# МЕТОДЫ DoS АТАК И ИХ ПРЕДОТВРАЩЕНИЕ В КОМПЬЮТЕРНЫХ СЕТЯХ

**Ковалев С.А., Волкогон А.В.**

Кафедра ЭВМ ДонНТУ
kovalev@pop.dgtu.donetsk.ua

## Abstract

***Kovalev S.A., Volkogon A.V. DoS attacks methods and its prevention in computer networks.*** *Active development and implementation of the modern information technologies demand increasing of computer systems' safety. This paper exams problem of the dental of service attacks to the computer system or local computer network. Some recommendations of prevention for "smurf" and "fraggle" attacks are proposed for different types of operation systems.*

## Введение

В период активного развития и внедрения в повседневную жизнь информационных технологий немаловажную роль играют надежность систем, обеспечивающих доступ к информации, и ее хранение. Однако, вместе с ростом важности информации растут и потери, понесенные вследствие кражи, разрушения или отсутствием доступа к той или иной информации. Атака, приводящая к невозможности получить информацию или к невозможности дальнейшей работы систем без перезагрузки, называется "атака отказа в обслуживании" – DoS (Denial of Service). По сути, атака такого рода препятствуют или полностью блокирует ответы службы законным пользователям.

Атаки DoS всегда злонамеренны и сегодня существует большое количество утилит для их проведения даже не профессионалом. На практике проще нарушить работу сети или системы, чем получить к ней неавторизированный доступ. Сетевые протоколы TCP/IP были разработаны для открытого и честного использования, и современная четвертая версия стека TCP/IP унаследовала эти «недостатки» предыдущих вариантов. Кроме того, многие системы имеют собственные ошибки в реализации стека, что снижает их способность противостоять атакам DoS. Атака отказа в обслуживании существенно изменила мир Internet, показав слабость защиты используемых технологий.

## 1. Основные типы атак DoS

*Захват полосы пропускания* – наиболее коварная атака DoS, которая связана с перегрузкой полосы пропускания (Bandwidth consumption). В этом случае атакующий занимает всю имеющуюся полосу пропускания сети. Рассмотрим примеры проведения подобной атаки.

Атакующий перегружает целевое сетевое соединение, имея в своем распоряжении канал связи с большей полосой пропускания, посылая множество пакетов, например, ICMP (Internet Control Message Protocol, протокол диагностики сети) на целевой хост. Этот способ характерен для блокировки линий T1 (1.544 Мбит/с) и более производительных сетевых связей. Для заполнения полосы пропускания таких

мощных линий могут использоваться сетевые линии с пропускной способностью всего 56 или 128 Кбит/с.

Второй способ заключается в следующем: нападающий усиливает атаку DoS, инициируя ее одновременно из нескольких точек. В этом случае даже по линии 56 Кбит/с можно полностью подавить линию Т3 (45 Мбит/с). Усиление атакующего потока происходит за счет направления трафика из нескольких серверов.

*Истощение ресурсов* – атака направленная не на ресурсы сети, а на ресурсы системы. В общем случае атака истощения ресурсов предполагает расходование процессорных циклов, памяти, квот файловой системы или других системных ресурсов. Атаки данного рода обычно приводит к полной недоступности одно из ресурсов, переполнению файловой системы или зависанию процессора.

*Использование ошибок программирования* – данный вид атаки DoS приводит к краху приложений, операционной системы или аппаратного обеспечения, которые не могут работать в нестандартной ситуации. Такие ситуации характерны, когда производится посылка на целевую систему пакетов, не совместимых со стандартом RFC (Request For Comments), или, когда программы ожидают пользовательский ввод, т.е. вводится огромное количество данных, что вызывает переполнение буфера, а иногда даже и выполнение привилегированных команд. От ошибок, скорее всего, не защищена ни одна из систем, будь то ОС или процессор компьютера (одна из атак DoS данного типа: если на процессоре Pentium выполнить инструкцию 0xF00FC7C8A, то произойдет крах любой операционной системы).[6]

### *2.Захват полосы пропускания*

Атака smurf относится к наиболее опасной разновидности DoS, поскольку имеет эффект усиления. Он является результатом отправки прямых широковещательных запросов ping к системам, которые обязаны послать ответ.

Чтобы использовать особенности широковещательной рассылки, нужно, как минимум, три участника: атакующий, усиливающая сеть и целевой хост. Атакующий посылает фальсифицированный пакет ICMP ECHO по адресу широковещательной рассылки усиливающей сети. Адрес источника заменяется адресом жертвы, чтобы представить дело, так будто именно целевая система послала запрос. Поскольку пакет ECHO послан по широковещательному адресу, все системы усиливающей сети возвращают жертве свои ответы. Рассмотрим процедуру формирования фальшивого ICMP запроса.[2]

1. С помощью функции connect создается программный интерфейс для соединения по протоколу TCP/IP.
2. Параметр SO_BROADCAST устанавливается в 1.
3. Организуется цикл, в котором производится:
   - выделение буфера для IP пакета (заголовки IP+ICMP)
   - очистка выделенного буфера
   - заполнение структуры пакета: (Рис.1)
   - посылка сформированного пакета
   - освобождение выделенной памяти

Послав один пакет ICMP в сеть из 100 систем, атакующий инициирует усиление атаки DoS в сто раз. коэффициент усиления зависит от состава сети, поэтому для организации успешной атаки выбирается большая сеть, способная подавить работу целевой системы.

Существует еще один вариант атаки базирующийся на smurf – fraggle. В данной атаке используются пакеты UDP вместо ICMP. Атакующий посылает фальсифицированные пакеты UDP по адресу широковещательной рассылки усиливающей сети, обычно на порт 7 (Табл.1).
Каждая система, в которой разрешен ответ на эхо – пакеты, возвратит пакеты системе

```
// Общая длина пакета ip
ip->tot_len = htons(sizeof(struct iphdr) + sizeof(struct icmphdr) + psize);
ip->ihl = 5;                          //Длина заголовка в 2-х байтных
словах
ip->version = 4;                      //Версия протокола
ip->ttl = 255;                        //Время жизни
ip->tos = 0;                          // Тип сервиса
ip->frag_off = 0;                     //Смещение данного пакета при
сборке
ip->protocol = IPPROTO_ICMP;  //Тип протокола ICMP
ip->saddr = sin.sin_addr.s_addr;  //Адрес целевой системы
ip->daddr = dest;                     // Широковещательный адрес
ip->check = in_chksum((u_short *)ip, sizeof(struct iphdr));
icmp->type = 8;                       //Echo Request см таблицу 1.
icmp->code = 0;
```

Рисунок 1 - Заполнение структуры IP пакета.

– жертве. Если в системах усиливающей сети запрещены эхо – ответы, то системы сгенерируют сообщения ICMP о невозможности получить эхо – ответ и все равно будет сгенерирован не нужный трафик большого объема.

Таблица 1. Часто используемые сервисы и соответствующие им порты.[11]

| Сервис | Порт | Протокол | Описание |
|---|---|---|---|
| echo | 7 | TCP | Эхо сервер |
| echo | 7 | UDP | Эхо сервер |
| daytime | 13 | TCP | Сервер времени |
| daytime | 13 | UDP | Сервер времени |
| ftp | 21 | TCP | Сервер FTP (File transfer protocol) |
| fsp | 21 | UDP | Сервер FTP (File Transfer Protocol |
| ssh | 22 | TCP | Сервер SSH Secure Shell |
| ssh | 22 | UDP | Сервер SSH Secure Shell |
| telnet | 23 | TCP | Сервер Telnet |
| www | 80 | TCP | Сервер WWW (World Wide Web) |
| www | 80 | UDP | Сервер WWW (World Wide Web) |
| pop3 | 110 | TCP | Сервер POP3 (Post Office Protocol 3),входящая почта |
| pop3 | 110 | UDP | Сервер POP3 (Post Office Protocol 3),входящая почта |
| nntp | 119 | TCP | Сервер NNTP (Network News Transfer Protocol),новости |
| netbios | 139 | TCP | Сервис NETBIOS, сеть Microsoft |
| netbios | 139 | UDP | Сервис NETBIOS, сеть Microsoft |
| squid | 3128 | TCP | squid web proxy (http и ftp прокси сервер |
| mysql | 3306 | TCP | Сервер баз данных MySQL |
| mysql | 3306 | UDP | Сервер баз данных MySQL |

### *3. Способы предотвращения smurf*

Предотвратить эффект усиления позволит запрет операций прямой широковещательной рассылки на всех граничных маршрутизаторах. В устройствах Cisco нужно применить команду no ip directed-broadcast. В Cisco IOS версии 12 прямая широковещательная рассылка запрещена по умолчанию. Дополнительно можно установить в ОС режим отбрасывания эхо – пакетов.

Для систем **Solaris**, чтобы заблокировать широковещательные эхо – запросы нужно добавить строчку в файл /etc/rc2.d/S69inet :

*ndd –set /dev/ip ip_respond_to_echo_broadcast 0 .*

В системах **Linux** для предотвращения smurf атаки нужно воспользоваться брандмауэром реализованным на уровне ядра системы. Приведенные ниже правила (рис.2) предназначены для противостояния smurf атаке и регистрации попыток ее проведения. Поскольку прохождение широковещательных ICMP пакетов явно не разрешено ни одним из правил, то такие пакеты будут удалены по умолчанию. В правилах указаны не только ECHO REQUEST, но и другие типы ICMP пакетов, так как атаку можно провести, используя и другие сообщения ICMP протокола.

```
#Описание переменных
EXTERNAL_INTERFACE="eth0"                  #Интерфейс, подключенный к Internet
BROADCAST_DEST="255.255.255.255"           #Целевой широковещательный адрес
NETMASK="255.0.0.0"                        #Маска сети для сети 10.0.0.0
NETWORK="10.0.0.0/8"                       #Адрес сети класса А

# Противодействие smurf атаке
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp -d $BROADCAST_DEST -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp -d $BROADCAST_DEST -j REJECT
-l

#Маска сети
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp -d $NETMASK -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp -d $NETMASK -j REJECT -l

#Адрес сети
ipchains -A input -i $EXTERNAL_INTERFACE -p icmp -d $NETWORK -j DENY -l
ipchains -A output -i $EXTERNAL_INTERFACE -p icmp -d $NETWORK -j REJECT -l
```

Рисунок 2 - Пример конфигурирования брандмауэра для защиты от smurf.

В данном примере настройки брандмауэра запрещается межсегментная пересылка пакетов ICMP с широковещательным адресом назначения, маске сети или адресу сети по цепочкам input и output.

Системы **FreeBSD** версии 2.2.5. и выше по умолчанию запрещают прямые широковещательные рассылки. Включение и выключение данной опции производится параметром sysctl в net.inet.icmp.bmcastecho.

В системах **AIX** 4 или выше ответы на широковещательные запросы запрещены. Команда no bcastping позволяет включать/выключать ответы.

Для предотвращения атаки fraggle во всех версиях **UNIX** в файле /etc/inetd/conf закомментировать строчку разрешения запуска служб echo и chargen. Важно предотвратить использование сайта в качестве усилителя атаки, но еще важнее выявить, что сайт используется для проведения подобной атаки. Следует сократить трафик ICMP и UDP на граничных маршрутезаторах до объема, действительно необходимого системам сети, либо ограничится определенным типом трафика ICMP. Усилить защиту позволит установка режима CAR (Commited Access Rate), реализованного в Cisco IOS 1.1CC, 11.1CE и 12.0. В этом случае трафик ICMP ограничивается разумной величиной, например на уровне 256 или 512 Кбайт. [6]

### *Заключение*

Сложно объяснить причины проведения DoS атак. Поскольку киберпространство отражает недостатки реальной жизни, атаки DoS стали мощным оружием кибер-террористов, которые стали довольно часто применяться в новом электронном тысячелетии. Защитить конкретную систему от smurf и fraggle атак практически невозможно, поэтому необходимо проведение ряда предлагаемых мер по предотвращению использования компьютерных сетей в качестве усиливающих.

### *Литература*

1. "Максимальная безопасность в Linux": Пер. с англ./Автор анонимный – К.: Издательство ДиаСофт" 2000. – 400с.
2. "Брандмауэры в Linux": Пер. с англ.: Уч. пос. – М. : Издательский дом "Вильямс", 2000. – 384с.
3. "Linux IP Stacks в комментариях": Пер. с англ./Стефен Т. Сэтчелл и Х.Б. Дж. Клиффорд. – К:Издательство "ДиаСофт", 2001. – 288 с.
4. "Безопасность глобальных сетевых технологий": Зима В.М. : BHV С-Петербург, 2000 г. 320с.
5. "Защита информации и безопасность компьютерных сетей": Домарев В.Н. :DiaSoft, 2000 г. 480с.
6. "Секреты хакеров": Пер. с англ./Стюарт Макклуре, Ждоел Скембрей—К : Издательство "Лори", 2001.–435с.
7. "Атака через Internet": И. Медведовский, П. Семьянов, В. Платонов М: Москва,2000г., 334с.
8. "Системное программирование на C++ для UNIX": Теренс Чан, под редакцией М. Коломыцева, - BHV, Киев 1999 г.589с.
9. "Руководство программиста для Linux": Свен Голдт, Свен ван дер Миир, версия 0.4 (существует только в электронном виде).
10. "Ядро Linux" : Девид А. Раслинг, (электронный вариант).
11. "Создание сетевых приложений в среде Linux": Пер. с англ. – М. : Издательский дом "Вильямс", 2001. – 464с.

Поступила в редакційну колегію 5.12.2001 р.