УДК 681.324

В.Н. ГУГНИН, ст. преп. НТУ «ХПИ» (г. Харьков),
Д.В. СОТНИК, вед. программист ЗАО "ИИТ Циклон" (г. Харьков)

АТАКА НА СЕЛЕКТИРУЮЩИЕ КОММУТАТОРЫ С ЦЕЛЬЮ ПЕРЕХВАТА ДАННЫХ В ЛОКАЛЬНОЙ СЕТИ

В статті розглядаються методи перехоплення даних у локальній мережі, побудованій на селектуючих комутаторах . Зроблені висновки та наведені рекомендації щодо визначення факту перехоплення даних та способів боротьби із зловмісниками.

In present article were overviewed methods of data interception in local network, based on switching hubs. Adducted some conclusions and recommendations for data intercepting detection and methods for delinquents control.

Постановка проблемы. Перехват данных в локальной сети является на сегодняшний день одной из наиболее значительных угроз безопасности. В зависимости от цели злоумышленника объектом перехвата являются либо внутрисетевой поток данных, либо данные, передаваемые из локальной сети в сеть Internet. В первом случае целью злоумышленника является перехват личных данных для обеспечения несанкционированного доступа к защищенным внутрисетевым ресурсам. Во втором случае целью злоумышленника является обеспечение доступа к сторонним Internet ресурсам или бизнес-данным (банковские счета и т.д.). Внутрисегментный перехват данных в локальной сети, несмотря на ее аппаратные ограничения, является выполнимым. Анализ атак и обнаруженных уязвимостей сети показывает, что перехват данных является технически возможным.

Анализ литературы. В настоящее время аппаратная архитектура Ethernet завоевала большую часть рынка при создании локальных сетей, хотя существуют и другие аппаратные решения не на IEEE 802.3, такие как FDDI, Token Ring (802.5), ARCNET, WAN, ATM и другие. Относительная недороговизна в сочетании с технической скоростью передачи данных в 10, 100 и 1000 мегабит в секунду способствует ее популярности.

Анализаторы пакетов относятся к классу инструментальных программных средств для мониторинга сетевого трафика и выявления некоторых типов сетевых проблем. По умолчанию сетевой интерфейс видит пакеты, предназначенные только для него. Практически все сетевые карты поддерживают возможность перехвата пакетов, передаваемых по общему каналу локальной сети [1]. Селектирующие коммутаторы перенаправляют пакеты только целевому узлу, анализируя проходящие пакеты для определения расположения подключенных узлов. Таким образом, перехват данных становится теоретически невозможным.

Цель статьи. В данной статье рассматриваются методы перехвата данных в локальной сети, построенной на селектирующих коммутаторах. Сделаны выводы и приведены рекомендации относительно определения факта перехвата данных и способов борьбы со злоумышленниками.

Основной раздел. Во многих протоколах на базе TCP пароль передается в открытом виде. К таким протоколам относятся telnet, ftp, pop3 и многие другие. На смену им пришли "ssh", "apop" и подобные, но полный переход на новые протоколы займет еще немало времени. При успешном перехвате данных в локальной сети злоумышленник получает возможность узнать пароль без необходимости декодирования [2].

Селектирующие коммутаторы позволяют направлять поток данных только целевому узлу, без копирования пакетов на остальные порты коммутатора. Таким образом, перехват данных в сети, построенной на такой аппаратной основе, становился практически невозможным без вмешательства в работу коммутатора или изменения маршрута передачи данных на узлах сети [3]. Атаки с целью перехвата данных могут быть следующих видов:

Таблица 1

Классификация атак с целью перехвата данных

Вид атаки	Тип атаки	Цель
Пассивный перехват	Пассивный	Перехват пакетов, ошибочно посланных на чужой порт
Переполнение буфера коммутатора	Атака на коммутатор	Переключение коммутатора в неселектирующий режим
Дублирующий адрес	Атака на коммутатор	Создание в таблице коммутации записи, эквивалентной записи атакуемой машины
«Человек в середине»	Атака на маршрут передачи	Перенаправление данных между узлами на атакующий узел
«Полукольцо»	Атака на маршрут передачи	Перенаправление исходящих данных одного из узлов на атакующий узел
Подмена узла сети	Атака на маршрут передачи	Перенаправление данных, адресованных атакуемому узлу, на атакующий узел

Рассмотрим указанные виды атак более детально:

Пассивный перехват

Пассивный перехват является одним из наиболее простых способов перехвата данных. Его эффективность зависит от модели используемого селектирующего коммутатора и делает эту атаку малоэффективной для использования. Цель атаки состоит в пассивном перехвате пакетов, которые коммутатор в моменты пиковой нагрузки или при обновлении таблиц маршрутизации может отправить на чужой порт или как широковещательный пакет.

Способов защиты от данной атаки не существует, кроме попытки обнаружения прослушивающих узлов или замены аппаратной части сети.

Переполнение буфера коммутатора

Для хранения таблицы коммутации используется кэш, размер которого в среднем, для наиболее распространенных моделей неинтеллектуальных селектирующих коммутаторов, равен 2 мегабайта. Каждая запись в кэше имеет метку времени, что позволяет коммутатору удалять устаревшие записи из памяти. Атака на переполнение буфера коммутатора ставит своей целью запись в кэш максимально возможного количества данных при помощи пакетов, содержащих произвольный аппаратный адрес. В результате переполнения часть коммутаторов, в зависимости от заложенного производителем алгоритма, может переключиться в неселектирующий режим. В отдельных случаях коммутатор может прекратить работу до перезагрузки. Неселектирующий режим работы коммутатора сильно уменьшает производительность сети, однако позволяет злоумышленнику перехватывать все данные, проходящие через атакованный коммутатор. Наиболее удобным способом выполнения данной атаки является направление на коммутатор потока ARP пакетов с произвольным адресом отправителя. Для затруднения обнаружения данной атаки рекомендуется в качестве аппаратного адреса назначения использовать адрес наименее опасного, с точки зрения обнаружения атак, узла сети. Крайне нежелательно использовать произвольный или собственный адрес, т.к. ARP пакеты будут отправлены как широковещательные или будут нести в себе адрес атакующего узла.

Для обнаружения данной атаки необходимо анализировать проходящие ARP пакеты. Резкое снижение производительности сети, большое количество ARP пакетов, ARP пакеты с произвольными аппаратными адресами могут быть следствием выполняемой атаки. Обнаружение злоумышленника возможно только последовательным физическим выключением каналов с целью обнаружить источник пакетов.

Дублирующий адрес

Аппаратный адрес сетевого адаптера является уникальным идентификатором карты и состоит из кода производителя и производственного номера адаптера. Таким образом, гарантируется уникальность аппаратного адреса в сети. В соответствии с этим, появление узлов с одинаковым аппаратным адресом на разных портах может быть рассмотрено коммутатором как образование кольца, что в некоторых случаях может привести к аварийному завершению работы коммутатора до перезагрузки. Однако большая часть коммутаторов изменяет для атакуемого адреса номер порта в таблице маршрутизации на номер, с которого пришел последний по времени пакет данных. Т.е. при наличии в сети двух узлов с одинаковым аппаратным адресом, коммутатор будет направлять поток входящих данных на порт, с которого пришел последний исходящий пакет. Соответственно входящий поток данных будет переключаться на последний по времени активный порт и при большом количестве исходящих пакетов с обоих узлов входящий пакет данных будет разорван и разбросан по этим двум узлам. Таким образом, и атакующий и атакуемый узел получат фрагменты входящего потока данных. Однако, т.к. протоколом TCP такая ситуация будет рассмотрена как потеря пакетов в канале, недостающие фрагменты будут запрошены каждым узлом и есть вероятность получения пакетов, переданных конкурирующему узлу. В результате этого скорость передачи данных на атакуемом узле сильно уменьшается, что позволяет обнаружить атаку. Использование атакующим узлом межсетевого экрана позволяет сделать его обнаружение практически невозможным.

Косвенным признаком данной атаки может служить резкое снижение скорости обмена данными на узле сети. Обнаружение злоумышленника, использующего межсетевой экран, возможно только последовательным физическим выключением каналов. Анализ ARP пакетов также в большинстве случаев позволяет обнаружить факт атаки, но в случае использования злоумышленником произвольных Ethernet кадров анализ пакетов будет практически невозможен.

«Человек в середине»

Целью атаки является изменение маршрута передачи данных на атакуемых узлах. При отправлении пакета протоколом IP указывается IP адрес назначения. При формировании Ethernet кадра происходит определение аппаратного адреса, соответствующего указанному IP адресу. Для этого используется протокол разрешения адресов ARP, результаты ARP запросов сохраняются в ARP кэше и хранятся в нем определенное время, зависящее от используемой ОС. Записи в кэше также обновляются при обработке чужих

ARP запросов. Таким образом, появляется возможность управлять содержимым данного кэша при помощи специально сформированных ARP запросов [4].

Для перехвата данных между двумя выбранными узлами необходимо изменить записи в кэше атакуемых машин таким образом, чтобы в кэше первого узла аппаратный адрес второго узла был заменен на адрес атакующего и наоборот. В результате этого узлы будут отправлять данные, адресованные другому узлу на адрес атакующего. Атакующий узел должен самостоятельно выполнять маршрутизацию, т.е. заменять адрес во входящем пакете на адрес атакуемого узла (для этого необходимо использовать IP адрес в теле IP пакета) и передавать его атакуемому узлу.

Данные в кэше удаляются через некоторое время или обновляются ARP запросом сторонних узлов, поэтому необходимо повторять перезапись данных в кэше с определенной частотой. Наилучшие результаты, с точки зрения перехвата данных и скрытности атаки, были достигнуты при периоде обновления записей кэша, равном 1 сек. Атака может быть легко обнаружена при просмотре ARP кэша или анализе ARP пакетов программой-монитором. В этом случае возможно определить аппаратный адрес атакующего узла.

Обнаружение атаки возможно при помощи анализа ARP кеша и анализе APR пакетов программой-монитором [5]. В случае, если злоумышленник изменил свой аппаратный адрес, обнаружение его возможно только последовательным физическим выключением каналов.

«Полукольцо»

Данная атака является модификацией атаки «Человек в середине» и применяется в случае, когда один из атакуемых узлов содержит в своем кэше неизменяемую запись или представляет опасность для атакующего с точки зрения обнаружения выполняемой атаки. В этом случае изменяется запись в кэше только одного узла. Таким образом, исходящие данные с атакованного узла будут отправляться на адрес злоумышленника, а входящие данные атакованного узла будут ему недоступны. Атакующий узел должен самостоятельно выполнять маршрутизацию данных с атакуемого узла на узел назначения, иначе атака будет обнаружена [6].

Обнаружение факта атаки и злоумышленника аналогичны атаке «Человек в середине».

Подмена узла

Данная атака является аналогом атаки «Дублирующий адрес», ориентированной на вмешательство в маршрутизацию данных на уровне узла, а не на уровне коммутатора. Атака может выполняться как для всех узлов сети, так и для выбранной группы узлов. Целью атаки является изменение

записи в кэше, соответствующей атакуемому узлу, что позволяет перенаправить весь входящий поток данных, адресованный атакуемому узлу, на атакующий. Атакующий узел должен самостоятельно выполнять маршрутизацию входящих данных на атакуемый узел, иначе атакуемый узел будет недоступен для сети и атака будет обнаружена.

При атаке для всех узлов сети возможно использование широковещательного ARP пакета, однако такой пакет вызовет сообщение о конфликте адресов на атакуемом узле и атака будет обнаружена [7]. Более сложным и скрытным является рассылка ARP пакетов каждому узлу, данные которого к атакуемому узлу необходимо перехватить.

Обнаружение факта атаки и злоумышленника аналогичны атаке «Человек в середине».

Выводы. Рассмотренные способы перехвата данных в локальной сети на селектирующих коммутаторах представляют собой серьезную угрозу безопасности и позволяют злоумышленнику получить доступ к защищаемой информации и, как следствие, к защищаемым объектам сети. Большинство атак не могут быть выявлены в автоматическом режиме. Сам факт атаки определяется в основном по косвенным признакам, поиск злоумышленника, если он использует грамотно настроенный межсетевой экран и измененный аппаратный адрес, возможен только последовательным физическим выключением каналов, с целью обнаружить источник пакетов, либо изменением аппаратной базы сети. Таким образом, администратору локальной сети, построенной на неинтеллектуальных селектирующих коммутаторах, рекомендуется производить регулярный анализ пакетов с целью обнаружения атак, особенно в случае необоснованного падения скорости обмена данными на определенных коммутаторах или для определенного узла [8].

Список литературы: 1. *Медведовский И.Д., Семьянов П.В., Леонов Д.Г.* Microsoft (R) Атака на internet. – С.-Пб.: БХВ – Санкт-Петербург, 2000. – 1056 с. **2.** *Семенов Ю.А.* Протоколы Internet. Энциклопедия. – М.: Горячая линия – Телеком, 2001. – 1100 с. **3.** *Crispin Cowan, Perry Wagle*. TCP/IP "Architecture, protocols, and implementation with IPv6 and IPv4 security". – Department of Computer Science and Engineering, Oregon Graduate Institute of Science & Technology, 2003. – 235 с. **4.** *Джон Д. Рули и др.,* Сети Windows NT 4.0. – К.: BHV, 1998. – 800 с. **5.** *Вильямс А.*, Системное программирование в Windows 2000. – СПб.: ПИТЕР, 2000. – 250 с. **6.** *Семенов Ю. А.* Протоколы и ресурсы Internet. – М.: Радио и связь, 1996. – 320 с. **7.** *Семененко В.А., Величкин А.М., Ступин Ю.В.* Операционные системы. – М.: Высш. шк., 1990. – 192 с. **8.** *Саркисян А.А.* Локальные сети. Руководство администратора. – М.: Радио и связь, 1985. – 208 с.

Поступила в редакцию 30.09.2004