Санкт-Петербург, ул. Седова, 80, телефон (812) 449-0770, факс (812) 449-0771, E-mail: info@bilim.com

Атаки на соединения TCP с помощью ICMP-пакетов

Николай Малых
по материалам
Фернандо Гонта

Протокол TCP [1] в настоящее время является основным транспортным протоколом в сетях IP и, в частности, в сети Internet. Широкое распространение этого протокола делает его привлекательным объектом атак. Известно множество типов атак, направленных на нарушение работы протокола TCP. Мы не будем здесь останавливаться на рассмотрении всех этих атак и ограничимся лишь анализом воздействий на соединения TCP с помощью пакетов ICMP, на которое обратил внимание Фернандо Гонт (Fernando Gont) из Национального технологического университета Аргентины. В серии документов IETF-draft [2] Гонт рассмотрел возможность существенного снижения скорости обмена данными и даже полного разрыва произвольных соединений TCP с помощью передачи потока специально подготовленных пакетов ICMP с удаленного хоста. Гонт также разработал несколько программ, которые могут использоваться для исследования уязвимости соединений TCP. Исходные коды этих программ можно загрузить с сайта автора[1].

Первый документ был выпущен Фернандо Гонтом 2 августа 2004 года. С тех пор прошло уже более года, но для многих реализаций стека TCP/IP актуальность проблемы сохраняется. В таблице приведена свода уязвимости для продукции Cisco Systems, взятая с сайта CIAC (редакция документа от 15 июня 2005 г[2]). Интересующиеся могут прочесть этот документ, воспользовавшись приведенной ссылкой http://www.ciac.org/ciac/bulletins/p-181.shtml.

Продукция	*reset*	*mtu*	*quench*
IOS	-	+	-
IOS XR	+	+	-
IP Phones	+	+	+
Cisco PIX Security Appliance	-	+	-
Catalyst 6608 and 6624	+	-	+
Cisco 11000 and 11500	-	-	+
Cisco GSS	-	-	+
MDS 9000	-	+	+
Cisco VPN 5000 Concentrator	-	+	-
Some ONS products	-	+	-
Cisco MGX-8250 and MGX-8850	+	+	+
Cisco Content Switching Module	-	-	+
Voice and IP Communication Products Using Cisco-Customized Microsoft Windows	+	+	-
Cisco ACS Solution Engine	+	+	-

Знак “+” означает наличие уязвимости, “-” ее отсутствие. Приведенные в заголовке колонок имена соответствуют суффиксам в именах тестовых программ, разработанных Фернандо Гонтом и доступных на его сайте. Информацию об уязвимости продукции Microsoft можно найти на сайте компании по ссылке http://www.microsoft.com/technet/security/Bulletin/MS05-019.mspx.

Методология атак

Протокол обмена управляющими сообщениями ICMP [3] предназначен для обнаружения ошибок и передачи информации о таких ошибках. При обнаружении тех или иных проблем промежуточные маршрутизаторы или конечные станции генерируют сообщения ICMP того или иного типа, указывая в них код ошибки, и передают отправителю исходного пакета. Протокол транспортного уровня (в частности, TCP), получая сообщения ICMP об ошибках в сети, может выполнять те или иные действия для преодоления возникших проблем. Зная детали работы транспортного протокола и протокола ICMP можно с помощью специально сформированных сообщений ICMP оказать существенное влияние на передачу данных через произвольное соединение TCP и даже разорвать такое соединение. При этом атакующему не нужно даже находиться на пути передачи пакетов между участниками соединения TCP, как это требуется для организации MITM[3]-атак. Для организации ICMP-атак на соединения TCP может потребоваться передача достаточно большого (до нескольких десятков тысяч) числа пакетов, но повсеместное распространение широкополосных каналов доступа в Internet позволяет без проблем организовать такие атаки практически с любого домашнего компьютера.

Для протокола TCP сообщения об ошибки, информация о которых передается в сообщениях ICMP, можно разделить на две категории:

- критические ошибки, которые могут приводить к полному разрыву соединения (reset)
- некритические ошибки, которые могут приводить к многократному повтору передачи сегментов TCP, пока не будет получено подтверждение или не завершится время ожидания (тайм-аут).

Атаки можно разделить на два основных типа по их результатам – сброс соединений или существенное снижение скорости передачи данных через соединение. Далее эти варианта будут рассмотрены более подробно, а сейчас мы вкратце рассмотрим некоторые особенности протокола ICMP, которые обеспечивают возможность организации успешных атак на соединения TCP.

[1] http://gont.com.ar/tools/icmp-attacks/index.html
[2] Оригинальный бюллетень компании Cisco доступен на сайте Cisco Systems по приведенной ниже ссылке http://www.cisco.com/en/US/products/products_security_advisory09186a0080436587.shtml
[3] Man in the middle – человек в центре [атаки].

Протокол ICMP

Как уже было сказано, протокол ICMP используется, в частности, для передачи сообщений об ошибках, возникающих в сети. В соответствии со стандартом Internet "Требования к хостам" [4] сообщения о недоступности адресата (Type 3, Destination Unreachable) с кодами 2 (Protocol Unreachable), 3 (Port Unreachable) и 4 (Fragmentation needed but DF bit set[4]) относятся к критическим ошибкам[5]. Следовательно, любое из этих сообщений может привести к разрыву соединения TCP (Reset).

Спецификация протокола ICMP [3] включает сообщения Source Quench (тип 4, код 0), которые используются для управления потоком данных и предотвращения перегрузки. Такие сообщения передаются в адрес отправителя, если получатель или промежуточный маршрутизатор не способен обрабатывать данные с той скоростью, которую выбрал отправитель. По сути дела эти сообщения являются запросом на снижение скорости передачи данных. Отметим, что в RFC "Требования к маршрутизаторам IPv4" [5] сказано, что данный тип сообщений не обеспечивает эффективного управления потоком данных и контроля насыщения.

Сообщения ICMP используются также в механизме определения значений MTU для пути (Path MTU), описанном в RFC 1191 [6]. Для определения MTU применяются сообщения ICMP типа 3 (Destination Unreachable) с кодом 4 (Fragmentation needed but DF bit set). В силу такого использования сообщений указанного типа системы, реализующие механизмы Path MTU Discovery, не рассматривают ошибки данного типа как критические.

Обработка сообщений ICMP

В соответствии со стандартом Internet "Требования к хостам" [4] протокол TCP должен передавать информацию об ошибке, полученную в сообщении ICMP, соединению, с которым связана эта ошибка. Для определения этого соединения реализации TCP нужно проанализировать данные, содержащиеся в сообщении ICMP.

В соответствии со спецификацией протокола [3] сообщение ICMP должно содержать в себе полный заголовок IP из пакета, вызвавшего ошибку, и 64 бита (8 байтов) из пакета. Очевидно, что в эти 64 бита попадает лишь часть заголовка транспортного уровня. Для случая TCP эти 8 дополнительных байтов будут включать номера портов отправителя и получателя (по 2 байта каждый), а также порядковый номер TCP (4 байта). Требования к хостам [4] позволяют включать в сообщение ICMP дополнительную информацию из вызвавшего ошибку пакет, но не требуют такого включения. Требования к маршрутизаторам [5] говорят, что в сообщения об ошибках **следует** включать максимальное число байтов из вызвавшего ошибку пакета, которое не приведет к тому, что размер дейтаграммы, содержащей сообщение ICMP превысит 576 байтов. Таким образом хост или маршрутизатор, получающий сообщения ICMP об ошибке, может надеяться лишь на наличие в них первых 8 байтов заголовка транспортного уровня.

В TCP связь сообщения ICMP с тем или иным из существующих соединений определяется на основе сравнения 4 значений – 2 адресов IP (отправитель и получатель) и 2 номеров портов[6]. Однако ни спецификация протокола ICMP [3], ни стандартные требования к хостам [4] не определяют каких-либо механизмов проверки корректности информации, содержащейся в сообщении ICMP. Благодаря отсутствию такой проверки атакующий может создать сообщение ICMP, содержащее специально подготовленную дезинформацию, реакция на которую со стороны протокола TCP (в соответствии с требованиями RFC) может привести к весьма печальным результатам вплоть до разрыва существующих соединений. Для того, чтобы сообщение ICMP оказало воздействие на интересующее соединение TCP организатор атаки кроме указания адресов IP участников соединения должен определить или угадать номера портов, через которые организовано соединение. Множество вариантов решения этой задачи рассмотрено в работе [7]. Кроме того, для многих служб в сети Internet используются стандартные номера портов, что существенно упрощает задачу подбора нужного квартета, поскольку 3 (IP-адреса и номер порта на сервер) из 4 значений можно определить достоверно без подбора. Учитывая специфику выделения номеров портов на клиентской стороне соединений TCP в различных операционных системах и приложениях, можно значительно сузить диапазон возможных значений остающегося неизвестным параметра (номер порта на клиентской стороне соединения) и ускорить подбор нужного номера. В крайнем случае, когда приходится перебирать все возможные значения номера порта на стороне клиента, число таких значений составляет 65536. Если в атакуемом соединении и сервер использует нестандартный номер порта, это может дополнительно осложнить задачу (число перебираемых значений возводится в квадрат), но такая ситуация является достаточно экзотической для современной практики в сети Internet, хотя в условиях частных IP-сетей могут применяться и нестандартные номера портов на серверах. Однако и в этом случае задача организации атаки путем подбора номеров остается вполне решаемой.

Сброс соединений (reset)

В соответствии со стандартом Internet "Требования к хостам" [4] хостам следует разрывать соответствующее соединение TCP в ответ на получение сообщения ICMP о критичной ошибке[7]. Используя это, атакующий может вслепую сбросить соединение между парой станций, передавая одному из хостов сообщения ICMP, указывающие на такой тип ошибки. Например, можно передавать одной из сторон соединения сообщения о том, что другая сторона не поддерживает соответствующий протокол (Protocol Unreachable), от имени того самого хоста (другой стороны соединения). В таких сообщениях сложно усмотреть что-либо подозрительное, поэтому можно надеяться, что они не будут отброшены тем или иным фильтром на пути от атакующего[8]. Необходимость выполнения атаки вслепую практически не осложняет ее организации, поскольку атакующему для успеха не требуется получать каких-либо пакетов от объекта атаки. Не требуется от атакующего и организации перехвата пакетов или изменения пути их доставки, поскольку он должен лишь направить подготовленные пакеты ICMP, содержащие код одной из критических ошибок и квартет идентификации соединения в поле данных ICMP, по адресу сервера или клиента в атакуемом соединении. В соответствии с заданной для протокола TCP политикой обработки ошибок получение сообщения ICMP, в поле данных которого содержится заголовок IP с адресами клиента и сервера, а также заголовок TCP с используемыми в данном соединении номерами портов, приведет к немедленному разрыву сообщения[9]. При этом ни у одного из участников соединения не остается в журнальных файлах никакой информации об источнике атаки, поскольку в полученных пакетах могут использоваться (и обычно используются) подставные адреса отправителя (обычно это адрес другой стороны атакуемого соединения).

Для организации такой атаки даже не потребуется писать каких-либо программ – достаточно взять исходный код icmp-reset с сайта Фернандо Гонта.

Следует отметить, что на сегодняшний день далеко не все реализации стека TCP/IP подвержены этой уязвимости. В работе Ф. Гонта приводятся рекомендации по решению проблемы и многие разработчики уже воспользовались ими. Однако проведенные в Internet эксперименты показали, что уязвимых хостов существует достаточно много.

---

[4]Требуется фрагментация пакета, но в заголовке установлен флаг запрета фрагментации.

[5]В стандарте используется термин hard error.

[6]В английском языке для этого квартета обычно используется термин four-tuple.

[7]В стандарте используется термин hard error.

[8]Следует принимать во внимание, что на многих маршрутизаторах используется ingress-фильтрация в соответствии с RFC 2267. В этом случае можно указывать в пакетах ICMP свой адрес или адрес из блока вашего провайдера, но тогда останется ведущий к источнику атаки след.

[9]Отмечу, что в некоторых реализациях TCP предусмотрены меры защиты (например, проверка порядкового номера TCP из сообщения ICMP), поэтому это срабатывает не во всех случаях.

Снижение скорости

Кроме возможности сброса соединений TCP пакеты ICMP позволяют существенно снизить скорость передачи данных через соединения, не нарушая их работу полностью. Для выполнения такой задачи передаются сообщения ICMP о некритических ошибках (тип 3 с кодом 4 и тип 4 с кодом 0). Механизм такой атаки весьма похож на описанную выше атаку для разрыва соединений.

Следует отметить, что атаки, приводящие к снижению скорости передачи данных через соединение в некоторых случаях могут доставить даже больше хлопот, нежели полный разрыв соединений.

Для тестирования вы можете использовать программы icmp-mtu и icmp-quench, доступные на сайте Фернандо Гонта.

Библиография

1.Postel, J., Transmission Control Protocol, STD 7, RFC 793, сентябрь 1981. Перевод этого документа имеется на сайте http://www.protocols.ru

2.F. Gont, ICMP attacks against TCP, декабрь 2004. http://www.gont.com.ar/drafts/draft-gont-tcpm-icmp-attacks-03.txt

3.Postel, J., Internet Control Message Protocol, STD 5, RFC 792, сентябрь 1981. Перевод этого документа имеется на сайте http://www.protocols.ru

4.Braden, R., Requirements for Internet Hosts - Communication Layers, STD 3, RFC 1122, октябрь 1989. Перевод этого стандарта имеется на сайте http://www.protocols.ru

5.Baker, F., Requirements for IP Version 4 Routers, RFC 1812, июнь 1995. Перевод этого документа имеется на сайте http://www.protocols.ru

6.Mogul, J., S. Deering, Path MTU discovery, RFC 1191, ноябрь 1990. Перевод этого документа имеется на сайте http://www.protocols.ru

7.Watson, P., "Slipping in the Window: TCP Reset Attacks", 2004 CanSecWest Conference, 2004. http://www.osvdb.org/reference/SlippingInTheWindow_v1.0.doc