Теоретический аспект. Теория электронных документов и электронного документооборота находится в самом начале разработки. Нашедшая распространение трактовка электронного документа как некоторого аналога традиционного документа, показала свою ограниченность в правовом поле. На современном этапе внедрения электронного взаимодействия отсутствие тщательно проработанной теоретической базы становится фактором, препятствующим разработке и совершенствованию прикладных технологий. Теоретическая и понятийная база электронного документооборота нуждается в более глубокой проработке. В связи с этим необходимо и далее поддерживать работы по созданию прикладной теории электронного документа.

Технологический аспект. Технически задача формирования, обработки, передачи и хранения электронного сообщения решена. Актуальной остается задача обеспечения унификации технологий защиты электронного документооборота, включая: собственно защиту информации; защиту среды формирования и обработки электронного документа; формирование и сохранение атрибутов электронного документа, подтверждающих его юридическую значимость.

Юридический аспект. Для того чтобы сообщение могло иметь статус электронного *документа*, оно обязательно должно включать в свой состав ряд атрибутов, позволяющих удостоверить соблюдение ряда специальных требований, которые обеспечат признание электронного документа субъектами права как *юридически* полноценного. Выполнение технических и технологических требований изготовления и транспортировки документа должно фиксироваться общепризнанным способом. Технология электронного взаимодействия должна соответствовать сертифицированному эталону, а ее соблюдение должно контролироваться уполномоченными органами. Необходима разработка соответствующей нормативной правовой базы.

Таким образом, **сообщение становится документом при условии доверия к технологии его формирования** и делает его таковым **инфраструктура электронного документооборота**.

Инфраструктура электронного документооборота представляет собой взаимоувязанную совокупность нормативных, законодательных, методических материалов, организационных решений и механизмов, технических, программных и технологических объектов. Эта совокупность должна гарантировать достаточность использованной технологии электронного взаимодействия для признания электронного документа юридически полноценным. Она должна обеспечивать полноту, аутентичность, доступность и актуальность государственного информационного ресурса и их информационную безопасность.

В состав такой инфраструктуры должны включаться следующие подсистемы:

- управляющая;
- нормативная и организационно–методическая;
- исполнительная (удостоверяющие центры, служба меток единого времени, электронный нотариат, обеспечение качества, арбитраж);
- управление рисками (аудит, мониторинг, аттестация, лицензирование, сертификация, надзор, страхование).

Литература: ***1.*** *Стрельцов А. А.. Обеспечение информационной безопасности России. Теоретические и методологические основы. – М.: МЦНМО, 2002. – 296 с.* ***2.*** *Гадасин В. А., Конявский В. А. От документа – к электронному документу. Системные основы. – М.: РФК-Имидж Лаб, 2001. – 192 с.* ***3.*** *Конявский В. А. Управление защитой информации на базе СЗИ НДС Аккорд. – М.: Радио и связь, 1999. – 325 с.*

УДК 681.3

ПЕРСПЕКТИВНЫЙ МЕТОД ЗАЩИТЫ ИФОРМАЦИОННЫХ РЕСУРСОВ КОРПОРАТИВНЫХ СЕТЕЙ ИНТРАНЕТ

Вячеслав Шорошев

НИИ Национальной академии внутренних дел Украины

Аннотация: **В дополнение к традиционным предлагается использовать новый перспективный мониторинго-адаптивный метод защиты путем обнаружения атак НСД, рассматриваемый как основной механизм реализации адаптивной безопасности сети Интранет организации.**

Summary: **In addition to traditional it is offered to use a new perspective monitoring-adaptive method of protection by detection of attacks UAA, considered(examined) as the basic mechanism of realization of adaptive safety of a network Intranet of organization.**

Ключевые слова: **Адаптивная безопасность, атака НСД, уязвимость, модель событя безопасности, MAMPDA-метод, узел сети, инциденты атак НСД, модель атаки НСД.**

I Введение

Ранее [1–3] уже освещались недостатки традиционных методов защиты ресурсов корпоративных сетей Интранет (межсетевые экраны, маршрутизаторы, системы обнаружения атак и др.). Предлагалось перейти к использованию нового мониторинго-адаптивного метода защиты путем обнаружения атак НСД (monitoring-adaptive method of protection by detection of attacks, MAMPDA-метод, МАМЗОА-метод) как дополнения к традиционным методам защиты [2].

Суть предложенного метода защиты можно сформулировать следующим концептуальным правилом адаптивной безопасности MAMPDA-1: если мы не можем построить абсолютно защищенную корпоративную систему, то хотя бы должны обнаруживать все (или практически все) нарушения политики безопасности и соответствующим образом (адаптивно) реагировать на них.

Практически это возможно только путем своевременного обнаружения атак НСД (первый этап успешной защиты) и их нейтрализации при попытке реализации (второй и заключительный этап защиты). Технология атак НСД имеет еще и третий этап их реализации – заметание следов (завершение атаки, скрытие источника и факта атаки НСД), поэтому обнаружение атак на третьем этапе равносильно поражению, на втором этапе – почти успешная зашита, но с потерями, а на первом этапе – почти 100% защита, если после обнаружения атаки НСД вы можете ее на 100% нейтрализовать.

Прежде чем рассматривать механизмы обнаружения атак НСД, логично рассмотреть модель события безопасности, уязвимость компьютерной системы, атак НСД и как они классифицируются по этапам реализации, неформальную модель и модель распределенной атаки НСД; базу данных атак НСД и т. д. Без этого трудно эффективно обнаруживать и блокировать атаки НСД на информационные ресурсы сети Интранет.

Кроме этого, чтобы предотвращать атаки НСД на узлы корпоративной сети Интранет, администраторы безопасности нуждаются также в понимании технологии и методов нападающих. Нельзя бороться с врагом без знания его оружия. Для этого можно рекомендовать концептуальные подходы известных работ [1–4, 10, 11, 16]. Но привести общие концепции с их детализацией и некоторыми примерами атак все же необходимо. Без знакомства с ними трудно понять предлагаемые методы и механизмы защиты от атак НСД.

II Модель события безопасности

При функционировании узлов сети Интранет происходят различные события (events), которые изменяют состояния этих узлов. Они могут рассматриваться компонентами некоторой модели (рис. 1) и быть представлены с точки зрения безопасности при помощи двух ее базовых составляющих – действия (action) и адресата (target). Действия – это шаги, предпринимаемые субъектом сети (пользователем, процессом и т. д.) для достижения некоего результата. К действиям можно отнести: чтение, копирование, модификацию, удаление и т. д. Адресат – это логический (учетная запись, процесс, данные) или физический (узел сети, сеть, компонент) объекты сети.

Примером события безопасности является доступ пользователя к файлу. В том случае, когда событие выполняется в соответствии с политикой безопасности, это рядовое санкционированное событие. Событие — это как бы минимальная единица, которой оперируют современные средства защиты, например, система обнаружения атак RealSecure [3]. И хотя многие защитные средства предполагают еще и третий параметр – источник события, мы выносим его за рамки описания модели события безопасности, поскольку этот параметр становится значимым только в случае реального осуществления атаки и нанесения ущерба. Но заранее ориентироваться на успешность атаки нельзя. Поэтому, как только событие нарушает политику безопасности, оно сразу рассматривается как часть атаки с ее источником.

Рисунок 1 – Базовая модель события безопасности

III Уязвимости компьютерной системы (сети)

Уязвимость (vulnerability) компьютерной системы (сети) – это любая ее характеристика, использование которой нарушителем может привести к реализации угрозы. Под угрозой (threat) компьютерной системе (сети) (далее просто системе) будем понимать любое событие, действие, процесс или явление, которое может быть причиной нарушения политики безопасности или нанесения ущерба (материального, морального или иного) ресурсам системы.

Пример №1.Ошибка в программе привела к аварии космической ракеты.

Год 1996, 4 июня, вторник, космодром во Французской Гвиане. 9 часов 33 минуты 59 секунд. Первый запуск ракеты-носителя Ariane 5. Ракета взмывает в небо и через 40 секунд после старта взрывается на 50-метровой высоте, ущерб составил по различным данным от пятисот миллионов до шести миллиардов долларов. Через полтора месяца, 19 июля, был опубликован исчерпывающий доклад комиссии по расследованию, в результате которого выяснилось, что взрыв произошел из-за ошибки переполнения одной из переменных в программном обеспечении бортового компьютера ракеты [3].

2.1. Классификация уязвимостей компьютерных систем (сетей).

Если вы не имеете никакой систематизированной информации об уязвимостях и частоте их появления, то вы не можете эффективно распределить свои ограниченные ресурсы для защиты от атак НСД.

Одно из первых исследований в этой области проводилось в рамках проекта Protection Analysis Project в середине 70-х годов [3]. Исследовались уязвимости операционных систем. В течение нескольких лет участники проекта опубликовали ряд статей, в которых описывались категории уязвимостей и способы их поиска по так называемым шаблонам. Однако предложенные методы не могли быть легко автоматизированы, и разработанная база данных уязвимостей так никогда и не была опубликована.

В 1996 году лаборатория COAST университета Пардью (Purdue) разработала свою классификацию [5], а компания ISS – свою [6]. Согласно последней выделяются уязвимости:

реализованные или созданные продавцом (разработчиком) программного или аппаратного обеспечения;

добавленные администратором в процессе управления компонентами системы;

привнесенные пользователем в процессе эксплуатации системы.

Уязвимости, реализуемые поставщиком (разработчиком), включают: ошибки, не установленные обновления операционной системы, уязвимые сервисы и незащищенные конфигурации as default.

Уязвимости, связанные с действиями администратора, представляют собой доступные, но неправильно используемые настройки и параметры системы, не отвечающие политике безопасности (например, требования к минимальной длине пароля и несанкционированные изменения в конфигурации системы).

Уязвимости, относящиеся к деятельности пользователя, включают уклонения от предписаний принятой политики безопасности, например, отказ запускать программное обеспечение (ПО) для сканирования вирусов или использование модемов для выхода в сеть Internet в обход межсетевых экранов и другие, более враждебные действия.

Анализ существующих классификаций уязвимостей показал, что для защищенных компьютерных систем (ЗКС) наиболее целесообразно придерживаться классификации, отражающей этапы их жизненного цикла (табл. 1).

Таблица 1 – Категории уязвимостей ЗКС

Этапы жизненного цикла ЗКС	Категории уязвимостей ЗКС
Проектирование ЗКС	Уязвимости проектирования ЗКС
Реализация ЗКС	Уязвимости реализации ЗКС
Эксплуатация ЗКС	Уязвимости конфигурации ЗКС

Аналогичная классификация, но без привязки к атакам НСД и к ресурсам ЗКС, приведена в [3]. Именно эта классификация (табл. 1) и будет использоваться в дальнейшем при описании атак НСД.

Уязвимость проектирования ЗКС. Данный тип уязвимостей наиболее серьезен – они обнаруживаются и устраняются с большим трудом [3]. В этом случае уязвимость свойственна проекту или алгоритму и, следовательно, даже совершенная его реализация (что в принципе невозможно) не избавит от заложенной в нем слабости. Например, уязвимость стека протоколов TCP/IP. Недооценка требований по безопасности при создании этого стека протоколов привела к тому, что не проходит и месяца, чтобы не было объявлено о новой уязвимости в протоколах стека TCP/IP. И раз и навсегда устранить эти недостатки уже невозможно - существуют только временные или неполные меры. Однако бывают и исключения. Например, внесение в проект корпоративной сети множества модемов, облегчающих работу персонала, но существенно усложняющих работу службы безопасности. Это приводит к появлению потенциальных путей обходов

межсетевого экрана, обеспечивающего защиту внутренних ресурсов от несанкционированного использования. Но обнаружить и устранить эту уязвимость уже достаточно легко.

Уязвимость реализации ЗКС. Смысл уязвимостей этой категории заключается в появлении ошибки на этапе реализации в программно-аппаратном обеспечении, корректном с точки зрения безопасности проекта или алгоритма.

Яркий пример такой уязвимости – "переполнение буфера" ("buffer overflow") во многих реализациях программ, например, sendmail или Internet Explorer [3]. Обнаруживаются и устраняются подобного рода уязвимости относительно легко. Если нет исходного кода программного обеспечения (ПО), в котором обнаружена уязвимость, то ее устранение заключается или в обновлении версии уязвимого ПО или в полной его замене, или в отказе от него.

Уязвимости конфигурации ЗКС. Причина возникновения таких уязвимостей – ошибки конфигурации программного или аппаратного обеспечения. Этот вид наряду с уязвимостями реализации является самой распространенной категорией уязвимостей [3]. Существует множество примеров таких уязвимостей. К их числу можно отнести, например, доступное, но не используемое на узле сервис Telnet неразрешение "слабых" паролей или паролей длиной менее 6 символов, учетные записи (accounts) и пароли, остановленные по умолчанию (например SYSADM или DBSNMP в СУБД Oracle), и т. д. Локализовать и исправить такие уязвимости проще всего (табл. 2).

Таблица 2. Возможности по обнаружению и устранению уязвимостей ЗКС

Категория уязвимости	Обнаружение	Устранение
Уязвимости реализации	Относительно трудно, долго	Легко, но относительно долго
Уязвимости конфигурации	Легко и быстро	Легко и быстро
Уязвимости проектирования	Трудно и долго	Трудно и долго (иногда невозможно)

Основная проблема – определить, является конфигурация уязвимой или нет. По статистике, опубликованной в 1998 году институтом SANS, пятерка наиболее распространенных групп уязвимостей выглядит следующим образом:

1. выслеживание информации (network snooping), особенно паролей и иной конфиденциальной информации;
2. переполнение буфера (buffer overflow), приводящее к удаленному выполнению произвольных команд;
3. уязвимости системы защиты узлов, например, уязвимости сценариев CGI или ошибки в sendmail;
4. подверженность атакам типа "отказ в обслуживании" (Denial of service);
5. допустимость загрузки деструктивного кода, к которому кроме программ типа "троянский конь" (Trojan) или вирусов можно отнести апплеты Java и элементы управления ActiveX.

Можно заметить, что в первую пятерку вошли все три категории уязвимостей. Выслеживание паролей возможно благодаря отсутствию механизмов шифрования в стандартных протоколах Internet (FTP, Telnet, POP3, HTTP и др.). Переполнение буфера, уязвимости защиты узлов и подверженность атакам типа "отказ в обслуживании" могут быть отнесены к разряду уязвимостей реализации и конфигурации. Возможность загрузки деструктивного кода может быть причислена к разряду уязвимостей конфигурации.

В 2001 году пятерка лидеров (п. п. 1 – 5) обновилась, что лишний раз подтверждает тезис о динамичности изменения сетевых технологий, в том числе и в области информационной безопасности. Вот она [7, 3]:

1. слабости BIND (nxt, qinv и in.named);
2. уязвимые CGI-сценарии и расширения приложений (например, ColdFu-sion), установленные на Web-сервере;
3. уязвимости RPC;
4. уязвимости Remote Data Services (RDS) в Microsoft Internet Information Server;
5. переполнение буфера в почтовой программе sendmail;

Эта пятерка частично совпадает с исследованиями компании ISS [8, 3]:

1. подверженность атакам типа "отказ в обслуживании" (в том числе и распределенным атакам этого типа);
2. "слабые" учетные записи (для серверов, маршрутизаторов и т. д.);
3. уязвимости ПО MS IIS (Microsoft Internet Information Server);
4. уязвимости СУБД (неправильные права доступа к расширенным хранимым процедурам, пароли, заданные по умолчанию и т. д.);
5. приложения в Commerce (Netscape FastTrack, MS Frontpage и др.).

2.2. Атаки НСД.

До сих пор у профессионалов в области информационной безопасности нет точного определения термина "атака" (вторжение – intrusion, нападение). Каждый специалист в области безопасности трактует его по-своему. Например, "вторжение – это любое действие, переводящее систему из безопасного состояния в опасное". Встречаются и такие определения: "вторжение – это любое нарушение политики безопасности" или "любое действие, приводящее к нарушению целостности, конфиденциальности и доступности системы и информации, в ней обрабатываемой". Однако более правильным применение нижеприведенного термина, которое тесно увязано с термином "уязвимость". Атакой (attack) на систему называется действие или последовательность связанных между собой действий нарушителя, которые приводят к реализации угрозы НСД путем использования уязвимостей этой информационной системы [2, 3].

Таким образом, атака НСД отличается от события безопасности тем, что в случае атаки злоумышленник пытается достичь некоторого результата, противоречащего политике безопасности. Например, доступ пользователя к файлу или вход в систему – это событие безопасности. Однако если этот доступ или вход осуществляется в нарушение правил доступа, это уже атака НСД. Понять, имеет ли в конкретном случае место нарушение прав доступа, поможет анализ признаков, характеризующих атаку НСД. Если построить неформальную модель атаки НСД, которая расширяет описанную выше, для события безопасности, то получится формальная модель атаки НСД, состоящая из пяти элементов: атака НСД – средство реализации атаки – уязвимость – событие безопасности – результат.

Для того чтобы реализовать атаку НСД, злоумышленник (intruder, attacker) моделирует некоторое событие безопасности, которое приводит к искомому результату при помощи некоего средства, использующего уязвимости системы. Первые два элемента данной модели применяются для реализации события безопасности, т. е. некоторого действия по отношению к адресату для достижения результата, приводящего к нарушению политики безопасности.

Предваряя описание автоматизированных средств обнаружения атак, необходимо заметить, что они определяют именно атаки НСД и события безопасности, а не инциденты. Ранее описанные модели события безопасности и атаки НСД не используют такой компонент, как “нарушитель” или "атакующий”. Он появляется только в описании инцидента безопасности. Это лишний раз объясняет тот факт, что системы обнаружения атак НСД не всегда могут "отловить" злоумышленников, реализующих те или иные атаки.

Неизвестно, сколько реально существует методов атак НСД. Связано это в первую очередь с тем, что до сих пор отсутствуют какие-либо серьезные математические исследования в этой области. Из близких по тематике исследований можно привести работу 1996 года Фреда Коэна (Fred Cohen), в которой описывались математические основы вирусной технологии атак НСД. Одним из интересных результатов этой работы является доказательство бесконечности числа вирусов. Эти же результаты можно перенести и на область атак, поскольку вирусы — это ничто иное, как одно из подмножеств атак НСД.

2.3. Неформальная модель атаки НСД.

Не вдаваясь глубоко в математическое описание модели атаки НСД, вместе с тем хотелось бы, чтобы читатель имел представление о том, как осуществляются эти атаки. Это поможет в понимании механизма атак, что, в свою очередь, является залогом успеха их обнаружения, отражения и предотвращения

В частном случае инициатор атаки НСД (злоумышленник) и цель атаки совпадают. В этом случае злоумышленник уже получил или имеет в рамках своих полномочий доступ к узлу (группе узлов), к ресурсам которого намерен несанкционированно обращаться. Целью атаки НСД, также как и инициатором атаки, может выступать одиночный узел или группа узлов (например, подсеть).

Логично предположить, что устранение одного из этих элементов позволит полностью защититься от атаки НСД. Удалить цель атаки на практике зачастую невозможно из-за особенностей технологии обработки информации. Хотя это решение было бы идеальным. Раз нет цели для атаки, то неосуществима и сама атака. Одним из механизмов попытки удаления объекта атаки НСД является сетевая трансляция адресов или блокирование доступа к определенным узлам корпоративной сети Интранет извне при помощи межсетевого экрана.

Но поскольку нельзя удалить цель атаки НСД, то необходимо попытаться устранить нарушителя или метод атаки. Но именно этого-то практически и не делают современные традиционные средства защиты. Они, как правило, сосредотачивают свое внимание на объекте атаки и немного на методе атаки. Это попустительство в отношении атакующего приводит к повторным атакам со стороны нарушителя (даже если они и безуспешны).

Необходим поэтому комплексный подход по правилу MAMPDA-1, включающий, кроме традиционных, и дополнительные средства, реализующие функции обнаружения атак НСД, отслеживания злоумышленника и расследование инцидентов этих атак.

Метод атаки НСД зависит от нескольких параметров [1 – 3]:

1. тип инициатора атаки и цели атаки;
2. результат воздействия;
3. механизм воздействия;
4. средство воздействия.

От типа инициатора атаки и цели атаки зависит, какой метод атаки следует ожидать. Например, если объектом атаки является почтовый сервер MS Exchange, то вряд ли для нападения на него будет использоваться метод, применяемый для атаки на sendmail или qmail.

От того, какого результата нарушитель ждет от атаки (отказ в обслуживании, компрометация и т. п.), зависит, какой метод атаки он применит. Например, если злоумышленник планирует получить несанкционированный доступ к файлу паролей вашего Web-сервера, то он будет скрывать свои несанкционированные действия и искать уязвимое и в открытых сервисах Web-сервера (HTTP, FTP, 1MAP и т. д.). Если же злоумышленник хочет нарушить доступность, то он может послать "лавину" запросов на соединение на ваш Web-сервер, тем самым выводя его из строя.

2.4. Модель традиционной атаки НСД.

Традиционная модель атаки НСД строится по принципу "один к одному" (злоумышленник – цель атаки НСД) или "один ко многим" (злоумышленник – множество целей атаки НСД), т. е. атака исходит из одной точки.

Очень часто для сокрытия источника атаки или затруднения его нахождения используется метод промежуточных хостов. Злоумышленник реализует атаку не напрямую на выбранную цель, а через цепь промежуточных узлов. Нередко эти узлы находятся даже в разных странах. В результате объекту атаки "кажется", что угроза исходит с промежуточного узла.

Разработчики средств защиты ориентированы именно на классическую модель атаки. В различных точках сети устанавливаются разные агенты системы защиты, которые передают информацию на центральную консоль управления. Это облегчает масштабирование системы (увеличение числа агентов не сказывается на консоли – она одна и та же), простоту удаленного управления и т. д.

2.5. Модель распределенной атаки НСД.

В ноябре 1999 года Координационный Центр CERT (http://www.cert.org) пригласил 30 ведущих экспертов в области информационной безопасности из различных организаций, в том числе из Internet Security Systems, NASA, NSWC SHADOW Team. Темой этой конференции были распределенные атаки {distributed attack) и средства, их реализующие. Эти атаки позволяют одному или нескольким злоумышленникам проводить сотни и тысячи нападений, осуществляемых в один момент времени, на один или несколько узлов Интернет, Интранет. Еще совсем недавно такая возможность относилась к разряду мифических. Считалось, что реализовать подобного рода атаку практически невозможно. Однако жизнь внесла свои коррективы [3, 11].

Одно из первых предупреждений о такого рода атаках было сделано в сентябре 1998 года. Naval Surface Warfare Center (http://www.nswc.navy.mil) проанализировал несколько зафиксированных в 1998 году случаев и на их основе выпустил один из первых отчетов, посвященных несанкционированным атакам. Традиционная модель атаки обычно оперирует одним узлом в качестве источника атаки НСД. Именно этот принцип и заложен как основополагающий во многие средства защиты сетей. Однако новая модель – модель распределенной атаки – вносит свои корректировки и вынуждает разрабатывать новые механизмы обнаружения нападений [2, 9].

Модель распределенной или скоординированной атаки (coordinated attack) опирается на иные принципы. В отличие от традиционной модели, использующей отношения "один к одному" и "один ко многим", в распределенной модели их заменили отношения "много к одному" и "много ко многим".

Все распределенные атаки основаны на "классических" атаках типа "отказ в обслуживании", точнее – на их подмножестве, известном как Flood- или Storm-атаки (указанные термины можно перевести как "шторм", "наводнение", "лавина"). Смысл данных атак заключается в посылке большого количества пакетов на заданный узел сети (цель атаки), что может привести к выведению этого узла из строя, поскольку он "захлебнется" в потоке посылаемых пакетов и не сможет обрабатывать запросы авторизованных пользователей. По такому принципу работают атаки SYN-Flood, Smurf, UDP Flood, Targa3 и т. д. Однако в том случае, когда полоса пропускания канала до цели атаки превышает пропускную способность атакующего, или целевой узел некорректно сконфигурирован, то к "успеху" обычная атака "отказ в обслуживании" не приведет. В случае же распределенной атаки ситуация коренным образом меняется. Атака происходит уже не из одной точки Internet, а сразу из нескольких, что обуславливает резкое возрастание трафика и выход атакуемого узла из строя.

Реализуется распределенная атака в два этапа.

Первый этап заключается в поиске в Internet узлов, которые можно было бы задействовать для реализации распределенной атаки. Чем больше будет найдено таких узлов, тем эффективнее будут

последствия. "Изюминка" в том, что в Internet таких узлов миллионы. Проводимые регулярно исследования показывают, что многие владельцы Intranet не следят за безопасностью своих узлов, имеющих выход в Internet. Эти-то узлы и становятся излюбленным местом приложения внимания злоумышленников, выбирающих их в качестве "базового лагеря" для дальнейшей атаки. Эти узлы могут относиться не только к сетям университетов и государственных структур, но и к Internet-провайдерам, финансовым и страховым компаниям и т. д. После нахождения уязвимых узлов злоумышленник осуществляет установку на них компонентов, реализующих атаку НСД. Такая установка оказывается возможной благодаря "слабым" звеньям в защите, которые и использует злоумышленник для себя.

Второй этап представляет собой посылку большого количества пакетов на атакуемый узел Интранет. Особенность этого этапа в том, что отправка пакетов осуществляется не с узла, за которым "сидит" злоумышленник, а со скомпрометированной им системы-посредника, на которой установлены специальные агенты, реализующие распределенную атаку (рис. 2, модель распределенной атаки НСД или схема событий безопасности: злоумышленник – мастер – демон – жертва). Существуют два типа таких агентов: "мастера" (master) и "демоны" (daemon), иначе называемые "клиентами" и "серверами". Иногда компьютеры с установленными агентами называют компьютерами "зомби". Злоумышленник управляет небольшим числом "мастеров", которые, в свою очередь, командуют "демонами". Казалось бы, что проблема не стоит и "выеденного яйца". Вместо обычной одноуровневой структуры простой атаки (злоумышленник – атакуемый) используется трехуровневая: злоумышленник – мастер – демон – атакуемый. Что мешает пройти по этой цепочке и определить все участвующие в атаке узлы? Но в том-то и состоит особенность распределенных атак, что не так просто это сделать [10].

Обнаружение и блокирование одного или нескольких "мастеров" или "демонов" не приводит к окончанию атаки, поскольку каждый "демон" действует независимо от других и, получив соответствующие команды от "мастера", уже не нуждается в дальнейшем поддержании связи с ним. То есть "демон" работает автономно, что существенно затрудняет обнаружение и блокирование всех демонов, участвующих в распределенной атаке. Кроме того, при атаке возможна подмена адреса отправителя враждебных пакетов, что также отрицательно сказывается на эффективности контрмер. Нападающий использует десятки и сотни незащищенных узлов для координации нападения.

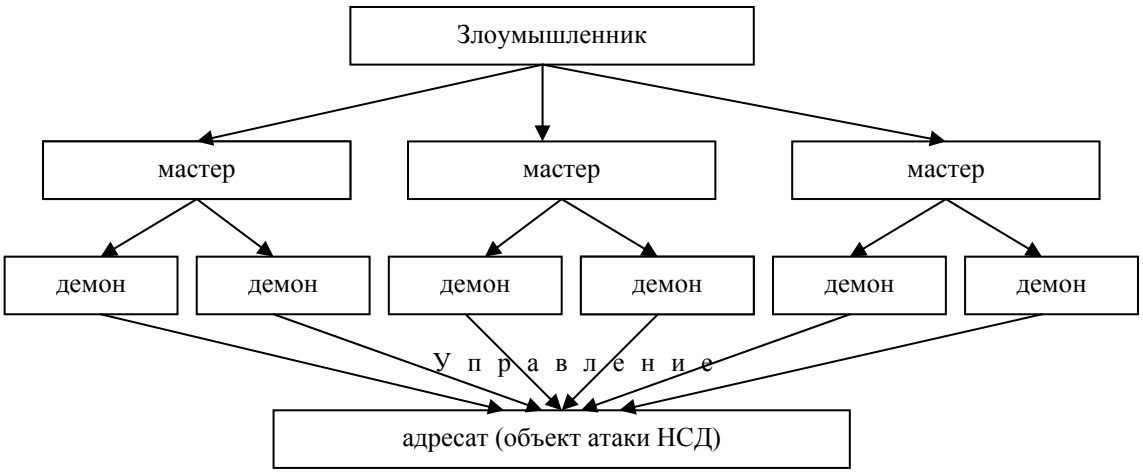

Рисунок 2 – Модель распределенной атаки НСД по правилу “злоумышленник – мастер – демон – атакуемый”

Эти узлы могут принадлежать различным провайдерам и находиться в различных странах и даже на различных материках, что существенно затрудняет обнаружение злоумышленника, координирующего атаку. Каждый узел, участвующий в скоординированной атаке, не позволяет получить информацию о том, кто и откуда инициировал нападение. Кроме того, на этих узлах нет полного списка участвующих в атаке узлов. Поэтому выявление одного узла не приводит к прекращению всей атаки.

Данный подход имеет для атакующей стороны следующие преимущества [11].

Скрытость. Работа сразу с нескольких адресов существенно затрудняет обнаружение нападавших стандартными механизмами (межсетевыми экранами, системами обнаружения атак и т. д.).

"Огневая мощь". Координация атак сразу из нескольких точек сети позволяет за короткий промежуток времени реализовать более мощную атаку, чем это было бы возможно в случае осуществления аналогичной

атаки из одной точки. Наиболее опасными из них являются атаки типа "отказ в обслуживании". Как и в предыдущем случае (скрытности), существующие методы обнаружения и блокирования распределенных атак малоэффективны.

Получение разнообразных данных. Работая с различных адресов, в т. ч. находящихся в различных сетях, можно получить больше данных о целевом объекте атаки по сравнению с аналогичными действиями, реализуемыми из одной точки. Таким образом можно выяснить наиболее короткие маршруты движения пакетов до цели атаки, "доверенные" отношения с различными узлами сети и т. д. Например, из узла А злоумышленник может получить доступ к цели атаки при помощи программ типа "троянский конь", а из узла В – не может.

Сложность блокирования. Указанные особенности затрудняют блокирование распределенных атак.

В зафиксированных в 1998 – 1999 годах случаях распределенные атаки использовали несколько сотен демонов. Согласно данным одного из потерпевших в атаке НСД участвовало до 10 тысяч демонов [3]. Эти демоны устанавливаются путем использования на скомпрометированных узлах различных уязвимостей, в т. ч. и позволяющих получить права администратора (root) на узле с установленным демоном. Как только демон установлен, он уведомляет об этом "мастера" (обычно трех или четырех). После получения определенных команд от злоумышленника "мастер" программирует "демона" на выполнение соответствующих действий против жертвы. Эти команды содержат следующую информацию: адрес жертвы; тип атаки; продолжительность атаки.

Злоумышленник может организовать посылку большого объема данных сразу из всех узлов, которые задействованы в распределенной атаке. В этом случае атакуемый узел "захлебнется" огромным трафиком и не сможет обрабатывать запросы от нормальных пользователей. В случае с обычной реализацией аналогичной атаки необходимо иметь достаточно "толстый" канал доступа в Internet, чтобы реализовать лавину пакетов на атакуемый узел Intranet. Для распределенной атаки выполнение этого условия уже не является обязательным (достаточно иметь обычное модемное соединение (dial-up) с Internet). Поддержание лавины или шторма пакетов достигается за счет большого числа таких относительно медленных соединений.

Злоумышленник использует десятки и сотни незащищенных узлов для координации нападения.

Особая опасность инструментальных средств, реализующих распределенные атаки, в том, что они настолько просты в использовании, что могут быть доступны даже неопытным пользователям (script kiddies), решившим "насолить" своему соседу.

Атаки НСД, построенные по данной схеме, очень трудно обнаружить. Сетевые классические системы обнаружения атак очень неуверенно обнаруживают такие атаки, особенно если соединения между агентами и серверами зашифрованы. Системы обнаружения атак уровня узла более пригодны для этой цели. Опознать такие атаки можно на этапе установки агента. Впоследствии это сделать намного труднее, поскольку агент действует как часть операционной системы (ОС). Особенно опасно внедрение агентов для "открытых" ОС, таких как Windows 95, 98, Linux и OpenBSD, т. к. агент может быть внедрен в ядро ОС, что сделает задачу обнаружения такого агента очень непростой. В традиционной атаке злоумышленнику придется периодически "посещать" скомпрометированный узел (например, по протоколу Telnet). Это может быть замечено путем анализа журналов регистрации или автоматизированными защитными средствами. В случае распределенной атаки такой проблемы не возникает, поскольку агент уже установлен и нет необходимости периодически посещать скомпрометированный узел – все сделает запрограммированный ("зомбированный") агент.

2.6. Результат атаки НСД.

Ниже приводится классификация некоторых результатов атак НСД по материалам [3].

Расширение прав доступа (increased access) – любое несанкционированное действие, приводящее к расширению прав доступа в сети или на конкретном узле Интранет (компьютере, маршрутизаторе и т. д.).

Искажение информации (corruption of information) – любое несанкционированное изменение информации, хранящейся на узлах сети или при ее передаче по сети.

Раскрытие информации (disclosure of information) – распространение информации среди лиц без соответствующих полномочий доступа.

Кража сервисов (theft of service) – несанкционированное использование компьютера или сетевых сервисов без ухудшения качества обслуживания других пользователей.

Отказ в обслуживании (denial of service) – умышленное снижение производительности или блокировка доступа к сети или компьютеру и его ресурсам.

IV Этапы реализации атак НСД

Можно выделить следующие этапы реализации атаки НСД: предварительные действия перед атакой или "сбор информации" (information gathering), "реализация" атаки (exploitation) и "завершение" атаки. Обычно,

когда говорят об атаке НСД, то подразумевают именно второй этап, забывая о первом и последнем. Сбор информации и завершение атаки ("заметание следов"), в свою очередь, также могут являться атакой и соответственно разбиваться на три этапа (предпосылки реализации атаки, реализация атаки, завершение атаки).

Основной этап атаки НСД – это сбор информации. Именно эффективность работы злоумышленника на данном этапе является залогом успешной атаки. В первую очередь выбирается цель нападения и собирается информация о ней (ОС, сервисы, конфигурация и т. д.). Затем идентифицируются наиболее уязвимые места атакуемой системы, воздействие на которые приводит к нужному результату.

На первом этапе злоумышленник пытается выявить все каналы взаимодействия объекта атаки с другими узлами. Это позволит не только выбрать тип реализуемой атаки, но и источник ее реализации. Предположим, атакуемый узел взаимодействует с двумя серверами под управлением ОС Unix и Windows NT. С одним сервером атакуемый узел имеет доверенные отношения, а с другим — нет. В зависимости от того, через какой сервер злоумышленник будет осуществлять нападение, зависит, какая атака будет задействована, какая утилита будет ее реализовывать и т. д. Затем, на основании полученной информации и преследуемого результата, выбирается атака, дающая наибольший эффект. Например, для нарушения функционирования узла можно использовать SYN Flood, Teardrop, UDP Bomb и т. п., а для проникновения на узел и кражи информации — сценарий для кражи узла паролей, удаленного подбора пароля и т. д. Затем приходит очередь второго этапа — реализации выбранной атаки НСД.

Традиционные средства защиты вступают в действие на втором этапе, совершенно "забывая" о первом и третьем. Это влечет за собой то, что зачастую совершаемую атаку очень трудно остановить даже при наличии мощных и эффективных средств защиты. Пример тому – распределенные атаки НСД. Логично было бы, чтобы средства защиты начали работать еще на первом этапе, т. е. предотвращали бы возможность сбора информации об атакуемой системе. Это позволит если и не полностью "обезглавить" атаку, то существенно усложнить работу злоумышленника.

Также традиционные средства не позволяют обнаружить уже совершенные атаки и оценить ущерб после их реализации (третий этап) и, следовательно, нельзя определить меры по предотвращению таких атак впредь.

В зависимости от достигаемого результата нарушитель концентрируется на том или ином этапе. Например, для отказа в обслуживании он в первую очередь подробно анализирует атакуемую сеть и выискивает в ней лазейки и слабые места для атаки на них и выведения узлов сети из строя. Для хищения информации злоумышленник основное внимание уделяет незаметному проникновению на анализируемые узлы при помощи обнаруженных ранее уязвимостей.

Как уже упоминалось выше, не ставилась задача подробного рассмотрения механизмов реализации тех или иных атак НСД. Однако основные механизмы все же рассмотрены, необходимые для понимания метода обнаружения этих атак. Понимание также принципов действий злоумышленников – залог успешной защиты вашей сети Интранет. Рассмотрим более детально три этапа атаки НСД.

3.1. Сбор информации.

Первый этап реализации атак – это сбор информации об атакуемой системе или узле. Он включает такие действия, как определение сетевой топологии, типа и версии операционной системы атакуемого объекта, а также доступных сетевых и иных сервисов и т. п. Эти действия реализуются различными методами.

3.1.1. Изучение окружения.

Выполняя эту задачу, нападающий исследует области вокруг предполагаемой цели атаки. К таким областям относятся, например, узлы interm t-провайдера "жертвы". На этом шаге злоумышленник может пытаться определить адреса "доверенных" систем (например, сети партнера), узлов, которые напрямую соединены с целью атаки (например, маршрутизаторов ISP) и т. д. Такие действия достаточно трудно обнаружить, поскольку они выполняются в течение довольно длительного периода времени и снаружи области, контролируемой средствами защиты (межсетевыми экранами, системами обнаружения атак и т. п.).

3.1.2. Идентификация топологии сети Итранет.

Можно назвать два метода определения топологии сети (network topology detection), используемых злоумышленниками: "изменение TL" ("T'L modulation") и "запись маршрута" ("record route"). Программы tiaceroute для Unix и tracert для Windows используют первый способ определения топологии сети. Они задействуют для этого поле Time to Live ("время жизни") в заголовке IP-пакета, значение которого изменяется в зависимости от числа пройденных сетевым пакетом маршрутизаторов. Утилита ping может быгь использована для записи маршрута ICMP-пакета.

Зачастую сетевую топологию можно выяснить при помощи протокола SNMP, установленного на многих сетевых устройствах, защита которых неверно сконфигурирована. При помощи протокола RIP можно попытаться получить информацию о таблице маршрутизации в сети и т. д.

Многие из упомянутых методов используются современными системами управления для построения карт сетей. И эти же методы могут быть с успехом применены злоумышленниками.

3.1.3. Идентификация узлов сети Интранет.

Идентификация узла (host detection), как правило, осуществляется путем посылки при помощи утилиты ping команды ECHO_REQUEST протокола CMP. Ответное сообщение ECHO_REPLY говорит о том, что узел доступен. Существуют программы, которые автоматизируют и ускоряют процесс параллельной идентификации большого числа узлов, например, fping или tomap. Опасность данного метода в том, что стандартными средствами узла Запросы ECHO_REQUEST не фиксируются. Для этого необходимо применять средства анализа графика, межсетевые экраны или системы обнаружения атак.

Это самый простой метод идентификации узлов. Однако эта легкость имеет ряд недостатков. Во-первых, многие сетевые устройства и программы блокируют ICMP-пакеты и не пропускают их во внутреннюю сеть (или наоборот не пропускают их наружу). Например, MS Proxy Server 2.0 не разрешает прохождение пакетов по протоколу ICMP. В результате возникает неполнота идентификации хостов. С другой стороны, блокировка ICMP-пакета говорит злоумышленнику о наличии "первой линии обороны" – маршрутизаторов, межсетевых экранов и т. д.

Во-вторых, применение ICMP-запросов позволяет с легкостью обнаружить их источник, что, разумеется, не должно входить в задачу злоумышленника.

Существует еще один метод определения узлов сети – использование "смешанного" ("promiscuous") режима сетевого интерфейса, который позволяет определить различные узлы в сегменте сети. Но он неприменим в тех случаях, в которых трафик сегмента сети недоступен нападающему со своего узла, т. е. действует только в локальных сетях. Другим способом идентификации узлов сети является так называемая разведка DNS [3], которая позволяет идентифицировать узлы корпоративной сети при помощи службы имен доменов.

3.1.4. Идентификация сервисов или сканирование портов сети Интранет.

Идентификация сервисов (service detection), как правило, выполняется путем обнаружения открытых портов — сканированием (port scanning). Такие порты очень часто связаны с сервисами, основанными на протоколах TCP или UDP. Например [3], открытый 80-й порт подразумевает наличие Web-сервера, 25-й порт – почтового SMTP-сервера, 31337-й – сервера троянского коня BackOrifice, 12345 – сервера троянского коня NetBus и т. д. Для идентификации сервисов и сканирования портов могут быть использованы различные программы, такие как nmap или netcat.

3.1.5. Идентификация операционной системы сети Интранет.

Основной механизм удаленного определения ОС (OS detection) – анализ TCP/IP-стека. В каждой ОС стек протоколов TCP/IP реализован по-своему, что позволяет при помощи специальных запросов и ответов на них определить, какая ОС установлена на удаленном узле.

Другой, менее эффективный и крайне ограниченный, способ идентификации ОС узлов – анализ сетевых сервисов, обнаруженных на предыдущем этапе. Например, открытый 139-й порт позволяет сделать вывод, что удаленный узел работает под управлением ОС семейства Windows. Для определения ОС могут быть использованы различные программы. Например, nmap [3].

3.1.6. Определение роли узла сети Интранет.

Последним шагом на этапе сбора информации является определение роли узла, например, межсетевого экрана или Web-сервера. Выполняется этот шаг на основе уже собранной информации об активных сервисах, именах узлов, топологии сети и т. п. Например [3], открытый 80-й порт может указывать на наличие Web-сервера, блокировка ICMP-пакета свидетельствует о потенциальном наличии межсетевого экрана, а имя узла proxy.domain.ru или fw.domain.ru говорит само за себя.

3.1.7. Определение уязвимостей узла сети Итранет.

Последняя стадия на этапе сбора информации – поиск уязвимостей (searching vulnerabilities). На этом шаге злоумышленник при помощи различных автоматизированных средств или вручную определяет уязвимости, которые могут быть использованы для реализации атаки. В качестве таких автоматизированных средств могут быть использованы ShadowSecurityScannei nmap, Retina и т. д.

3.2. Реализация атаки НСД.

С этого момента начинается попытка доступа на атакуемый узел Интранет. При этом доступ может быть как непосредственный, т. е. проникновение на узел, так и опосредованный, как при реализации атаки типа "отказ в обслуживании".

Реализация атак в случае непосредственного доступа также может быть разделена на два этапа: проникновение; установление контроля.

3.2.1. Проникновение атаки НСД.

Проникновение подразумевает под собой преодоление средств защиты периметра (например, межсетевого экрана). Реализовываться это может различными путями. Например, использованием уязвимости сервиса компьютера, "смотрящего" наружу, или путем передачи враждебного содержания по электронной почте (макровирусы) или через апплеты Java [3, 19]. Такое содержание может задействовать так называемые "туннели" в межсетевом экране (не путать с туннелями VPN), через которые затем и проникает злоумышленник. К этому же шагу можно отнести подбор пароля администратора или иного пользователя при помощи специализированной утилиты (например, LOphtCrack или Crack).

3.2.2. Установление контроля атаки НСД.

После проникновения злоумышленник устанавливает контроль над атакуемым узлом. Это может быть осуществлено путем внедрения программы типа "троянский конь" (например, NetBus или BackOrifice [3]). После установки контроля над нужным узлом и "заметания" следов злоумышленник может производить все необходимые несанкционированные действия дистанционно без ведома владельца атакованного компьютера. При этом установление контроля над узлом корпоративной сети должно сохраняться и после перезагрузки операционной системы. Это может быть реализовано путем замены одного из загрузочных файлов или вставкой ссылки на враждебный koj. в файлы автозагрузки или системный реестр. Известен случай, когда злоумышленник смог перепрограммировать EEPROM сетевой карты и даже после переустановки ОС он смог повторно реализовать несанкционированные действия. Более простой модификацией этого примера является внедрение необходимого кода или фрагмента в сценарий сетевой загрузки (например, для ОС Novell NetWare).

3.2.3. Цели реализации атак НСД.

Необходимо отметить, что данный этап может преследовать две цели. Во-первых, получение несанкционированного доступа к самому узлу Интранет и содержащейся на нем информации. Во-вторых, получение несанкционированного доступа к узлу для осуществления дальнейших атак на другие узлы Интранет. Первая цель, как правило, достигается только после реализации второй. То есть, сначала злоумышленник создает себе базу для дальнейших атак и только после этого проникает на другие узлы. Это необходимо для того, чтобы скрыть или существенно затруднить нахождение источника атаки НСД.

Различных атак может быть большое множество, и в данной книге они в полном объеме рассматриваться не будут. Для более глубокого изучения различных атак можно порекомендовать [4].

3.2.4. Методы реализации атак НСД.

Если нарушитель имеет физический доступ к компьютеру, он сможет проникнуть в него или провести на него атаку. Методы могут быть разными – от использования специальных привилегий, которые имеет консоль или терминал, до процедуры снятия жесткого диска и его чтения/записи на другом компьютере [12]. Это – физическое вторжение.

Системное вторжение – тип несанкционированной деятельности, предполагающий, что нарушитель уже имеет учетную запись в атакуемой системе как пользователь с некоторыми (обычно невысокими) привилегиями. Если в системе не установлены самые последние "заплаты", то у нарушителя есть хороший шанс попытаться реализовать известную атаку для получения дополнительных административных полномочий.

Несанкционированная деятельность удаленного вторжения подразумевает, что нарушитель пытается дистанционно проникнуть в систему через сеть. При этом нарушитель действует без каких-либо специальных привилегий. Существует несколько типов такой деятельности [20]:

локальное сетевое вторжение, при котором злоумышленник атакует компьютер или группу компьютеров, находящихся в одном с ним сегменте;

вторжение через сети открытого доступа, при котором злоумышленник атакует компьютер или группу компьютеров, находящиеся в другое сегменте; при этом атака НСД осуществляется через сети открытого доступа, как правило, через Internet;

вторжение через Dial-up, при котором злоумышленник агакует компьютер или группу компьютеров через модем.

Пример № 2. Компьютеры NASA. В 1997 хакер подверг смертельной опасности астронавтов во время стыковки в космосе американского шаттла Atlantis и росийской станции Мир. Была на время прервана связь между центром управления полетом, астронавтами и медицинским оборудованием, следящим за здоровьем астронавтов (связь была восстановлена через станцию Мир). До сих пор эта информация оставалась неизвестной для широкой общественности. В NASA после этого было создано собственное подразделение кибер-полиции для борьбы с такими атаками НСД [3].

3.3. Завершение атаки НСД.

Этапом завершения атаки является "заметание следов" со стороны злоумышленника. Обычно это реализуется путем удаления соответствующих записей из журналов регистрации узла и выполнением других

действий, возвращающих атакованную систему в исходное состояние.

V Сокрытие источника и факта атаки НСД

Одна из целей обнаружения атак заключается в том, чтобы идентифицировать того, кто вас атакует. Эта задача может оказаться очень трудной, т. к. часто злоумышленники используют различные способы сокрытия своей несанкционированной деятельности. К таким способам можно отнести [12, 3]:

подмена адреса источника атаки НСД; создание фальшивых пакетов трафика; использование чужих компьютеров в качестве базы для атаки НСД; фрагментация атаки НСД; шифрование атаки НСД; отказ от значений по умолчанию (as default); изменение стандартного сценария атаки НСД; замедление атаки НСД; чистка журналов регистрации; скрытие файлов и данных; скрытие процессов.

Рассмотрим эти способы атак НСД более детально.

4.1. Подмена адреса источника атаки НСД.

Большинство злоумышленников организуют свои атаки промежуточных серверов, которые они уже взломали, или с proxy-серверов. Таким образом, найти того, кто атакует ваш узел, будет очень трудно. При этом, чем больше промежуточных узлов использует злоумышленник, тем сложнее его обнаружить и наказать. Мало того, активное блокирование атак с помощью межсетевых экранов, фильтров на маршрутизаторах и других устройствах может привести к отрицательному результату, т. е. к тому, что вы заблокируете не злоумышленника, а вполне реальный адрес (возможно, принадлежащий вашему клиенту или партнеру), которому необходим доступ к информационным ресурсам Интранет организции.

4.2. Создание фальшивых пакетов НСД.

Сканер nmap имеет возможность обманного (decoy) сканирования, когда вместо реальных IP-адресов источника проставляются (подменяются) другие IP-адреса. Тем самым перед администратором Интранет обнаружения атак ставится непростая задача: обнаружить среди множества зафиксированных в журналах регистрации IP-адресов только один реальный, с которого действительно производилось сканирование.

4.3. Фрагментация атаки НСД.

Фрагментация — механизм разбиения IP-пакета на множество более мелких. При получении таких пакетов TCP/IP-устройство собирает эти пакеты и передает конечному приложению или повторно фрагментирует их и передает дальше. Большинство современных систем обнаружения атак не имеет механизма дефрагментации IP-пакетов. Эти системы пропускают такого рода пакеты (возможно, выдавая на консоль администратора соответствующее сообщение об обнаружении фрагментированных пакетов). Зафиксированы отдельные случаи, когда системы обнаружения атак "падали" от фрагментированных атак. Следовательно, имеется возможность обойти эти системы при помощи специальных средств (например, fragrouter).

4.4. Отказ от значений атаки НСД по умолчанию.

Очень часто механизмы обнаружения атак исходят из предположения, что порт однозначно идентифицирует протокол или сервис. Например [3], порт 80 относится к протоколу HTTP, порт 25 – к протоколу SMTP, порт 23 – к протоколу Telnet, порт 31337 – к "троянцу" BackOrifice, и т. д. Злоумышленники пользуются этим и могут задействовать стандартные протоколы на нестандартных портах. Например, злоумышленник может заменить значение по умолчанию для BackOrifice (31337) на 31338. В результате многие механизмы обнаружения атак дадут сбой в этом случае и не смогут обрабатывать такой "непривычный" для них трафик.

4.5. Изменение стандартного сценария атаки НСД.

Многие механизмы обнаружения атак работают по принципу сопоставление с образцом (шаблоном). Использование баз данных известных атак позволяет обнаруживать атаки с высокой степенью достоверности. Однако от таких систем можно очень легко уклониться, немного изменяя шаблон. Частным примером такой маскировки является отказ от значений as default. Другой пример – замена символа пробела в действиях, реализующих команду, на символ табуляции.

4.6. Замедление атаки НСД.

Из-за большого объема регистрируемых данных механизмы обнаружения атак неэффективно отслеживают атаки, растянутые во времени. Таким образом, трудно обнаруживать "распределенное по времени сканирование" (pin sweep или port scan), при котором нарушители проверяют один юрт/адрес каждые 5 минут или даже каждый час. Это замедление существенно затрудняет диагностику атаки современными средствами обнаружения атак НСД.

4.7. Чистка журналов регистрации атак НСД.

Достаточно распространенный способ, заключающийся в удалении всех записей журнала регистрации, фиксирующих произведенные несанкционированные действия. Это позволяет скрыть от администратора атакованной системы все следы подозрительной деятельности.

4.8. Скрытие файлов и данных по атакам НСД.

Скрытие файлов и данных очень часто используется для того, чтобы замаскировать несанкционированную деятельность злоумышленника. При этом могут быть применены совершенно различные методики, различающиеся по сложности реализации. Например, установка атрибута Hidden на файл, внедрение вредоносного кода в ядро ОС (для Unix-подобных систем) или присоединение такого кода к какому-либо исполняемому файлу или библиотеке. По последнему принципу очень часто реализуется распространение "троянцев" – к обычному исполняемому файлу (например, игре) присоединяется код "троянского коня", автоматически внедряющего себя в систему, в которой запускается измененный исполняемый файл.

4.9. Скрытие процессов по атакам НСД.

Аналогично предыдущему примеру, данный метод используется для скрытия деятельности злоумышленника на атакуемом узле Интранет. Для этого может быть также проведено изменение ядра ОС или ее специальных утилит, отвечающих за работу с процессами (например, утилиты ps в Unix) Примером такого сокрытия является использование комплекта rootkit для ОС SunOS. Этот комплект, позволяющий перехватывать различные данные, подменять контрольные суммы файлов и т. д., изменял некоторые системные утилиты (login, ls, ifconfig, ps, netstat, du), что не позволяло обнаружить его присутствие. Самым простым методом скрытия несанкционированной деятельности процесса является изменение его имени на "стандартное" или похожее на стандартное. Например, враждебный процесс может иметь имя in.netd, iexplore.exe (на узле с не установленным MS Internet Explorer) или NDDAGNT.EXE (очень похожее на NDDEAGNT.EXE).

VI Классификация атак НСД

Существуют различные типы классификации атак НСД. Однако, чтобы не запутать читателя большим разнообразием классификаций, мало применимых на практике, представим следующую классификацию атак НСД, наиболее применимых, по нашему мнению, и для корпоративных сетей Интранет [3].

Удаленное проникновение (remote penetration). Атаки, которые позволяют реализовать удаленное управление компьютером через сеть. Примером такой программы является NetBus или BackOrifice.

Локальное проникновение (local penetration). Атака, приводящая к получению несанкционированного доступа к узлу, на котором она запущена. Примером такой программы является GetAdmin.

Удаленный отказ в обслуживании (remote denial of service). Атаки, которые позволяют нарушить функционирование системы или перегрузить компьютер через Internet. Примером такой атаки является Teardrop ил1 trin00.

Локальный отказ в обслуживании (local denial of service). atikh, позволяющие нарушить функционирование системы или перегрузить компьютер, на котором они реализуются. В качестве примера такой атаки можно привести враждебный апплет, который загружает центральный процессор бесконечным циклом, что приводит к невозможности обработки запросов других приложений.

Сетевые сканеры (network scanners). Программы, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки. Примером такой программы можно назвать систему nmap.

Сканеры уязвимостей (vulnerability scanners). Программы, осуществляющие поиск уязвимостей на узлах сети и которые могут быть использованы для реализации атак. Примеры: система SATAN или ShadowSecurityScanner.

Взломщики паролей (password crackers). Программы, которые подбирают пароли пользователей. Примером взломщика паролей может служить LOphtCrack для Windows или Crack для Unix.

Анализаторы протоколов (sniffers). Программы, которые "прослушивают" сетевой трафик. При помощи этих программ можно автоматически искать такую информацию, как идентификаторы и пароли пользователей, информацию о кредитных картах и т. д. Анализатором протоколов можно назвать Microsoft Network Monitor, NetXRay компании Network Associates или LanExplorer.

Компания Internet Security Systems, Inc. еще больше сократила число возможных категорий, доведя их до 5 [13]: сбор информации (Information gathering); попытки НСД (Unauthorized access attempts); отказ в обслуживании (Denial of service); подозрительная активность (Suspicious activity); системные атаки (System attack).

Первые четыре категории относятся к удаленным атакам, а последняя –к локальным, т. е. реализуемым на атакуемом узле Интранет. Можно заметить, что в данную классификацию не попал целый класс так называемых "пассивных" атак. Помимо "прослушивания" графика в эту категорию также попадают такие атаки, как "ложный DNS-сервер", "подмена ARF-сервера" [4].

VII Инциденты атак НСД

Инцидент – более высокий уровень описания нарушений политики безопасности. Инцидент – это группа атак, связанных между собой по различным параметрам. Например, по адресату атаки или достигаемой цели и т. д. Именно на этом уровне появляется понятие "источник атаки", которое отсутствовало в других моделях.

Инцидент может быть реализован как при помощи всего одно й атаки, так и при помощи нескольких следующих друг за другом или параллельно атак. Успех нападения определяется достижением цели злоумышленником. Неудача нападения означает, что злоумышленник не достиг ни одной поставленной задачи. Однако жертва остается жертвой и в этом случае – какие-либо последствия возможны и здесь.

Как показывает статистика, количество инцидентов, связанных с безопасностью, растет пропорционально расширению Internet и Intranet. Интерес к электронной коммерции только усилит этот рост в последующие годы. Отмечена и другая тенденция. В 80-х – начале 90-х гг. внешние злоумышленники атаковали узлы Internet из любопытства или для показа своей квалификации. Сейчас атаки преследуют чаще всего финансовые или политические цели. Как показано в [3], число успешных проникновений в информационные системы возросло вдвое – с 12% в 1998 году до 23% в 1999 году.

Существенно меняется и квалификация злоумышленников. Если в 80-х годах это были эксперты в области информационных технологий, досконально знающие ОС Unix, язык С или Peri и лично создающие новые сценарии атак, то сейчас ситуация в корне изменилась. Современные злоумышленники в большинстве своем пользуются уже готовым инструментарием, обладающим удобным графическим интерфейсом. По некоторым данным число таких "хакеров", называемых script kiddies, достигает 95%. Создание новых сценариев – удел единиц. Сегодня любой пользователь, имеющий выход в Internet, Intranet может напасть на своего "соседа" и причинить последнему немалый ущерб.

Раньше злоумышленник вручную вводил команды на своем компьютер и не мог физически обратиться больше чем к десятку или сотне удаленных систем. Сейчас вы можете одновременно атаковать тысячи и десятки тысяч узлов, нажав всего одну кнопку. В прежние годы достаточно "просто" можно было обнаружить взломщика, "промышляющего" в ваших системах. Сегодня это крайне сложно. Он может проникнуть к вам, реализовать атаку и "скрыться с места происшествия" в течение нескольких секунд, заодно "подчистив" за собой все следы. Атаки типа "отказ в обслуживании" в былые годы не пользовались большой популярностью и им не придавали большого значения. Ныне ситуация изменилась.

6.1. Нарушители.

Атакующий, т. е. инициатор атаки НСД, является самым первым элементом атаки. Данный элемент может быть описан при помощи так называемой неформальной модели нарушителя, которая отражает его практические и теоретические возможности, априорные знания, время и место действия, квалификацию и т. п. Атакующий может быть один или их может быть несколько.

Всех атакующих можно разделить на 6 категорий [17, 3].

Хакеры (hackers) – осуществляют атаки с целью самоудовлетворения, повышения собственной значимости в глазах других и т. п. То есть материальной выгоды от атаки хакеры не получают.

Шпионы (spies) – организуют атаки для получения информации, которая может быть использована для каких-либо политических целей.

Террористы (terrorists) – осуществляют атаки с целью шантажа.

Охотники за промышленными секретами (corporate raiders) – осуществляют атаки для получения промышленных секретов, кража которых приносит существенную финансовую выгоду для конкурента.

Профессиональные преступники (professional criminals) – осуществляют атаки с целью получения личной финансовой выгоды.

Вандалы (vandals) – осуществляют атаки с целью нанесения ущерба.

Наибольшую известность получили следующие категории нарушителем – хакеры и профессиональные преступники. Первые за счет того, что они сами, как правило, афишируют удачно осуществленные ими атаки. Вторые – благодаря прессе, кино и телевидению. На самом деле до сих пор существует путаница в понимании термина "хакер". Рядовой обыватель не без помощи средств массовой информации понимает под этим специалистов, преследующих "дурные" цели, в то время как на самом деле этим термином обозначаются просто высококвалифицированные специалисты в области информационных технологий. Наиболее приемлемым является термин "злоумышленник".

В 60 – 70-х годах хакерами называли людей, которые создавали программы или фрагменты программ, заставляющие аппаратное обеспечение выполнять функции, обычно ими не выполняемые [3, 18]. То есть имела место некая игра ума, интеллектуальные упражнения. Потом этим термином стали называть высококвалифицированных специалистов. Они обменивались между собой особо изящными трюками, тем

самым заявляя о себе среди себе подобных. В конце 70-х – начале 80-х годов эта традиция стала извращаться, и хакеры стали не только делиться своими достижениями, но и проникать в информационные системы, оставляя свои "визитные карточки". Зачастую после таких визитов системы уже не могли в полном объеме выполнять свои функции. Именно тогда термин "хакер" получил негативный смысл. Помимо "хакеров" существуют еще "крекеры" (crackers), "фикеры" (phieakers) и т. д.

6.2. Цели злоумышленников.

На основе описанных категорий злоумышленников в таблице 4 выделяются следующие мотивы, которые они преследуют [3].

Таблица 4 – Мотивы злоумышленников

Цель	Нарушение доступности	Нарушение конфиденциальности	Нарушение целостности
Любопытство		+	
Вандализм	+		+
Месть	+		+
Финансовая выгода			+
Конкурентная выгода	+	+	+
Сбор информации		+	
Военная или политическая выгода	+	+	+

VIII Выводы

1. Мы попытались свести воедино имеющиеся данные об атаках, атакующих (злоумышленниках) и распространить их на атаки НСД как наиболее потенциальные и обобщенные деструктивные действия. Дело в том, что в западных критериях компьютерной безопасности (американские критерии TCSEC, 1983 г., европейские критерии ITSEC, 1991 г.) уже давно ее оценивали тремя классами (уровнями) по степени защищенности всей компьютерной системы именно от угроз НСД – минимальный рейтинг защиты от НСД (классы C2 по TCSEC, F-C2 по ITSEC), относительно стойкая защита от НСД (классы B2 по TCSEC, F-B2 по ITSEC) и стойкая защита от НСД (классы B3 по TCSEC, F-B3 по ITSEC).

2. Приведенная систематизация дает необходимый базис для понимания технологий обнаружения атак НСД. Как было показано, не будь уязвимостей в компонентах корпоративных сетей Интранет, нельзя было бы реализовать многие атаки НСД и, следовательно, традиционные средства защиты вполне эффективно справлялись бы с возможными атаками. Однако программы пишут люди, которым свойственно делать ошибки. Вследствие чего и появляются уязвимости, которые используются для реализации атак НСД. Однако это только полбеды. Если бы все атаки НСД строились по модели "один – к одному", то с некоторой натяжкой фильтрующие маршрутизаторы, межсетевые экраны и другие традиционные защитные средства смогли бы противостоять и им. Но появились скоординированные атаки, против которых традиционные методы защиты уже не так эффективны. Поэтому появляются новые методы защиты, основанные на технологии обнаружения атак вообще и атак НСД в частности.

3. Суть предложенного перспективного метода защиты можно сформулировать следующим концептуальным правилом адаптивной безопасности информационных ресурсов Интранет MAMPDA-1: если мы не можем построить абсолютно защищенную корпоративную систему, то хотя бы должны обнаруживать все (или практически все) нарушения политики безопасности и соответствующим образом (адаптивно) реагировать на них.

*Литература: **1**. В. Шорошев, Е. Маевский. Брандмауэры – основа защиты корпоративных сетей Интранет. Бизнес и безопасность. N6, 2002; **2**. Шорошев В. В. Недостатки традиционных средств защиты корпоративных сетей Интранет и необходимость применения новых методов их защиты. Бизнес и безопасность № 2, 2003; **3**. Лукацкий А. В. Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.: ил.; **4**. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Интернет. М.: ДМК, 1999; **5**. Taimur Aslam, Ivan Krsul, Eugene H. Spafford. Use of A Taxonomy of Security Faults. CJAST Laboratory. 1996; **6**. Анализ защищенности: сетевой или системный уровень? Руководство по выбору технологии анализа защищенности. Internet Security Systems, 1999. Перевод с англ. Лукацкого А.В. и Цаплева Ю. Ю.; **7**. How To Tliminate The Ten Most Critical Inernet Security Threats. Version 1.32. SANS. January 18, 2001; **8**. Chris Klaus. Top Threats Facing Inernet Security Today. ISS Connect 2000. 19-24, March, 2000; **9**. Andrew J. Stewart.*