые экраны в целях предотвращения взлома последних. IDS вовсе не являются самодостаточными. Они разрабатываются с учетом взаимодействия с файрволлами и антивирусными системами.

Следует учитывать, что степень сложности IDS требует соответствующей квалификации обслуживающего ее персонала. Прежде чем приобретать IDS следует подумать, кто будет заниматься ее поддержкой.

Как и любая система детектирования, IDS имеют свой процент ложноположительных (сигнал опасности при отсутствии таковой) и ложноотрицательных (когда вторжение все же проходит незамеченным) срабатываний. Следует настроить IDS так, чтобы попасть на золотую середину - конфигурацию, при которой система не станет доставать ежеминутными сообщениями о мнимой опасности, но все же сможет достаточно уверенно определять известные ей типы атак.

IDS & Firewall

Существует ошибочное мнение, что если есть firewall, то нет необходимости ставить IDS. Брандмауэры – это устройства, которые просто выключают все и разрешают только некоторый набор операций. Их используют для того, чтобы предостерегаться от «дырок» в безопасности, случайно оставленных открытыми. При установке firewall, он первым делом закрывает все соединения. А потом администратор добавляет правила, которые разрешают некоторые виды трафика через firewall. Например, типичный корпоративный firewall запрещает все UDP и ICMP пакеты, запрещает все входящие соединения и разрешает только исходящие. Эти настройки не позволяют хакерам подключаться извне, но все же исходящие соединения разрешены. Этим может как-то воспользоваться злоумышленник.

Можно сказать, что firewall – это ограждение вокруг сети с определенным количеством хорошо выбранных дверей. У ограждения нет возможности определить, пытается ли кто-то ворваться внутрь (например, злоумышленник роет яму под ограждением), также оно не может определить, действительно ли человеку, который входит в дверь, разрешено это делать, а просто запрещает доступ к определенным точкам.

Иными словами, firewall – это не динамическая система защиты, каким является IDS. Системы обнаружения вторжений замечают те действия, которые firewall – не в состоянии заметить.

Еще одна проблема firewall – это то, что они находятся на границе сети и не видят ничего, что происходит внутри. Он только замечает то, что проходит сквозь него.

Вывод

Прежде, чем выбирать какую-то конкретную IDS, нужно решить, нужны ли они вообще для данной сети. В некоторых ситуациях бывает достаточно установить firewall. Для банковских систем, где должна прослеживаться почти каждая операция, без таких систем вряд ли можно обойтись. Для работы с IDS требуется соответствующий квалифицированный персонал. Любая IDS потребляет какие-то ресурсы. Перед тем, как выбирать IDS, следует учесть все эти факторы.

Список некоторых систем обнаружения вторжений

AAFID, ACME!, ADS, AFJ, AID, AIMS, ALERT-PLUS, ALVA, APA, ARMD, ARMOR, ASAX, ASIM, AudES, BlackICE, Bro, Centrax, CERN-NSM, Cisco, Secure, IDS, CMDS, ComputerWatch, CSM, CyberCop, Monitor, CyberTrace, DEC, DIDS, Discovery, DPEM, Dragon, DRISC, EASEL, EMERALD, ERIDS, ESSENSE, eTrust, ID, FW-1, specific, NID, GASSATA, GrIDS, Haystack, HAXOR, Hummer, Hyperview, IDA(1), IDA(2), IDA(3), IDEAS, IDES, IDIOT, ID-Trak, Inspect, INTOUCH, INSA, ISM, ISOA, ITA, JiNao, KSE, KSM, MIDAS, MIDS, NADIR, NAURS, NetProwler, NetStalker, NetSTAT, NFR, NID, NIDAR, NIDES, NIDX, NSM, PDAT, PReCis, ProxyStalker, POLYCENTER, Security, ID, RealSecure, RETISS, RID, SecureNet, PRO,

SecureSwitch, SHADOW, SIDS, Snort, Stake, Out, Stalker, TIM, Tivoli, Cross-Site, for, Security, TRW-IDS, T-sight, UNICORN, USTAT, VisionIDS, WebStalker, W&S

Список литературы

1. ВИКИПЕДИЯ

Система обнаружения вторжений [1]

https://ru.wikipedia.org/

1. STUDWOOD.

Анализ систем обнаружения вторжений [2]

https://studwood.ru

1. Компьютерра β

http://www.computerra.ru/[3]

1. Издательство «Открытые системы» [4]

http://www.osp.ru/