Д11-2002-292

П. М. Васильев[1], В. В. Иванов[2,3], В. В. Кореньков[2],
Ю. А. Крюков[1], С. И. Купцов[1]

ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ ССАУ «ТРАФИК»

[1]Отдел информатизации, Международный университет природы, общества и человека «Дубна», 141980, Дубна
[2]Лаборатория информационных технологий, Объединенный институт ядерных исследований, Дубна
[3]Международный Сольвеевский институт физики и химии, Брюссель

Введение

Мы живем в современном, динамично развивающемся мире. Казалось бы, не так давно были определены основные понятия безопасности в межгосударственной политике, однако наступает момент, и мы осознаем необходимость кардинальных перемен. День 11 сентября 2001 года заставил политиков всего мира задуматься об основных угрозах для современных государств.

Аналогичные процессы происходят и в сфере телекоммуникационных технологий. Самая большая на сегодняшний день глобальная сеть Интернет проектировалась в условиях возможности ядерного удара, с учетом обеспечения максимальной надежности коммуникаций путем введения избыточных связей и сетевых узлов. Обеспечение максимальной надежности физических линий и сетевых устройств вытекало из угрозы, которая на тот момент была реальной. Применение в сетевых устройствах интегральных схем с высокой плотностью элементов позволило значительно увеличить надежность используемой электронной аппаратуры. Этот фундамент и сегодня обеспечивает бесперебойное функционирование линий связи и хостов в сети.

Что же представляет на сегодняшний день наибольшую угрозу миллионам пользователей корпоративных систем и телекоммуникационных услуг?

Так же как и в политике, наибольшую угрозу нормальному функционированию информационных систем представляют небольшие группы людей (часто одиночки), независимо от места их проживания, имеющие не совсем адекватные (с точки зрения большинства населения) понятия и цели. К этим же группам можно отнести и тех, кто, используя телекоммуникационные технологии, пытается решать свои финансовые проблемы. Всех их в полной мере можно назвать телекоммуникационными террористами.

Жесткая конкуренция между организациями, предприятиями и банками заставляет их обеспечить широкий доступ пользователей к своим информационным базам данных, сервисам, услугам и, соответственно, интегрировать свои корпоративные системы в общедоступные глобальные сети.

Стоимость конфиденциальной информации, хранящейся на электронных носителях и передающейся по линиям связи, можно оценить, например, путем подсчета убытков в случае использования конкурентами [1]. Очевидно, что размеры таких потерь могут быть соизмеримыми со стоимостью основных фондов предприятия. Не стоит также недооценивать нематериальные потери граждан, предприятий, стран в случае распространения или искажения конфиденциальной информации.

Конечно же, не стоит думать, что информационные системы, обеспечивающие функционирование критичных объектов (военные объекты, атомные станции, аэропорты и т.д.), предоставляют аналогичные возможности для несанкционированного доступа к конфиденциальной информации и управлению. Обычно такие системы работают в рамках локальных сетей, не имеющих физических связей с сетями общего доступа. Кроме того, в них, как правило, применяются нестандартные операционные системы и протоколы передачи данных. Однако и в этом случае проблемы информационной безопасности должны находиться под постоянным контролем специалистов в

связи с возможностью несанкционированного доступа "изнутри" системы со стороны обслуживающего персонала.

Таким образом, вопросы обеспечения информационной безопасности сети постепенно выходят на передний план в исследованиях по созданию информационно безопасных автоматизированных систем и протоколов передачи данных, применению сетевых узлов, адекватно реагирующих на различные сетевые сообщения и т. д.

В работе [2] была создана система сбора, анализа и управления сетевым трафиком (ССАУ «Трафик») для сегмента компьютерной сети ОИЯИ – локальной сети (ЛКС) университета «Дубна». Эта система расположена на входном шлюзе ЛКС и позволяет проводить непрерывный мониторинг параметров сетевого трафика, обеспечивает наглядную визуализацию результатов анализа трафика и помогает сетевому администратору в принятии решений по управлению ЛКС.

Цель настоящей работы – классификация сетевых атак для оперативного отслеживания нежелательных событий в локальных сетях ОИЯИ и университета "Дубна", а также выработка рекомендаций по модернизации сетевых устройств и топологий ЛКС для уменьшения вероятности реализации угроз компьютерным сетям и системам.

В первой главе рассмотрены основные понятия теории компьютерной безопасности и основные типы удаленных атак на компьютерные комплексы. Во второй главе анализируются структуры сетевого трафика в процессе выполнения основных типов удаленных атак в рамках протокола TCP/IP. В третьей главе обсуждаются основные задачи и структура подсистемы обеспечения безопасности ЛКС на основе ССАУ «Трафик».

1. Основные понятия безопасности компьютерных сетей

Современная теория компьютерной безопасности оперирует тремя основными понятиями [3]:

- *Угроза* - любое нежелательное событие в работе аппаратного и программного обеспечения хостов, сетевых устройств, линий связи, приводящее к неадекватному функционированию системы в целом. Нежелательное событие необязательно является следствием действий злоумышленника, оно может наступить и в случае ошибочных действий системного администратора (например, случайное удаление таблицы базы данных) или аппаратных сбоев (например, в случае выхода из строя жесткого диска).
- *Технологическая возможность (уязвимость)* - следствие неудачных, с точки зрения безопасности, инженерных решений в области реализации алгоритмов и программного кода операционных систем, протоколов передачи данных, потенциально позволяющих злоумышленнику реализовать нежелательное событие.
- *Атака* - целенаправленная деятельность злоумышленника, использующего известные ему *технологические возможности* для реализации нежелательного события.

Рассмотрим первую группу нежелательных событий [3], объединенных понятием "угроза":

- *Угроза раскрытия* - утечка конфиденциальной информации, приводящая к наиболее тяжелым последствиям, так как факт раскрытия информации не всегда может быть вовремя установлен.
- *Угроза целостности* - изменение или подмена истинной информации фальшивой, обычно сопровождается раскрытием информации. Угроза целостности может быть минимизирована путем применения нестандартных систем контроля достоверности информации.
- *Угроза отказа в обслуживании* приводит к временной недоступности одного или нескольких сетевых ресурсов, приводящих к потере работоспособности автоматизированной системы в целом. Это самый распространенный тип атак, так как его проще всего реализовать.

Предотвратить вероятность реализации указанных трех типов нежелательных событий можно путем "экспресс-анализа" сетевого трафика на основе ССАУ "Трафик" [2]. Однако для проведения такого анализа необходима дальнейшая классификация возможных типов атак, а также систематизация особенностей сетевого трафика на примере наиболее известных сценариев выполнения удаленных атак на сетевые устройства и хосты.

Основные типы сетевых атак на ЛКС можно классифицировать [3]:

- По характеру воздействия - на *активные и пассивные* атаки. *Активная* атака нацелена на изменение алгоритмов работы частей системы и, соответственно, всей системы в целом. Изменение алгоритмов достигается, например, изменением конфигурации системы, логики работы сетевых соединений и сервисов, вывода из строя отдельных частей системы. *Пассивный тип* атаки реализует угрозу раскрытия путем прослушивания каналов связи и не оказывает при этом воздействия на функционирование системы.
- По расположению источника - на *внутренние, сетевые* и *межсетевые* атаки. При *внутренней* атаке источник расположен в одном домене коллизий с атакуемым объектом и имеет возможность прослушивать абсолютно все сетевые пакеты объекта. Во время *сетевой* атаки источник находится в одной IP-сети с атакуемым объектом, но сеть может быть сегментирована коммутатором, вследствие чего атакующий может прослушивать только широковещательные пакеты объекта. В случае *межсетевой* атаки источник и объект расположены в разных IP-сетях, разделенных либо маршрутизатором, либо межсетевым экраном firewall.
- По условию начала выполнения - на *условные и безусловные* атаки. В первом случае атакующий ожидает от объекта генерации запроса определенного типа (например, генерации DNS-запроса к DNS-серверу) либо наступления в работе объекта ожидаемого события (например, выключение компьютера легального пользователя без команды LOGOUT). *Безусловная* атака подразумевает активное воздействие на объект, невзирая на состояние атакуемой системы. Примером может служить генерация атакующим большого количества пакетов открытия сеансов связи для реализации угрозы отказа в обслуживании.
- По наличию обратной связи - на атаки, требующие получения атакующим ответных пакетов от объекта, и атаки, не требующие обратной связи.

- По уровню модели OSI, на котором предпринимается атака. На *физическом уровне* возможно, например, непосредственное подключение к проводам линий связи для проведения прослушивания линии или фактический обрыв коммуникаций для нейтрализации одного из субъектов атаки. На *канальном уровне* возможен захват пакетов из единой, разделяемой среды. На *сетевом уровне* объектом атаки становится дейтаграммная передача IP-пакетов. На *транспортном* уровне объектом воздействия становятся алгоритмы протоколов TCP и UDP, на *сеансовом уровне* возможна, например, атака с подменой одного из субъектов TCP-соединения, на *представительском* - атаки с подменой портов и сокетов. Атака на *прикладном уровне* воздействует на алгоритмы работы конкретного приложения.

Каждый из известных типов атак характеризуется свойственным только ему сценарием обмена сетевыми пакетами, и, как следствие, существует потенциальная возможность формализации сценариев сетевого трафика для атак конкретного типа. В этой связи становится возможным без разработки сложных интеллектуальных систем (и, соответственно, без больших временных затрат) на основе набора типовых признаков (шаблонов) зафиксировать факт проведения сетевой атаки определенного типа.

Предлагаемая нами схема обеспечения безопасности ЛКС очень похожа на весьма эффективные системы антивирусного программного обеспечения, в которых для обнаружения присутствия вируса используются наборы типовых текстов с фрагментами кодов программ-вирусов. Подобный подход позволяет использовать для защиты ЛКС типовые схемы сетевого трафика, а также оперативно разрабатывать эффективные алгоритмы защиты от новых сценариев сетевых атак.

2. Анализ трафика для некоторых сценариев сетевых атак

Как уже отмечалось, одной из наиболее опасных угроз является угроза раскрытия - утечки конфиденциальной информации. Как правило, компьютерные сети, как минимум, на уровне рабочих групп больших предприятий, а также мелких офисов используют один из популярных стандартов локальных сетей (чаще Ethernet), представляющих единую разделяемую по времени всеми компьютерами физическую среду передачи данных. Такой подход резко удешевляет создание ЛКС за счет минимизации затрат на оборудование и прокладку кабеля, но в то же время обеспечивает доступ каждого компьютера абсолютно ко всем сетевым пакетам, передаваемым в рамках данной сети.

2.1. Прослушивание канала связи

Именно широковещательный аспект в работе большинства локальных сетей таит в себе потенциальную опасность для реализации разного вида атак, и, как будет показано ниже, прослушивание канала связи является непременным условием для проведения большинства атак.

В результате прослушивания каналов связи злоумышленник может получить всю необходимую ему информацию о ЛКС: структуру сети, используемые службы и сервисы, адреса хостов и серверов, имена, а иногда и

пароли пользователей, маршрутную информацию, временные графики работы узлов в сети и т.д.

Исходя из перечисленных фактов непременным условием для успешной борьбы не только с внешними, но и, что гораздо сложнее, с внутренними типами атак является оперативное выявление фактов прослушивания каналов связи.

Прослушивание канала является пассивным типом атаки, не оставляющим никаких следов в общем объеме сетевого трафика. Борьба с пассивным типом атаки невозможна путем пассивного наблюдения за поведением сетевого трафика. Нужны активные периодические мероприятия, направленные на выявление работы программы захвата сетевых пакетов, – программы сниффера.

Задача выявления работы таких программ может быть реализована с помощью ССАУ "Трафик" активного воздействия на программу сниффера, основанного на известном факте независимости работы программных модулей, работающих на различных сетевых уровнях модели OSI.

В нормальном режиме работы сетевой адаптер начинает прием любого передаваемого по сети пакета, записывая получаемые данные в свой приемный буфер. Как только полученных битов становится достаточно для проведения анализа поля адреса получателя пакета, сетевой адаптер принимает решение о необходимости дальнейшего приема пакета (когда адрес получателя совпадает с собственным адресом сетевого адаптера) или о прекращении приема и очистки приемного буфера (если адрес не совпадает). Процедура проверки «свой-чужой» возложена на канальный уровень модели OSI (аппаратуру сетевого адаптера).

С помощью команд спецификации NDIS можно заменить режим нормальной работы канального уровня сетевого адаптера, предписанной стандартом Ethernet, на захват всех сетевых пакетов. При этом работа программных модулей протокола TCP/IP не меняется, и стек протокола полностью выполняет свои функции. Исходя из этого возможен следующий алгоритм обнаружения работающего компьютера-сниффера.

Система ССАУ "Трафик" формирует «неправильный» пакет, содержащий не существующий в локальной сети MAC-адрес, но имеющий в IP-заголовке реальный (отвечающий проверяемому ПК) IP-адрес. Исходя из принципа захвата всех транслирующихся по сети пакетов, канальный уровень компьютера-сниффера примет «неправильный» пакет (а не отбросит его, как того требует стандарт Ethernet) и передаст для анализа программному модулю, реализующему сетевой уровень модели (IP-протокол). Сетевой уровень получит "чистый" IP-пакет с удаленным заголовком и концом кадра канального уровня, поэтому у него не остается возможности проверить правильность обработки его канальным уровнем сетевого адаптера.

И если пакет в поле данных будет содержать, например, команду протокола ICMP, предназначенную для проверки работоспособности IP-сетей (команду PING), то подпрограмме реализации протокола ICMP в модуле IP не остается ничего другого, как обработать команду стандартным образом, результатом чего будет формирование ответного пакета, информирующего о работоспособности системы и адресованного источнику.

Прием такого пакета дает основание зафиксировать факт прослушивания информации в локальной сети конкретным пользователем. В противном случае, когда канальный уровень исследуемого компьютера работает в штатном режиме, формирование ответного пакета не произойдет.

Кроме того, некоторые современные сетевые адаптеры, осуществляя конвейерную обработку приходящих пакетов, позволяют разделять потоки данных, из которых одна часть направляется на обработку стандартному стеку протоколов, а другая - одновременно работающей программе-снифферу. В этом случае для получения ответного пакета необходимо сделать так, чтобы стандартные алгоритмы сетевого адаптера не могли однозначно идентифицировать принадлежность пакета одному из потоков и направляли "спорный пакет" в оба направления. Используемый в этом случае MAC-адрес получателя может иметь, например, следующий вид: FF-00-00-00-00-00.

Следует отметить, что направляемые ССАУ "Трафик" пакеты-исследователи являются адресными на IP-уровне (а не широковещательными), поэтому для выявления факта прослушивания сети необходимо исследовать все возможные адреса данной IP-сети, включая и не задействованные в данный момент IP-адреса. В случае сети университета "Дубна" необходимо, чтобы ССАУ "Трафик" сгенерировала 512 пакетов исследователей, каждый с уникальным IP-адресом исследуемого компьютера в локальной сети. Пакет с командой PING протокола ICMP имеет минимальный размер: 64 байта без преамбулы. Учитывая, что 10 Мб/с сеть Ethernet обладает производительностью до 14800 пакетов минимального размера в секунду, то генерируемый таким образом служебный трафик не ограничит пропускную способность сети в целом, даже в течение небольших интервалов времени.

Периодическое (например, каждые 10 минут) сниффер-сканирование трафика сети с помощью ССАУ «Трафик» позволяет предотвратить не только возможность прослушивания злоумышленником сегмента локальной сети, но и её использование в качестве плацдарма для реализации удаленных атак другого типа.

Важным элементом по мониторингу состояния ЛКС с помощью ССАУ "Трафик" является проверка соответствия MAC-адресов сетевых адаптеров ПК в ЛКС выданным при регистрации IP-адресам, а также отсутствия в сети компьютеров с незарегистрированными IP-адресами. В связи с невозможностью применить программу прослушивания сети может оказаться заманчивым использовать чужой MAC-адрес, IP-адрес или NETBIOS компьютера.

ССАУ "Трафик" поддерживает базу данных по оборудованию компьютеров в данной локальной сети [2] и на основе протокола ICMP (например, с помощью программы NBTSTAT.EXE) обеспечивает возможность контроля соответствия этих трех адресов адресам, зарегистрированным в базе данных. Такой дополнительный контроль несколько увеличивает служебный трафик в ЛКС, однако он является исключительно действенным инструментом в обеспечении безопасности ЛКС.

2.2. Технологические особенности работы ARP -сервера в сетях TCP/IP

К сожалению, адрес сетевого адаптера (MAC-адрес) не позволяет строить большие распределенные сети, так как в нем нет возможности (параметра) для группирования компьютеров по территориальному признаку для создания подсетей. С другой стороны, он однозначно и автоматически идентифицирует компьютер в рамках конкретного сегмента сети. Кроме того, для идентификации конкретного компьютера в ЛКС применяются разные адреса на разных уровнях OSI: на канальном уровне MAC-адрес, на сетевом IP-адрес,

используются также и символьные адреса. Это может быть одной из причин технологической уязвимости, используемой для реализации сетевых атак.

Применение нескольких идентификаторов приводит к необходимости построения систем, позволяющих устанавливать соответствие одного из имен остальным. В частности, при поиске в сети сервера по имени TIGGER (по команде net view tigger) устанавливается соответствие имени TIGGER IP-адресу этого сервера, например, 159.93.167.50 и далее соответствия IP-адреса MAC-адресу его сетевого адаптера, например, 00-01-1A-16-B8-CA.

Задачу поиска MAC-адреса по IP-адресу выполняет протокол сетевого уровня ARP (Address Resolution Protocol). Рассмотрим схему адресации пакетов в Internet и возникающие при этом проблемы безопасности. Базовым протоколом обмена в Internet является протокол IP, позволяющий передавать IP-пакеты в любую точку глобальной сети. Поиск адресата промежуточными сетевыми устройствами производится на основе анализа IP-адреса. После доставки IP-пакета в подсеть получателя локальный маршрутизатор должен доставить пакет с использованием той технологии передачи данных, которую использует сетевой адаптер адресата. И здесь не обойтись без ряда необходимых действий, так как маршрутизатор может обращаться к адресуемому хосту впервые и не иметь в своей базе соответствующих имен.

Рассмотрим схему работы протокола ARP:

- маршрутизатор посылает широковещательный запрос, в котором указывает свой MAC-адрес и просит ответить ему компьютеру, имеющему указанный IP-адрес;
- широковещательный запрос получат все компьютеры сегмента сети, но ответит лишь тот ПК, у которого запрашиваемое имя совпадает с его собственным. Причем IP- и MAC-адреса маршрутизатора, полученные из запроса, перед отправкой ответа будут занесены в ARP-таблицу соответствия адресов на запрашиваемом компьютере;
- получив ответ, маршрутизатор занесет данные в ARP-таблицу и направит сообщение адресату, используя полученный MAC-адрес.

Протокол ARP работает в рамках конкретного сегмента сети и поэтому имеет локальный характер. Анализ протокола ARP показывает, что на его основе существует возможность проведения атаки с внедрением в сеть ложного объекта. В результате такой атаки можно изменить маршрут следования пакетов и, соответственно, отвести на компьютер злоумышленника трафик с интересующего его сетевого хоста. Для ЛКС на основе концентраторов такая атака теряет смысл, так как злоумышленник может легко получить доступ к трафику любого из сетевых компьютеров, воспользовавшись программой сниффера.

Иная ситуация имеет место для сетей, разбитых на сегменты с помощью коммутаторов. В этом случае атака на основе протокола ARP является наиболее вероятной.

Рассмотрим возможный сценарий такой атаки. Пусть злоумышленнику необходимо получить несанкционированный доступ к информации экзаменационной сессии, хранящейся на сервере дистанционного обучения университета "Дубна". Сеть университета хорошо сегментирована и не предоставляет атакующему возможности доступа к трафику данного сервера. К тому же присутствие на его ПК программы-сниффера будет немедленно зафиксировано ССАУ "Трафик".

В таких условиях возможен следующий сценарий внедрения ложного ARP-сервера (рис.1):

- ожидание широковещательного ARP-запроса от ПК одного из легальных пользователей системы дистанционного обучения, обладающего необходимыми привилегиями; этот запрос идентифицирует пользователя, который собирается работать с сервером;
- после получения такого запроса осуществляется передача на запросивший хост ложного ARP-ответа, где указывается MAC-адрес атакующей станции и IP-адрес затребованного сервера дистанционного обучения.

Рис.1. Сценарий внедрения ложного ARP-сервера

При этом следует заметить, что, например, ОС Windows меняет свою ARP-таблицу в момент прихода ARP-ответа, даже если компьютер не посылал запроса. Поэтому злоумышленнику необязательно даже торопиться с посылкой ложного ответа. Такой ответ может быть послан сразу же после ARP-ответа сервера, т.к. в ARP-таблице атакованного компьютера-клиента остается лишь соответствие IP- и MAC-адресов последнего ответа.

Далее легальный пользователь попытается зарегистрироваться в системе под своим именем и паролем. Однако, начиная с этого момента, все пакеты будут направляться на компьютер злоумышленника, а уже потом перенаправляться по правильному маршруту (рис.2).

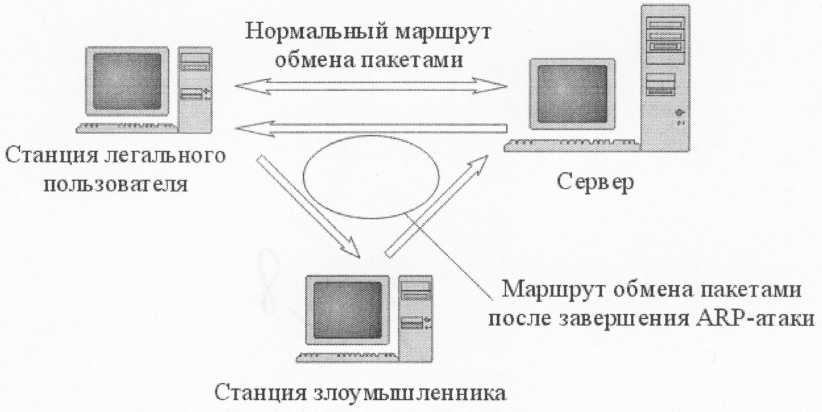

Рис.2. Изменение маршрута обмена пакетами после завершения ARP-атаки

Все передаваемые пакеты с ответами являются одноадресными и направляются коммутаторами «адресату» по оптимальным маршрутам, поэтому ССАУ "Трафик" не сможет зафиксировать такую атаку только на основе анализа трафика.

На первый взгляд может показаться, что невозможно применить систему анализа сетевых атак, расположенную на внешнем шлюзе, для обнаружения таких внутрисегментных действий. Однако это не так, поскольку мы упустили одну небольшую деталь. Дело в том, что прием пакетов от обманутой сетевой станции атакующим будет невозможен без перевода сетевого адаптера в режим сниффера либо без изменения IP-адреса, так как пакеты будут приходить с правильным MAC-адресом, но содержать IP-адрес сервера дистанционного обеспечения. Поэтому в этом случае пакеты будут отбрасываться не на канальном уровне (т.е. сетевым адаптером), а модулем IP-протокола, и атака не достигнет своей цели.

2.3. Технологические возможности атаки на службу DHCP

Использование нескольких типов адресов на хостах, работающих под протоколом TCP/IP, приводит к необходимости ручного конфигурирования компьютеров сетевыми администраторами. Процесс этот рутинный и достаточно трудоемкий, так как приходится практически вручную отслеживать все перемещения компьютеров в ЛКС, изменения сетевого оборудования, установку новых ПК и т.д. Объем подобных работ резко возрастает в больших ЛКС, содержащих сотни и тысячи компьютеров.

Для ускорения этой процедуры используется динамический протокол конфигурирования хоста DHCP в ЛКС. Сервис DHCP централизует настройку протокола TCP/IP, управляет выделением конфигурационной информации, автоматически назначает IP-адреса компьютерам ЛКС. С установкой DHCP-сервера отпадает необходимость ручной конфигурации сети, т.к. инсталляция сетевых сервисов операционной системы на новом компьютере по умолчанию

настраивает протокол TCP/IP на автоматическое получение необходимых параметров [4]:

- IP - адреса компьютера;
- маски подсети,

а также дополнительных параметров:

- IP- адреса шлюза по умолчанию;
- IP- адреса DNS-сервера;
- IP- адреса WINS-сервера.

При этом во время запуска нового компьютера стек протокола TCP/IP не располагает необходимой информацией для организации его взаимодействия с другими хостами в сети. Получение нужных настроек происходит в результате обмена клиента и сервера DHCP следующими четырьмя пакетами [4]:

- DHCP Discover - запрос на получение настроек от сервера DHCP. Клиент не знает расположения DHCP-сервера, поэтому кадр является широковещательным как на уровне MAC-адреса, так и на уровне IP-адреса.
- DHCP Offer - предложение сервера DHCP, содержащее предлагаемый к использованию IP-адрес. Сервер не может напрямую адресоваться к запросившему компьютеру, так как тот еще не имеет адреса.
- DHCP Request - выбор адреса, отправляется клиентом после принятия решения о том, что предложенный адрес его устраивает. Отправляется также широковещательным пакетом (т.к. адрес клиенту еще не назначен).
- DHCP ACK - подтверждение сервера об окончательном закреплении за клиентом ранее предложенного IP-адреса и передача списка всех установленных на DHCP-сервере дополнительных параметров.

Анализ работы данного протокола на предмет безопасности показывает его полную незащищенность. Во-первых, все используемые протоколом кадры - широковещательные, что снимает необходимость использования злоумышленником программы сниффера, а также не требует решать проблему сегментации трафика коммутаторами. Во-вторых, используется не идентифицирующий соединение дейтаграммный протокол UDP. Кроме того, существует возможность настройки трансляции широковещательных DHCP-запросов маршрутизаторами в соседние подсети (для уменьшения общего количества DHCP-серверов в сети), что многократно увеличивает число потенциальных объектов атаки.

В рамках такой практически незащищенной службы сетевого сервиса можно реализовать много различных вариантов несанкционированного использования ЛКС.

Рассмотрим один из возможных сценариев. Злоумышленник использует схему широковещательного поиска клиентом DHCP-сервера и действует по схеме "внедрение ложного объекта". Получив, как и все компьютеры ЛКС, DHCP-запрос, атакующий субъект генерирует стандартное DHCP-предложение и указывает свой IP-адрес в качестве источника сообщения. При этом атака может не сопровождаться подавлением работы настоящего DHCP-сервера (в больших сетях может использоваться несколько DHCP-серверов), клиент довольствуется получением первого пришедшего ответа и отбрасывает остальные (рис.3).

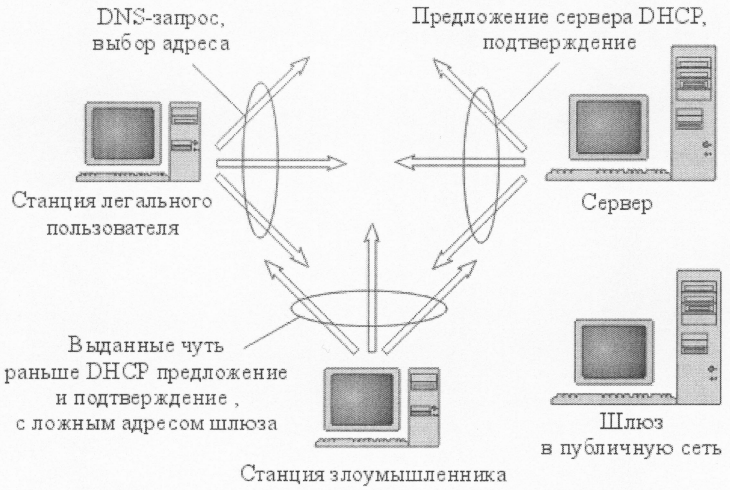

Рис.3. Реализация схемы внедрения «ложного объекта» с помощью DHCP-предложения с ложным адресом шлюза

Далее процесс "выдачи" IP-адреса протекает по обычной схеме, однако, при этом легальный пользователь сети получит ложные дополнительные адреса (адрес шлюза по умолчанию, а также адреса WINS- и DNS-серверов), а весь его трафик будет находиться под контролем атакующего субъекта (будет проходить через его компьютер). Таким образом, будет реализована угроза раскрытия.

Необходимо также учитывать и то, что запросы на получение адресов генерируются в массовом порядке во время утреннего включения компьютеров пользователями (например, около 9 утра). В этот момент «атакованными» могут оказаться десятки и сотни ПК, трафик которых может быть использован атакующим субъектом аналогичным образом (рис.4).

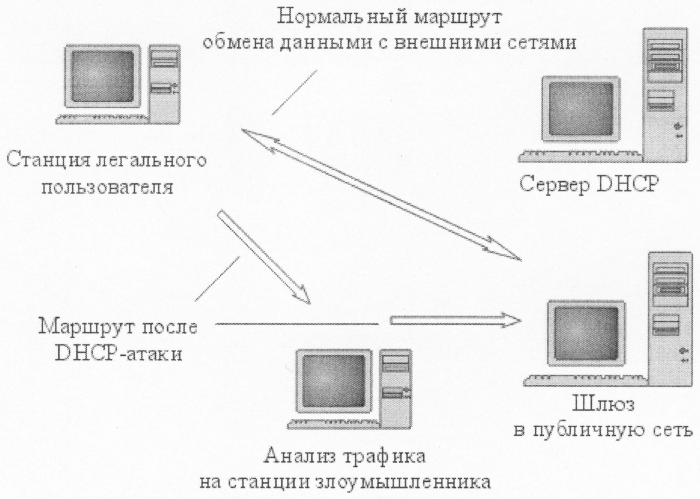

Рис.4. Изменение маршрута трафика после реализации DHCP-атаки

Другой целью такой атаки может быть провоцирование угрозы отказа в обслуживании. В этом случае злоумышленник может просто распространить недостоверную информацию о настройках протокола, в результате чего станет невозможным выполнение сетевых операций конкретным пользователем (рис.5).

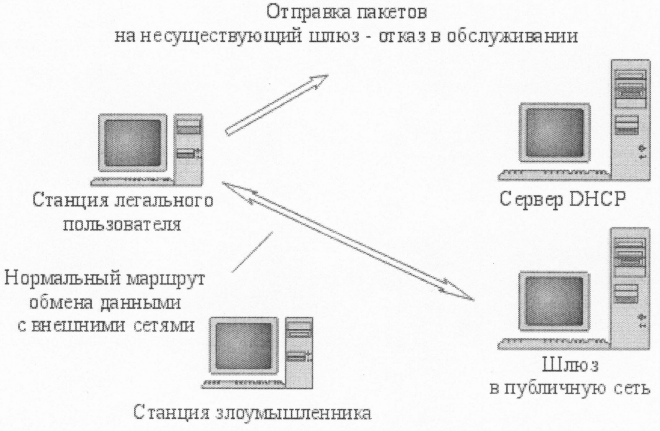

Рис.5. Реализация угрозы отказа в обслуживании с помощью DHCP-атаки

Возможное решение проблемы защиты службы DHCP на основе ССАУ "Трафик" состоит в следующем. Широковещательность DHCP-трафика позволяет пассивным прослушиванием определить наличие в ЛКС незарегистрированного ПК, который генерирует DHCP-трафик, а затем по необходимости подавить его активность мини-штормом запросов на TCP-соединение (исходя из предположения о выводе из строя большого числа корпоративных ПК) и проинформировать системного администратора о происшедших событиях.

2.4. Технологические возможности атаки на службу DNS

Как известно, в сети Internet хосты адресуются не только с помощью MAC- и IP-адресов. Для удобства запоминания имен хостов применяется дополнительная адресация, никак не связанная с протоколом передачи данных и использующая составные символьные адреса серверов, которые однозначно связаны с IP-адресом. Примером такого имени является адрес: WWW.UNI-DUBNA.RU. Доступ к WWW-серверу в Интернет через броузер возможен как по IP-адресу, так и с помощью символьного имени.

Поддержка соответствия IP-адреса и символьного имени возлагается на DNS (Domain Name System) службу. DNS-сервис построен по иерархической схеме на основе серверов DNS, каждый из которых отвечает за свою зону обслуживания. Сервера поддерживают работу базы данных соответствия имен хостов IP-адресам, причем ввод данных выполняется вручную сетевым администратором. Также вручную (если в данной сети нет службы DHCP) конфигурируется любая, подключенная к Internet рабочая станция пользователя, где указывается IP-адрес и DNS-сервер, обслуживающий данную зону.

Выполняемый в рамках транзакции DNS-обмен данными между рабочей станцией и DNS-сервером состоит из запроса и ответа. Запрос на разрешение имени посылается клиентом в виде небольшого кадра, размер которого определяется длиной запрашиваемого имени. Кадры запросов DNS являются одноадресными и направляются прямо на DNS-сервер. Следует отметить, что используемый UDP-протокол (53-й порт) является дейтаграммным, и он не требует идентификации пользователя с помощью процедуры установления соединения.

Получив запрос, DNS-сервер проверяет наличие в базе данных записи, соответствующей запрошенному имени. Ответный кадр содержит раздел DNS Answer, где помещается как запрошенное имя, так и его IP-адрес. Если имя не существует, сервер либо возвратит клиенту сообщение "Name does not exist", либо (в режиме рекурсии) передаст запрос на другой сервер. Если первый рекурсивный DNS-сервер не имеет данных по запрошенному имени, он передает рекурсивный запрос на следующий по иерархии DNS-сервер. Размер кадра при этом не меняется и корректируется только адрес назначения и источника. Если вышестоящий DNS-сервер располагает необходимой информацией, он передаёт её первому серверу, который в свою очередь пересылает ответ клиенту (рис.6).

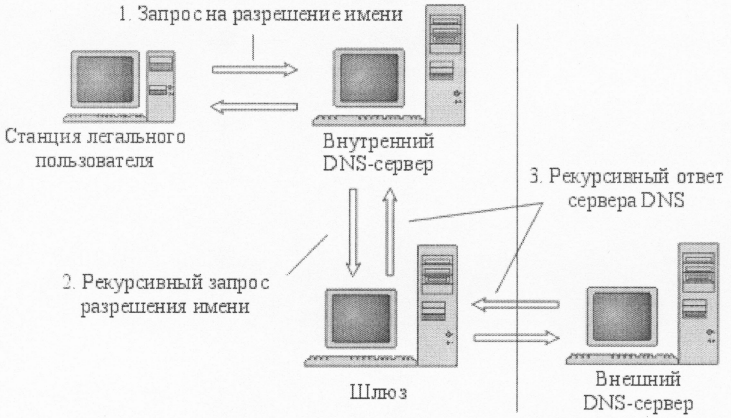

Рис.6. Схема обмена данными между рабочей станцией и DNS-сервером в случае запроса на разрешение имени

Использование такого сервиса предоставляет злоумышленнику несколько сценариев для проведения атаки на DNS-службу.

Во-первых, может существовать две цели такой атаки:

- ввод ложного объекта для изменения маршрута следования пакетов при взаимодействии хостов в сети;
- изменение имени хоста или его IP-адреса с целью навязывания легальным пользователям сети получения посторонней информации при обращении к известным сетевым ресурсам.

Во-вторых, атака может быть направлена на сетевую станцию (и тогда пострадает конкретный пользователь) либо на DNS-сервер определенного уровня иерархии. В последнем случае пострадают не только пользователи, работающие с этим сервером, но и другие пользователи ЛКС, так как информация о ложном маршруте будет со временем продублирована в кэше других DNS-серверов, совершающих рекурсивные запросы.

Заметим, что атаки на DNS-службу, в отличие от атак на протокол ARP, могут быть внутренними, сетевыми, а также межсетевыми, когда атакующий компьютер может находиться на огромном расстоянии от объекта атаки. При этом ввод ложного маршрута позволит "перебросить" трафик ЛКС, например, на другой континент, а после анализа вернуть его обратно. В этом случае атакованный объект почувствует только увеличение времени реакции системы, что, в принципе, может быть вызвано и другими причинами.

Рассмотрим несколько сценариев проведения атак указанного типа.

2.4.1. Перехват DNS-запроса

В случае внутренней атаки возможен перехват DNS-запроса компьютером с программой-сниффером. В случае сетевой атаки перехват одноадресного DNS-запроса возможен после успешной ARP-атаки. Перехват влечет за собой ложный ответ, так как значение порта отправителя в UDP-пакете и значение идентификатора запроса (ID) указаны в перехваченном запросе. Ложный ответ может содержать IP-адрес атакующего компьютера либо IP-адрес постороннего

сайта. Далее атакующий ожидает получение первого информационного пакета от обманутого хоста для сохранения и анализа, затем информационный пакет направляется по реальному адресу назначения (рис.7), либо атакованный ПК получает информацию постороннего содержания (рис.8).

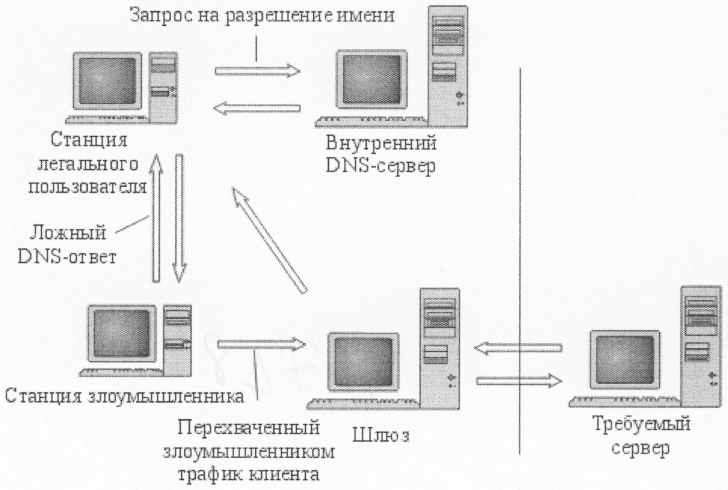

Рис.7. Атака «перехват DNS-запроса» с целью отвода трафика атакованного ПК на атакующую станцию

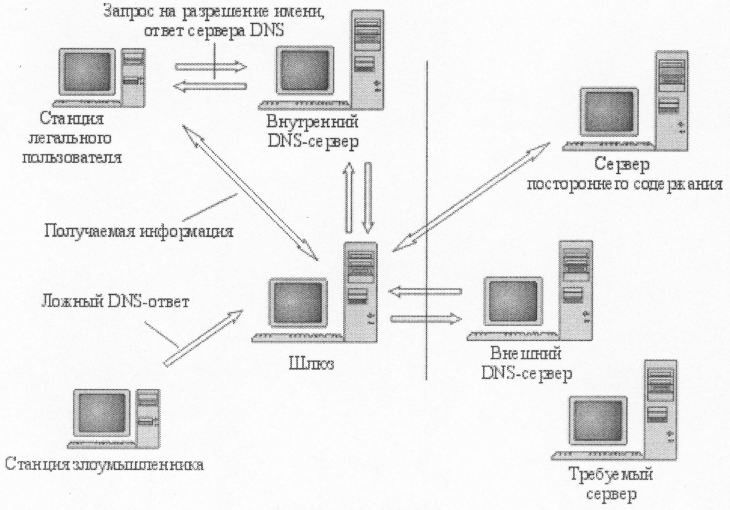

Рис.8. Атака «перехват DNS-запроса» с целью подмены IP-адреса, запрошенного легальным пользователем

Защита ЛКС от внутренней или сетевой атак легко осуществляется с помощью ССАУ "Трафик" в рамках анти-снифферной программы.

2.4.2. Направленный шторм DNS-ответов

Значительно более опасной может оказаться межсегментная атака. В случае её проведения злоумышленнику не удается получить в свою сеть одноадресный DNS-запрос. Мало того, для организации успешной атаки ему необходимо знать как минимум адрес сервера, имя которого может быть запрошено объектом.

В этом случае злоумышленник пойдет путем поиска легальных клиентов интересующего его ресурса. Поиск может быть реализован не только технологическими средствами, но и путем общения по переписке, из различных печатных источников и т.д.

Обнаружив, что какой-то пользователь сети подключается к нужному ресурсу, злоумышленник может организовать атаку, основанную на передаче большого количества направленных на IP-адрес объекта DNS-ответов, указывающих на IP-адрес атакующего ПК как на искомый адрес. Атакующий не может знать конкретного времени появления необходимого ему запроса, поэтому ему придется осуществлять шторм DNS-ответов в течение длительного промежутка времени.

Следует учитывать то, что атакующему субъекту неизвестен номер UDP-порта, с которого будет послан DNS-запрос, а также двухбайтовый идентификатор DNS-запроса (ID). Однако известно, что номер порта имеет ограниченный диапазон значений, начиная с цифры 1023. Перебором всех возможных значений UDP-порта в DNS-ответах может быть достигнута цель атаки, если учесть возможность "притормозить" с ответом реальный DNS-сервер. Атака, позволяющая резко уменьшить производительность сервера, будет рассмотрена в разделе «Направленный шторм TCP- запросов на создание соединения». Двухбайтовый идентификатор запроса ID обычно не является проблемой, так как в DNS-запросах большинства браузеров этот идентификатор задается равным единице.

Таким образом, анализ атаки данного типа показывает, что имеет место вполне определенный сценарий поведения трафика в момент начала атаки - последовательность приходящих на внешний шлюз сети пакетов с идентификатором DNS-ответа, имеющих вполне определенную периодичность в единицу времени и содержащих перебор значения номера UDP-порта отправителя. Такой тип трафика может быть легко идентифицирован в общем потоке проходящих через ССАУ "Трафик" пакетов и заблокирован на основе ввода временного фильтра.

2.4.3. Направленный шторм рекурсивных DNS-ответов на DNS-сервер

DNS-сервер регулярно получает запросы от своих клиентов, разрешение которых невозможно из-за отсутствия соответствующей информации в его базе данных. В этом случае DNS-сервер сам выступает в роли генератора DNS-запроса, обращаясь за разрешением символьного имени к DNS-серверу более высокого уровня, а затем уже транслирует полученную информацию

запросившему хосту. Из этой схемы видно, что злоумышленник может применить описанную выше схему атаки (перехват запроса и штурм DNS-ответов) для ввода в заблуждение DNS-сервера. При этом необходимо учитывать, что в случае успешной атаки ложный IP-адрес будет со временем транслирован большому количеству хостов-клиентов, использующих DNS-сервис данного сервера. Кроме того, полученный от вышестоящего сервера ответ будет храниться в памяти DNS-сервера обычно не очень долго (по умолчанию 60 минут). Поэтому даже часто используемые корпоративными компьютерами адреса наверняка будут обновляться рекурсивными запросами сервера каждое утро, что значительно упрощает задачу злоумышленника.

Такая атака может преследовать цель отвода потока информации на ложный объект для анализа перехваченного трафика, либо может быть направлена на реализацию угрозы целостности - например, замену доступа пользователя к нужной ему информации доступом к сайтам "сомнительного содержания" (рис.9).

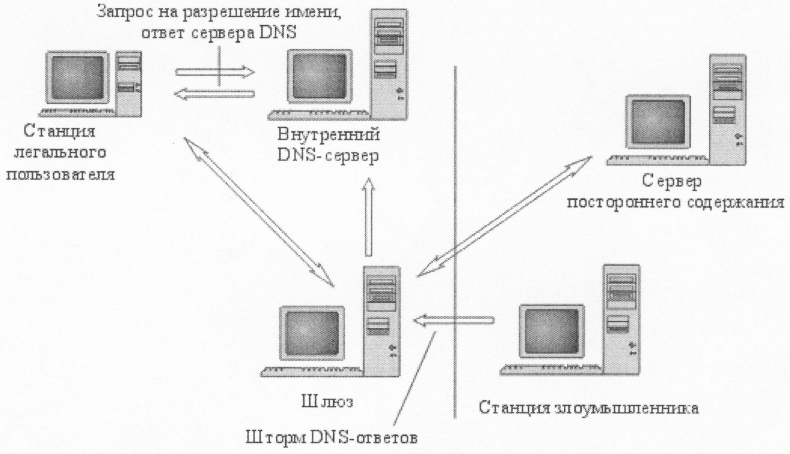

Рис.9. Подмена доступа пользователя к нужной ему информации демонстрацией сайта "сомнительного содержания"

При реализации атаки перехват запроса достаточно проблематичен, так как эти пакеты предназначены обычно DNS-серверам, находящимся в других подсетях, и они передаются по магистральным коммуникациям, подключение к которым простых пользователей не предусматривается.

Поэтому для осуществления атаки необходим шторм DNS-ответов. В отличие от аналогичной DNS-атаки на хост, DNS-сервер при генерации запросов активно использует двухбайтовый идентификатор ID в заголовке запроса. Значение увеличивается при каждом новом запросе на единицу. Определить примерное текущее значение возможно, например, генерацией стандартных DNS-запросов злоумышленником с последующим анализом средней скорости изменения идентификаторов ID из заголовков DNS-ответов. В противном случае атакующий может попытаться решить свою проблему "в лоб", т.е. простым перебором всех возможных значений. Перебор достаточно

длительный процесс (в предельном случае нужно передать 65536 вариантов запросов). Возможна также попытка вывода DNS-сервера из строя, например применением одного из описанных ниже способов, с целью добиться перезагрузки операционной системы сервера, что приблизит значение ID к единице.

В обоих вариантах атак присутствует явно выраженный шторм DNS-ответов, только с перебором значения ID в заголовках пакетов. Для обеспечения защиты ЛКС от атак такого типа в базе возможных сценариев удаленных атак ССАУ "Трафик" нужно иметь ряд шаблонов для идентификации атаки на службу DNS-сервера.

2.5. Атаки на основе технологических особенностей протокола TCP

Одним из базовых протоколов в сетях TCP/IP по доставке данных от одного ПК сети к другому является TCP (Transmission Control Protocol) протокол. Перед началом передачи данных на основе этого протокола необходимо установить виртуальное соединение между этими компьютерами (простая передача данных может быть реализована и без использования протокола TCP). После того как виртуальное соединение установлено, существует возможность выделить пакеты данного виртуального соединения в общем потоке приходящих пакетов на основе нумерации отправляемых компьютером-источником пакетов начиная с первого, а также контролировать пакетами подтверждения успешную доставку адресату очередного (пронумерованного) пакета.

Дополнительной задачей протокола является обеспечение защиты от подмены одного из субъектов TCP-соединения. Для идентификации пакета, кроме IP-адреса отправителя, используют счетчик отправленных пакетов, называемый здесь Sequence Number (номер последовательности), а также Acknowledgment Number (номер подтверждения). При создании виртуального TCP-соединения номера последовательности и подтверждения начинаются не с единицы, а с некоторого, почти случайного значения (каждый из номеров имеет 32 бита в TCP-заголовке). Дополнительно к этому для передачи используются 6 управляющих бит:

- URG - поле безотлагательного указателя;
- ACK - значение поля подтверждения;
- PSH - функция продвижения;
- RST - восстановить соединение;
- SYN- синхронизировать числа последовательности;
- FIN - конец передачи данных.

Несколько упрощенная схема создания TCP-соединения выглядит следующим образом (рис.10):

- инициатор TCP-соединения передает кадр-запрос на создание соединения, в котором поднят флаг SYN (SYN=1), и устанавливает некоторое начальное значение номера последовательности;
- адресат отвечает кадром подтверждения готовности установить соединение с поднятыми флагами SYN и ACK и предлагает некоторое начальное значение своего номера последовательности; при этом номер подтверждения содержит номер из поля последовательности первого пакета, увеличенный на единицу;

- инициатор заканчивает процедуру установления соединения третьим кадром, с поднятым флагом ACK и номерами последовательности и подтверждения, увеличенными на единицу.

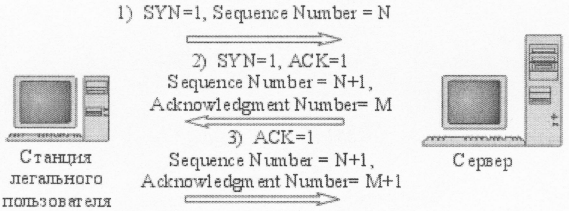

Рис.10. Упрощенная схема TCP-соединения

После того как виртуальное соединение установлено, выполняется передача сообщения между передающим и принимающим компьютерами.

2.5.1. Подмена субъекта TCP-соединения

Очевидно, что процесс установления соединения, идентифицирующий источник принятого пакета в рамках TCP-соединения по трем значениям полей (IP-адрес, номера последовательности и подтверждения), предоставляет возможности для взаимодействия от ложного имени. Достаточно заманчивой для злоумышленника оказывается следующая ситуация. Существует возможность подождать момента, когда один из легальных пользователей-администраторов системы, создав TCP-соединение, произведет идентификацию и аутификацию на сервере и слегка замешкается. Нет никаких препятствий, захватив предыдущие пакеты с необходимыми номерами, продолжить работу с сервером от имени и с IP-адреса легального пользователя-администратора. Тем более, что в момент возобновления работы администратора его пакеты будут отвергнуты в рамках установленного TCP-соединения, так как сохранившиеся на компьютере клиента номера "устареют" (работа злоумышленника с системой приводит к увеличению значений номеров последовательности и подтверждения), и администратору придется устанавливать новое соединение.

Такой сценарий может быть реализован только при наличии возможности у атакующего захватывать сетевые пакеты для анализа номеров последовательности и подтверждения с помощью программы сниффера (используя внутреннюю или сетевую атаки). В этой связи применение анти-снифферной подсистемы ССАУ «Трафик» может обеспечить защиту ЛКС от атак рассмотренного типа.

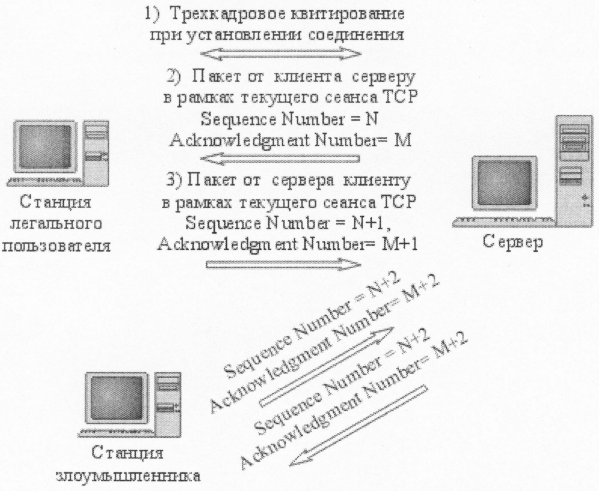

Рис.11. Схема атаки с заменой субъекта TCP-соединения

2.5.2. Направленный шторм TCP-запросов на создание соединения

Существует большое количество сценариев удаленных сетевых атак, направленных на провоцирование угрозы отказа в обслуживании путем нарушения работоспособности сетевых компьютеров.

Рассмотрим наиболее простые из таких сценариев.

Направленный шторм TCP-запросов на создание соединения - один из указанных сценариев.

Очевидно, что сервер, предназначенный для взаимодействия одновременно со многими клиентами, имеет возможность установить более одного сеанса TCP-соединения. При этом соединение устанавливается не сразу, а в течение некоторого времени, требуемого для генерации пакетов процедуры трехкадрового квитирования. Сервер, в случае получения нескольких пакетов подряд с запросом на создание соединения, не может ответить всем клиентам сразу. Поэтому он должен сохранить эти запросы в своей памяти и обработать их последовательно, поставив в очередь на обработку в соответствии со временем прихода.

В такой ситуации возможна атака, основанная на передаче большого количества запросов на создание TCP-соединения (рис.12). При этом процессор сервера обязан сгенерировать для каждого запроса свой номер подтверждения и сформировать пакет для ответа, что занимает определенное время. В случае использования на предприятии высокоскоростных магистральных линий связи можно передать такое количество запросов на соединение, что даже самый высокопроизводительный сервер будет тратить 100% процессорного времени на генерацию ответов. В результате сервер перестает отвечать на легальные запросы (отказ в обслуживании), либо полностью "зависает".

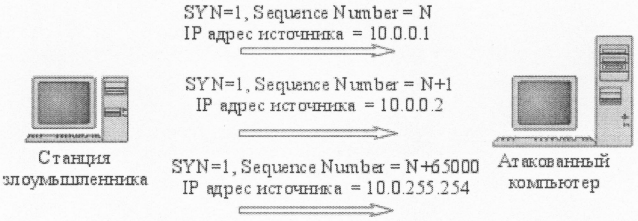

Рис.12. Направленный штурм TCP-запросов на создание соединения

Ситуация осложняется еще и тем, что четвертая версия TCP/IP не позволяет отслеживать маршруты пакетов из удаленных подсетей. Поэтому попытки реализации протокола TCP/IP некоторых производителей сетевых операционных систем с ограничением количества открытых TCP-сеансов с одним IP-адресом не приведут к защищенности от атак такого типа. Ничего не мешает генерировать шторм TCP-запросов с перебором любых IP-адресов, ведь атакующий не ждет на них ответа.

Защита от атак указанного типа может быть реализована системой ССАУ "Трафик". Расположение системы на внешнем шлюзе ЛКС позволяет реально ограничить количество запросов на создание TCP-соединения с конкретным IP-адресом получателя пакета.

2.6. Атаки с использованием ошибок в модулях сетевых служб

Конечно, большинство злоумышленников, не являясь специалистами в области телекоммуникационных технологий, вряд ли смогут осуществить атаку, требующую, например, проведения анализа сетевого трафика. Их главной целью является реализация угрозы отказа в обслуживании с применением готовых программ, использующих известные ошибки в модулях сетевых служб. Производители сетевых операционных систем, конечно же, знают о существовании таких уязвимостей, но устранить ошибку не всегда удается локально, без кардинальной переработки ядра системы.

2.6.1. Атака с использованием некорректных данных в заголовке

Одним из таких способов является атака с использованием пакета, в заголовке которого IP-адрес источника совпадает с IP-адресом получателя, а в TCP-заголовке порт назначения совпадает с портом источника (рис.13). Как показывают эксперименты, многие операционные системы неадекватно реагируют на получение такого пакета. Сервер может тратить 100% процессорного времени в течение нескольких десятков секунд на обработку принятой информации, отказывая в обслуживании легальным пользователям сети. Таким образом, можно "притормозить" работу сервера и на более длительный срок, периодически посылая ему некорректные данные.

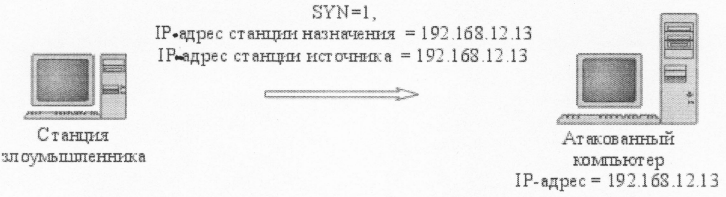

Рис.13. Атака с использованием некорректного адреса в заголовке пакета

Анализ адресной части прибывающих пакетов в ССАУ "Трафик" позволяет предотвратить реализацию такой атаки на ЛКС.

2.6.2. Атака с использованием ошибки в модуле сборки фрагментированных пакетов

Одним из концептуальных достоинств TCP/IP-протокола является возможность фрагментации пакетов при передаче информации в сетях, использующих различные технологии. Действительно, сеть Интернет представляет собой совокупность локальных сетей, сопряженных между собой шлюзами. Локальные сети могут быть построены с использованием различных технологий. Например, для передачи данных из одной сети Ethernet (размер пакета варьируется в пределах от 64 до 1518 байт) в другую сеть Ethernet, может потребоваться транзитная передача через сеть стандарта ATM (размер пакета 53 байта). Такая передача не была бы возможной без разделения большого пакета Ethernet на фрагменты для передачи через ATM.

К сожалению, процедура фрагментации не свободна от ошибок. Разработчики сетевых протоколов постарались предусмотреть различные нестандартные ситуации, возникающие в процессе сборки-разборки пакетов. В частности, может возникнуть ситуация, когда началу следующего фрагмента отвечает адрес, попадающий не в конец, а в середину предыдущего. В этом случае нужно выровнять фрагменты и поставить данные на положенные им места. Алгоритм выравнивания приводит к отрицательной величине смещения, если длина пришедшего фрагмента меньше размера перекрытия. Этим может воспользоваться злоумышленник. Так как смещение указывает на текущий адрес в оперативной памяти компьютера, то его отрицательная величина приводит к записи фрагмента по случайному адресу, и это, в свою очередь, может вызвать отказ в работе программ операционной системы.

Атаку такого типа можно идентифицировать с помощью ССАУ "Трафик" путем анализа длин фрагмента и смещения.

2.7. Удаленное сканирование портов на объектах атаки

На начальном этапе организации удаленной атаки злоумышленнику важно определить потенциальные возможности для её проведения. Для этого ему необходимо собрать информацию о задействованных на объекте службах и сервисах. Каждая из таких программ является серверным приложением, отвечающим на запросы клиентов. Обращение к требуемому сервису

происходит после идентификации соответствующего номера порта протокола TCP. При этом каждый из обращающихся клиентов перед началом взаимодействия с сервером обязан установить виртуальное TCP-соединение, независимо от интересующей его службы.

То есть на начальном этапе все обращения имеют одинаковую форму, меняется только номер порта назначения. Атакующему остается лишь сгенерировать TCP-запросы с перебором возможных TCP-портов. Получение на посланный им запрос подтверждения с поднятыми флагами SYN и ACK позволяет обнаружить работающую серверную программу.

Сканирование TCP-портов может быть обнаружено с помощью ССАУ "Трафик" по регулярному поступлению на определенный IP-адрес пакетов с запросами, содержащими последовательный перебор портов назначения.

3. Основные задачи подсистемы защиты ЛКС

Попытки создания систем для эффективной защиты ЛКС от сетевых атак предпринимаются уже достаточно давно. На решение таких задач нацелены, в частности, программные продукты семейства firewall, обеспечивающие защиту ЛКС путем включения в процесс маршрутизации процедур различных фильтров, чем существенно ограничивается спектр реализуемых в сети приложений. На рынке коммерческих продуктов существуют и более развитые системы противодействия сетевым атакам, ряд из которых представлен нами ниже.

3.1. Система обнаружения вторжения ICEcap Security Suite

ICEcap Security Suite – это гибридная система безопасности, которая включает в себя несколько компонентов. ICECAP Manager устанавливает, управляет и сопровождает на всех компьютерах сети программные продукты трех типов: BlackICE Agents, BlackICE Sentries и BlackICE Guards.

BlackICE Agents развертываются на каждом сервере, рабочей станции и терминале удаленного пользователя и обеспечивают защиту как всей ЛКС, так и ее отдельных элементов. BlackICE Agents поддерживают широкий набор средств обеспечения безопасности сети. BlackICE агенты реализованы для ОС Solaris, Linux и Windows и совместимы с VPN-клиентами.

BlackICE Guards нацелены на обнаружение и обезвреживание сетевых атак, прежде чем те достигают своего результата.

BlackICE Sentries обеспечивают обнаружение вторжения на Gigabit- и Fast Ethernet-сегментах сети без применения дорогих аппаратных средств.

С помощью указанных компонентов менеджер собирает информацию о различных нестандартных ситуациях в сети, производит запись сетевого трафика для документирования процесса сетевой активности и для принятия административных мер. Совместная работа компонентов позволяет отслеживать нежелательные события по всем сегментам сети.

3.2. Система обнаружения вторжения Dragon

Dragon (Enterasys) – это гибридная система, которая включает в себя Dragon Sensors, Dragon Squire и Dragon Server.

Dragon Sensors – это датчик реального времени, который работает непосредственно с трафиком канального уровня. В случае обнаружения вторжения Dragon Sensors может посылать E-mail сообщения сетевому администратору для принятия мер по пресечению сетевой атаки и делает запись в Log-файлы для последующего анализа.

Dragon Squire – это датчик, контролирующий трафик сетевой активности сетевого адаптера сервера или хоста. Он просматривает Log-файлы с целью установления факта злонамеренной или нестандартной активности приложений. Dragon Squire также может анализировать firewall Log-файлы, процессы на маршрутизаторах и других сетевых компонентах, которые могут применять протокол SNMP или вести Syslog.

Dragon Server обеспечивает управление всеми компонентами Dragon Sensors и Dragon Squire, записывает нестандартные события в основную базу данных. Dragon Server включает разнообразные сообщения и инструменты анализа E-mail, SNMP- или Syslog-сообщений.

3.3. Система обнаружения вторжения Cisco Secure

Cisco Secure – это система обнаружения сетевых атак посредством контроля сетевого трафика. Она включает систему датчиков и администраторов.

Cisco Secure датчик – это сетевое устройство, которое используется для анализа больших объемов IP-трафика в сети и Syslog-информации от Cisco маршрутизаторов. Атаки транслируются в значимые случаи безопасности, которые передаются Cisco Secure администратору. Датчик может также регистрировать данные Log-файла безопасности, сокращать TCP-сессии и динамически управлять таблицами маршрутизаторов.

Cisco Secure администратор имеет централизованный графический интерфейс для управления безопасностью распределенной сети. Он также выполняет следующие функции: управляет трафиком с помощью приложений сторонних производителей, осуществляет доступ к базе данных безопасности сети, производит удаленное управление датчиками, посылает электронную почту системному администратору. Администратор централизованно контролирует деятельность множества датчиков, расположенных в сетях с различными сетевыми стандартами.

3.4. Система обнаружения вторжения RealSecure

Один из самых быстроразвивающихся программных продуктов - это сетевой монитор безопасности RealSecure 3.0 компании Internet Security Systems.

RealSecure – это гибридная система, состоящая из сетевых датчиков, OS-датчиков и менеджера. Сетевые датчики анализируют сетевой трафик на предмет обнаружения известных сценариев атак, нарушений в работе различных протоколов и повторных попыток доступа. OS-датчики анализируют работу ядра ОС, просматривают Log-файлы с целью обнаружения и предотвращения случаев несанкционированной деятельности в реальном масштабе времени.

RealSecure также обеспечивает защиту ЛКС от сетевых атак с помощью межсетевого экрана и маршрутизатора, управляя правилами фильтрации сетевого трафика.

3.5. Задачи подсистемы защиты ЛКС

Анализ существующих систем безопасности показывает, что доступные коммерческие системы обнаружения атак не способны обеспечить эффективную защиту ЛКС [5]. Существует множество нерешенных на данный момент проблем, сдерживающих интенсивное развитие и массовое внедрение систем обнаружения вторжения.

Вот некоторые из таких проблем:

- теоретически только системы, основанные на принципе идентификации аномальных событий (принцип «свой-чужой») в ЛКС, способны обнаружить новые и неизвестные типы атак; к сожалению, в существующих системах слишком высок уровень ложных срабатываний, что перекладывает основную часть работы по анализу спорных фрагментов сетевого трафика на администратора сети и делает применение таких систем малоэффективным;
- системы обеспечения безопасности различных производителей используют разные протоколы обмена сообщениями и управляющей информацией, т.к. не существует ни международных, ни де-факто стандартов для систем защиты сетевых ресурсов;
- системы обнаружения вторжений на основе высокоскоростных аппаратных датчиков чрезвычайно дороги (требуется большое количество датчиков, изготовленных на заказ, да еще с необходимостью конфигурирования каждого датчика в отдельности);
- системы на основе баз данных содержат широкий набор известных атак, однако это требует их регулярной модификации – необходимы организационные мероприятия по стимулированию обновления баз широким кругом заинтересованных фирм и организаций;
- многие коммерческие решения в области систем обнаружения вторжения нацелены на запись Log-файлов трафика обнаруженных сетевых атак в целях дальнейшего судебного разбирательства, однако основная задача систем должна быть сосредоточена на недопущении вторжения;
- существует тенденция разработки систем обнаружения вторжений с большим количеством датчиков и агентов для установки «внутри» локальных сетей, однако высокая сложность соединений в глобальных сетях, рост размеров сетей подчеркивают перспективность разработки систем работающих именно на границах сетей [5];
- коммерческие системы, будучи полностью закрытыми для пользователей, не позволяют добавлять собственные сценарии для борьбы с новыми типами атак, чем сильно огранивают свои возможности.

С учетом вышесказанного, на первом этапе разработки подсистемы обеспечения безопасности ЛКС в среде ССАУ «Трафик» мы планируем:

- создать базу данных со сценариями поведения сетевого трафика (база шаблонов) для рассмотренного выше набора типовых атак;
- разработать систему кэширования сетевого трафика с последующим анализом по шаблонам сетевых атак;
- разработать комплекс методов противодействия сетевым атакам в режиме реального времени, основанных на принципе «свой-чужой».

Заключение

В рамках данной статьи мы постарались отразить наиболее известные сценарии сетевых атак и предложить методы борьбы с ними на основе ССАУ «Трафик». В настоящее время разрабатывается открытая подсистема с наращиваемой базой сценариев сетевых атак, которая, в первую очередь, будет играть роль полигона для отработки различных подходов по защите ЛКС. Кроме того, такой полигон позволит исследовать возможности установления факта атаки уже на канальном уровне, не привлекая для этого данных сетевого, сеансового и прикладного уровней модели OSI. Такой подход должен существенно ускорить процесс идентификации реализуемой сетевой атаки.

На первом этапе разработки подсистемы защиты ЛКС основное внимание уделяется решению следующих задач:

- формирование базы шаблонов с представлением в ней различных по своей природе типов атак;
- оптимизация структуры базы шаблонов для быстрого поиска шаблона, адекватного сценарию предполагаемой атаки, с тем, чтобы обеспечить возможность мониторинга сетевого трафика в режиме реального времени;
- разработка максимально простой структуры базы данных для предоставления возможности ее наполнения широким кругом заинтересованных специалистов;
- разработка программных средств для генерации искусственных сетевых атак, включаемых в базу шаблонов; такой набор программных средств необходим, в частности, для разработки алгоритмов идентификации аномальных событий при анализе сетевого трафика уже на канальном уровне;
- подготовка подробного описания структуры базы шаблонов, а также каждого шаблона в отдельности; подготовка соответствующих описаний для публикаций.

В заключение следует отметить следующую важную особенность разрабатываемого нами подхода. Несмотря на то, что система защиты ЛКС устанавливается на компьютере-маршрутизаторе, т.е. на границе между подсетями, она не является аналогом firewall-а, а значит не препятствует функционированию распределенных сетевых приложений. В этой связи появляется возможность применения такого подхода в GRID-технологиях, где защита на основе firewall-а не может использоваться в принципе.

Литература:

[1] А.В. Лукацкий. Обнаружение атак. - СПб.: БХВ-Перербург,2001

[2] П.М. Васильев, В.В. Иванов, В.В. Кореньков, Ю.А. Крюков, С.И. Купцов. Система сбора, анализа и управления сетевым трафиком фрагмента сети ОИЯИ на примере подсети университета "Дубна", Сообщения ОИЯИ,

Д11-2001-266, Дубна, 2001.

[3] И.Д. Медведовский, П.В. Семьянов, Д.Г. Леонов. Атака на Internet. М.: ДМК,1999.

[4] Корпоративные технологии Microsoft Windows NT Server 4.0. Учебный курс.Пер. с англ. - М.: Издательский отдел "Русская Редакция" ТОО "Channel Nrading Ltd.". - 1998.

[5] North Atlantic Treaty Organisation, Research and Technology Organisation, RTO Technical Report 49, Intrusion Detection: Generics and State-of-the-Art. Copyright RTO/NATO, 2002.

[6] Материалы сайта http://www.microsoft.com

[7] Материалы сайта http://www.hackzone.ru/

[8] А.В. Лукацкий, Адаптивная безопасность сети. "КомпьютерПресс". №8, 1999.

[9] Microsoft Corporation. Microsoft System Management Server 2.0. Учебный курс: Официальное учебное пособие. «Русская редакция», 2000г.

[10] В.Б. Вехов. Компьютерные преступления: способы совершения и раскрытия. М.: Право и Закон, 1996.

[11] В. Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. "Питер", 1999, 672 стр.

[12] А.В. Галатенко. О применении методов теории вероятностей для решения задач информационной безопасности. Вопросы кибернетики. М.: 1999, РАН, НИИСИ.

[13] Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларированных возможностей. Гостехкомиссия России, 1999.

[14] В.В. Дрожжин. Логические средства анализа защищенности программных систем. Тезисы межрегиональной конференции "Информационная безопасность регионов России", 1999.

[15] Е. Ерхов. Сценарии атак на банковские системы в сети Internet. "Аналитический банковский журнал". № 7, 1998.

[16] Peter Capell. Analysis of Courses in Information Management and Network System Security & Survivability. December 1998. SPECIAL REPORT, CMU/SEI-99-SR-006.

[17] Конфигурация системы защиты ОС Windows® NT 4.0 для использования системы RealSecure. Защита узла Windows NT при обнаружении атак. Internet Security Systems. Перевод с англ. Лукацкого А. В. и Цаплева Ю. Ю. March 26, 1998.

Получено 27 декабря 2002 г.

Васильев П. М. и др. Д11-2002-292

Основные принципы обеспечения безопасности локальной компьютерной сети на основе ССАУ «Трафик»

Ранее нами была создана система сбора, анализа и управления сетевым трафиком (ССАУ «Трафик») для сегмента компьютерной сети ОИЯИ. В настоящей работе рассмотрены наиболее известные сценарии сетевых атак и предложены методы борьбы с ними на основе ССАУ «Трафик». Несмотря на то, что система защиты локальной сети устанавливается на компьютере-маршрутизаторе, она не является аналогом firewall и не препятствует функционированию распределенных сетевых приложений. В этой связи появляется возможность применения такого подхода в GRID-технологиях, где защита сети на основе firewall не может использоваться в принципе.

Работа выполнена в Лаборатории информационных технологий ОИЯИ.

Сообщение Объединенного института ядерных исследований. Дубна, 2002

Перевод авторов

Vasiliev P. M. et al. D11-2002-292

Main Concept of Local Area Network Protection on the Basis the SAAM «Traffic»

In our previous paper we developed a system for acquisition, analysis and management of the network traffic (SAAM «Traffic») for a segment of the JINR local area computer network (JINR LAN). In our present work we consider well-known scenaria of attacks on local area networks and propose protection methods based on the SAAM «Traffic». Although the system for LAN protection is installed on a router computer, it is not analogous to the firewall scheme and, thus, it does not hinder the performance of distributed network applications. This provides a possibility to apply such an approach to GRID-technologies, where network protection on the firewall basis can not be basically used.

The investigation has been performed at the Laboratory of Information Technologies, JINR.

Communication of the Joint Institute for Nuclear Research. Dubna, 2002

Редактор *М. И. Зарубина*
Макет *Н. А. Киселевой*

Подписано в печать 28.01.2003.
Формат 60 × 90/16. Бумага офсетная. Печать офсетная.
Усл. печ. л. 1,75. Уч.-изд. л. 2,9. Тираж 240 экз. Заказ № 53728.

Издательский отдел Объединенного института ядерных исследований
141980, г. Дубна, Московская обл., ул. Жолио-Кюри, 6.
E-mail: publish@pds.jinr.ru
www.jinr.ru/publish/