IDS/IPS — Системы обнаружения и предотвращения вторжений.

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS)) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть.

IDS всё чаще становятся необходимым дополнением инфраструктуры сетевой безопасности. В дополнение к межсетевым экранам (firewall), работа которых происходит на основе политики безопасности, IDS служат механизмами мониторинга и наблюдения подозрительной активности. Они могут обнаружить атакующих, которые обошли Firewall, и выдать отчет об этом администратору, который, в свою очередь, предпримет дальнейшие шаги по предотвращению атаки. Технологии обнаружения проникновений не делают систему абсолютно безопасной. Тем не менее, практическая польза от IDS существует и не маленькая.

Использование IDS помогает достичь нескольких целей:

- Обнаружить вторжение или сетевую атаку;
- Спрогнозировать возможные будущие атаки и выявить уязвимости для предотвращения их дальнейшего развития. Атакующий обычно выполняет ряд предварительных действий, таких как, например, сетевое зондирование (сканирование) или другое тестирование для обнаружения уязвимостей целевой системы;
- Выполнить документирование существующих угроз;
- Обеспечить контроль качества администрирования с точки зрения безопасности, особенно в больших и сложных сетях;
- Получить полезную информацию о проникновениях, которые имели место, для восстановления и корректирования вызвавших проникновение факторов;
- Определить расположение источника атаки по отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

Архитектура IDS

Обычно IDS включает:

- Сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;
- Подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;
- Хранилище, в котором накапливаются первичные события и результаты анализа;
- Консоль управления, позволяющая конфигурировать IDS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты.

По способам мониторинга IDS системы подразделяются на ***network-based (NIDS)*** и ***host-based (HIDS)***.

Основными коммерческими IDS являются *network-based*. Эти IDS определяют атаки, захватывая и анализируя сетевые пакеты. Слушая сетевой сегмент, NIDS может просматривать сетевой трафик от нескольких хостов, которые присоединены к сетевому сегменту, и таким образом защищать эти хосты.

Преимущества NIDS:

- Большое покрытие для мониторинга и в связи с этим централизованное управление;

Несколько оптимально расположенных NIDS могут просматривать большую сеть.

- Не влияют на производительность и топологию сети.

NIDS обычно являются пассивными устройствами, которые прослушивают сегменты сети без воздействия на её нормальное функционирование. Таким образом, обычно бывает легко модифицировать топологию сети для размещения таких IDS.

Недостатки NIDS:

- Обладают высокой ресурсоёмкостью;

Для NIDS может быть трудно обрабатывать все пакеты в большой или занятой сети, и, следовательно, они могут пропустить распознавание атаки, которая началась при большом трафике.

- Требуют дополнительной настройки и функциональности сетевых устройств;

Например, многие коммутаторы, на которых построены сети, не предоставляют универсального мониторинга портов, и это ограничивает диапазон мониторинга сенсора NIDS только одним хостом. Даже когда коммутаторы предоставляют такой мониторинг портов, часто единственный порт не может охватить весь трафик, передаваемый коммутатором.

- Не могут анализировать зашифрованную информацию;

Эта проблема возрастает, чем больше организации (и атакующие) используют VPN.

- Не могут распознать результат атаки;

NIDS не могут сказать была ли атака успешной, они могут только определить, что атака была начата. Это означает, что после того как NIDS определит атаку, администратор должен вручную исследовать каждый атакованный хост для определения, происходило ли реальное проникновение.

- Некоторые NIDS имеют проблемы с определением сетевых атак, которые включают фрагментированные пакеты. Такие фрагментированные пакеты могут привести к тому, что IDS будет функционировать нестабильно.

Host-based IDS имеют дело с информацией, собранной внутри единственного компьютера. Такое выгодное расположение позволяет HIDS анализировать деятельность с большой достоверностью и точностью, определяя только те процессы и пользователей, которые имеют отношение к конкретной атаке в ОС. HIDS обычно используют информационные источники двух типов: результаты аудита ОС и системные логи.

Преимущества HIDS:

- Имеют возможностью следить за событиями локально относительно хоста, могут определять атаки, которые не могут видеть NIDS;
- Могут функционировать в окружении, в котором сетевой трафик зашифрован;

Это становится возможным, когда host-based источники информации создаются до того, как данные шифруются, и/или после того, как данные расшифровываются на хосте назначения.

- Не требуют дополнительной функциональности сетевых устройств.
  Например, на функционирование HIDS не влияет наличие в сети коммутаторов.

Недостатки HIDS:

- Не имеют централизованного управления;

HIDS более трудны в управлении, так как они должны быть сконфигурированы и управляться для каждого целевого хоста.

- Могут быть блокированы некоторыми DoS-атаками или даже запрещены;

Так как по крайней мере источники информации (сенсоры) или часть средств анализа для HIDS расположены на том же хосте, который является целью атаки, то, как составная часть атаки, IDS может быть атакована и запрещена.

- Обладают высокой ресурсоёмкостью;

HIDS используют вычислительные ресурсы хостов, за которыми они наблюдают, что влияет на производительность наблюдаемой системы.

- Малое покрытие для мониторинга.

HIDS не полностью соответствуют возможности определения сканирования сети или других аналогичных исследований, когда целью является вся сеть, так как IDS наблюдает только за сетевыми пакетами, получаемыми конкретным хостом.

По способам определения вредоносного трафика IDS системы подразделяются на: ***signature-based (сигнатурного метода), anomaly-based (метода аномалий)*** и ***policy-based (метода, основанного на политике)*.**

Детекторы атак анализируют деятельность системы, используя для этого событие или множество событий на соответствие заранее определенному образцу, который описывает известную атаку. Соответствие образца известной атаке называется *сигнатурой*, определение атаки или вторжения иногда называют "сигнатурным определением".

Преимущества сигнатурного метода:

- Эффективное определение атак и отсутствие большого числа ложных сообщений;
- Надежная диагностика использования конкретного инструментального средства или технологии атаки.
- Это позволяет администраторам, независимо от уровня их квалификации в области безопасности, начать процедуры обработки инцидента, а также скорректировать меры обеспечения безопасности.

Недостатки сигнатурного метода:

- Обязательное обновление базы данных для получения сигнатур новых атак.

Метод аномалий состоит в определении ненормального (необычного) поведения на хосте или в сети. Детекторы аномалий предполагают, что атаки отличаются от "нормальной" (законной) деятельности и могут, следовательно, быть определены системой, которая умеет отслеживать эти отличия. Детекторы аномалий создают профили, представляющие собой нормальное поведение пользователей, хостов или сетевых соединений. Эти профили создаются, исходя из данных истории, собранных в период нормального функционирования. Затем детекторы собирают данные о событиях и используют различные метрики для определения того, что анализируемая деятельность отклоняется от нормальной

Преимущества метода аномалий:

- Определение атаки без знания конкретных деталей (сигнатуры);
- Детекторы аномалий могут создавать информацию, которая в дальнейшем будет использоваться для определения сигнатур атак.

Недостатки метода аномалий:

- Большое количество ложных сигналов при непредсказуемом поведении пользователей и непредсказуемой сетевой активности;
- Временные затраты на этапе обучения системы, во время которого определяются характеристики нормального поведения.

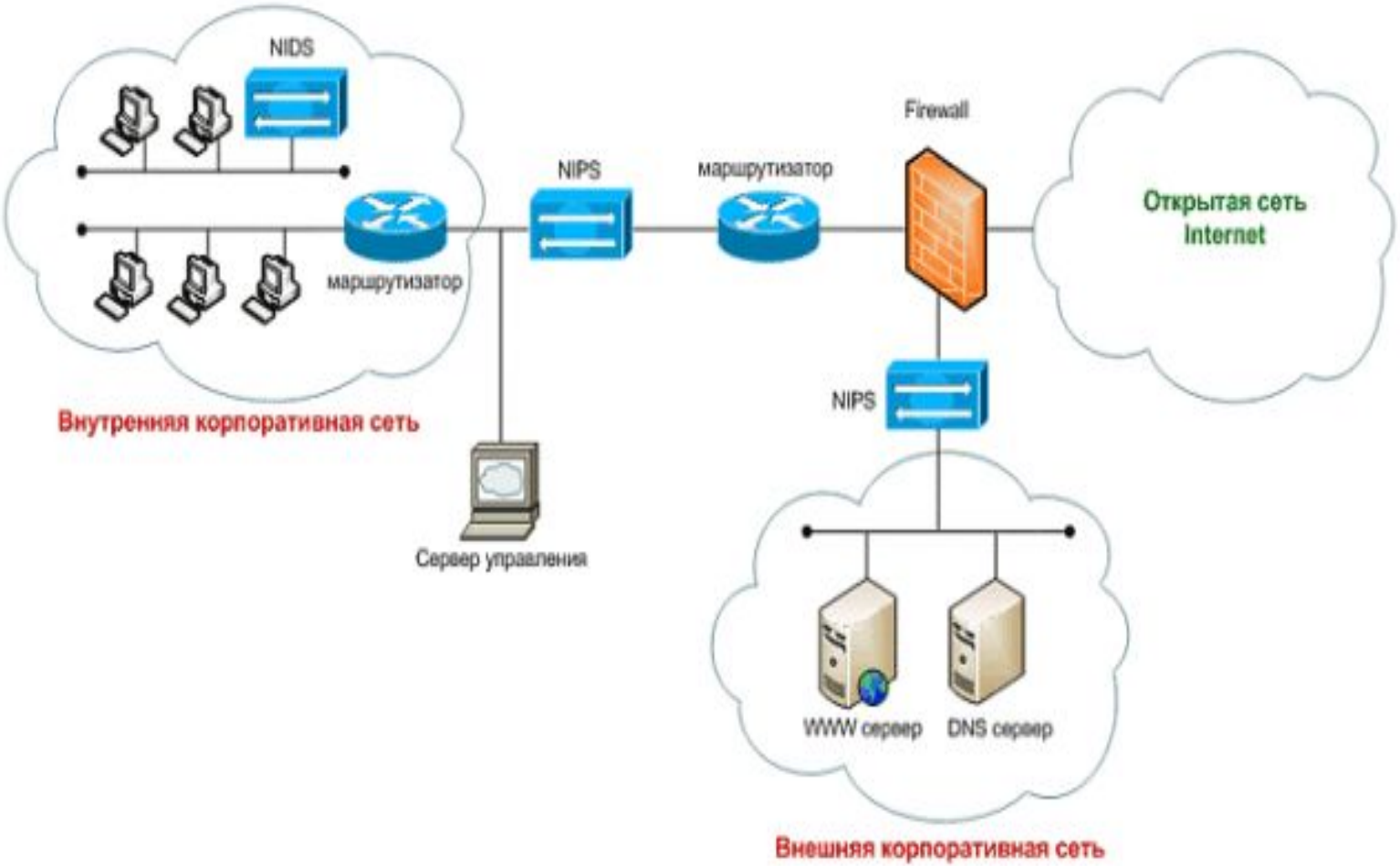
Метод, основанный на политике (*policy-based*) заключается в написании правил сетевой безопасности. В терминах распределения доступа, например какие сети могут взаимодействовать друг с другом и какие протоколы при этом могут использоваться.

Преимущества метода политик:

- Имеет преимущество при обнаружении новых (неизвестных) атак.

Недостатки метода политик:

- Трудоёмкость создания базы политик.



Детекторы (сенсоры) размещены в точках входа в сегменты сети. Сетевые сегменты имеют как внутренние, так и внешние корпоративные ресурсы. Сенсоры отправляют свои отчеты о событиях на сервер управления, расположенный за Firewall.

Система предотвращения вторжений (англ. Intrusion Prevention System (IPS)) — программное или аппаратное средство, которое осуществляет мониторинг сети или компьютерной системы в реальном времени с целью выявления, предотвращения или блокировки вредоносной активности.

В целом IPS по классификации и свои функциям аналогичны IDS. Главное их отличие состоит в том, что они функционируют в реальном времени и могут в автоматическом режиме блокировать сетевые атаки. Каждая IPS включает в себя модуль IDS.

Правильное размещение систем IDS/IPS в сети не оказывает влияния на её топологию, но зато имеет огромное значение для оптимального мониторинга и достижения максимального эффекта от её защиты. На рисунке ниже приведён конкретный пример.

Snort — мощный бесплатный пакет NIDS.

В отличие от многих пакетов с открытым кодом, он совместим с Windows.

Первый разработчик Snort Мартин Реш предоставил программу открытому сообществу на условиях лицензии GNU General Public License (GPL). История этого пакета началась в 1998 г., и с тех пор он не раз доказал свою надежность. Благодаря вкладу членов открытого сообщества и сетевых администраторов во всем мире Snort превратился в очень мощный продукт. Текущая версия обеспечивает анализ сетевого трафика в реальном времени и регистрацию IP-трафика со скоростями Fast Ethernet и Gigabit Ethernet.

Майкл Дэвис перенес Snort 1.7 на платформу Win32, сделав его доступным для сообщества Windows. Затем Крис Рейд взял на себя задачу компиляции новых версий Snort в готовые исполняемые файлы, которые можно без труда развернуть в среде Windows.

Администраторы, незнакомые с NIDS, могут считать инструмент особой разновидностью сетевого анализатора. NIDS проверяет каждый пакет, проходящий через интерфейс, в поисках известных последовательностей в информационном наполнении, где обычно скрыт вредоносный программный код. С помощью Snort можно выполнять операции поиска и сопоставления над каждым пакетом, проходящим через сеть организации, и обнаруживать множество типов атак и нелегитимного трафика в реальном времени.

Для работы Snort необходим компьютер Windows, оснащенный по крайней мере одним сетевым адаптером. Лучше иметь два сетевых адаптера, один из которых подключен к контролируемой сети, а другой — к производственной сети; последний пересылает отчеты.

В небольших сетях развернуть Snort можно на сервере начального уровня. Для обнаружения попыток несанкционированного доступа выделенная машина большой мощности не нужна.

В каком месте сети лучше расположить NIDS? Первая мысль — поместить устройство перед брандмауэром. В этом месте NIDS обнаружит больше всего нападений, но и число ложных срабатываний будет наиболее велико, и администратор получит массу бесполезных предупреждений об опасности. Не следует беспокоиться об угрозах, остановленных брандмауэром, гораздо важнее обнаружить опасные программы, проникшие за него. Поэтому в любом случае лучше разместить Snort позади брандмауэра.

Однако если пользователи подключаются к сети через соединение VPN (по Internet или беспроводной линии связи), имеет смысл разместить NIDS еще дальше за брандмауэром, например за VPN-сервером или концентратором, где пакеты расшифровываются на выходе из туннеля VPN. В противном случае NIDS не сможет противостоять вредоносным программам, встроенным в трафик VPN, так как анализируемые пакеты будут зашифрованы. То же относится и к зашифрованному SMTP-трафику, зашифрованным .zip-файлам, вложенным в сообщения электронной почты, и зашифрованным данным других типов.

В идеале NIDS следует разместить достаточно далеко за любыми компонентами, шифрующими трафик, и довольно близко к периметру сети для анализа трафика в максимальном количестве сегментов и подсетей. В коммутируемой сетевой среде коммутатору, как правило, требуется диагностический порт, в котором собираются все пакеты, проходящие через сеть. В результате NIDS получает удобный доступ ко всему сетевому трафику.

Установка и тестирование Snort

Данный процесс состоит из семи этапов:

1. Установка WinPcap
2. Установка Snort
3. Тестирование Snort
4. Настройка Snort
5. Задание правил
6. Настройка предупреждений и журналов
7. Запуск в качестве службы

Этап 1. Установка WinPcap

В сущности, Snort представляет собой сетевой анализатор, работающий в режиме приема всех пакетов, поэтому ему необходима поддержка на уровне драйверов. Эту поддержку обеспечивает WinPcap. Лорис Диджиоанни создал WinPcap, перенеся в среду Windows широко распространенный среди пользователей Unix драйвер перехвата пакетов libpcap. В состав WinPcap входят фильтр пакетов на уровне ядра, низкоуровневая DLL (packet.dll) и высокоуровневая системно-независимая библиотека (wpcap.dll, на базе libpcap 0.6.2).

Драйвер совместим с Windows Server 2003, XP, Windows 2000, Windows NT, Windows Me и Windows 9x. WinPcap также поддерживает открытый анализатор пакетов Ethereal. С помощью Ethereal можно убедиться в корректности установки Snort.

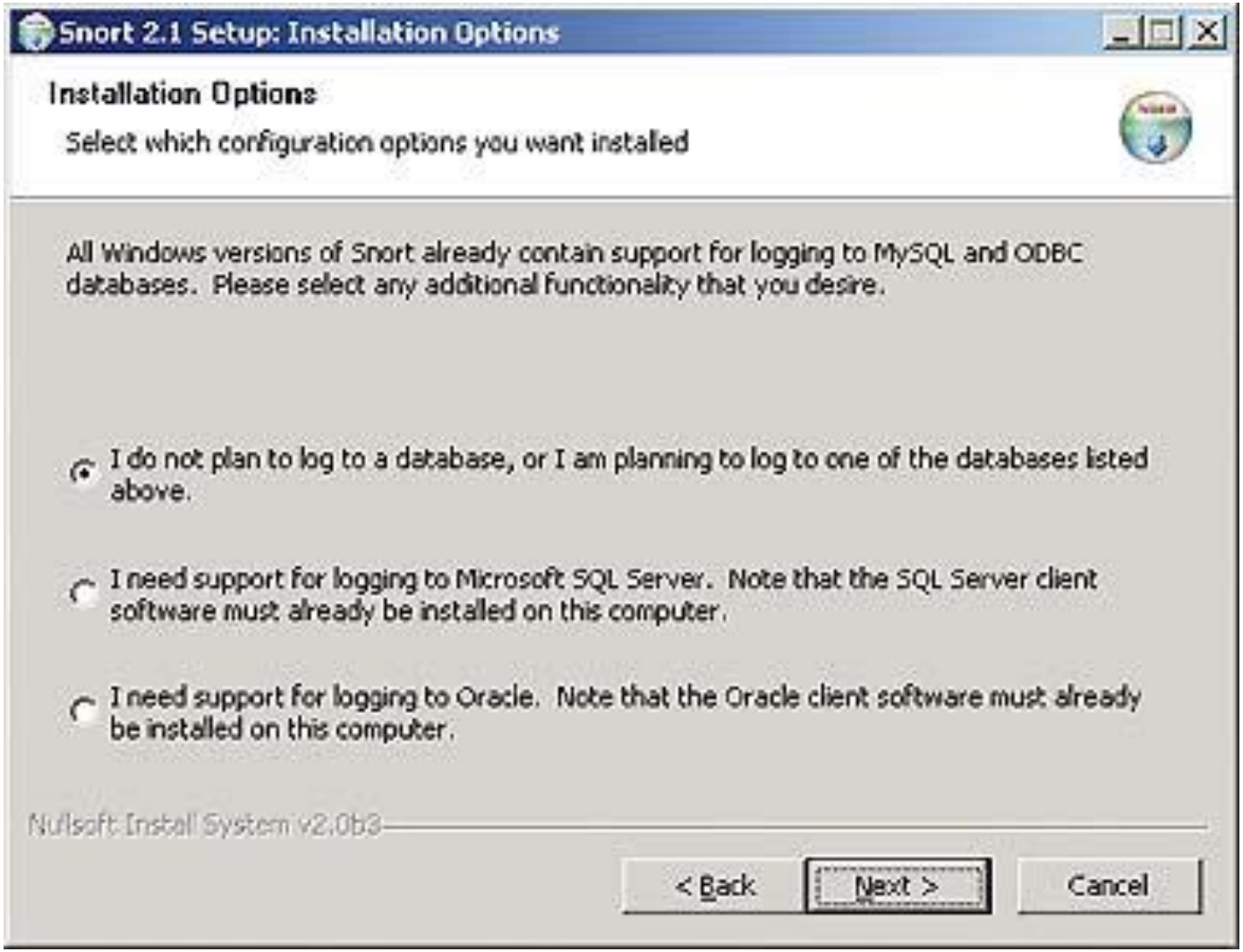
Загрузив из сети установочный файл WinPcap, достаточно пройти по нескольким экранам процедуры инсталляции. Самых больших усилий со стороны пользователя требует экран, на котором необходимо выразить согласие с условиями лицензии.

Этап 2. Установка Snort

Следующий шаг — установка Snort. Новейшую версию можно найти на Web-узлах CodeCraft Consultants

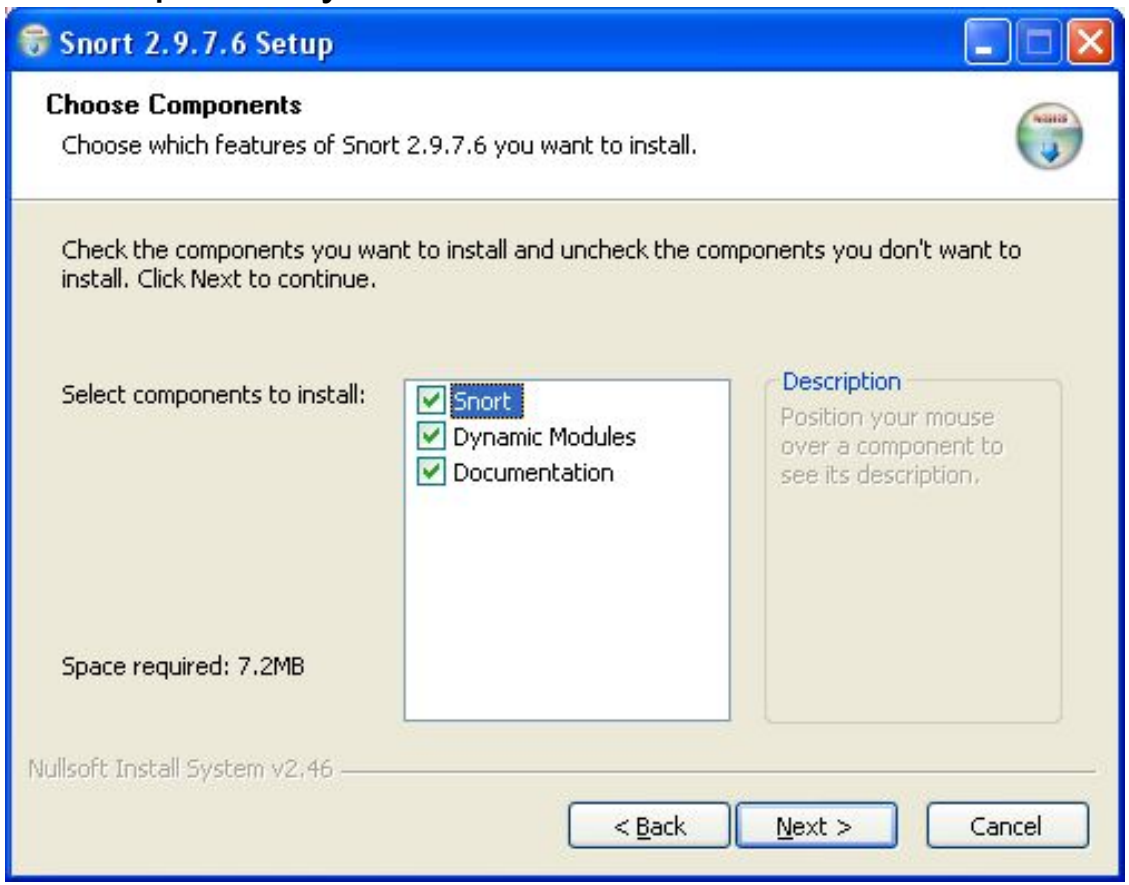
(*http://www.codecraftconsultants.com/snort.aspx*) или Snort.org (*http://www.snort.org*). При загрузке Snort из CodeCraft Consultants, можно получить саморазворачивающийся исполняемый файл. Программа даже проводит пользователя по элементарным операциям установки Snort на компьютере.

При запуске программы установки в первом диалоговом окне необходимо выбрать режим настройки базы данных для хранения результатов. Если используется MySQL или ODBC-совместимая база данных, можно согласиться на режим, выбираемый по умолчанию. Но если предстоит хранить протоколы в базе данных Microsoft SQL Server или Oracle, то необходимо выбрать соответствующий режим и убедиться, что на машине имеется нужная клиентская программа.



Экран 1. Выбор базы данных для журналов

На следующем шаге следует определить компоненты Snort, которые требуется установить. Стандартный набор (экран 2) вполне приемлем, поэтому я рекомендую принять его и щелкнуть на кнопке Next. В диалоговом окне Choose Install Location необходимо указать каталог, в котором будет развернут Snort. Введя имя каталога, следует щелкнуть на кнопке Next, чтобы завершить процесс установки.



Экран 2. Выбор компонентов установки

Этап 3. Тестирование установки Snort

Завершив процесс установки, Snort требуется протестировать.

Если система располагает несколькими сетевыми интерфейсами, то по умолчанию Snort прослушивает первый обнаруженный интерфейс. Если порядок сетевых интерфейсов на машине неизвестен, можно выполнить команду Snort с одним ключом -W. Snort выдает список имен и номеров сетевых интерфейсов в том порядке, в котором их обнаруживает программа. Чтобы заставить Snort использовать определенный сетевой интерфейс, необходимо ввести ключ -i с номером интерфейса при запуске Snort.

Запустив Snort, можно проверить его чувствительность, направив в NIDS специально подготовленный трафик. Один из самых простых способов вызвать предупреждение об опасности — обратиться к командному интерпретатору (cmd.exe) на удаленной машине в рамках запроса HTTP URL (типичный прием «червей» Code Red и Nimda). Чтобы имитировать эту фазу нападения, следует обратиться к любому URL и добавить в конце запроса символы /cmd.exe. Например, в ответ на обращение к http://www.a-website-that-I-can-trust.com/cmd.exe Snort должен вывести предупреждение в командном окне. Эти сообщения и записываются в журнал.

Целевые Web-узлы для тестирования следует выбирать с осторожностью. С технической точки зрения большинство администраторов Web-узлов будут рассматривать подобные действия как попытку взлома. Такая попытка не приведет к успеху (если только в конфигурации сервера не допущены серьезные ошибки), но я рекомендую проводить тестирование только с собственным сервером или доверенным сервером, администраторам которого известно о проведении испытаний.

Если тестирование сделать невозможно, существует другой способ проверить Snort — послать через сеть необычайно длинный эхо-запрос на сервер или компьютер с активной программой Snort. Например, можно воспользоваться командой Ping

ping -l 32767 ip_address где ip_address — IP-адрес целевого сервера или Snort-компьютера. Данная команда должна послать очень длинный пакет (точная длина — 32 Кбайт), что явно необычно для команды Ping. Snort должен обнаружить этот пакет.

Если предупреждения получены, можно приступать к настройке Snort для конкретных условий. В противном случае необходимо вернуться к процедуре установки и проверить, не был ли пропущен какой-нибудь этап.

Этап 4. Настройка Snort

Основные данные о конфигурации Snort хранятся в файле snort.conf, который по умолчанию располагается в каталоге %systemdrive%snortetc. Файл можно оставить в этой папке или переместить в другую, если указать программе путь в командной строке.

Рассмотрим основные параметры Snort.

Чтобы отличить входящий трафик от исходящего, необходимо сообщить Snort узлы и IP-адреса сети предприятия. Для ввода этой информации в файле snort.conf должна быть задана переменная HOME_NET. Следует отыскать строку

var HOME_NET any и заменить ее диапазоном IP-адресов. Можно задать один диапазон, например

var HOME_NET 192.168.0.1/24 или несколько диапазонов. Указывая несколько диапазонов, необходимо заключить набор диапазонов в квадратные скобки и отделить каждый диапазон запятой. Вводить пробелы между диапазонами IP-адресов нельзя. Например, строка

var HOME_NET[10.0.1.0/24,10.0.2.0/24,10.0.3.0/24] указывает Snort, что подсети 10.0.1.0/24, 10.0.2.0/24 и 10.0.3.0/24 относятся к сети предприятия. По умолчанию Snort воспринимает все остальные адреса как внешние. Можно явно указать сети, которые следует считать внешними, задав переменную EXTERNAL_NET. В файле snort.config необходимо отыскать строку

var EXTERNAL_NET any и заменить ее IP-адресом сети, которую следует считать внешней. Однако, как правило, для начала лучше оставить переменную EXTERNAL_NET со значением any.

Этап 5. Задание правил

В одной из строк snort.conf встречается переменная RULE_PATH. Примерный вид этой строки:

var RULE_PATH ../rules Параметр ../rules указывает, что правила (т. е. сигнатуры) можно найти в каталоге rules, который находится в структуре каталогов на одном уровне с двоичными файлами Snort. Поэтому, например, если установить Snort в типовой папке F:snort, двоичные файлы Snort находятся в F:snortbin, а правила — в F:snort rules. При желании можно изменить переменную RULE_PATH, но вполне приемлем и вариант, выбираемый по умолчанию.

Правила — основа Snort. Они представляют собой последовательности байтов, сигнатуры нападений и данные других типов, при обнаружении которых генерируется предупреждение. Snort располагает более чем 1500 готовых сигнатур.

По умолчанию файлы правил некоторых типов (например, icmp-info.rules, chat.rules) представлены комментариями в snort.conf. Используемая по умолчанию конфигурация правил в snort.conf вполне удачна. После активизации блокированных правил программа, как правило, генерирует много лишних предупреждений.

В некоторых файлах содержится ряд полезных правил, но несколько правил генерируют слишком много ненужных предупреждений. Чтобы отключить то или иное правило, нужно обозначить как комментарий соответствующую строку в файле правил. В дальнейшем Snort будет игнорировать это правило при работе с файлом.

При появлении новых источников угрозы файл правил необходимо обновить. Лучший ресурс для новых правил — Web-узел Snort.org. На этом Web-узле нет службы автоматического обновления, поэтому администратору придется регулярно обращаться к нему за обновлениями при возникновении очередной опасности.

Этап 6. Настройка предупреждений и журналов

Как уже отмечалось, Snort обеспечивает запись информации в MySQL, SQL Server, Oracle и ODBC-совместимых базах данных. Достаточно выбрать подходящий тип базы данных в процессе установки Snort. Чтобы чрезмерно не увеличивать объем статьи, рассмотрим стандартные режимы протоколирования с использованием текстового файла и функции записи сообщений в журнал событий Windows.

Текущая версия Snort обеспечивает протоколирование в журнале событий Windows. Многие организации уже приобрели инструменты централизованного мониторинга событий, протоколирования и сбора данных, и данная функция будет отличным дополнением для среды Windows.

NIDS бесполезен, если администратор заглядывает в журналы событий (или текстовые журналы) раз в неделю. Если что-то случается в сети, администратор должен узнать об этом незамедлительно. Централизованная система мониторинга и обработки событий может посылать сообщения по электронной почте, на пейджер и другие устройства связи. Но если такой системы нет, это не повод для беспокойства. Компания NETIKUS.NET предлагает бесплатный пакет EventSentry Light, с помощью которого можно посылать предупреждения.

С помощью EventSentry Light можно настроить систему на мониторинг журналов событий и автоматическую рассылку по электронной почте подробных сообщений о любых событиях Snort, записанных в журнал.

Этап 7. Запуск в качестве службы

Завершив все приготовления, можно задействовать Snort в качестве службы, вместо того чтобы регистрироваться на настольном компьютере всякий раз, когда требуется запустить программу. Если запустить Snort с параметрами /SERVICE и /INSTALL (наряду с другими параметрами командной строки), то Snort настраивается на работу в качестве службы Windows и автоматически запускается вместе с Windows без вмешательства пользователя.

Следующий уровень: модули расширения

Snort представляет собой полнофункциональное приложение. Однако в некоторых случаях программа нуждается в расширении. Например, если в разных участках сети развернуто несколько NIDS, то управлять Snort удобно из графического интерфейса. Такие возможности реализованы в модулях расширения IDScenter фирмы Engage Security и IDS Policy Manager компании Activeworx. Иногда бывает необходимо проанализировать информацию, которая содержится в сообщениях. Просмотреть и проанализировать сохраненные данные можно с помощью модуля Analysis Console for Intrusion Databases (ACID), разработанного в Университете Карнеги — Меллона.

Надежная защита

Snort — полнофункциональная программа, которая не нанесет ущерба бюджету компании. Объединив Snort с мощным приложением мониторинга событий, таким как EventSentry Light, можно своевременно предупреждать атаки против сети.