

## icmp-reset

Программа разработана Фернандо Гонтом ([fernando@gont.com.ar](mailto:fernando@gont.com.ar)) и позволяет генерировать поток пакетов ICMP с заданными или случайно изменяющимися параметрами, адресованных указанному хосту. Программа может служить полезным инструментом для проверки устойчивости стека TCP/IP к атакам на соединения TCP, выполняемым с помощью пакетов ICMP. Программа поддерживает возможности управления параметрами генерируемых пакетов. По умолчанию для параметров используются случайные значения. Программа может также служить инструментом для проверки систем детектирования попыток вторжения (IDS).

Описание механизмов, используемых программой, вы можете найти в подготовленном автором этой программы проекте документа на странице <http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.html><sup>1</sup>

## Синтаксис

```
icmp-reset -c <адрес клиента>[:port-port] -s <адрес сервера>[:port-port] -t client|server -r n
```

Опция **-c (--client)** задает параметры, связанные с клиентом. IP-адрес клиента является обязательным параметром и может сопровождаться (через двоеточие) номером порта или диапазоном (через дефис) номеров портов. Если порт не задан, будут последовательно перебираться все номера портов из диапазона 0 до 65535. Если задан диапазон портов, программа будет последовательно выбирать номера портов из этого диапазона. Если указан единственный порт (например, **-c 192.168.0.1:1024**), программа будет использовать только этот номер, что может существенно ускорить получение результата (успешного завершения атаки).

Опция **-s (--server)** задает параметры, связанные с сервером. Вслед за обязательным адресом сервера может быть указан номер порта или диапазон номеров. По умолчанию используется диапазон портов от 0 до 65535.

Если вы не укажете номер или диапазон для портов клиента и сервера, количество пакетов, требуемых для успешного завершения атаки будет умножаться на 65536<sup>2</sup>, что приведет к существенному замедлению.

Опция **-t (--target)** указывает адресата генерируемых пакетов (клиент или сервер). Можно также указывать клиента или сервер с помощью опций **--target-is-client (-C)** и **--target-is-server (-S)**, соответственно.

Опция **-r (--rate)** позволяет ограничить полосу используемую для передачи сгенерированных программой пакетов (в килобит/сек). Данная опция полезна в тех случаях, когда промежуточный маршрутизатор будет ограничивать полосу для трафика ICMP и может отбрасывать некоторые пакеты в случае превышения. Полезна эта опция и в тех случаях, когда адресат не может принимать пакеты с той скоростью, которую обеспечивает программа по умолчанию и часть пакетов будет теряться. На практике разумно использовать для этого параметра значение 10. Можно также ограничивать скорость генерации пакетов с помощью опции **-d (--delay)**, указывающей задержку между последовательными пакетами в наносекундах. Отметим, что опции **-r** и **-d** не могут использоваться совместно. С помощью опции **-D (--pause)** можно задать паузу (в секундах) после каждого цикла генерации пакетов (цикл включает перебор всех возможных комбинаций номеров портов для клиента и сервера).

По умолчанию в пакетах будет указываться подставной адрес отправителя, в качестве которого используется адрес другой стороны атакуемого соединения. Например, при генерации пакетов в адрес клиента в поле отправителя будет указываться адрес сервера. С помощью опции **-n (--noforge)** можно заставить программу генерировать пакеты с реальным IP-адресом атакуемого хоста. Этот вариант может оказаться полезным для тех случаев, когда промежуточные маршрутизаторы могут фильтровать пересылаемые пакеты по адресу отправителя (egress-filter). С помощью опции **-f (--forge)** можно задать произвольный адрес отправителя для генерируемых программой пакетов. Например, при использовании опции **-f 10.0.0.1** пакеты ICMP будут передаваться от имени хоста 10.0.0.1.

По умолчанию поля пакетов TTL, payload TTL, IP ID, payload ID, TCP SEQ и т. п. будут содержать случайные значения. Опция **-l (--ttl)** позволяет задать значение поля TTL в заголовке пакета, а **-L (--payload-ttl)** позволяет установить значение TTL в заголовке IP, содержащемся в поле данных сообщения ICMP. С помощью опции **-p (--id)** можно задать значение идентификатора IP в заголовке пакета ICMP, а опция **-P (--payload-id)** позволяет задать IP ID в заголовке IP, содержащемся в поле данных сообщения ICMP.

Поле TOS пакета IP и заголовок IP, содержащегося в поле данных (payload) сообщения ICMP будет содержать значение 0x00 (обычный трафик). С помощью опции **-o (--tos)** можно задать значение поля TOS в заголовке пакета ICMP, а опция **-O (--payload-tos)** позволяет указать значение поля TOS в заголовке IP, содержащемся в поле данных сообщения ICMP.

Программа по умолчанию будет генерировать сообщения ICMP типа 3 (Destination Unreachable) с кодом 2 (Protocol Unreachable). Вы можете изменить код ICMP с помощью опции **-i (--icmp-code)**, задавая значение в диапазоне от 0 до 15.

Содержащийся в сообщении ICMP заголовок IP будет заявлять размер дейтаграммы 576 байтов. Опция **-z (--payload-size)** позволяет изменить это значение. Следует отметить, что данная опция не оказывает влияния на размер передаваемых в реальности данных – она лишь устанавливает соответствующее значение в поле заголовка, содержащегося в пакете.

Опция **-q (--tcp-seq)** позволяет задать значение порядкового номера TCP, указываемого в генерируемых ICMP-пакетах.

С помощью опции **-v (--verbose)** можно обеспечить вывод дополнительной информации в процессе работы программы.

<sup>1</sup> Срок действия последнего предварительного (draft) варианта документа истек 22 июня 2005 года, но какого-либо RFC на основании этого документа пока не выпущено.