УДК 681.3

Хорошко В.А., Шорошев В.В.

НЕДОСТАТКИ ТРАДИЦИОННЫХ СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ ИНТРАНЕТ И НЕОБХОДИМОСТЬ ПРИМЕНЕНИЯ НОВЫХ МЕТОДОВ ИХ ЗАЩИТЫ

Обнаружение атак несанкционированного доступа (атак НСД) – новый и довольно актуальный механизм защиты, который в настоящее время применяется не только в области информационной безопасности. Он находит широкое применение и в охранной сигнализации, и в системах обнаружения телефонного или финансового мошенничества, и для обнаружения атак НСД в банкоматах, и т.д. Однако в статье будут рассматриваться только проблемные вопросы, связанные с неоходимостью перехода к новой концепции безопасности путем создания мониторингово-адаптивных систем обнаружения и нейтрализации, прежде всего, атак НСД на корпоративные сети Интранет, имеющих постоянное или временное соединение с глобальной информационной супермагистралью Интернет.

Дело в том, что абсолютное большинство публикаций описывают традиционные, претендующие на универсальность, защитные механизмы и средства. Например, рассматриваются механизмы и системы санкционированного разграничения доступа пользователей, защитные межсетевые экраны (брендмауэры), фильтрующие маршрутизаторы, идентификация и аутентификация пользователя, криптографические и даже стеганографические методы защиты информации и др. Но пока очень мало публикаций по реализации защиты от атак НСД с использованием нормативных требований отечественных критериев защищенности информации в компьютерных системах разных классов и подклассов, а также с использованием перспективных радиоизотопных методов защиты материальных носителей информации и элементов конфигурации корпоративных компьютерных систем.

Представляют интерес новые технологии, о которых до недавнего времени практически ничего не известно [2, 4, 5]. К таким технологиям можно отнести механизмы активной безопасности информации в компьютерных системах на основе адаптивно-мониторингового контроля выполнения всех требований выбранной политики безопасности. К ним можно отнести, например, использование экспертных систем искусственного интеллекта, в частности, для анализа и количественной оценки реализованных по требованиям отечественных нормативных документов механизмов функциональной (четыре услуги безопасности типа К, Ц, Д, Н) и гарантийной (семь уровней гарантии Г-1…Г-7) защищенности информации в компьютерных системах. К таким относятся КС 1, 2, 3 класса и подклассов К (повышенные требования к защите от угроз конфиденциальности), Ц (повышенные требования к защите от угроз целостности), Д (повышенные требования к защите от угроз доступности), КЦ (повышенные требования к защите от угроз конфиденциальности и целостности), КД (повышенные требования к защите от угроз конфиденциальности и доступности), ЦД (повышенные требования к защите от угроз целостности и доступности), КЦД (повышенные требования к защите от угроз конфиденциальности, целостности и доступности). Требования наблюдаемости Н информации и ресурсов КС являются обязательными для реализации услуг безопасности типа К, Ц, Д и их сочетаний. При этом приоритетным направлением является обязательное выполнение регламентированных требований некоторой совокупности частных критериев функциональной и гарантийной защищенности информации (их всего 110, в том числе критериев К – 17, Ц – 13, Д – 12, Н - 26, Г1…Г7 - 42). Но все они должны реализоваться в автоматизированных (компьютерных) системах согласно требованиям действующих нормативных документов Департамента СТСЗИ Службы безопасности Украины [3].

Отечественных публикаций на поднятую тему не так уж и много. Большинство из них вкратце представляют тот или иной механизм или продукт, их реализующий, не охватывая

целиком взаимосвязь всех компонентов адаптивной безопасности для конкретных объектов защиты, угроз и политик безопасности. Одна из трудностей, которая предстает перед пользователем, выбирающим систему обнаружения атак или анализа защищенности, заключается в том, чтобы отделить зерна истины от плевел рекламы. Ведь не секрет, что цель абсолютного большинства поставщиков средств защиты – это продать как можно больше предлагаемых ими средств. Именно поэтому очень сильно раздувается мыльный пузырь рекламных обещаний, которые не всегда соответствую действительности. А поскольку технология обнаружения, анализа и количественной оценки атак НСД еще незрела, то перед ее потребителем становится задача не запутаться в разнообразии средств и предложений и выбрать именно то, что является предпочтительным для заказчика.

Материал статьи ориентирован на специалистов-практиков, которым по долгу службы приходится обеспечивать безопасность информации в корпоративны сетях своих организаций. В первую очередь, - это администраторы безопасности, а также системные и сетевые администраторы. Именно они сталкиваются с различными нарушениями информационной безопасности. Только они занимаются конфигурацией средств защиты.

Необходимость технологии обнаружения атак НСД к информации компьютерных систем обусловливается такими статистическими данными, полученными Институтом Компьютерной Безопасности (CSI) и группой компьютерных нападений отделения ФБР в Сан-Франциско, опубликованных в отчете “2000 Computer Crime and Security Survey”. Согласно этим данным [1]:

90% респондентов (крупные корпорации и государственые организации) зафиксировали различные атаки на свои информационыые ресурсы;

70% респондентов зафиксировали серьезные нарушения политики безопасности, например, вирусные атаки, атаки типа «отказ в обслуживании, злоупотребления со стороны сотрудников и т. д.;

74% респондентов понесли немалый финансовый урон вследствие этих нарушений.

Объем потерь вследствие нарушений политики безопасности также возрос за последние годы. Если в 1999 году сумма ущерба равнялась 124 миллионам долларов, в 2000 году до 266 миллионам долларов, то в 2002 году более 510 долларов. При этом размер убытков от атак типа «отказ в обслуживании» достиг более 16 миллионов долларов США. К другим интересным данным [5] можно отнести информацию об источниках атак (табл. 1) и размерах потерь от них (табл. 2).

Из анализа приведенных данных следует, что поскольку число, разнообразие и частота атак все время увеличивается, становится очень важным идентифицировать атаки, прежде всего, на раннем этапе их развития, а также своевременно среагировать на них. В лучшем случае, - это для блокирования атак или, что тоже приемлемо при непрерывно совершенствующихся технологиях атак, для максимального снижения ущерба от них. Кардинальным средством решения этой проблемы является автоматизация защиты от подобных атак.

Таблица 1
Источники атак

Источник атак (название)	**Источник атак (%)**
Недобросовестные сотрудники	81
Хакеры	77
Конкуренты	44
Зарубежные компании	26
Зарубежные правительства	21

Таблица 2
Частота обнаружения атак

Тип атаки	Частота обнаружения, (%)
Компьютерные вирусы	85
Злоупотребления сотрудников в Интернет	79
Несанкционированный доступ сотрудников	71
Отказ в обслуживании	27
Атаки внешних злоумышленников	25
Кража конфиденциальной информации	20
Саботаж	17
Финансовые мошенничества	11
Мошенничества по телекоммуникациям	11

Во-первых, в критических ситуациях вмешательство в атаку должно быть реализовано намного быстрее, чем сможет среагировать человек. Другая причина для автоматизации процесса обнаружения атак заключается в том, что все чаще и чаще злоумышленники используют автоматизированные средства реализации атак. Так, например, был отмечен случай осуществления 2000 попыток проникновения на сервер Интернет из 500 мест в течение 8 часов, т. е. 4 атаки в минуту. И только автоматизированная система обнаружения атак помогла отследить источник атаки. В ее отсутствие задача обнаружения самой атаки и злоумышленника, ее реализующего, стала бы просто невозможной.

Существует и российская статистика в данной области [5]. И хотя она неполна и, по мнению многих специалистов, является лишь верхушкой айсберга, все же она весьма показательна. За 2000 год, по статистике МВД, было зарегистрировано 1375 компьютерных преступлений, По сравнению с 1999 годом эта цифра выросла более чем в 1,6 раза. По данным управления по борьбе с организованной преступностью в сфере высоких технологий МВД РФ больше всего преступлений - 584 от общего количества – относятся к неправомерному доступу к компьютерной информации. Далее 258 случаев – это причинение имущественного ущерба с использованием компьютерных средств, затем 172 преступления связаны с созданием и распространением различных вирусов или по принятой терминологии в МВД РФ - «вредоносных программ для ЭВМ». Остальные: 101 преступление из серии «незаконное производство или приобретение с целью сбыта технических средств для незаконного получения информации», 210 – случаи мошенничества с применением компьютерных и телекоммуникационных сетей, 44 – нарушения правил эксплуатации ЭВМ и их сетей.

Информация компьютерных систем должна быть защищена от любых атак. С этим тезисом никто не спорит. Обеспечить же безопасность можно двумя кардинальными способами. Первый способ - предотвратить все попытки несанкционированного доступа. Второй способ – создать полностью безопасную систему. Однако на практике это неосуществимо по ряду причин.

Во-первых, создать абсолютно защищенную компьютерную систему невозможно по причине наличия в программном обеспечении различных ошибок. Программное обеспечение, свободное от ошибок, все еще является мечтой. Да и практика такова, что даже производители brandname не всегда пытаются разработать такое программное обеспечение. Как правило, в острой конкурентной борьбе они стремятся выпустить свой продукт как можно быстрее и получить при этом максимальную прибыль. Но самое интересное, что наличием различных ошибок страдают и сами средства защиты. Особенно это проявилось в 2000 году, когда не проходило недели, чтобы не появилось сообщение об обнаружении уязвимости в межсетевых экранах (брендмауэрах), серверах аутентификации, серверах безопасности и т. д.

Во-вторых, даже самая защищенная компьютерная система уязвима перед хакерами и другими высокопрофессиональными пользователями. Привилегированные пользователи также могут нарушить требования политики безопасности, что может привести к снижению уровня защищенности.

В-третьих, универсальных систем защиты не существует, потому что каждая система защиты создается под конкретные объекты защиты, угрозы и политику безопасности.

И наконец, срабатывает принцип бумеранга - чем защищеннее система, тем неудобнее с ней работать, тем вероятнее могут быть отдельные, казалось бы мелкие, но все же нарушения политики безопасности (усталость пользователя, притупление бдительности, отступления в повторяемых операциях и т. д.).

Таким образом, мы приходим к необходимости использования мониторингово-адаптивного метода защиты путем обнаружения атак НСД (МАМЗОА) - если мы не можем построить абсолютно защищенную компьютерную систему, то хотя бы должны обнаруживать все (или практически все) нарушения политики безопасности и соответствующим образом реагировать на них.

Для любой компании и организации существует своя типовая компьютерная (в общем случае информационная или автоматизированная) система, состоящая из компонент, решающих свои специфические задачи, но в общем случае компьютерная система включает в себя 4 уровня (рис.1).

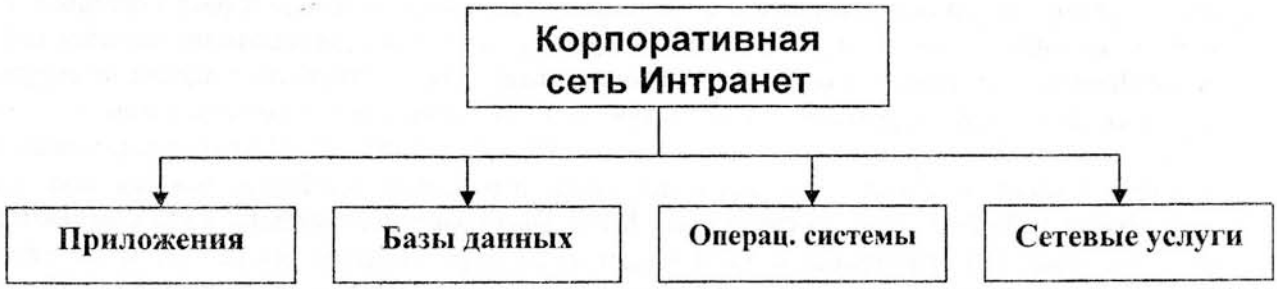

Рис.1. Уровни корпоративной сети Интранет

Уровень прикладного программного обеспечения, отвечающий за взаимодействие с пользователем. Примером элементов компьютерной системы, работающей на этом уровне, можно назвать текстовый редактор WinWord, редактор электронных таблиц Excel, почтовую программу Outlook Express, системы MS Query и т. д.

Уровень системы управления базами данных (СУБД), отвечающий за хранение и обработку данных компьютерной системы. Примером элементов компьютерной системы, работающих на этом уровне, можно назвать СУБД Oracle, MS SQL Server, Sybase, MS Access.

Уровень операционной системы (ОС), отвечающий за обслуживание СУБД и прикладного программного обеспечения. В качестве примеров элементов компьютерной системы этого уровня можно привести ОС MS Windows 98, 2000, NT, Sun Solaris, Novell NetWare.

Уровень сети, отвечающий за взаимодействие узлов компьютерной системы. Для этого уровня характерными примерами соответствующих элементов компьютерной системы являются модули, взаимодействующие по протоколам TCP/IP, IPS/SPX или SMB/NetBIOS.

У злоумышленников имеется широчайший спектр возможностей по нарушению политики безопасности, которые могут быть осуществлены на всех четырех вышеназванных уровнях компьютерной системы.

Например, для получения несанкционированного доступа к информации в СУБД MS SQL Server злоумышленник может реализовать одну из следующих возможностей:

1. Прочитать записи базы данных при помощи SQL-запросов через программу MS Query или через редактор MS Excel, которые позволяют получить доступ к записям СУБД (уровень прикладного программного обеспечения);

2. Прочитать нужные сведения средствами самой СУБД (уровень СУБД);

3. Прочитать файлы базы данных, обращаясь непосредственно к файловой системе (уровень ОС);

4. Перехватить передаваемые по сети данные (уровень сети).

А теперь кратко рассмотрим недостатки традиционных средств защиты от атак НСД по данным статистики, ибо статистика - вещь упрямая. Особенно когда дело касается информационной безопасности. И статистика эта очень неутешительная.

По данным Национального отделения ФБР по компьютерным преступлениям от 85% до 95% нападений на корпоративные сети не то что блокируются, но и не обнаруживаются. Проведенные испытания защищенности корпоративных сетей, которые финансировало Министерство обороны США, показало следующие результаты, сходные с теми, которые были получены и агентством DISA [5].

Специальные группы экспертов, так называемые «команды тигров» (tiger team), провели анализ защищенности 8932 военных информационных систем. В 7860 (т. е. 88%) случаях проникновение в святая святых Министерства Обороны США было успешным. Администраторы безопасности только 390 из этих систем обнаружили атаки НСД и всего 19 из них (вдумайтесь в это число) своевременно сообщили о нападениях. Итак, только 5% защищенных систем смогли зафиксировать атаки на себя и только 0,24% от общего числа атакованных систем (4,9% от числа зафиксировавших атаки) сообщили о них в соответствующие инстанции [5, 6].

Почему это произошло? На наш взгляд, причина кроется не в том, что традиционные средства защиты, такие как разграничение доступа, фильтрация, идентификация, аутентификация и другие не лишены недостатков, а потому, что при их создании не были учтены многие аспекты, связанные с современными атаками НСД. Проанализируем их и на этой основе рассмотрим проблемы, существующие у традиционных средствах защиты, а также возможные пути решения этих проблем [2 - 6].

Недостатки традиционных средств защиты

Рассмотрим для этого этапы осуществления атаки НСД.

Первый, подготовительный, этап заключается в поиске предпосылок для осуществления той или иной атаки. На этом этапе ищутся уязвимости, использование которых обеспечивает возможность в принципе реализовать атаку НСД, которая и составляет второй этап. На третьем этапе атака завершается, «заметаются» следы и т. д. При этом первый и третий этапы сами по себе могут являться атаками. Например, поиск нарушителем уязвимостей при помощи сканеров безопасности, скажем, nmap или SATAN, сам по себе считается атакой.

Существующие средства защиты, реализованные в межсетевых экранах (firewall), серверах аутентификации, системах разграничения доступа и т. д., работают только на втором этапе. По существу они являются средствами блокиро́вки, а не упреждения атаки. В абсолютном большинстве случаев они защищают от атак, которые уже находятся в процессе осуществления. И даже если эти средсва смогли предотвратить ту или иную атаку НСД, то намного было бы эффективнее упреждение этих атак, устранение самих предпосылок реализации вторжений. Одно бесспорно, что система обеспечения информационной безопасности должна работать на всех трех этапах обнаружения атаки. И обеспечение адекватной, а лучше адаптивно-мониторинговой, защиты на третьем, завершающем, этапе не менее важно, чем на первых двух. Ведь только в этом случае предоставляется возможным реально оценить возможный ущерб от «успешной» атаки, а также разработать адаптивные меры по устранению дальнейших попыток реализовать аналогичную атаку.

Однако даже если наряду с традиционными методами защиты вы используете средства поиска уязвимостей, которые своевременно обнаруживают и рекомендуют меры по устранению слабых мест в системе защиты, то это еще не гарантирует вашу защищенность. Дело в том, что существует еще ряд факторов, которые необходимо учитывать при использовании популярных в настоящее время межсетевых экранов, систем идентификации и аутентификации, систем разграничения доступа и т. д. Эти факторы характеризуют не слабости упомянутых технологий, а особенности их архитектуры. Большинство систем защиты корпоративных компьютерных систем построено на классических моделях разграничения доступа (дискреционных, мандатных, верифицированных и др.), разработанных еще в 70-х, 80-х годах.

Согласно этим моделям субъекту (пользователю, программе, процессу или сетевому пакету) разрешается или запрещается доступ к какому-либо объекту защиты (файлу, каталогу или папке, узлу сети, домену и т.д.) при предъявлении некоторого уникального персонифицированного элемента санкционированного доступа. В 80% случаев этот элемент – пароль. В других случаях таким уникальным элементом санкционированного доступа является таблетка Touch Memory, Smart или Proximity Card, биометрия пользователя и др. Для сетевого пакета таким элементом санкционированного доступа могут быть адреса или флаги в заголовке пакета, а также некоторые другие параметры.

Можно заметить, что самым слабым местом описанной защиты является уникальность элемента санкционированного доступа. Если нарушитель каким-либо образом получил этот самый элемент и предъявил системе защите, то она воспринимает его как своего, санкционированного пользователя и разрешает действовать в рамках полномочий того субъекта, секретным (закрытым) элементом которого несанкционированно воспользовались. При современных темпах развития технологий атак НСД получить доступ к самому секретному ключу не составляет большого труда. Его можно прослушать при передаче по сети при помощи анализатора протоколов (sniffer) или подобрать при помощи специальных программ, например Crack и др.

Кроме того, в каждой организации есть пользователи, которые обладают неограниченными правами в своей корпоративной сети. Это, прежде всего, администраторы безопасности, сетевые администраторы. Они никому не подконтрольны и могут делать в сети практически все, что угодно. Как правило, они используют свои санкционированные полномочия для выполнения своих функциональных обязанностей. А если такой администратор чем-то обижен (зарплата, премия, недооценка его возможностей и др.)? К сожалению, известны случаи, когда такие обиженные администраторы действовали и «портили кровь» не одной организации или компании и их действия приводили к очень серьезному ущербу.

Указанные проблемы в международной практике компьютерной безопасности были известны давно, но они не выходили на первый план. Происходило это по нескольким причинам.

Во-первых, корпоративные сети получили широкое распространение совсем недавно, десять-двадцать лет назад. Во-вторых, модели разграничения санкционированного доступа, на основе которых строятся современные системы защиты информации в компьютерных системах, были разработаны, как правило, в интересах конкретных государственных и коммерческих структур, в которых есть своя специфика, т.е. они не универсальны. Например, в интересах Министерства Обороны США был разработан и затем опубликован в 1983г. стандарт компьютерной безопасности TCSEC (Оранжевая книга), в интересах коммерческих организаций Германии, Франции, Англии, Нидерландов были разработаны и использовались европейские критерии компьютерной безопасности ITSEC, 1991г. и др. И, наконец, количество уязвимостей сетевых операционных систем, прикладного программного обеспечения и возможных атак на них растет с угрожающей быстротой. Ситуация усугубляется еще и тем, что многие администраторы безопасности, как это ни парадоксально звучит, не осознают всей серьезности проблемы сетевой безопасности. Немногие их них

имеют время для анализа сообщений о новых обнаруженных угрозах и уязвимостей. Еще меньшему количеству администраторов доступно проведение аудита и постоянного мониторинга корпоративной сети. Для устранения этих недостатков и должны применяться системы обнаружения атак НСД, в том числе с использованием популярных .

Недостатки межсетевых экранов

Если спросить любого квалифицированного пользователя корпоративной сети, чем надо защищать свою сеть от хакеров и других нарушителей, то в 99% случаев на первое место он поставит межсетевые экраны. Однако эти решения хоть и достаточно эффективны, но они, к сожалению, не обеспечивают действительно надежной защиты от всех видов атак.

Дело в том, что межсетевой экран не распознает атаки и не блокирует их. Он сначала запрещает все, а потом разрешает только, так сказать, хорошие и прописанные в нем трафики. Иными словами, при установке межсетевого экрана первым делом запрещаются все соединения между защищаемой и открытой сетями. Затем администратор добавляет специфические правила, которые позволяют определенному трафику проходить через межсетевой экран. Типичная конфигурация межсетевого экрана запретила бы весь входящий UDP-, ICMP-, TCP-трафик, оставив разрешенным только исходящий TCP-трафик. Это позволит пользователям корпоративной, в общем случае Интранет-сети, работать с сетью Интернет и запретить несанкционированный доступ к внутренним ресурсам своих сетей. Но не стоит забывать, что межсетевые экраны – это просто системы, основанные на правилах разграничения доступа, которые, которые разрешают или запрещают прохождение трафика через них. Даже межсетевые экраны, использующие технологию stateful inspection, не позволяют однозначно сообщить, присутствует ли атака в трафике или нет, они могут лишь уведомить, соответствует ли трафик правилу или нет.

Можно провести хорошую аналогию с охранной системой. Межсетевой экран – это просто ограждение вокруг вашей сети, которое не может обнаружить, когда кто-то роет подкоп под него. Межсетевой экран просто ограничивает доступ к некоторым точкам за вашим ограждением. Чтобы убедиться в справедливости этого, приведем несколько типовых примеров, когда межсетевые экраны не спасут вас от злоумышленников.

Атаки через туннели в межсетевом экране

Туннелирование, как известно, является методом инкапсуляции (маскирования) сообщения одного типа, которые не могут быть блокированы фильтрами межсетевого экрана. Атаки через «туннели» возникают вследствие наличия соответствующих свойств у многих сетевых протоколов. Межсетевой экран фильтрует сетевой трафик и принимает решения о пропуске или блокировании пакетов на основе информации об используемом сетевом протоколе. Обычно правила предусматривают соответствующую проверку с целью определения того, что задействован или нет конкретный протокол. Если «да», то пакету разрешается пройти. Например, такой дефект в межсетевых экранах используется при реализации атаки Loki, которая позволяет туннелировать различные команды в запросы ICMP Echo Request и реакции на них в ответы ICMP Echo Reply, что существенно изменяет размер поля данных по сравнению со стандартным (листинг 1).

Листинг 1. Передача файла паролей в рамках атаки LOKI2

```
luka # loki -d server.test.ru
LOKI2 route [(c) 1997 guild corporation worldwide]
loki> ls /etc/passwd
/etc/passwd
loki> more /etc/passwd
. . . . . .
/etc/passwd
```

. . . . . .

root:3QZC8SBkLivns:0:0:root:/root:/bin/bash

daemon::1:1:daemon:/usr/sbin:/bin/sh*

bin::2:2:bin:/bin:/bin/sh*

sys::3:3:sys:/dev:/bin/sh*

man::6:100:man:/var/catman:/bin/sh*

lp::7:7:lp:/var/spool/lpd:/bin/sh*

mail::8:8:mail:/var/spool/mail:/bin/sh*

news::9:9:news:/var/spool/news:/bin/sh*

uucp::10:10:uucp:/var/spool/uucp:/bin/sh*

proxy::13:13:proxy:/bin:/bin/sh*

loki>

Для межсетевого экрана и любого другого традиционного средства сетевой безопасности данные действия выглядят вполне обычно. Например, вот как отображается передача файла паролей в 1CMP-"туннеле" анализатором протоколов TCP-dump (листинг 2).

Листинг 2. Обнаружение атаки LOKI2 (фрагмент журнала регистрации TCP-dump)

12:58:22.225 client.test.ru > server.test.ru icmp: echo request

12:58:22.225 server.test.ru > client.test.ru icmp: echo reply

12:58:22.275 server.test.ru > client.test.ru icmp: echo reply

12:58:22.285 server.test.ru > client.test.ru icmp: echo reply

12:58:28.985 client.test.ru > server.test.ru icmp: echo request

12:58:28.985 server.test.ru > client.test.ru icmp: echo reply

12:58:29.035 server.test.ru > client.test.ru icrap: echo reply

12:58:29.055 server.test.ru > client.test.ru icmp: echo reply

12:58:29.075 server.test.ru > client.test.ru icmp: echo reply

12:58:29.095 server.test.ru > client.test.ru icmp: echo reply

12:58:29.115 server.test.ru > client.test.ru icmp: echo reply

12:58:29.135 server.test.ru > client.test.ru icmp: echo reply

12:58:29.155 server.test.ru > client.test.ru icmp: echo reply

12:58:29.175 server.test.ru > client.test.ru icmp: echo reply

12:58:29.195 server.test.ru > client.test.ru icmp: echo reply

12:58:29.215 server.test.ru > client.test.ru icmp: echo reply

12:58:29.235 server.test.ru > client.test.ru icmp: echo reply

12:58:29.255 server.test.ru > client.test.ru icmp: echo reply

12:58:29.275 server.test.ru > client.test.ru icmp: echo reply

Другим примером туннельных атак можно назвать атаки на уровне приложений, которые связаны с практикой использования уязвимостей в приложениях путем отправки пакетов,

непосредственно связанных с этими приложениями. Таким образом, можно воспользоваться "слабым местом" в Web-приложении путем посылки HTTP-команды, которая позволяет выполнить любую команду на узле с установленным Web-сервером. Если МСЭ сконфигурирован на то, чтобы не препятствовать HTTP-трафику, пакет, содержащий атаку, будет пропущен. Например, как в случае атаки на Internet Information Server 5.0 с установленным патчем Q277873. Эта информация была опубликована Георгием Гунинским в конце ноября 2000 года в списке рассылки Buqtraq.

http://SOMEHOST/scripts/georgi.bat/..%C1%9C..%C1%9C..%Cl%9Cwinnt/system32 /cmd.exe?/c%20dir%20C:

Этот запрос, пропускаемый межсетевым экраном, приводит к выполнению команды "dir C:\". Аналогичным образом можно прочитать любой файл, в том числе и содержащий конфиденциальную информацию.

http://SOMEHOST/scripts/georgi.asp/..%C1%9C..%C1%9C..%Cl%9Ctest.txt

Чтение конфиденциальных данных, которые хранятся в ASP-файлах Internet Information Server, также может быть осуществлено с помощью атаки "HTTP IIS 3.0 Asp Dot". К обычному запросу

http://www.domain.ru/default.asp

злоумышленник добавляет всего лишь одну точку:

http://www.domain.ru/default.asp.

Это приводит к тому, что Web-сервер посылает данный ASP-файл Web-клиенту, где он может быть проанализирован в поисках конфиденциальной информации (пароли, параметры доступа к СУБД и т. д.).

Атаки вследствие неправильной конфигурации межсетевого экрана (МСЭ)

Как известно, межсетевые экраны, как и другие средства защиты, настраиваются людьми. А людям свойственно ошибаться. Именно этот факт и используется многими злоумышленниками. Достаточно найти всего лишь одну "дырочку" в конфигурации межсетевого экрана и далее можно считать, что "ваше дело табак" (листинг 3). Неправильная конфигурация может возникать вследствие некомпетентности или низкой квалификации администратора межсетевого экрана или вследствие других причин. Например, не редки случаи, когда к администратору приходят знакомые сотрудники (или руководители отделов) и просят (или требуют) разрешить доступ по тому или иному порту, сервису (например, ICQ) или к какому-либо Web-серверу (например, к www.playboy.com).

Листинг 3. Разрешение доступа удаленных клиентов к локальным серверам по протоколу Telnet (для МСЭ IPCHAINS)

```
ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
-s $ANYWHERE $UNPRIVPORTS \
-d $IPADDR 23 -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
-s $IPADDR 23 \
-d $ANYWHERE $UNPRIVPORTS -j ACCEPT
```

Со временем в результате таких действий число правил фильтрации "распухает" до невозможности и межсетевой экран превращается в дырявое решето, которое не способно не то, что защитить, но и обнаружить злоумышленников. Мало того, большое количество

правил снижает производительность межсетевого экрана и, как следствие, пропускную способность каналов связи, проходящих через него.

Атаки, осуществляемые в обход межсетевого экрана

Другая проблема состоит в том, что от 65% до 80% всех компьютерных инцидентов исходят изнутри компании. Периметровая защита при помощи МСЭ "не видит" ничего, что происходит внутри сети и не может защитить от таких атак. Пользователи по целому ряду причин устанавливают модемы в свои системы, подключенные к внутренней сети. Это позволяет им (пользователям) соединяться с внешним Internet-провайдером в обход межсетевого экрана, который не может устранить риск, связанный с такими соединениями, поскольку он их никогда "не видит".

Пример №1 из смежной области. 21 февраля 1990 г. аналитик по бюджету Мэри Пирхем (Mary Pircham) пришла на работу. Однако она не смогла пройти на свое рабочее место даже после набора четырехзначного кода и произнесения кодового слова в системе безопасности. Желая попасть на работу, Мэри открыла дверь черного хода при помощи пластиковой вилки и карманной отвертки. Новейшая защитная система, которую обошла Мэри Пирхем, рекламировалась как "безотказная и надежная" и стоила 44 000 долларов [5].

Не всегда *угрозы* исходят только с внешней стороны МСЭ. Большое количество потерь связано как раз с инцидентами защиты со стороны внутренних пользователей. Еще раз необходимо повторить, что МСЭ только просматривает трафик на границах между внутренней сетью и сетью Internet. Если трафик, использующий "бреши" в защите, никогда не проходит через межсетевой экран, то МСЭ не находит нечего предосудительного.

Атаки, осуществляемые из доверенных узлов и сетей

Поскольку большинство организаций используют шифрование для защиты файлов и внешних сетевых соединений, интерес злоумышленника будет направлен к тем местам в сети, где информация, представляющая для него интерес, вероятно, не является защищенной, т.е. к узлам или сетям, с которыми установлены доверенные отношения, например доверенная сеть через VPN-соединение. И даже в случае создания VPN-соединений между сетью, защищаемой при помощи МСЭ, и доверенной сетью злоумышленник сможет с той же эффективностью реализовывать свои атаки. Мало того, эффективность его атак будет еще выше, поскольку зачастую требования по безопасности к доверенным узлам и сетям намного ниже всех остальных узлов.

Можно привести и более интересный пример. Злоумышленник вследствие халатного отношения к безопасности на доверенном узле устанавливает на него "троянского коня". А затем со своего компьютера осуществляет атаку на защищаемую сеть. Для межсетевого экрана все действия выглядят так, как будто они исходят со стороны доверенного узла (листинг 4).

Листинг 4. Разрешение доступа удаленных клиентов к локальным серверам по протоколу FTP (для МСЭ IPCHAINS)

```
# входящие и исходящие FTP-запросы
ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
-s $ANYWHERE $UNPRIVPORTS \
-d $IPADDR 21 -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
-S $IPADDR 21 \
-d $ANYWHERE $UNPRIVPORTS -j ACCEPT
#       нормальный режим передачи
```

```
ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
-s $ANYWHERE $UNPRIVPORTS \
-d $IPADDR 20 -j ACCEPT
ipchains -A output -i $EXTERNAL_INTERFACE -p tcp ! -y \
-s $IPADDR 20 \
-d $ANYWHERE $UNPRIVPORTS -j ACCEPT
#       пассивный режим передачи
ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
-s $ANYWHERE $UNPRIVPORTS \
-d $IPADDR $UNPRIVPORTS -j ACCEPT
ipchains -A output -i $EXTERNAL__INTERFACE -p tcp ! -y \
-s $IPADDR $UNPRIVPORTS \
-d $ANYWHERE $UNPRIVPORTS -j ACCEPT
```

Атаки путем подмены адреса источника

Подмена адреса — это способ сокрытия реального адреса злоумышленника. Однако он может использоваться и для обхода защитных механизмов межсетевого экрана. Такой простейший способ, как замена адреса источника сетевых пакетов на адрес из защищаемой сети, уже не может ввести в заблуждение современные межсетевые экраны. Все они прибегают к различным способам защиты от такой подмены. Однако сам принцип подмены адреса остается по-прежнему актуальным. Например, злоумышленник может подменить свой реальный адрес на адрес узла, у которого установлены доверенные отношения с атакуемой системой. Этот способ отличается от описанного выше тем, что в данном случае злоумышленник только подменяет адрес доверенного узла, и в действительности находится не на нем.

Атаки на сам межсетевой экран

Межсетевые экраны зачастую сами являются объектами атаки. Напав на МСЭ и выведя его из строя, злоумышленники могут спокойно, не боясь быть обнаруженными, реализовывать свои преступные замыслы по отношению к ресурсам защищаемой сети.

Уязвимости межсетевых экранов ipfw и BorderWare

В январе 2001 года было обнаружено немало уязвимостей в реализации различных известных межсетевых экранов. Например, неправильная обработка TCP-пакетов с флагом ECE в МСЭ ipfw или ip6fw позволяла удаленному злоумышленнику обойти созданные правила. Еще одна уязвимость была обнаружена в межсетевом экране BorderWare Firewall Server 6.1.2. Данная уязвимость, связанная с широковещательной посылкой запросов ICMP Echo Request, приводила к нарушению доступности МСЭ BorderWare.

Атаки на подсистему аутентификации межсетевого экрана

Как уже было отмечено выше, даже самый мощный и надежный межсетевой экран не защитит от проникновения в корпоративную сеть нарушителя, если последний смог подобрать или украсть пароль авторизованного пользователя. Мало того, межсетевой экран даже не зафиксирует нарушения, т. к. для него нарушитель, укравший пароль, является авторизованным пользователем.

Пример №2. Атака на БелАКБ "Магнатбанк". 22 марта 1995 г. неустановленный злоумышленник при помощи украденного пароля и программного обеспечения Пинского

филиала БелАКБ "Магнатбанк" проник в компьютерную сеть Белорусского межбанковского расчетного центра и перевел на расчетный счет ООО "Арэса ЛТД" в Советское отделение БелАКБ "Промстройбанк" 1 млрд 700 млн рублей [5].

Уязвимость межсетевого экрана Firebox II

В январе 2001 года была обнаружена уязвимость в межсетевом экране серии Firebox II компании WatchGuard. Она позволяла считывать пароли, используемые для аутентификации на межсетевом экране. Это давало возможность злоумышленнику сохранять свои файлы (например, троянского коня) или выполнять любые команды на компьютере с установленным межсетевым экраном WatchGuard Firebox II, Firebox II Plus и Firebox II FastVPN.

Другой пример, который уже приводился выше, — администраторы, имеющие неограниченную власть в управляемой ими сети.

Пример №3. Атака на Внешэкономбанк. Хищение при помощи компьютерной техники валютных средств из Внешэкономбанка в 1991 г. на сумму 125,5 тыс. долларов и подготовка к хищению еще свыше 500 тыс. долларов. Механизм хищения был очень прост. Житель Москвы совместно с начальником отдела автоматизации неторговых операций ВЦ Внешэкономбанка открыл по шести поддельным паспортам счета и внес на них по 50 долларов. Затем, путем изменения банковского программного обеспечения на открытые счета были переведены 125 тысяч долларов, которые и были получены по поддельным паспортам. Необходимо отметить, что это одно из немногих дел, в которых к процессу расследования привлекались различные специалисты: программисты, системные аналитики, операторы ЭВМ, инженеры по телекоммуникациям, эксперты в области информационной безопасности, аудиторы, ревизоры КРУ ЦБ РФ и т. д. [5].

Выводы

1. Традиционные средства защиты не обеспечивают достаточного уровня защищенности. Хотя ни в коем случае от них нельзя отказываться. Они могут помочь обеспечить минимальный уровень защиты корпоративных ресурсов. Как уже было отмечено выше, традиционные средства были построены на основе моделей, разработанных в то время, когда корпоративные сети не получили такого широкого распространения и способы атак НСД на эти сети не были так развиты, как сейчас. Чтобы противодействовать новым и непрерывно совершенствующимся методам атак НСД, необходимо разобраться, как они реализуются, вследствие чего они могут возникать и т. д. Это позволит не только противодействовать нападениям, но и понять, какие средства могут их обнаруживать и предотвращать, дополняя традиционные защитные системы.

2. Создать абсолютно защищенную корпоративную сеть невозможно по причине наличия в программном обеспечении различных ошибок. Программное обеспечение, свободное от ошибок, все еще является мечтой. Да и практика такова, что даже производители brandname не всегда пытаются разработать такое программное обеспечение ради быстрой прибыли в острой конкурентной борьбе.

3. Даже самая защищенная компьютерная система уязвима перед хакерами и другими высокопрофессиональными пользователями.

4. Универсальных средств защиты корпоративных сетей не существует, потому что каждая система защиты создается под конкретные объекты защиты, угрозы и политику безопасности.

5. Наконец, срабатывает принцип бумеранга - чем защищеннее система, тем неудобнее с ней работать, тем вероятнее могут быть отдельные, казалось бы мелкие, но все же нарушения политики безопасности (усталость пользователя, притупление бдительности, отступления в повторяемых операциях и др.).

6. Таким образом, мы приходим к необходимости перехода к новой концепции безопасности корпоративных сетей Интранет путем использования мониторингово-

адаптивного метода защиты с обнаружением и нейтрализацией всех атак НСД - если мы не можем построить абсолютно защищенную корпоративную сеть Интранет, то хотя бы должны обнаруживать все (или практически все) нарушения политики безопасности и соответствующим образом (адаптивно) реагировать на них.

Список литературы

1.2000 CSI/FBI Computer and Security Survey.Computer Security Institue. Federal Bureau Investigation's Computer Intrusion Squad.

2. Ільніцький А.Ю., Шорошев В.В., Близнюк І.Л.Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах ОВС Уаїни. Видавництво НАВСУ, 2003. С.316.

3. Пакет из пяти нормативных документов по вопросам защиты информации от несанкционированного доступа Департамента СТСЗИ СБ Украины, К., 1999.

4. В.В.Шорошев. Базовая модель экспертной системы оценки безопасности информации в компьютерных системах. // Научно-технический сборник КПИ, Минобразования и науки Украины, ДСТСЗИ СБ Украины. Выпуск 3. - 2001.

5. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2001. С.624.

6. Richard Power. Crrent and Future Danger: A CSI Primer on Computer Crime and Information Warfare. Computer Sequrity Institute. 1995.

Поступила 25.04.2007 г.

УДК 681.3.06

Дирда О.В., Скрипник Л.В.

УДОСКОНАЛЕННЯ МЕТОДУ КОРЕЛЯЦІЙНОГО КРИПТОАНАЛІЗУ ДЛЯ ОДНОГО ТИПУ КОМБІНАЦІЙНОГО ГЕНЕРАТОРА

Одним із потужних методів криптографічного аналізу, який може бути застосовано проти потокових шифрів, є кореляційний метод криптоаналізу [1, 2]. Цей метод засновано на обчисленні кореляції вихідних значень двійкових (булевих) функцій з їх вхідними значеннями. Для двійкової функції $f = f(x_1, x_2, ...x_n)$ від n змінних кореляція між i-им "входом" та значенням функції обчислюється за формулою

$$c_i = p\left(x_i = 1 \middle/ f = 1\right).$$

Розглянемо випадок, коли у потоковому шифрі використовується S-блок розміру $n \times n$ (або $n \times n$ S-блок), який являє собою функцію $S : V_n \to V_n$, де V_n – лінійний простір бітових векторів довжини n. S-блок розміру $n \times n$ може бути поданий як система з n булевих функцій $f_j : V_n \to \{0,1\}$, $j = \overline{1,n}$, які носять назву координатних функцій S-блоку.

Для $n \times n$ S-блоку вводять так звану матрицю кореляційних коефіцієнтів, яка визначає кореляцію між i-им "входом" та j-им "виходом". Елемент $c_{i,j}$ цієї матриці носить назву кореляційного коефіцієнту та обчислюється за формулою

$$c_{i,j} = p\left(x_i = 1 \middle/ f_j = 1\right),$$

де $i, j = \overline{1,n}$.