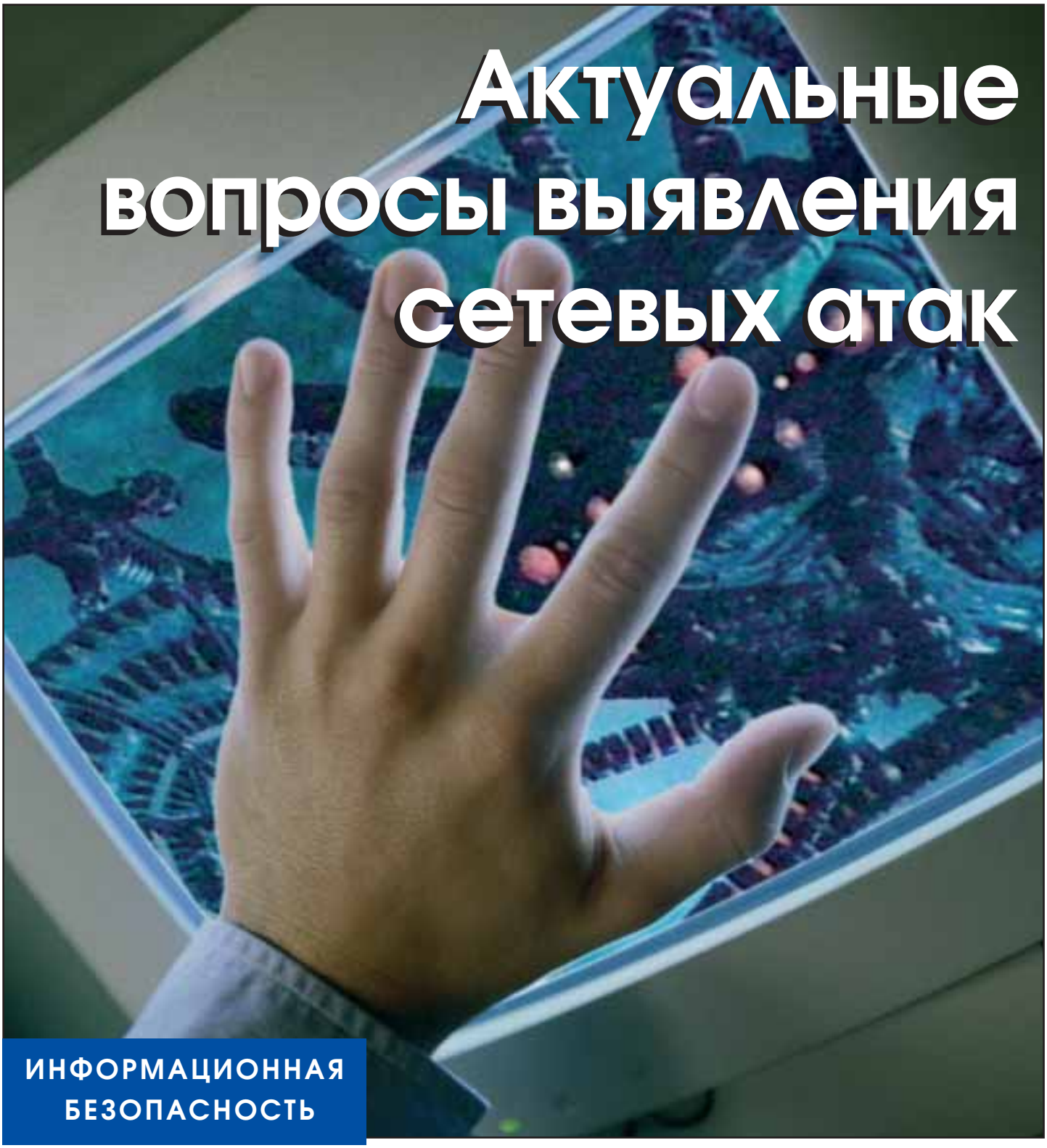
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 3 (106)/2002



Актуальные вопросы выявления сетевых атак

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Актуальные вопросы выявления сетевых атак

Александр Астахов
CISA

СОДЕРЖАНИЕ

1. Введение

С увеличением зависимости мировой экономики и государственных структур от Интернет, возрастает и уровень риска, связанного с осуществлением сетевых атак на ресурсы сетей, подключенных к Интернет. Осуществление атак через сеть Интернет становиться мощным средством ведения информационных войн между государствами, совершения преступлений в финансовой и других сферах, включая и акты терроризма. 22 сентября 2001 года Американским институтом изучения технологий обеспечения безопасности (Institute for Security Technology Studies At Dartmouth College) был опубликован отчет под названием «Кибер-атаки во время войны с терроризмом» (Cyber Attacks During The War on Terrorism: A Predictive Analysis). Данный отчет содержит анализ ситуаций, в которых политические конфликты стимулировали рост числа сетевых атак на ресурсы сети Интернет. Рассмотрению подверглись конфликты между Индией и Пакистаном, Израилем и Палестиной, NATO и Сербией в Косово, США и Китаем в результате столкновения между китайским истребителем и американским самолетом-разведчиком. Целью предпринятого исследования было прогнозирование ситуации в Интернет в результате осуществления США широкомасштабной антитеррористической кампании после трагедии 11 сентября 2001 года. Хотя, при проведении данного исследования, в качестве объектов нападения рассматривались Интернет-ресурсы, принадлежащие США, сделанные выводы применимы и ко всем остальным государствам, включая Россию.

Потенциальные источники сетевых атак были разделены на следующие группы:

- террористические группы;

Список терминов и обозначений

IDS — система выявления атак (Intrusion Detection System)

NIDS — система выявления сетевых атак (Network Intrusion Detection System)

IDS sensor — сенсор системы выявления атак

DMZ — демилитаризованная зона (Demilitarized Zone)

Firewall policy — политика безопасности МЭ

CVE — Common Vulnerabilities and Exposures — тезаурус уязвимостей

CIDF — Common Intrusion Detection Framework — стандарт, определяющий методы взаимодействия между компонентами системы выявления атак

IDWG — Intrusion Detection Working Group — рабочая группа IETF по выявлению атак

IDMEF (Intrusion Detection Message Exchange Format) — формат обмена данными между компонентами IDS

IAP (Intrusion Alert Protocol) — протокол прикладного уровня, предназначенный для обмена сообщениями об атаках (alerts) между компонентами системы выявления атак: сенсорами, анализаторами и менеджерами. Протокол не зависит от формата представления данных.

GIAC (Global Incident Analysis Center) — центр анализа компьютерных инцидентов. GIAC является ведущим в США центром анализа и реагирования на компьютерные инциденты.

GCIA (GIAC Intrusion Analyst) — сертифицированный в GIAC эксперт по выявлению атак. GCIA наиболее уважаемый в мире сертификат в области выявления атак.

SANS (System Administration, Networking, and Security) Institute — Институт системного, сетевого администрирования и администрирования безопасности.

SANS/GIAS (SANS Global Information Assurance Centification) - программа проффессионального обучения и сертификации, учрежденная институтом SANS.

Ingress filtering (RFC 2267) - фильтр входящего трафика предполагает отфильтровывание на внешнем маршрутизаторе входящих пакетов, в которых адреса отправителя принадлежат зарезервированному диапазону адресов, неиспользуемых в адресном пространстве сети Интернет (например 192.168.0.0/255.255.0.0 или 10.0.0.0/255.0.0.0).

Egress filtering (http://www.sans.org/y2k/egress.htm) - фильтр исходящего трафика предполагает отфильтровывание на внешнем маршрутизаторе исходящих пакетов, в которых адреса отправителя не принадлежат диапазону адресов, используемых во внутренней сети.

- хакеры, одобряющие действия террористов или настроенные против США;
- государства, считающиеся оплотом мирового терроризма, против которых может быть направлена антитеррористическая кампания США (включая Афганистан, Сирию, Иран, Ирак, Судан и Ливию);
- любопытствующие и самоутверждающиеся хакеры.

В качестве основных целей осуществления сетевых атак рассматривались:

1. Подмена страниц на Web-серверах (Web defacing) в США и странах союзниках, распространение дезинформации и пропаганды;
2. Осуществление атак на отказ в обслуживании (DoS attacks) на критичные элементы информационной инфраструктуры в США и странах союзниках с использованием «сетевых червей», вирусов, уязвимостей сетевого ПО;
3. Осуществление НСД к Интернет ресурсам США и стан союзников, результатом которых является отказ критичных элементов информационной инфраструктуры и нарушение целостности жизненно важной информации.

Основные выводы по результатам анализа:

1. Физические атаки незамедлительно сопровождаются ростом числа сетевых атак;
2. Количество, сложность и скоординированность сетевых атак неизменно возрастают;
3. Сетевые атаки направлены против особо критичных сетевых ресурсов, к числу которых относятся серверы и активное сетевое оборудование, подключенные к сети Интернет.

Проведенное исследование позволило рекомендовать в качестве первоочередных мер обеспечения безопасности во время войны с терроризмом следующие меры:

1. Повышение уровня журналирования (logging) и оповещения (alert) в системах выявления сетевых атак;
2. Незамедлительное сообщение о подозрительной активности в правоохранительные органы, с целью проведения расследования и принятия предупредительных мер;
3. Следование стандартам и использование передового опыта в области обеспечения информационной и физической безопасности; регулярное обновление ПО, защита от вирусов, использование систем выявления атак и МЭ;
4. Использование рекомендованных мер защиты против известных программных средств осуществления атак (exploites) и резервное копирование критичных информационных ресурсов;
5. Использование методов фильтрации IP-пакетов (ingress and egress filtering) на маршрутизаторах и МЭ для защиты от DoS атак.

Как видно из представленных рекомендаций, наряду со стандартными средствами защиты, без которых немыслимо нормальное функционирование АС (таких как МЭ, системы резервного копирования и антивирусные средства), существует необходимость использования IDS (систем выявления атак), которые являются основным средством борьбы с сетевыми атаками.

В настоящее время IDS начинают все шире внедряться в практику обеспечения безопасности корпоративных сетей. Однако существует ряд проблем, с которыми неизбежно сталкиваются организации, развертывающие у себя систему выявления атак. Эти проблемы существенно затрудняют, а порой и останавливают процесс внедрения IDS. Вот некоторые из них:

- высокая стоимость коммерческих IDS;
- невысокая эффективность современных IDS, характеризующаяся большим числом ложных срабатываний и несрабатываний (false positives and false negatives);
- требовательность к ресурсам и порой неудовлетворительная производительность IDS уже на 100 Мбит/с сетях;
- недооценка рисков, связанных с осуществлением сетевых атак;
- отсутствие в организации методики анализа и управления рисками, позволяющей адекватно оценивать величину риска и обосновывать стоимость реализации контрмер для руководства;
- высокая квалификация экспертов по выявлению атак, требующаяся для внедрения и развертывания IDS.

Специфичной для России также является относительно невысокая зависимость информационной инфраструктуры предприятий от Интернет и финансирование мероприятий по обеспечению информационной безопасности по остаточному принципу, что не способствует приобретению дорогостоящих средств защиты для противодействия сетевым атакам.

Тем не менее, процесс внедрения IDS в практику обеспечения информационной безопасности продолжается, в том числе и в России.

Американский институт SANS учредил программу профессиональной сертификации специалистов по выявлению атак — GIAC Certified Intrusion Analyst (GCIA). Сертификат GCIA, являясь свидетельством продвинутых практических навыков специалиста, ценится в США даже выше, чем скажем CISSP (Certified Information Systems Security Professional), учрежденный ISC (International Security Consortium) и являющиеся эталоном профессиональной зрелости в области информационной безопасности.

В настоящей статье делается попытка охватить ряд существенных вопросов, связанных с выявлением атак и использованием для этих целей современных коммерческих продуктов. Базовую информацию по предметной области можно получить, изучив список часто задаваемых вопросов по выявлению атак (Intrusion Detection FAQ), который можно найти по адресу http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm.

В основе большинства ошибок при принятии решений, в том числе и по защите от сетевых атак, лежит неправильная оценка рисков. Точность оценки рисков, связанных с осуществлением любого вида деятельности, по мнению автора, является основной характеристикой профессиональной зрелости специалиста в предметной области. При отсутствии адекватной оценки рисков сложно ответить на вопросы о том, с чего следует начинать построение системы защиты информации, какие ресурсы и от каких угроз надо защищать и какие контрмеры являются наиболее приоритетными. Сложно также решать вопрос о необходимости и достаточности того или иного набора контрмер и их адекватности существующим рискам.

Таким образом, вопрос оценки рисков, связанных с осуществлением сетевых атак, является первоочередным и рассматривается в первую очередь.

2. Анализ и управление рисками, связанными с осуществлением сетевых атак

2.1. Выявление атак как один из методов управления рисками

Понятие риска является фундаментальным для любой области человеческой деятельности. Чем бы мы не занимались, всегда существует вероятность того, что цели нашей деятельности по тем или иным причинам не будут достигнуты. Само наше существование сопряжено с серьезными рисками, в результате осуществления которых мы можем понести более или менее серьезный ущерб. Таким образом, ***под риском понимается возможность понести ущерб***. На протяжении всей нашей жизни мы постоянно вполне осознано, либо машинально занимаемся оценкой различных рисков: переходя через дорогу, обменивая рубли на доллары или вставляя дискету в дисковод.

В области информационной безопасности оценка рисков играет такую же первостепенную роль, как и во всех других областях человеческой деятельности. Из-за неадекватной оценки рисков, связанных с осуществлением угроз информационной безопасности в современном высокотехнологичном обществе государство, организации и отдельные личности несут весьма существенный ущерб, подсчитать который вряд ли кому-либо удастся.

Величина риска определяется вероятностью успешного осуществления угрозы и величиной ущерба, который в результате будет нанесен. Величина возможного ущерба далеко не всегда может быть выражена в денежных единицах, а вероятность успешного осуществления угрозы вообще не поддается точной оценке. Поэтому наши оценки рисков весьма приблизительны. Их точность зависит от того, насколько хорошо мы ориентируемся в текущей ситуации, представляем себе природу и способы осуществления угроз, а также от нашей способности анализировать и оценивать их последствия.

Оценив риски необходимо принять решение о том, что с ними делать. Этот процесс называется управлением рисками.

Задача управления рисками включает выбор и обоснование выбора контрмер, позволяю-

щих снизить величины рисков до приемлемой величины.

Управление рисками включает в себя оценку стоимости реализации контрмер, которая должна быть меньше величины возможного ущерба. Разница между стоимостью реализации контрмер и величиной возможного ущерба должна быть тем больше, чем меньше вероятность причинения ущерба.

Контрмеры могут уменьшать уровни рисков различными способами:

- уменьшая вероятность осуществления угроз безопасности;
- ликвидируя уязвимости или уменьшая их величину;
- уменьшая величину возможного ущерба;
- способствуя восстановлению ресурсов АС, которым был нанесен ущерб.
- выявляя атаки и другие нарушения безопасности;

Таким образом, ***выявление атак является одним из методов управления рисками, в то время как МЭ являются средством ликвидации уязвимостей и уменьшения их величины.***

Деятельность по выявлению сетевых атак при помощи сетевых IDS заключается в мониторинге сетевого трафика между атакующими и атакуемыми системами, выявлении и анализе подозрительного трафика, оценке уровня серьезности атаки и величины риска, связанного с ее осуществлением, а также принятии решения по реагированию на атаку. Выявление подозрительного трафика, а также, зачастую и определение уровня серьезности атаки, осуществляется IDS автоматически. Наиболее распространенным методом выявления атак является сигнатурный анализ, используемый во всех коммерческих IDS и рассматриваемый ниже. Оценка величины риска, связанного с осуществлением сетевой атаки, требует участия эксперта. На основании оценки риска принимается решение о реагировании на атаку. Если риск незначителен, то атака может вообще не заслуживать внимания. В то же время, в отдельных случаях, может потребоваться принятие незамедлительных мер по реагированию.

Рассмотрим методику оценки рисков, связанных с осуществлением сетевых атак, используемую в SANS/GIAC.

2.2. Оценка серьезности сетевой атаки

Атаки разной степени критичности требуют разного уровня реагирования. Критичность атаки (Severity) определяется величиной риска, связанного с ее осуществлением. Величина риска, в свою очередь, определяется вероятностью успешного осуществления атаки и величиной возможного ущерба. Величина возможного ущерба определяется критичностью ресурсов (Criticality), против которых направлена атака. Вероятность успешного осуществления атаки (Lethality) определяется эффективностью методов и величиной уязвимости системы защиты, используемых для ее осуществления. Величина уязвимости определяется эффективностью контрмер системного (System countermeasures) и сетевого уровня (Network countermeasures), используемых для противодействия данному виду угроз.

Формула для определения уровня серьезности атаки выглядит следующим образом:

SEVERITY = (CRITICALITY + LETHALITY) − (SYSTEM COUNTERMEASURES + NETWORK COUNTERMEASURES)

Данная формула может использоваться для определения величины рисков, связанных с атаками, выявленнными при помощи IDS, при анализе результатов мониторинга сетевого трафика. Обычно интерес представляют только те атаки, для которых величина риска превышает некоторое установленное значение.

Для определения уровня серьезности атаки (SEVERITY) используется числовая шкала от −10 до +10.

SEVERITY {-10, 10} - Величина риска, связанного с осуществлением сетевой атаки.

Критичность сетевого ресурса (CRITICALITY) определяется по 5-бальной шкале исходя из назначения данного сетевого ресурса и выполняемых им функций. На практике обычно ориентируются на следующую шкалу:

5: МЭ, DNS сервер, маршрутизатор
4: почтовый шлюз
2: UNIX рабочая станция
1: персональные компьютеры MS-DOS, Windows 3.11

Вероятность успешного осуществления атаки и вид ущерба (LETHALITY) определяется по следующей шкале:

5: атакующий может получить права суперпользователя на удаленной системе
4: отказ в обслуживании в результате осуществления сетевой атаки
3: получение прав непривилегированного пользователя на удаленной системе, напри-

мер, путем перехвата пароля, передаваемого по сети в открытом виде
2: раскрытие конфиденциальной информации в результате осуществления несанкционированного сетевого доступа, например, атака «null session» на Windows системы
1: вероятность успешного осуществления атаки очень мала

Эффективность реализованных контрмер системного уровня (SYSTEM COUNTERMEASURES) можно оценить по следующей шкале:
5: современная ОС, установлены все программные коррекции (пакеты обновления), используются дополнительные (наложенные) сетевые средства защиты (например, «tcp wrappers» или «secure shell»)
3: Устаревшая версия ОС, неустановлены некоторые программные коррекции
1: Отсутствуют специализированные средства защиты, отсутствует политика управления паролями, пароли передаются по сети в открытом виде

Эффективность реализованных контрмер сетевого уровня (NETWORK COUNTERMEASURES) можно оценить по следующей шкале:
5: МЭ, реализующий принцип минимизации привилегий, является единственной точкой входа в сеть
4: МЭ и наличие дополнительных точек входа в сеть
2: МЭ разрешающий все, что явным образом не запрещено (разрешительная политика управления доступом).

Как уже было отмечено, данная методика оценки рисков, связанных с осуществлением сетевых атак, используется в SANS/GIAC при анализе подозрительных фрагментов сетевого трафика (detects), обнаруженных при помощи сетевых IDS.

3. Недостаточность МЭ для защиты сети от внешних угроз

В настоящее время становится очевидным недостаточность использования для защиты сетей от угроз со стороны Интернет традиционных МЭ, которые не позволяют обеспечить защиту от целого класса угроз безопасности (включая угрозы, направленные против самих МЭ). Традиционные средства защиты информации, включая МЭ, эффективны только против известных уязвимостей. Они вряд ли способны помешать хакерам в поиске новых способов реализации атак. Для этого используются специализированные средства выявления атак (IDS). Мало того, нередко приходится наблюдать ситуации, при которых установка МЭ только снижает общую защищенность корпоративной сети от угроз со стороны Интернет. Неправильно настроенный МЭ создает «дырку» в системе защиты порой большую, чем его отсутствие.

Напрашивается аналогия с американским экспериментом по оснащению всех такси антиблокировочными системами тормозов (ABS), предназначенными для увеличения активной безопасности автомобиля. В результате этого эксперимента, по статистике, количество ДТП с участием таксистов увеличилось, так как водители такси стали вести себя на дорогах более рискованно, больше доверяя тормозам. Таким образом, оказалось, что ABS увеличивает безопасность только в случае сохранения водителем прежнего стиля вождения.

Тот же самый принцип справедлив по отношению к МЭ и любым другим средствам защиты.

Добавление в систему нового средства защиты увеличивает общую защищенность системы только при условии, что существующая практика обеспечения безопасности не изменилась в сторону ослабления механизмов защиты.

При установке МЭ зачастую создается такая ситуация, когда, полагаясь на реализуемые МЭ механизмы защиты, сетевые администраторы перестают предпринимать какие-либо дополнительные меры по обеспечению защиты от угроз со стороны внешней сети, которые обязательно должны быть реализованы в случае его отсутствия. В результате общая защищенность сети от внешних атак может увеличиться, может остаться неизменной, а, вполне вероятно, может и снизить-

ся. Происходит это потому, что администраторы и пользователи сети склонны переоценивать роль МЭ в обеспечении защиты сети от внешних угроз со стороны сети Интернет, всецело на него полагаясь. Они представляют себе МЭ как некий щит, закрывающий их от дождя, града, снега, штормов и прочей непогоды. При этом забывается, что в щите имеется немало дырок, а иногда он даже может напоминать решето. «Дырки» в щите необходимы для общения с внешним враждебным миром. По ошибке, и это весьма вероятно, могут быть открыты не те «дырки» или «дырки» могут оказаться слишком большими, а еще «дырки» в щите иногда можно пробить снаружи.

Таким образом, для обеспечения адекватного уровня защиты, МЭ должны обязательно дополняться специализированными средствами выявления атак. На эту тему было уже достаточное количество публикаций, поэтому нет необходимости еще раз отстаивать этот тезис, иллюстрируя его большим количеством примеров, взятых из печального опыта российских и зарубежных компаний. Однако, приобретя МЭ, руководство российских компаний пока не торопится выделять средства на приобретение и эксплуатацию систем выявления атак.

4. Выявление и анализ подозрительного трафика

4.1. Сигнатуры как основной механизм выявления атак

Системы выявления атак (IDS) решают задачу мониторинга информационной системы на сетевом, системном и прикладном уровне с целью выявления нарушений безопасности и оперативного реагирования на них. Сетевые IDS используют в качестве источника данных для анализа сетевые пакеты, IDS системного уровня (хостовые — host based) анализируют записи журналов аудита безопасности ОС и приложений. При этом методы анализа (выявления атак) остаются общими для всех классов IDS.

Было предложено немало различных подходов к решению задачи выявления атак (в общем случае речь идет о злоумышленной активности, включающей в себя помимо атак, также действия, выполняемые в рамках предоставленных полномочий, но нарушающие установленные правила политики безопасности). Однако все существующие IDS можно разделить на два основных класса: системы, использующие статистический анализ и системы, использующие сигнатурный анализ.

Статистические методы основаны на предположении о том, что злоумышленная активность всегда сопровождается какими-то аномалиями, изменением профиля поведения пользователей, программ и аппаратуры.

Основным методом выявления атак, используемом в большинстве современных коммерческих продуктов, является сигнатурный анализ. Относительная простота данного метода позволяет с успехом использовать его на практике. IDS, применяющие сигнатурный анализ, обычно ничего не знают о правилах политики безопасности, реализуемых МЭ, (поэтому в данном случае речь идет не о злоумышленной активности, а только об атаках). Основной принцип их функционирования — сравнение происходящих в системе/сети событий с сигнатурами известных атак — тот же принцип, который используется и в антивирусном ПО.

Общие критерии оценки безопасности ИТ (ISO 15408) содержат набор требований FAU_SAA под названием «Анализ данных аудита безопасности» (Security audit analysis). Эти требования определяют функциональность IDS, использующих для выявления злоумышленной активности, как статистические методы, так и сигнатурный анализ.

Компонент FAU_SAA.2 «Выявление аномальной активности, основанное на применении профилей» (Profile based anomaly detection) предполагает использование для выявления аномальной активности профилей использования системы, определяющих опасные с точки зрения безопасности действия пользователей системы, и выявления этих действий. С целью определения степени опасности действий того или иного пользователя вычисляются соответствующие «рейтинги недоверия» к пользователям. Чем выше опасность действий пользователя, тем выше его «рейтинг недоверия». Когда «рейтинг недоверия» достигает установленного критического значения, предпринимаются предусмотренные

политикой безопасности действия по реагированию на злоумышленную активность.

Компоненты FAU_SAA.3 «Простая эвристика атаки» (Simple attack heuristics) и FAU_SAA.4 «Сложная эвристика атаки» (Complex attack heuristics) предполагают использование сигнатурного анализа для выявления злоумышленной активности. В случае использования сложной эвристики атаки (FAU_SAA.4), сигнатура определяет последовательность событий, являющуюся признаком нарушения установленных в системе правил политики безопасности.

4.2. Анализ сетевого трафика и анализ контента

Существует два не исключающих друг друга подхода к выявлению сетевых атак: анализ сетевого трафика и анализ контента. В первом случае анализируются только заголовки сетевых пакетов, во втором — их содержимое.

Конечно, наиболее полный контроль информационных взаимодействий может быть обеспечен только путем анализа всего содержимого сетевых пакетов, включая их заголовки и области данных. Однако с практической точки зрения эта задача является трудновыполнимой из-за огромного объема данных, которые приходилось бы анализировать. Современные IDS начинают испытывать серьезные проблемы с производительностью уже в 100 Мб/с сетях. Поэтому в большинстве случаев целесообразно использовать для выявления атак методы анализа сетевого трафика, в некоторых случаях сочетая их с анализом контента.

Сигнатура сетевой атаки концептуально практически не отличается от сигнатуры вируса. Она представляет собой набор признаков, позволяющих отличить сетевую атаку от других видов сетевого трафика. Например, перечисленные ниже признаки могут рассматриваться в качестве сигнатур атак:

Примеры сигнатур атак, используемых при анализе трафика (заголовков сетевых пакетов):

- В заголовке TCP пакета установлен порт назначения 139 и флаг OOB (Out of Band). Это является признаком атаки аля WinNuke.
- Установлены одновременно противоречащие друг другу флаги TCP пакета: SYN и FIN. Данная комбинация флагов используется во многих атакующих программах для обхода фильтров и мониторов, проверяющих только установку одиночного SYN флага.

Пример сигнатуры атаки, используемой при анализе контента:

- «GET . cgi-bin ./etc/passwd». Наличие данной строки в области данных HTTP-пакета свидетельствует об использовании эксплойтов типа phf, php или aglimpse.

Методы анализа контента имеют еще один существенный недостаток. Они не работают, когда атакующие программы (DDoS, trojans) используют методы шифрования трафика. Например, Back Orifice trojan или Barbwire DDoS осуществляют шифрование команд, передаваемых между клиентом и сервером, (менеджером и агентом), с использованием алгоритма blowfish. Методы выявления такого рода атак ограничиваются анализом заголовков сетевых пакетов.

4.3. Пример анализа подозрительного трафика

Покажем как управление рисками, связанными с сетевыми атаками реализуется на практике. Прежде всего, необходимо установить и настроить какую-нибудь «достойную» систему мониторинга сетевого трафика, например NFR, NetProwler, Tcpdump + Shadow и т.п. (автор предпочитает Snort). После этого можно приступать к анализу подозрительного трафика, событий и разного рода сетевых атак, оценивать риски и управлять ими.

```
17:50:22.499014 eth0 > intruderhost.4265 > myhost.netbios-ssn: S
2828114481:2828114481(0) win 32120 <mss 1460,sackOK,timestamp 17250647
0,nop,wscale 0> (DF) (ttl 64, id 11091)

17:50:22.499428 eth0 < myhost.netbios-ssn > intruderhost.4265: S
1070635944:1070635944(0) ack 2828114482 win 17520 <mss 1460,nop,wscale
0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) (ttl 128, id 33514)

17:50:22.499462 eth0 > intruderhost.4265 > myhost.netbios-ssn: . 1:1(0) ack 1
win 32120 <nop,nop,timestamp 17250647 0> (DF) (ttl 64, id 11093)

17:50:22.500379 eth0 > intruderhost.4265 > myhost.netbios-ssn: P 1:13(12) ack
```

Листинг 1. (Начало)

```
1 win 32120 urg 12 <nop,nop,timestamp 17250647 0>>>> NBT (DF) (ttl 64, id
11095)             4500 0040 2b57 4000 4006 78e4 c0a8 0aae
                   c0a8 0a7e 10a9 008b a891 9a32 3fd0 9ba9
                   8038 7d78 7dcb 000c 0101 080a 0107 3957
                   0000 0000 796f 7520 6172 6520 6465 6164
                    E^@ ^@ @  + W  @^@  @^F  x.. .... ^J..
                   .... ^J ~ ^P.. ^@.. .... .. 2  ?.. ....
                   .. 8  } x  }.. ^@^L ^A^A ^H^J ^A^G  9 W
                   ^@^@ ^@^@  y o u   a r  e   d e a d

17:50:22.500791 eth0 > intruderhost.4265 > myhost.netbios-ssn: F 13:13(0) ack
1 win 32120 <nop,nop,timestamp 17250647 0> (DF) (ttl 64, id 11097)

17:50:22.500873 eth0 < myhost.netbios-ssn > intruderhost.4265: FP 1:6(5) ack
13 win 17509 <nop,nop,timestamp 6007121 17250647>>>> NBT (DF) (ttl 128, id
33517)
                   4500 0039 82ed 4000 8006 e154 c0a8 0a7e
                   c0a8 0aae 008b 10a9 3fd0 9ba9 a891 9a3e
                   8019 4465 7642 0000 0101 080a 005b a951
                   0107 3957 8300 0001 8f

                    E^@ ^@ 9 ....  @^@ ..^F .. T .... ^J ~
                   .... ^J.. ^@.. ^P..  ?.. .... .... .. >
                   ..^Y  D e  v B ^@^@ ^A^A ^H^J ^@ [ .. Q
                   ^A^G  9 W ..^@ ^@^A
                   ..

17:50:22.500920 eth0 > intruderhost.4265 > myhost.netbios-ssn: . 14:14(0) ack
7 win 32120 <nop,nop,timestamp 17250647 6007121> (DF) (ttl 64, id 11098)

17:50:22.501139 eth0 < myhost.netbios-ssn > intruderhost.4265: . 7:7(0) ack 14
win 17509 <nop,nop,timestamp 6007121 17250647> (DF) (ttl 128, id 33518)

17:50:22.516930 eth0 > intruderhost.4265 > myhost.netbios-ssn: R 14:14(0) ack
7 win 32120 <nop,nop,timestamp 17250647 6007121> (DF) (ttl 64, id 11111)

17:50:32.508044 eth0 > intruderhost.www > myhost.www: .
2493876034:2493876034(0) ack 749177432 win 8 (ttl 64, id 16912)
17:50:32.508096 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)

17:50:32.508179 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)
17:50:32.508262 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)

17:50:32.508344 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)
17:50:32.508514 eth0 < myhost.www > intruderhost.www: R 749177432:749177432(0)
win 0 (ttl 128, id 33778)

17:50:32.508672 eth0 < myhost.www > intruderhost.www: R 749177432:749177432(0)
win 0 (ttl 128, id 33779)
17:50:32.508739 eth0 < myhost.www > intruderhost.www: R 749177432:749177432(0)
win 0 (ttl 128, id 33780)

17:50:32.508821 eth0 < myhost.www > intruderhost.www: R 749177432:749177432(0)
win 0 (ttl 128, id 33781)
17:50:32.508902 eth0 < myhost.www > intruderhost.www: R 749177432:749177432(0)
win 0 (ttl 128, id 33782)
```

Листинг 1. (Продолжение)

В качестве примера подозрительного трафика, заслуживающего внимания эксперта, рассмотрим следующий фрагмент журнала регистрации событий программы Tcpdump – Листинг 1.

По результатам многолетней практики, была сформирована методика анализа фрагментов подозрительного трафика и определен формат представления данных. Данный формат используется при выполнении практических работ при сдаче экзамена на степень GCIA (GIAC Intrusion Analyst) в SANS/GIAC.

Источник данных:
Тестовая ЛВС

IDS, сгенерировавшая сообщение об атаке:
Tcpdump v. 3.6.2

Формат данных сообщения:
Tcpdump использует следующий формат для отображения TCP пакетов:
time (hh:mm:ss.microseconds)
network interface name [eth0 in our case]
source IP address **.** source port **>** destination IP address **.** destination port **:**
TCP flags [«**.**» – indicates that all the flag bits set to 0, «**P**» – PUSH flag, «**F**» – FIN flag, «**S**» – SYN flag , «**R**» – RESET flag]
beginning sequence number:ending sequence number(data bytes transfered)
ack the sequence number of the next block of data expected from the other end of the TCP connection
win the number of bytes free in the receive buffer for receipt of data from the other end of the TCP connection
<nop,nop,timestamp 6007121 17250647> – tcp options:
nop – no operation [pad options to 4-byte boundaries]
timestamp – carries a timestamp for each segment
(DF) don't fragment flag set
(ttl time to live value **, id** IP identifier **)**

Вероятность подделки IP-адреса отправителя атакующей стороной:
В данном случае между сторонами был установлен сеанс связи, поэтому вероятность подделки IP-адреса невелика. Однако, нельзя исключать возможность внедрения атакующего в сеанс связи (session hijacking) (в случае взаимодействия между Windows системами, предсказание номера TCP-пакета является тривиальной задачей). Для осуществления данного вида атаки атакующий хост должен быть подключен к линии связи между взаимодействующими сторонами («man-in-the-middle» position).

Описание атаки:
Данный фрагмет трафика является примером осуществления атаки на отказ в облуживании против Windows 95/NT out of band (OOB) data denial of service через порт NetBIOS, известной под названием WinNuke (CVE-1999-0153).

Атака осуществляется путем отправки out-of-band data на 139 порт атакуемого хоста, что может привести к «зависанию» Windows системы. Другие ОС также могут оказаться уязвимыми по отношению к данному виду атаки, например, SCO OpenServer 5.0 также подвержен этой атаке.

Ожидаемый результат осуществления данного вида DoS-атаки – «зависание» атакуемой системы.

Механизм осуществления атаки:
Программу, реализующую данный вид атаки, можно найти в Интернет. Когда Windows система получает пакет с установленным флагом «URGENT», она ожидает, что за этим флагом последуют данные. Отсутствие данных после флага URG приводит ее в замешательство. Эта особенность Windows систем (на которых неустановлены соответствующие программные коррекции) используется для осуществления DoS-атаки Winnuke. Сервис Netbios (TCP порт 139) известен в качестве наиболее подверженного данной уязвимости и чаще всего атакуемого. Однако потенциально существует возможность успешного осуществления данного вида атаки с использованием и других портов.

Данная атака может применяться как удаленно, так и локально (т. е. с той же машины, на которой запускается программа Winnuke).

Windows NT: Успешное осуществление данной атаки против Windows NT системы приводит к ее зависанию и появлению «синиго экрана смерти». Последствия атаки обычно заключаются в потере пользователем несохраненных документов (изменений).

Windows 95, Windows for Workgroups 3.11: В случае успешного осуществления данной атаки против Windows for Workgroups или Windows 95 систем на экране появляется сооб-

щение о программной ошибке — «синий экран», сообщающий пользователю о том, что приложение не отвечает. Последствия атаки обычно заключаются в потере пользователем несохраненных документов (изменений).

Ссылки на источники информации об атаке/уязвимости:

Описание атаки Winnuke можно найти по следующим ссылкам:
http://support.microsoft.com/support/kb/articles/q179/1/29.asp
http://ciac.llnl.gov/ciac/bulletins/h-57.shtml
ftp://ftp.sco.com/SSE/security_bulletins/SB.98:01a

Цели атаки и мотивация атакующей стороны (Адресность и целенаправленность атаки):

На вопрос о целях и мотивации атакующей стороны существует два возможных ответа:

1) Эта атака является адресной и направлена против конкретной системы, содержащей соответствующую уязвимость.
2) Это сканирование сети в поисках систем, содержащих данную уязвимость.

Для ответа на этот вопрос необходимо дополнительное изучение журналов регистрации событий на МЭ и IDS, для выяснения предистории данного события.

Величина риска:

Величина риска (**Severity)**, ассоциированного с этим событием, рассчитывается по формуле:

(CRITICALITY + LETHALITY) − (SYSTEM COUNTERMEASURES + NETWORK COUNTERMEASURES) = SEVERITY

Оцениваем критичность атакуемого хоста:
Criticality: 2 (Windows 2000 хост)

Оцениваем возможные последствия:
Lethality: 0 (Win2000 хосты не подвержены данной уязвимости, следовательно последствия отсутствуют)

Оцениваем эффективность контрмер системного уровня:
Sys Counters: 5 (Установлены последние программные коррекции)
Оцениваем эффективность контрмер сетевого уровня:
Net Counters: 5 (Атакуемый хост расположен за фильтрующим маршрутизатором и МЭ во внутренней сети)

Severity: (2 + 1) − (5 + 5) = -7

Таким образом, уровень риска в данном случае существенно меньше 0 (событие, не заслуживающее серьезного внимания эксперта).

Рекомендации по защите:

Поскольку величина риска очень мала, в данном случае, о защите вообще можно не беспокоиться. Однако, в общем случае, можно дать следующие рекомендации по защите:

1) Лучшим способом защиты от подобного рода атак со стороны внешней сети традиционно является использование МЭ. Блокирование сервиса Netbios на МЭ и маршрутизаторе, выполняющих функции внешнего шлюза корпоративной сети является обычной практикой.
2) Периодическое сканирование сети при помощи сканера, является хорошей профилактической мерой против подобного рода атак (конечно, если базы данных уязвимостей сканера регулярно обновляются).
3) Если результаты сканирования сети выявили Windows системы, уязвимые по отношению к данному виду атаки, то на них необходимо установить пакет программных коррекций от Microsoft (SP4 или более старшая версия), который можно загрузить по следующему адресу:
http://support.microsoft.com/support/ntserver/content/servicepacks/

5. IDS как средство управления рисками

5.1. Типовая архитектура системы выявления атак

Типовая архитектура системы выявления атак, как правило, включает в себя следующие компоненты:

1. Сенсор (средство сбора информации);
2. Анализатор (средство анализа информации);

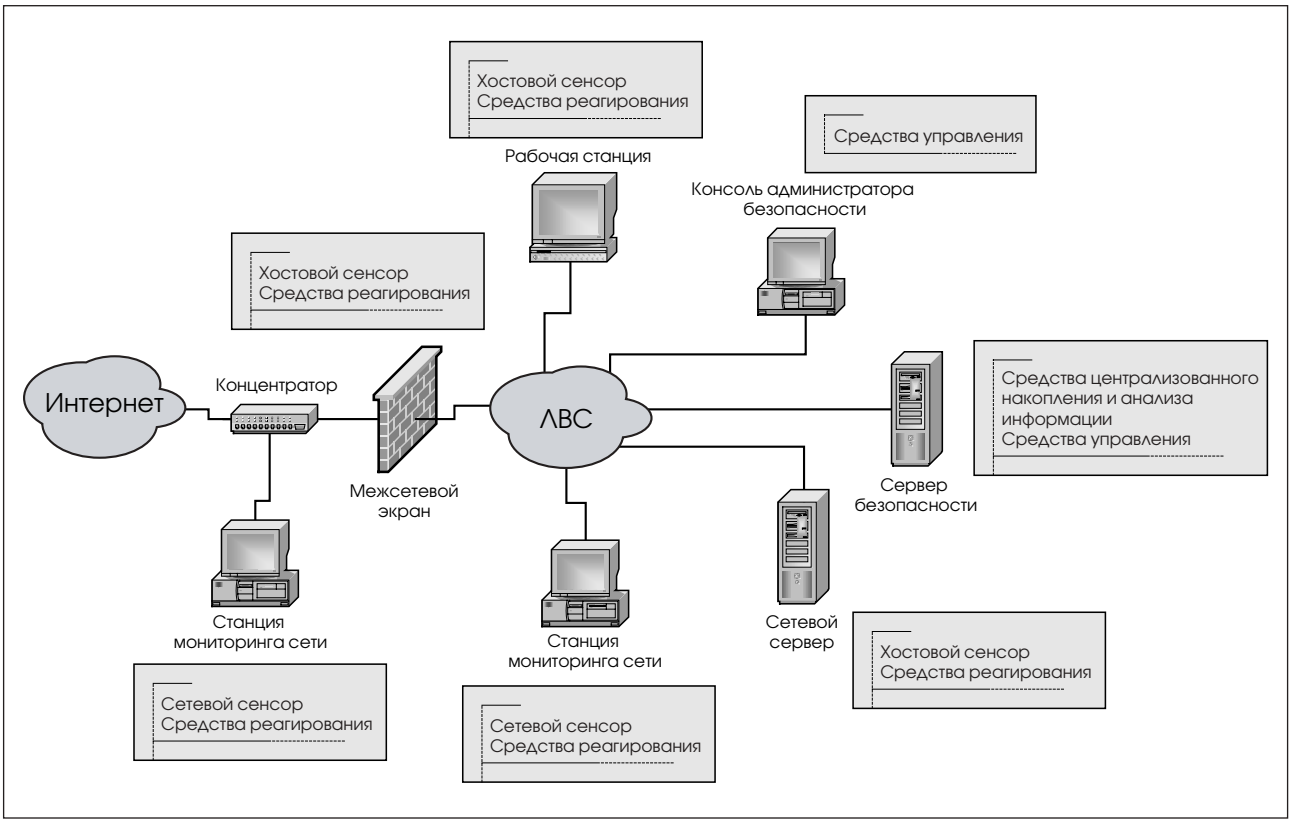


Рис. 1. Типовая архитектура системы выявления атак

3. Средства реагирования;
4. Средства управления.

Конечно, все эти компоненты могут функционировать и на одном компьютере и даже в рамках одного приложения, однако чаще всего они территориально и функционально распределены. Такие компоненты IDS, как анализаторы и средства управления, опасно размещать за МЭ во внешней сети, т. к. если они будут скомпрометированы, то злоумышленник может получить доступ к информации о структуре внутренней защищаемой сети на основе анализа базы правил, используемой IDS.

Типовая архитектура системы выявления атак изображена на рисунке 1. Сетевые сенсоры осуществляют перехват сетевого трафика, хостовые сенсоры используют в качестве источников информации журналы регистрации событий ОС, СУБД и приложений. Информация о событиях также может быть получена хостовым сенсором непосредственно от ядра ОС, МЭ или приложения.

Анализатор, размещаемый на сервере безопасности, осуществляет централизованный сбор и анализ информации, полученной от сенсоров.

Средства реагирования могут размещаться на станциях мониторинга сети, МЭ, серверах и рабочих станциях ЛВС. Типичный набор действий по реагированию на атаки включает в себя оповещение администратора безопасности (средствами электронной почты, вывода сообщения на консоль или отправки на пэйджер), блокирование сетевых сессий и пользовательских регистрационных записей с целью немедленного прекращения атак, а также протоколирование действий атакующей стороны.

Средства управления предназначены для администрирования всех компонентов системы выявления атак, разработки алгоритмов выявления и реагирования на нарушения безопасности (политик безопасности), а также для просмотра информации о нарушениях и генерации отчетов.

5.2. Стандарты, определяющие правила взаимодействия между компонентами системы выявления атак

Необходимость стандартизации форматов данных и протоколов обмена данными, используемых в IDS, обусловлена ниже перечисленными причинами.

1. Для защиты ЛВС, подключенных к сети Интернет, от распределенных скоординированных атак необходимо обеспечить определенную степень взаимодействия между IDS, используемыми для защиты различных точек входа в различные ЛВС. Например, в случае осуществления атаки против одной ЛВС, правила реагирования, на которую предусматривают изменение конфигурации МЭ путем блокирования IP-адреса источника атаки, соответствующие изменения должны быть произведены на всех МЭ, используемых для защиты всех остальных ЛВС. Для этого между различными IDS должен осуществляться обмен информацией об источнике атаки и способе реагирования.

2. Центральным компонентом IDS является специализированное программное ядро (analysis engine) — анализатор, предназначенное для анализа данных, поступающих от сенсоров, и принятия решений о способах реагирования на подозрительные события. Стандартизация протоколов и форматов обмена данными между анализатором с одной стороны и сенсорами и средствами реагирования с другой, позволяет применять общее программное ядро анализатора с различными типами сенсоров и средств реагирования.

Процесс стандартизации протоколов и форматов обмена данными, используемых в IDS, начался уже довольно давно. Рассмотрим несколько популярных форматов данных, используемых в Интернет «Центрами реагирования» для обмена информацией о нарушениях безопасности.

Форматы обмена данными

AusCERT (portmap probe)

Source: 210.177.64.1
Ports: tcp 111
Incident type: network scan
re-distribute: yes
timezone: GMT + 1300
reply: no
Date: 30th Jan 2000 at 22:01 (UTC)

Система AusCERT используется для сбора и анализа статистической информации об атаках. Данный формат записи применяется для автоматического добавления данных об атаках в базу данных AusCERT.

Списки Грифина (Griffin list)

«Списки Грифина» используются в казино для идентификации карточных шулеров. Файлы с фотографиями известных шулеров сравниваются с изображением, полученным и с видеокамеры. В качестве идентифицирующих признаков используются черты лица, не подверженные изменению с течением времени.

«Списки Грифина», используемые в системах выявления атак содержат сетевые адреса компьютеров, с которых наиболее часто осуществляются подозрительные действия. Интернет-центры по реагированию на компьютерные инциденты, такие как CERT или GIAC, занимаются формированием таких списков и предоставлением доступа к ним для широкой общественности (www.incidents.org). Эти данные могут использоваться в IDS. При анализе подозрительного трафика особое внимание должно, прежде всего, уделяться скомпроментировавшим себя IP-адресам.

CVE – тезаурус уязвимостей

CVE (Common Vulnerabilities and Exposures) — это единый тезаурус всех известных уязвимостей, определяющий единые правила их именования, доступ к которому через сеть Интернет открыт для всех заинтересованных лиц (cve.mitre.org). CVE не является классификацией уязвимостей и не претендует на их систематизацию. Вот краткая история его возникновения.

Дэвид Манн (David Mann) и Стивен Кристи (Steven Christey) из американской корпорации MITRE работали над созданием базы данных уязвимостей. Необходимо было установить соответствие между уязвимостями, обнаруживаемыми при помощи различных видов сканеров защищенности, предупреждающими сообщениями и рекомендациями по устранению этих уязвимостей. Здесь они столкнулись с проблемой именования уязвимостей. Например, известная уязвимость CGI phf позволяет осуществлять удаленное выполнение команд с использованием метасимволов командного интерпретатора SHELL. Классический пример использования этой уязвимости для получения файла с паролями путем выполнения команды 'cat /etc/passwd'. В сообщениях CERIAS эта уязвимость называется httpd_escshellcmd, а в сообщениях CERT она обозначается как CA-96-06.CGI_Example_code и т. п. В различных сетевых сканерах, например в Internet Scanner и CyberCop Scanner также используются разные способы именования уязвимостей.

Изучение проблемы классификации уязвимостей информационных ресурсов вывело Девида Манна и Стивена Кристи на работы, про-

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IDMEF-Message PUBLIC "-//IETF//DTD RFCxxxx IDMEF v0.5//EN"
  "idmef-message.dtd">

<IDMEF-Message version="0.5">
  <Alert ident="abc123456789">
    <Analyzer analyzerid="bc-sensor01">
      <Node category="dns">
        <name>sensor.bigcompany.com</name>
      </Node>
    </Analyzer>
    <CreateTime ntpstamp="0xbc71f4f5.0xef449129">
      2000-03-09T10:01:25.93464Z
    </CreateTime>
    <Source ident="a1a2" spoofed="yes">
      <Node ident="a1a2-1">
        <Address ident="a1a2-2" category="ipv4-addr">
          <address>222.121.111.112</address>
        </Address>
      </Node>
    </Source>
    <Target ident="b3b4">
      <Node>
        <Address ident="b3b4-1" category="ipv4-addr">
          <address>123.234.231.121</address>
        </Address>
      </Node>
    </Target>
    <Target ident="c5c6">
      <Node ident="c5c6-1" category="nisplus">
        <name>lollipop</name>
      </Node>
    </Target>
    <Target ident="d7d8">
      <Node ident="d7d8-1">
        <location>Cabinet B10</location>
        <name>Cisco.router.b10</name>
      </Node>
    </Target>
    <Classification origin="cve">
      <name>CVE-1999-128</name>
      <url>http://www.cve.mitre.org/</url>
    </Classification>
  </Alert>
</IDMEF-Message>
```

Листинг 2.

водимые в CERIAS, в рамках которых была разработана концепция единообразного именования уязвимостей. Эта концепция была сформулированна в отчете «Towards a Shareable Vulnerability Database», представленном на конференции, проводимой CERIAS в 1999 г. «CERIAS Workshop for Vulnerability Databases».

CVE существенно упрощает задачу сравнения между собой возможностей различных сетевых сканеров. Для CVE-совместимых сканеров достаточно сопоставить между собой списки обнаруживаемых уязвимостей. Если же сканеры используют для именования уязвимостей разные системы обозначений, то задача их сравнения становится сильно нетривиальной.

В настоящее время большинство разработчиков сетевых сканеров и других средств контроля защищенности, включая Symantec, NAI, ISS, Cisco и др., заявили о поддержке CVE,

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE IDMEF-Message PUBLIC "-//IETF//DTD RFCxxxx IDMEF v0.5//EN"
  "idmef-message.dtd">

<IDMEF-Message version="0.5">
  <Alert ident="abc123456789">
    <Analyzer analyzerid="hq-dmz-analyzer62">
      <Node category="dns">
        <location>Headquarters Web Server</location>
        <name>analyzer62.bigcompany.com</name>
      </Node>
    </Analyzer>
    <CreateTime ntpstamp="0xbc72b2b4.0x00000000">
      2000-03-09T15:31:00-08:00
    </CreateTime>
    <Source ident="abc01">
      <Node ident="abc01-01">
        <Address ident="abc01-02" category="ipv4-addr">
          <address>222.121.111.112</address>
        </Address>
      </Node>
    </Source>
    <Target ident="def01">
      <Node ident="def01-01" category="dns">
        <name>www.bigcompany.com</name>
        <Address ident="def01-02" category="ipv4-addr">
          <address>123.234.231.121</address>
        </Address>
      </Node>
      <Service ident="def01-03">
        <portlist>5-25,37,42,43,53,69-119,123-514</portlist>
      </Service>
    </Target>
```

Листинг 3.

в качестве стандартного способа именования уязвимостей в своих продуктах.

CIDF (Common Intrusion Detection Framework)

Единая архитектура систем выявления атак CIDF является инициативой, в рамках которой осуществляется разработка сетевых протоколов и интерфейсов прикладного программирования, предназначенных для взаимодействия между собой компонентов IDS.

CIDF определяет следующее:

- модель данных для представления информации об атаках, уязвимостях, событиях и способах реагирования на события;
- модель взаимодействия компонентов IDS;
- протоколы и интерфейсы взаимодействия компонентов IDS.

В модели CIDF атаки и уязвимости описываются при помощи S-выражений. Для того чтобы понять, что это такое, не углубляясь в теорию, приведем пример S-выражения, описывающего событие, связанное с удалением файла:

```
(Delete
   (Context
      (HostName      'first.example.com')
      (Time    '16:40:32 Jun 14 1998')
   )
   (Initiator
      (UserName      'lp')
   )
   (Source
      (FileName      '/etc/passwd')
   )
)
```

Данное S-выражение описывает событие, заключающееся в том, что пользователь **lp** в **16:40:32 14 июня 1998 г.** удалил файл **/etc/passwd** на компьютере **first.example.com**.

В настоящее время статус CIDF не определен, однако он остается концептуальной основой для разработки стандартов в области ID и возможно будет взят за основу при разработке стандартов IDWG.

IDWG (Intrusion Detection Working Group)

IDWG является рабочей группой IETF, созданной для разработки Интернет стандартов, в области выявления атак. IDWG решает задачу определения общих форматов данных и протоколов для взаимодействия и обмена информацией между различными компонентами IDS.

При создании рабочей группы IDWG перед ее участниками были поставлены следующие задачи:

1. Обоснованый выбор функциональных требований высокого уровня, определяющих правила взаимодействия между системами выявления атак, а также между IDS и средствами сетевого управления.
2. Спецификация единого языка взаимодействия IDS, отвечающего этим требованиям и определяющего форматы обмена данными между IDS.
3. Разработка документа, описывающего существующие протоколы взаимодействия между IDS, и возможность использования в этих протоколах единого формата обмена данными.

К настоящему времени силами рабочей группы IETF IDWG уже закончена разработка основных стандартов Интернет на форматы и протоколы обмена данными между IDS.

Существующие проекты стандартов сети Интернет, разработанные IDWG:

1. Intrusion Detection Message Exchange Format Extensible Markup Language (XML) Document Type Definition
2. The TUNNEL Profile
3. The Intrusion Detection Exchange Protocol (IDXP)

IDMEF (Intrusion Detection Message Exchange Format) – формат обмена данными между компонентами IDS. Он используется для передачи предупреждающих сообщений о подозрительных событиях между системами выявления атак. Данный формат должен обеспечить совместимость между коммерческими и свободно распространяемыми IDS и возможность их совместного использования для обеспечения наивысшего уровня защищенности.

Модель данных IDMEF описывается в виде XML DTD.

Сообщение сетевого сенсора/анализатора об атаке **«ping of death»** приведено на листинге. Имеется несколько объектов атаки. IP-адрес атакующего подделан (Листинг 2).

Сообщение сетевого сенсора/анализатора о сканировании портов, представленное в формате IDMEF, (элемент языка разметки <portlist> обозначает номера сканируемых портов) (Листинг 3).

IAP (Intrusion Alert Protocol) – протокол прикладного уровня, предназначенный для обмена сообщениями от атаках (alerts) между компонентами системы выявления атак: сенсорами/анализаторами (S) и менеджерами (M), между которыми могут также находится прокси-сервисы (P) и шлюзы (G). Протокол не зависит от формата представления данных.

6. Примеры коммерческих IDS

6.1. Средства защиты информации компании Symantec

Компания Symantec является в настоящее время крупнейшим разработчиком программных средств защиты информации и наряду с NAI, Cisco и CheckPoint занимает лидирующее положение на рынке. Разрабатываемые компанией Symantec программные продукты позволяют строить систему защиты корпоративной сети на базе интегрированных между собой инструментальных средств одного разработчика. Программные средства защиты информации от Symantec, ориентированные на корпоративных клиентов, включают в себя, следующие классы программных продуктов:

- средства контроля защищенности (ESM, NetRecon);
- системы выявления атак (Intruder Alert, NetProwler);

- межсетевые экраны (Desktop Firewall, Enterprise Firewall);
- средства шифрования и аутентификации (Defender, WebDefender, Security Briefcase),
- средства VPN (PowerVPN),
- средства управления доступом и корпоративными ресурсами (Enterprise Resource Manager, Privilege Manager for UNIX, Resource Manager for UNIX),
- средства анализа контекста (I-Gear, Mail-Gear);
- антивирусные средства (NAV Enterprise Edition, NAV for Firewall, NAV for Gateways).

Продукты компании Symantec позволяют создавать комплексные системы выявления атак для защиты корпоративных сетей любого уровня сложности. Не претендуя на исчерпывающее описание функциональных возможностей, рассмотрим программные продукты Symantec Intruder Alert и Symantec NetProwler в качестве примера современных коммерческих IDS.

6.2. Хостовая система выявления атак Intruder Alert

Назначение и основные возможности

Программный продукт Symantec Intruder Alert (ITA) является достойным представителем класса IDS системного уровня (host-based), построенных на технологии интеллектуальных программных агентов. Выявление локальных и удаленных атак осуществляется путем анализа журналов регистрации событий системного и прикладного ПО. Отличительными чертами этой системы являются гибкость, масштабируемость и простота администрирования. ITA может быть легко интегрирован практически с любыми типами приложений.

Выявление атак и реагирование на них осуществляется в реальном времени, при этом предусмотрено 14 вариантов действий по автоматическому реагированию на атаки.

Значительное количество предопределенных политик безопасности сочетается с возможностью создания собственных политик без программирования.

В составе ITA имеются программные агенты для 35 различных программно-аппаратных платформ, включая различные версии ОС UNIX, Windows и NetWare. По широте охвата платформ продукт не имеет себе равных.

Архитектура Intruder Alert и описание основных компонентов

ITA построен на распределенной трехкомпонентной архитектуре Агент/Менеджер/Консоль. Все компоненты ITA взаимодействуют между собой по защищенному клиент-серверному протоколу. Аутентификация между компонентами и выработка сеансовых ключей осуществляется по алгоритму Диффи-Хелмана. Защита сеанса связи осуществляется путем использования алгоритма шифрования с 400-битными ключами.

Средства управления ITA представлены двумя графическими приложениями: ITA Admin и ITA View.

Приложение ITA Admin предназначено для управления компонентами системы, создания и настройки политик безопасности, определяющих правила выявления и реагирования на подозрительную активность. При помощи приложения ITA Admin администратор безопасности может осуществлять следующий набор действий по администрированию системы выявления атак:

- объединять агентов в домены;
- создавать политики безопасности и применять их на контролируемых доменах;
- загружать новые политики безопасности с Web-сервера компании Symantec;
- экспортировать политики безопасности в файлы экспорта;
- настраивать параметры программных агентов;
- подключать дополнительные источники данных для анализа программными агентами;
- определять привилегии пользователей ITA и осуществлять распределение административных ролей по управлению системой выявления атак.

ITA View является средством просмотра регистрационной информации об атаках и других подозрительных событиях, зарегистрированных агентами ITA согласно установленным правилам политики безопасности. Данное средство позволяет выполнять запросы к базе данных ITA, содержащей консолидированные данные обо всех контролируемых системах, а также, на основании результатов запроса, формировать отчеты, представленные в различных графических форматах.

Центральным компонентом системы выявления атак является ITA Manager. Он осуществляет управление, подключаемыми к нему агентами, получая от них информацию о состоя-

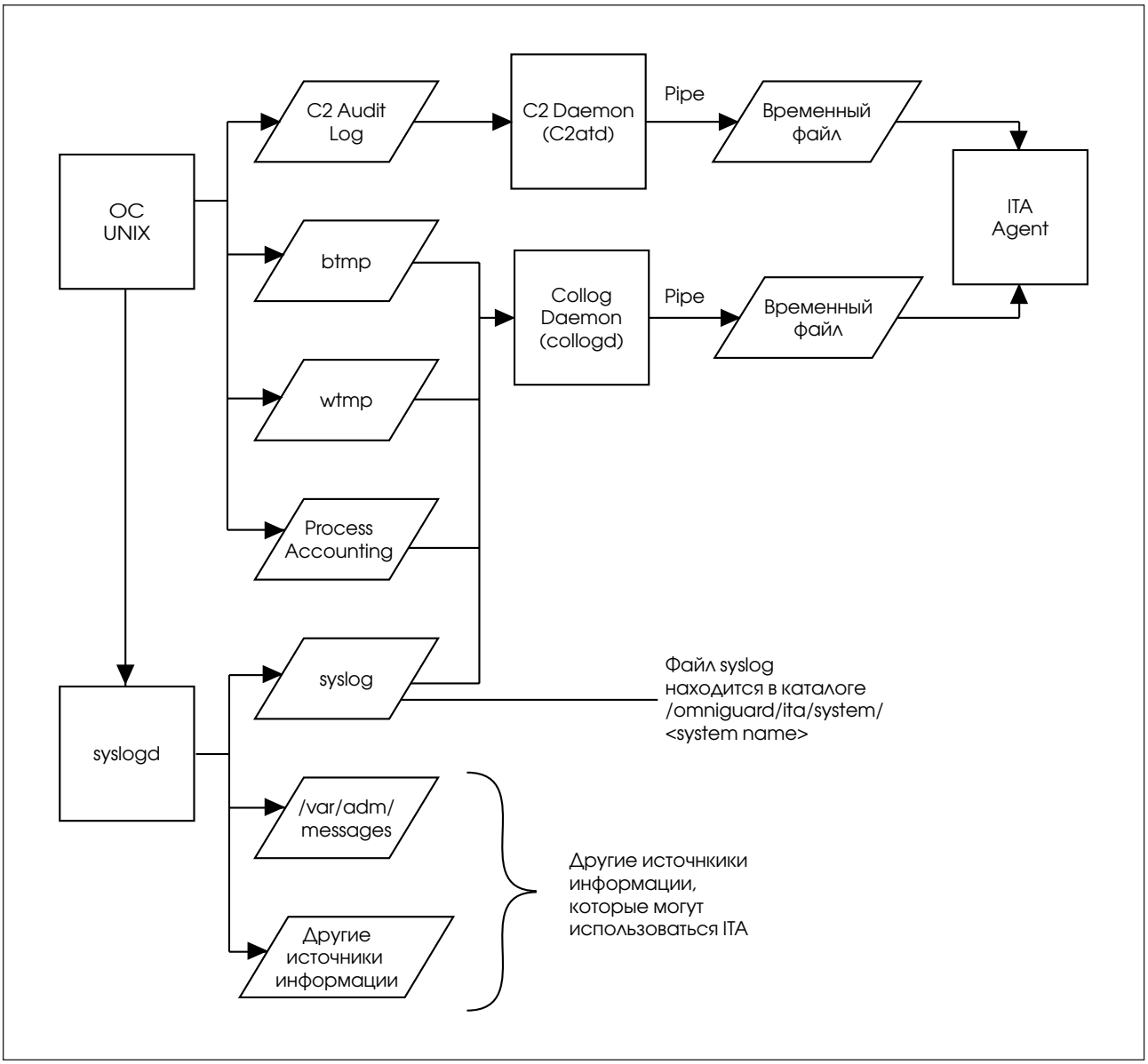


Рис. 2. Источники информации о событиях для ITA в ОС UNIX

нии контролируемых объектов, поддерживает список доменов и активизированных на них политик безопасности и управляет базой данных безопасности. База данных безопасности содержит консолидированные данные о нарушениях безопасности, происходящих на контролируемых объектах.

В ОС UNIX ITA Manager реализован в виде демона. Он представляет собой службу в ОС Windows NT и NLM-модуль в ОС NetWare.

ITA Agent является «рабочей лошадкой» системы выявления атак, выполняющей одновременно функции сенсора, анализатора и средства реагирования на атаки. Он осуществляет сбор и анализ данных аудита безопасности из различных источников с использованием сигнатур атак, задаваемых правилами политик безопасности ITA. В случае выявления в составе исходных данных сигнатуры атаки предпринимается набор действий, предписываемый соответствующим правилом.

Выявление и реагирование на атаки осуществляется в реальном масштабе времени по специальным алгоритмам (в терминологии ITA — политики безопасности). В среде ОС UNIX агенты реализованы в виде демонов, в ОС Windows NT — в виде служб, а в NetWare представляют собой NLM-модули. Для каждой поддерживаемой ОС используются собственные источники информации аудита. В системах UNIX и Windows NT реги-

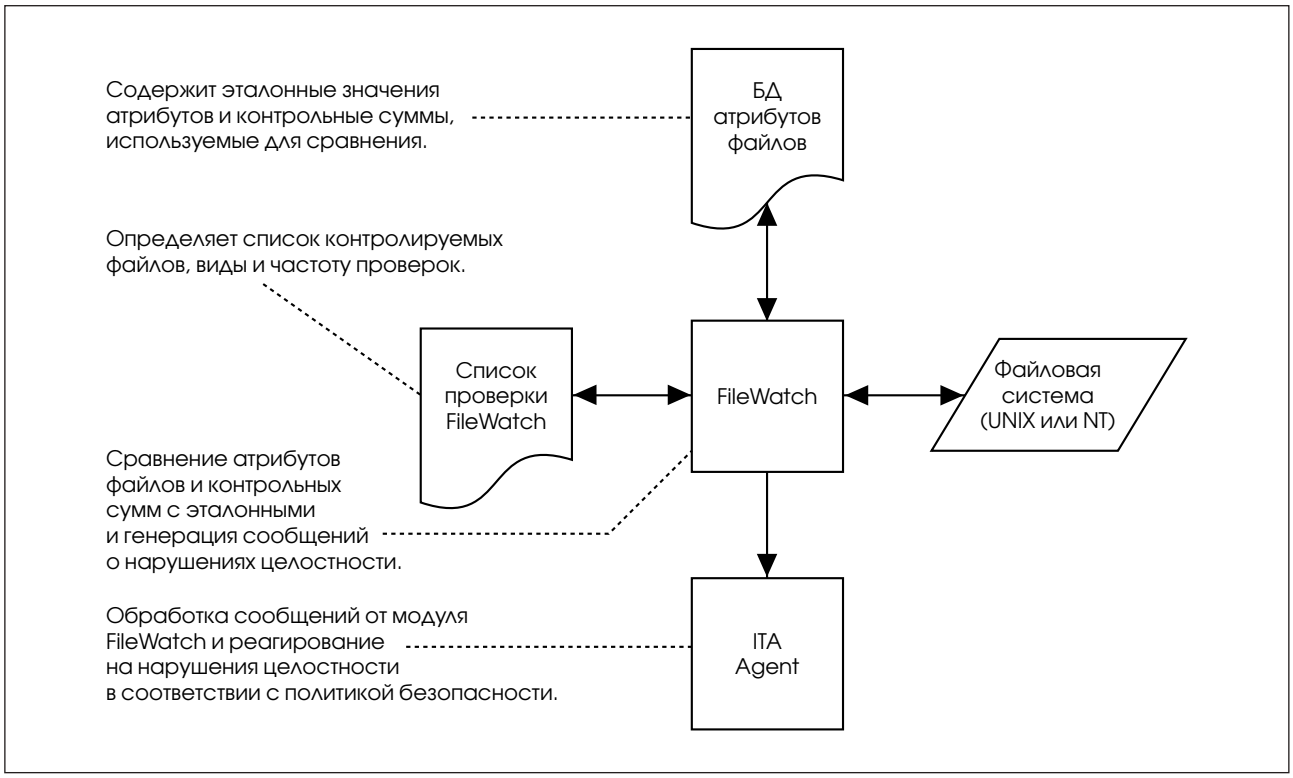


Рис. 3. Контроль целостности системных файлов при помощи модуля FileWatch

страция событий, связанных с безопасностью, осуществляется при помощи стандартных средств регистрации системных событий и средств аудита безопасности (syslog, wtmp, process accounting, btmp, подсистема C2 и т. п. в ОС UNIX и системный журнал, журнал приложений и журнал безопасности в ОС Windows NT). Сенсорные модули ITA Agent с определенной периодичностью сканируют файлы системных журналов и журналов аудита, осуществляют чтение данных аудита и их преобразование в свой внутренний формат. В NetWare сенсорные модули ITA Agent самостоятельно регистрируют и обрабатывают данные о событиях, получая эту информацию непосредственно от ядра ОС.

Процесс сбора информации о состоянии системы в среде UNIX проиллюстрирован на рис. 2. Intruder Alert автоматически осуществляет мониторинг следующих источников информации:

- файла syslog, содержащего данные от ядра ОС и приложений, регистрация которых осуществляется через систему syslog;
- файла wtmp, содержащего информацию о пользователях, зарегистрировавшихся в системе и запущенных ими процессах;
- файла btmp, содержащего информацию обо всех неудачных попытках входа в систему;
- системы учета пользовательских процессов pacct, регистрирующей различную информацию, связанную с их функционированием и использованием системных ресурсов;
- журналов аудита безопасности C2 (использование этого источника возможно после специальной настройки ITA, т. к. подсистема аудита безопасности в различных реализациях UNIX устроена по-разному).

Помимо перечисленных источников информации, представляющих из себя файлы, данные в которых хранятся в двоичном формате, возможно подключение дополнительных источников информации, использующих текстовый формат хранения данных, например файла /var/adm/messages и любых других текстовых файлов журналов регистрации событий ОС и приложений.

Сбор информации из журналов регистрации событий осуществляется демоном collogd, который передает эти данные агенту ITA по программному каналу. Сбор данных от подсистемы аудита безопасности C2 осуществляется демоном C2atd, который преобразует эти данные во внутренний формат ITA и передает их агенту. По-умолчанию сканирование источников информации осуществляется с интервалом в одну секунду.

Использование программного модуля FileWatch для контроля целостности системных файлов

Сценарий осуществления многих атак предполагает подмену важных системных файлов «троянскими программами», заражение программ вирусами, либо модификацию системных конфигурационных файлов с целью создания «черного входа» в систему. Для контроля целостности программной и информационной частей на контролируемых системах, в составе ITA имеется специальный модуль под названием FileWatch, способный обнаруживать нарушения целостности, связанные с добавлением, удалением и модификацией файлов и каталогов. Выявление нарушений целостности производиться путем сравнения атрибутов этих файлов и каталогов с эталонными значениями. Контроль изменения содержимого файлов производится по контрольным суммам. Вычисление контрольных сумм файлов может осуществляться по различным алгоритмам, включая использование хэш-функции MD5.

Принцип функционирования модуля FileWatch проиллюстрирован на рис. 3. Создаваемый пользователем «FileWatch List» определяет список контролируемых файлов, виды используемых проверок и их периодичность. База данных атрибутов файлов (File Attribute Database), создается модулем FileWatch и содержит эталонные значения атрибутов файлов и контрольные суммы, используемые для контроля целостности. Сообщения о результатах проверок, выполняемых модулем FileWatch, передаются агенту ITA, который обрабатывает их в соответствии с заданной политикой безопасности. Для того, чтобы агент ITA мог воспринимать, обрабатывать и осуществлять реагирование на сообщения FileWatch, на нем должна быть активизирована специальная политика безопасности (UNX Critical Files — для UNIX и NT Critical Files — для Windows NT).

Политики безопасности Intruder Alert

Политика безопасности Intruder Alert выражается набором правил. Правила представляют собой логические выражения, построенные на предикатах первого порядка. Предикаты используются для определения условий возникновения отслеживаемых ситуаций, а логические выражения определяют способы реагирования в зависимости от истинности или ложности предикатов.

Правила политики безопасности

Правило политики безопасности представляет собой импликацию трех логических высказываний: Предиката SELECT, предиката IGNOR и логического высказывания ACTION. Предикат SELECT определяет условия возникновения отслеживаемой ситуации, предикат IGNOR определяет исключения из этих условий, а логическое высказывание ACTION предписывает выполнение одного из 14 действий по реагированию на возникшую ситуацию.

На языке алгебры логики правило политики безопасности определяется тождеством:

$$\mathbf{ACTION = SELECT \rightarrow \overline{IGNOR}}$$

Таблица истинности данной логической фукнции выглядит следующим образом:

SELECT	IGNOR	ACTION
True	False	True
True	True	False
False	False	False
False	True	False

Таблица 1. Таблица истинности логической функции ACTION

Истинность высказывания ACTION означает необходимость выполнения действий, предписываемых этим высказыванием. Высказывание ACTION может быть простым или составным, во втором случае оно может состоять из нескольких высказываний, разделенных операцией /\ (логическое «И»).

ACTION = Действие1 /\ Действие2 /\ ... Действие N, N = { 1,14.}

В Табл. 2 описаны способы реагирования на попытки НСД, поддерживаемые ITA.

Действие	Описание
Append To File	Присоединить регистрационную запись, содержащую данные о событии в конец указанного файла.
Send E-mail	Послать сообщение, содержащее данные о событии, указанному пользователю или группе пользователей.
Notify	Вывести сообщение о событии на консоль пользователю или группе пользователей.
Pager action	Послать сообщение на пэйджер указанным пользователям по модему.
Kill process	Завершение процесса, явившегося причиной происшедшего события в UNIX системе. В Windows NT завершаются все процессы пользователя, чьи действия привели к возникновению события. В NetWare данная функция не поддерживается.
Disconnect session	Завершить все процессы, имеющие одинаковые идентификаторы пользователя и сеанса с процессом, вызвавшим событие.
Raise Flag	Установить флаг в сигнальное состояние на определенный период времени. (Используется для отслеживания последовательности событий).
Cancel Flag	Установить флаг в несигнальное состояние.
Start Timer	Установить значение таймера на определенный промежуток времени.
Cancel Timer	Сбросить значение таймера.
Execute Command	Выполнить команду операционной системы, файл сценария или исполняемый файл.
Record To ITA View	Поместить запись с данными о событии в базу данных безопасности менеджера ITA.
Disable User Account	Заблокировать регистрационную запись пользователя.
Run Shared Actions	Выполнить действие, определяемое другим правилом политики безопасности, активизированной на агенте ITA.

Таблица 2. Способы реагирования на попытки НСД, поддерживаемые программой ITA

Ранжирование попыток НСД

С целью определения степени критичности тех или иных событий, происходящих в системе, производится ранжирование правил политики безопасности. Каждому правилу присваивается приоритет в диапазоне от 0 до 100. Все события, отслеживаемые правилами политики безопасности, в зависимости от значения их приоритета делятся на три уровня критичности, обозначаемых на диаграммах ITA различными цветами, в соответствии со следующей таблицей:

Приоритет	Уровень критичности	Угроза безопасности
0–33	Зеленый	Некритичные события, не требующие немедленного реагирования.
34–66	Желтый	Критичные события средней важности, требующие реагирования.
67–100	Красный	Критичные события высокой важности, представляющие серьезную угрозу безопасности и требующие немедленного реагирования.

Табл. 3. Уровни приоритетов событий, отслеживаемых программой ITA

Предопределенные политики безопасности

ITA содержит базовый набор предопределенных политик безопасности для каждой из поддерживаемых операционных систем, который устанавливается вместе с продуктом. Часть предопределенных политик безопасности активизируется сразу же после установки ITA. Остальные, прежде чем быть активизированными, требуют дополнительной настройки.

Например, политика ITA Reports генерирует отчеты о работе программного агента при получении им команды report от ITA View (ITA View может использоваться также для управления ITA агентами путем посылки им команд по сети). Политика UNX Failed telnet служит для выявления неудачных попыток удаленной регистрации в системе Solaris 2.5 с использованием сервиса telnet, а политика UNX System Problems выявляет проблемы, возникающие при выполнении системных задач, таких как неудачная операция монтирования тома, истечение времени ожидания ответа на запрос, неверный IP-адрес или MAC-адрес. Для ОС Windows NT политика NT SYN Flood обнаруживает атаки на отказ в обслуживании SYN Flood, а политика NT Guest User Logon регистрирует случаи локального или удаленного входа пользователя с именем «Гость» в систему.

Часть предопределенных политик, прежде чем они могут быть активизированы, требует дополнительной настройки. Среди них, политика APACHE HTTP Start/Stop, обнаруживающая запуск и останов Web-сервера Apache 1.1.1 и политика Cisco Config Change, выявляющая изменение конфигурации маршрутизатора Cisco v11.1.

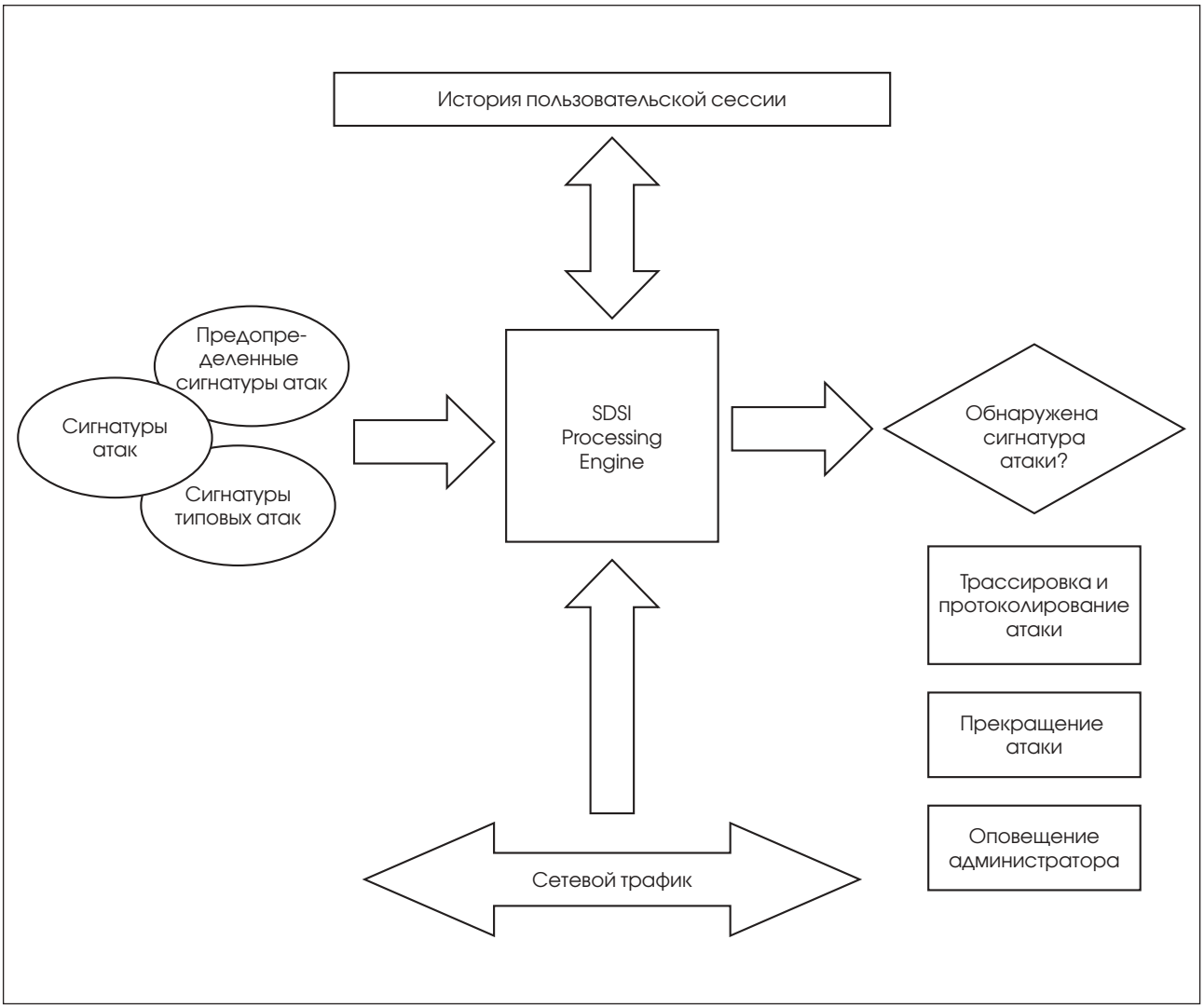


Рис. 4. Принцип функционирования NetProwler

6.3. Сетевая система выявления атак NetProwler

Принципы функционирования и основные возможности

Программный продукт Symantec NetProwler по результатам многочисленных сравнительных испытаний признается одной из лучших на сегодняшний день коммерческих систем выявления сетевых атак. NetProwler является развитием известного в прошлом программного продукта ID-Trak компании Internet Tools. Для выявления сетевых атак NetProwler анализирует заголовки и области данных сетевых пакетов с использованием сигнатур атак. Принцип функционирования системы NetProwler проиллюстрирован на рис. 4.

Анализ пакетов осуществляется в соответствии с запатентованным алгоритмом контекстно-зависимого динамического анализа сигнатур атак (SDSI – Statefull Dynamic Signature Inspection). Название алгоритма отражает его основные свойства. Зависимость от контекста означает, что NetProwler запоминает содержание активных пользовательских сессий, с целью выявления более сложных комплексных видов атак, осуществление которых приводит к генерации определенных последовательностей сетевых пакетов. Создание и активация сигнатур атак производится динамически – без прерывания работы системы, в соответствии с принципом непрерывности защиты во времени. Метод анализа сигнатур атак заключается в сравнении сигнатур атак с содержимым сетевых пакетов. Сигнатура представляет собой последова-

Port Scan	Сканирование сетевых портов используется для сбора информации о доступных на сканируемой системе сетевых сервисах, типах ОС и версиях ПО. На основе этой информации может быть сделан вывод о наличие тех или иных уязвимостей сетевого ресурса. Информация полученная в результате сканирования может использоваться потенциальным злоумышленником для планирования сетевых атак. По умолчанию, NetProwler регистрирует этот вид атаки в случае сканирования 20 портов в течении 60 секунд. Пользователь имеет возможность модифицировать эти настройки.
SYN Flood	Этому виду атаки на отказ в обслуживании подвержены многие системы, работающие по протоколам TCP/IP. Для ее реализации используются особенности процедуры установки TCP- соединения, состоящей из трех последовательных шагов. Сначала клиент посылает на удаленную систему запрос на установление соединения пакет запроса синхронизации (synchronization request SYN). Удаленная система, получив пакет SYN, посылает в ответ пакет подтверждения синхронизации (synchronization acknowledgment packet SYN/ACK) и ожидает подтверждение установки соединения от клиента. Получив пакет SYN/ACK, клиент посылает на удаленную систему пакет подтверждения установки соединения (ACK). При реализации этого вида атаки, атакующий посылает на удаленную систему множество пакетов SYN, обычно с ложными адресами отправителя, инициируя тем самым установление множества TCP-соединений. Удаленная система посылает в ответ пакеты подтверждения синхронизации SYN/ACK и ожидает пакетов подтверждения установки соединения, которых она никогда не получит. Это приводит к замедлению работы, полному останову системы, либо недоступности определенных сетевых сервисов. NetProwler регистрирует данный вид атаки в случае обнаружения восьми неподтвержденных соединений, затем он пытается «сбросить» эти соединения, посылая восемь пакетов с установленным флагом Reset в заголовке TCP-пакета, тем самым ликвидируя угрозу отказа в обслуживании.
Denial of Service	Атака осуществляется путем использования команды ping для непрерывной посылки пакетов ICMP echo request на атакуемую систему с одного или нескольких удаленных компьютеров. В результате атакуемая система тратит большую часть своего процессорного времени, посылая ответы на ложные запросы, что приводит к замедлению работы системы и недоступности ее сетевых ресурсов. По умолчанию, NetProwler регистрирует данный вид атаки при обнаружении в течении пятнадцати секунд пяти пакетов ICMP echo request.
TCP/IP Spoofing	При реализации многих видов сетевых атак, включая атаки на отказ в обслуживании, используется подделка IP-адресов. Многие сетевые сервисы используют IP-адреса отправителей сообщений для управления доступом к разделяемым ресурсам. Подделав адрес отправителя в заголовке IP-пакетов, злоумышленник осуществляет атаку типа «маскарад», выдавая свою систему за другую, которая пользуется доверием у атакуемой стороны. NetProwler обнаруживает эту атаку выявляя пакеты, пришедшие из внешней сети, чьи IP-адреса отправителя совпадают с одним из внутренних адресов локальной сети.
Ping of Death	Данная атака осуществляется путем отправки на атакуемую систему, при помощи команды ping, ICMP-пакета, размер которого превышает максимально допустимый. При получении такого пакета на атакуемой системе переполняется системный буфер, что может привести к различным последствиям, включая сбои, перезагрузку или зависание системы. Данная атака представляет из себя серьезную проблему, так как ее воспроизведение, в отличие от подделки IP-адресов является делом простым и доступным каждому. Для этого достаточно выполнить следующую команду: ping –l 65510 <IP-адрес атакуемой системы> (Размер пакета = Заголовок IP-пакета (20 байт) + ICMP заголовок + информация команды ping (8 байт) + 65510 байт > 65535 байт – максимально допустимый размер ping-пакета). Необходимо отметить, что большинство реализаций команды ping не позволяют отправлять дейтаграммы неправильного размера. Лучшей защитой от данного вида атаки является своевременная установка соответствующих пакетов программных коррекций для ОС. Например, компания Microsoft ликвидировала эту уязвимость в третьей версии пакета обновлений ОС Windows NT. NetProwler позволяет осуществлять коррекцию размеров ping-пакетов.
Man in the Middle	Этот вид атаки достаточно сложен в реализации и заключается в том, что злоумышленник внедряется между двумя системами, взаимодействующими по виртуальному TCP/IP каналу, перехватывая сообщения, посылаемые взаимодействующими сторонами, и подменяя их своими сообщениями. Таким образом, могут перехватываться номера кредитных карточек, пароли и другая конфиденциальная информация. При этом обманутыми оказываются обе взаимодействующие стороны, которые считают, что обмениваются сообщениями друг с другом. NetProwler способен обнаруживать подобного рода атаки для определенных сетевых приложений.

Табл. 4. Шесть типовых атак, выявляемых программой NetProwler

тельность действий злоумышленника по реализации конкретного вида сетевой атаки. Она задается в виде набора шаблонов, накладываемых на содержимое сетевых пакетов, и правил, описывающих порядок и последовательность применения этих шаблонов.

В состав продукта входят средства для автоматического составления профиля локальной сети и активизации подходящих сигнатур для контролируемых сетевых ресурсов. Благодаря наличию средств профилирования, процесс администрирования IDS существенно упрощается. Для первоначальной настройки NetProwler не требуется высокой квалификации пользователя. В отличие от большинства конкурирующих продуктов, NetProwler оказывается готовым к работе практически сразу после его установки.

NetProwler рассчитан на работу в постоянно изменяющемся сетевом окружении. В процессе работы системы, средства автоматического профилирования периодически корректируют настройки NetProwler с целью взятия под наблюдение вновь подключаемых к сети ресурсов.

NetProwler также ключает в себя специализированное инструментальное средство — Wizard, позволяющее определять новые сигнатуры атак в интерактивном режиме без программирования.

Стандартные действия NetProwler по реагированию на атаки

В случае обнаружения в анализируемом трафике сигнатуры атаки NetProwler может предпринимать действия по реагированию из следующего набора:

- принудительное завершение пользовательской сессии;
- протоколирование пользовательской сессии;
- отправка сообщения администратору по электронной почте;
- отправка сообщения администратору на пэйджер;
- выполнение команды ОС или командного файла;
- посылка управляющего SNMP-сообщения программному агенту ITA;
- корректировка параметров МЭ или маршрутизатора.

Наиболее распространенные способы реализации сетевых атак, обнаруживаемые программой NetProwler

База данных NetProwler содержит несколько сотен сигнатур атак, для различных типов ОС и сетевых приложений. Особая группа сигнатур предназначена для выявления наиболее общих и часто встречающихся типов сетевых атак, обычно не связанных с конкретными приложениями. Эти атаки ввиду своей общности заслуживают отдельного рассмотрения. Их описание приводится в табл. 4.

Одной из важнейших характеристик IDS является количество сигнатур атак, содержащихся в ее базе данных, и регулярность их обновления. Обновления базы данных сигнатур атак выполняются из управляющей консоли NetProwler с использованием функции синхронизации сигнатур (Signature Sync). Обновления устанавливаются на NetProwler Manager без прерывания процесса мониторинга сетевого трафика.

Дополнительные возможности

В дополнение к реализованной в нем базовой функциональности сетевой IDS, NetProwler может использоваться в качестве средства разграничения сетевого доступа. Специальный модуль NetProwler позволяет ограничивать доступ пользователей к сетевым серверам и приложениям в зависимости от дня недели и времени суток.

Реализуемая NetProwler возможность перехвата сетевых сессий с последующим их воспроизведением позволяет производить анализ и расследование инцидента, а также собирать улики для привлечения нарушителей безопасности к ответственности. Данная функция NetProwler позволяет также анализировать характер сетевых информационных взаимодействий.

С целью защиты самого NetProwler от сетевых атак, существует возможность отключения TCP/IP стека на машине с установленным агентом NetProwler. За счет этого агент NetProwler становится невидимым для потенциальных злоумышленников, т. к. он не имеет IP-адреса. Данный режим функционирования IDS (называемый стелс-режимом) является предпочтительным с точки зрения обеспечения собственной безопасности. При функционировании в стелс-режиме, управления агентом NetProwler осуществляется через дополнительных сетевой интерфейс, подключаемый к NetProwler Manager. Однако, в этом случае, отключаются средства профилирования и автоматическое переконфигурирование алгоритмов выявления атак при изменении состава и конфигурации сетевых ресурсов становится невозможным.

По результатам мониторинга сетевого трафика NetProwler создает различные виды отчетов, которые могут быть представлены в фор-

матах HTML, DOC, Excel, ASCII и Crystal Reports. Отчеты могут генерироваться с заданной периодичностью и отправляться администратору по электронной почте. «Executive summary» содержит обзор количества и типов атак за определенный период времени. «Cost analysis» содержит оценку величины ущерба, причиняемого в случае успешного осуществления атаки, а «Attack details» содержит детальную информацию по каждой атаке.

Интеграция NetProwler и Intruder Alert

Наиболее эффективный подход к выявлению атак заключается в интеграции средств сетевого (network-based) и системного (host-based) уровней. Такая интеграция между продуктами ITA и NetProwler реализована на базе протокола SNMP. В то время, как NetProwler осуществляет контроль сетевых информационных взаимодействий и выявление сетевых атак, Intruder Alert следит за событиями, происходящими на контролируемых системах «изнутри». Интеграция этих продуктов дает возможность осуществлять централизованный контроль всех происходящих в сети событий, связанных с безопасностью, как на уроне сетевых взаимодействий, так и на уровне отдельных хостов.

Стандартный клиент-серверный протокол прикладного уровня SNMP, предназначенный для управления сетевыми ресурсами в TCP/IP сетях, также используется для управления компонентами подсистемы безопасности распределенных систем. В соответствии с этим протоколом для управления сетевыми устройствами, называемыми SNMP-агентами, такими как коммутаторы и маршрутизаторы, межсетевые экраны, серверы и рабочие станции, X-Терминалы и терминальные серверы, используются станции управления сетью — SNMP-менеджеры. Агенты ITA включают поддержку протокола SNMP и могут выступать одновременно и в роли SNMP-менеджера и в роли SNMP-агента. Функционируя в качестве SNMP-менеджеров они способны посылать управляющие сообщения сетевым устройствам, оперативно изменяя их параметры. В качестве SNMP-агентов они способны принимать управляющие сообщения от других компонентов системы защиты, в частности от агентов NetProwler, выдавая на них определенную реакцию в соответствии с настройками политики безопасности.

6.4. Применение средств выявления атак компании Symantec для защиты корпоративной сети

Типовая схема размещения средств выявления атак компании Symantec для защиты корпоративной сети, подключенной к Интернет, приведена на рис. 5. Состав, конфигурация и размещение отдельных компонентов IDS определяется по результатам обследования безопасности и анализа рисков.

Агенты NetProwler размещаются в особо критичных сегментах сети, контролируя внешние информационные взаимодействия и выявляя сетевые атаки против особо уязвимых серверов (Web и SMTP), расположенных в DMZ.

Ангенты ITA размещаются на всех контролируемых системах корпоративной сети, включая серверы и рабочие станции, и осуществляют мониторинг системных журналов и журналов приложений, выявляя различные виды аномальной активности. Пользовательские рабочие станции, как правило, являются менее критичными элементами информационной инфраструктуры, поэтому на них устанавливаются облегченные версии агентов, обозначенных на рисунке как ITA Workstation Agents. Для осуществления контроля за событиями, происходящими при функционировании прикладных подсистем, на серверных агентах ITA активизированы специализированные политики безопасности для МЭ, почтового и Web-серверов, а также для SQL-сервера.

Ядром системы выявления атак является сервер безопасности, на котором функционируют ITA Manager и NetProwler Manager. На сервере безопасности накапливается вся информация о событиях, происходящих в сети, поступающая от агентов. Здесь размещается вся конфигурационная информация IDS, включая сигнатуры атак и политики безопасности. С сервера безопасности осуществляется управление всеми агентами IDS путем отправки им управляющих сообщений.

Конфигурирование системы выявления атак, создание собственных сигнатур атак и политик безопасности, просмотр и анализ данных аудита, а также генерация отчетов осуществляется с управляющей консоли администратора безопасности, на которой устанавливаются графические средства администрирования ITA Admin, ITA View и NetProwler Console. Данные приложения реализуют интерфейс для взаимодействия администратора с сервером безопасности.

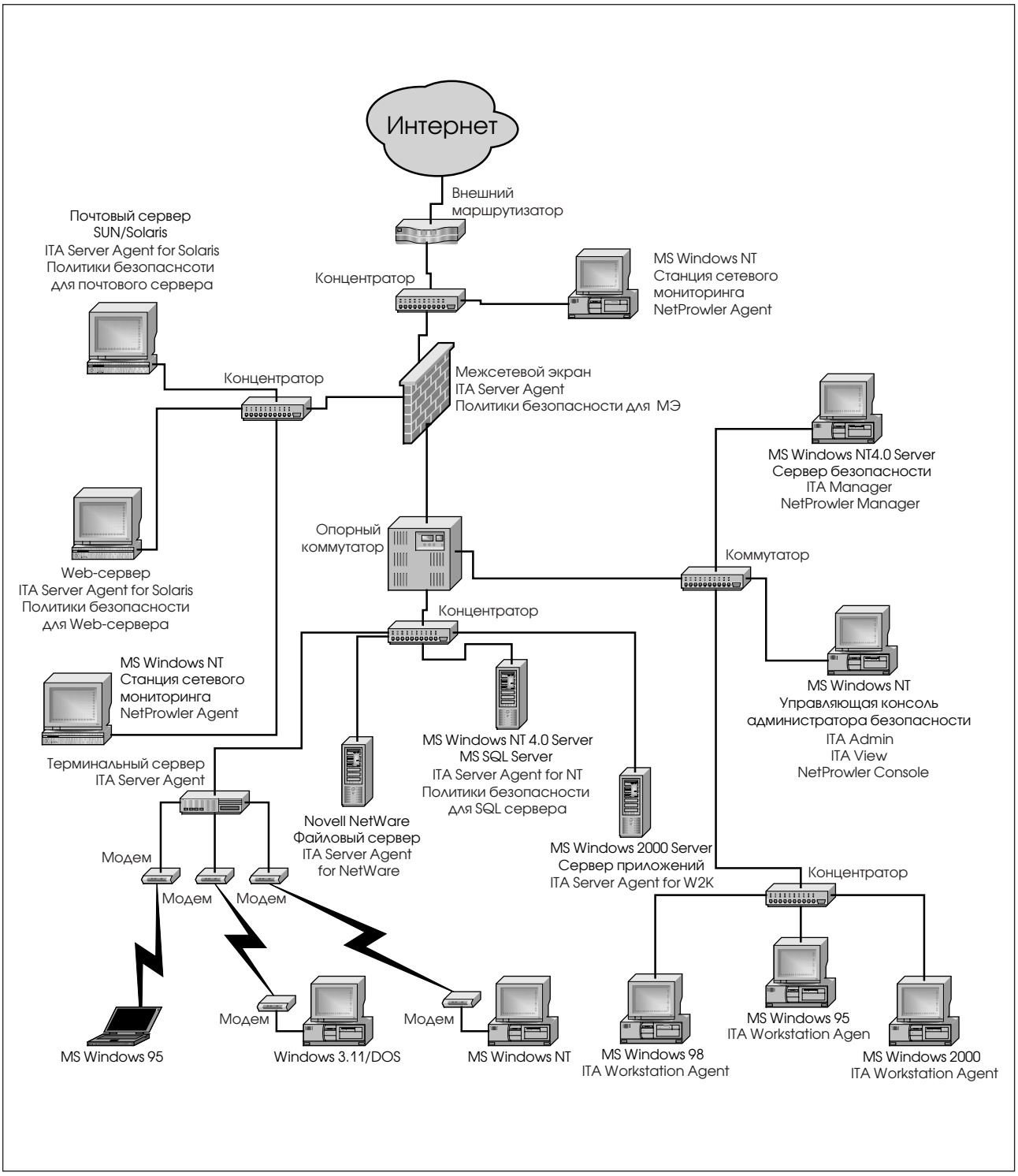


Рис. 5. Применение средств выявления атак компании Symantec для защиты корпоративной сети

7. Заключение

Для решения задачи защиты от сетевых атак необходима концепция, определяющая объекты защиты, цели, задачи и основные принципы защиты, а также состав и последовательность работ по предупреждению, выявлению и реагированию на атаки.

Достаточно простым и эффективным подходом к обеспечению защиты внешнего периметра, который хотелось бы порекомендовать, является использование списка десяти наиболее часто используемых для осуществления атак уязвимостей (Top Ten List), публикуемых институтом SANS http://www.sans.org/topten.htm. (Данный список содержит описание десяти уязвимостей, наиболее часто используемых хакерами для осуществления сетевых атак, и способов их ликвидации.) Фактически эти уязвимости используются более чем в 80% случаев всех предпринимаемых атак. Большинство хакеров не утруждают себя поиском уникальных уязвимостей конкретных хостов. Вместо этого, располагая небольшим арсеналом средств для осуществления атак, они просто сканируют сети в поисках одной из известных им уязвимостей. Современные сетевые сканеры способны обнаруживать эти уязвимости. Поиск и ликвидация данных уязвимостей может существенно затруднить жизнь современным взломщикам сетей. Им придется искать новые более изощренные способы взлома, пополнять свой арсенал атакующих средств, разрабатывая новые методы и средства. Это существенно сузит круг возможных взломщиков и уменьшит общее количество предпринимаемых ими атак.

В настоящее время список наиболее часто используемых уязвимостей расширен и включает в себя уже 20 уязвимостей (http://www.sans.org/top20.htm).

Конечно, предложенный подход не отличается полнотой и не в состоянии обеспечить защиту от многих видов сетевых атак. Более комплексная концепция защиты сети от внешних атак предполагает проведение как минимум следующих мероприятий:

1. Разработка политики безопасности по осуществлению контроля сетевого доступа
2. Анализ рисков и уязвимостей, использование положительного опыта и существующих решений по обеспечению безопасности
3. Создание инфраструктуры (назначение ответственных, распределение ролей и т.п.)
4. Проектирование системы защиты, определение требований, предъявляемых к используемым средствам и механизмам защиты
5. Выделение ресурсов, ранжирование выбранных контрмер по степени важности и реализация наиболее приоритетных
6. Проведение аудита и периодического тестирования эффективности реализованных контрмер
7. Реализация и сопровождение системы выявления атак и реагирования на атаки

8. Библиографический список

1. AXENT Intruder Alert User Manual, Version 3.0
2. AXENT NetProwler User Manual, Version 3.0
3. Common Criteria for Information Technology Security Evaluation, 96/01/31
4. Stephen Northcutt, IDS Signatures and Analysis, Parts 1 & 2, SANS 2001 Baltimore, Maryland, May 2001

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su
http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем