Бабенко Людмила Климентьевна – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: blk@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2, корпус "И"; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Крамаров Леонид Сергеевич – e-mail: l.s.kramarov@gmail.com; кафедра безопасности информационных технологий; аспирант.

Babenko Lyudmila Klimentevna – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: blk@tsure.ru; Block “I”, 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security of information technologies; professor.

Kramarov Leonid Sergeevich – e-mail: l.s.kramarov@gmail.com; the department of security of information technologies; postgraduate student.

УДК 004.056

Я.В. Тарасов, О.Б. Макаревич

МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ НИЗКОИНТЕНСИВНЫХ DOS-АТАК НА BGP-ИНФРАСТРУКТУРУ*

Представлены результаты анализа и имитационного моделирования исследования атак типа «отказ в обслуживании» на различные сервисы хранения, обработки и передачи данных в сети Интернет. Основное внимание уделено имитации низкоинтенсивных DoS-атак на инфраструктуру глобального протокола динамической маршрутизации BGP (Border Gateway Protocol). В качестве программного обеспечения были выбраны apache2, nginx, quagga, debian, vmware и citrix xenserver с использованием самых популярных вариантов конфигурации. В некоторых случаях специально модифицировались конфигурационные параметры для снижения безопасности служб, что бы получить заранее предполагаемые результаты для сравнения. В рамках исследования были проанализированы уязвимости протоколов передачи данных транспортного и прикладного уровня, приводящие к возможности реализации угрозы низкоинтенсивных DoS-атак. Данное исследование должны наглядно продемонстрировать способы реализации атак данного типа на реальные вычислительные системы и вычислительные сети. Результатом проведения исследования является оценка критичности низкоинтенсивных атак типа отказ в обслуживании на инфраструктуру BGP.

Ннизкоинтенсивные DoS-атаки; Border Gateway Protocol; моделирование атак; безопасность вычислительных сетей.

Y.V. Tarasov, O.B. Makarevich

MODELING AND STUDY OF LOW-INTENSITY DOS-ATTACKS ON BGP-INFRASTRUCTURE

The results of the analysis and simulation study of attacks such as " denial of service " for a variety of services that store, process and transmit data to the Internet. Focuses on the simulation of low-intensity DoS-attacks on the infrastructure of the global dynamic routing protocol BGP (Border Gateway Protocol). As the software was chosen apache2, nginx, quagga, debian, vmware and citrix xenserver using the most popular configuration options . In some cases, specially modified configuration parameters to reduce the security services, which would get pre- expected results for comparison. The study analyzed the vulnerability of data communication protocols of the

* Работа выполнена при поддержке грантов РФФИ № 12-07-00013-а, РФФИ № 12-07-00014-а.

transport and application layer , leading to the possibility of the threat of low-intensity DoS-attacks . This study should demonstrate how to implement this type of attack on the real computer systems and computer networks . The result of the study is to assess the criticality of low-intensity attacks such as denial of service on the infrastructure of BGP.

Low-rate DoS-attacks; Border Gateway Protocol; attack modeling; security of computer networks.

Введение. DoS-атаки нацелены как на сети в целом, серверные кластеры, так и на конечные хосты, их задачей является максимальное потребление предоставляемых ресурсов с целью значительного ухудшения или прекращения предоставления сервиса нормальным пользователям. Обычно атакуемыми ресурсами являются: ширина канала, процессорное время серверов и роутеров и конкретные реализации протоколов. В качестве примеров можно привести SYN-атаку, нацеленную на переполнение стека TCP операционной системы; направленные широковещательные ICMP-атакуемому отправляются подобные пакеты, ответы от него снижают пропускную способность сети; DNS флуд атаки, использующие определенную слабость протокола DNS и направленные на существенное увеличение трафика к атакуемому.

Основной способ распознавания DDoS-атаки заключается в обнаружении аномалий в структуре трафика. Традиционные механизмы обеспечения безопасности – межсетевые экраны и системы обнаружения вторжений – не являются эффективными средствами для обнаружения DDoS-атак и защиты от них, особенно атак трафиком большого объема [1, 2]. Фундаментальной предпосылкой для обнаружения атак является построение контрольных характеристик трафика при работе сети в штатных условиях с последующим поиском аномалий в структуре трафика (отклонения от контрольных характеристик) [3]. Аномалия сетевого трафика – это событие или условие в сети, характеризуемое статистическим отклонением от стандартной структуры трафика, полученной на основе ранее собранных профилей и контрольных характеристик. Любое отличие в структуре трафика, превышающее определенное пороговое значение, вызывает срабатывание сигнала тревоги. Вместе с тем, существующие методы обнаружения DDoS-атак, позволяющие эффективно распознавать DDoS-атаки транспортного уровня (SYN-флуд, UDP-флуд и другие), малоэффективны для обнаружения низкоинтенсивных DDoS-атак (Low-Rate DDoS) прикладного уровня («медленный» HTTP GET флуд и «медленный» HTTP POST флуд) [4]. Данный класс DDoS-атак возник сравнительно недавно и на сегодняшний день представляет основную угрозу доступности информации в распределенных компьютерных сетях [5, 6]. Отличить трафик, генерируемый в ходе данных атак, от легального HTTP-трафика достаточно сложно, кроме того, каналы передачи данных практически не перегружаются. Данные атаки приводят к потерям запросов и ответов, т.е. фактическому отказу веб-серверов на основе Microsoft IIS, Apache и других систем. Кроме того, атака может быть адаптирована для воздействия на SMTP и даже на DNS-серверы. Данные факты обуславливают необходимость изучения механизмов низкоинтенсивных распределенных атак прикладного уровня типа «отказ в обслуживании» в компьютерных сетях при помощи методов имитационного моделирования.

1. Анализ механизма Low-Rate DDoS. Общим фактором, необходимым для осуществления Low-Rate DDoS атак, является наличие большого количества компрометированных или добровольно участвующих хостов и грубое "заваливание" пакетами атакуемый узел. Именно «грубость» в реализации данных атак может свести на нет весь эффект в случае обнаружения больших объемов аномального трафика сетевыми мониторами [2, 7].

Low-Rate DDoS-атаки представляют из себя периодический трафик малого объема, то есть всплески. В момент, когда открытая сессия подключения должная закрыться по таймауту, посылается новый всплеск для поддержания данной сессии в открытом состоянии. Постепенно буфер маршрутизатора или сервера будет переполнятся, что приведет к отказу обработки легитимного трафика. При таком подходе не требуется большой пропускной способности и вычислительной мощности у атакующей стороны.

Показательным примером являются DoS-атаки, направленные на снижение полосы пропускания TCP потоков трафика, осуществляемые с низкой интенсивностью во избежание обнаружения. Используя уязвимость в механизме таймаута повторной передачи TCP-стека, можно добиться нулевой пропускной способности, путем смешивания с основным трафиком специально подобранных шаблонов DoS-трафика.

Управление полосой пропускания в TCP осуществляется на 2-х временных шкалах. На малой временной шкале отметки времени прохождения пакетов по каналу связи до адресата и обратно (RTT), обычно от 10 до 100 миллисекунд, TCP-стек использует аддитивно-мультипликативное (в оригинале additive-increase multiplicative-decrease) управление (AIMD) для передачи каждого потока трафика на одинаковых скоростях через самое узкое место, т.н. бутылочное горлышко. Когда канал связи начинает «забиваться» и возникает большое количество потерь, TCP-стек начинает работать по 2-й, большей временной шкале с отметками таймаутов повторной передачи пакетов (RTO, рекомендованное минимальное значение 1 секунда). Что бы избежать «забития» канала, поток трафика уменьшается до одного пакета и по прошествии времени RTO пакет пересылается заново. При последующих потерях, время RTO удваивается с каждым следующим таймаутом. В случае удачного получения пакета, TCP-стек начинает использовать AIMD-управление [8].

Для проведения Low-Rate DoS-атаки необходимо взять потоки трафика в виде импульсов и рассмотреть периодические импульсные атаки, состоящие из коротких пиков со специально подобранной длительностью, повторяющихся с определенной, специально выбранной, частотой по медленной временной шкале. Если для первого потока TCP-трафика общий трафик (DoS-атаки и обычный) в течение пика достаточен, чтобы произошли потери пакетов, то этот поток "отвалится" по тайм-ауту и будет произведена попытка отправить новый пакет по прошествии времени RTO. В случае, если периодичность посылки DoS-трафика совпадает (даже примерно) с RTO нормального трафика, обычный трафик будет постоянно получать таймаут, как следствие, потери будут приближаться к 100 % и пропускная способность приблизится к нулю. Кроме того, если период DoS-посылок примерно равен, но лежит вне диапазона RTO, то будет наблюдаться существенное (но не полное) снижение полосы пропускания. Более подробно данный механизм рассмотрен в работе [7], а механизм таймаута TCP-стека в [8].

2. Описание системы исследования атак типа отказ в обслуживании

2.1. Аппаратная составляющая экспериментального стенда. Во время моделирования сетевого взаимодействия, использовались технологии виртуализации, для обеспечения чистоты экспериментальных данных. Так как системы виртуализации позволяют создавать изолированные виртуальные машины с набором выделенных ресурсов. Для каждой виртуальной машины выделяется процессорное время и оперативная память, при исчерпании, которых не будет происходить вмешательства в ресурсы других виртуальных машин. Так же системы виртуализации позволяют изменять пропускную способность виртуальных сетей и регулировать потери при передаче данных в этих сетях, тем самым можно создать модель, максимально близко приближенную к реальным условиям в глобальных сетях.

В качестве аппаратной площадки использовался персональный компьютер на базе процессора Intel Core i7-3770 с тактовой частотой 3,4 ГГц, объемом оперативной памяти в размере 16 Гб и высокоскоростной твердотельный жесткий диск объемом 120 Гб.

На компьютер был установлен «Citrix XenServer 6.1», является бесплатно распространяемым продуктом компании Citrix, с активированным параметром в BIOS – аппаратная виртуализация.

2.2. Программная составляющая экспериментального стенда. Для исследования различных видов атак типа отказ в обслуживании была создана среда, в которой для передачи, хранения и обработки информации используются сетевые протоколы различных уровней модели OSI. В ходе проведения экспериментов были выделены более критичные протоколы прикладного уровня и для проведения были настроены самые распространенные сервисы сети интернет: HTTP, DNS, BGP, ICMP.

Для моделирования атаки на HTTP были сконфигурированы веб-серверы nginx и Apache2. Разрешением доменных имен в тестовой сети занимаются сервисы под управлением bind9. В сети, изображенной на рис. 1, для приближения к реальным условиям сети интернет организованна сильно разветвленная топология с динамической маршрутизацией для обеспечения бесперебойной доступности узлов сети и сервисов.

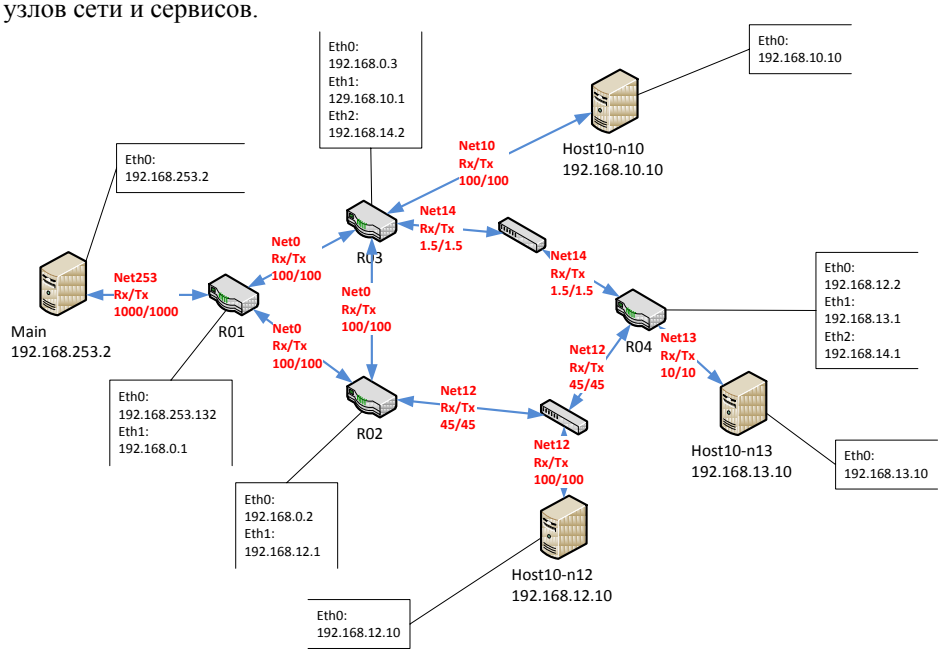

Рис. 1. Общая схема имитационной модели

3. Моделирование низкоинтенсивных DoS-атак

3.1. Моделирование низкоинтенсивной атаки на HTTP сервис. Механизм таймаутов, с одной стороны, обеспечивает устойчивый алгоритм управления "забития" канала, с другой стороны, предоставляет возможность проведения низкоскоростной атаки, который использует уязвимость динамики изменения таймеров повторной передачи (по малой временной шкале). В частности, атакующий может вызвать циклическое «отваливание» по таймауту потока трафика путем отправки

мощных коротких импульсов трафика, имеющих длительность, сопоставимую с RTT шкалой и периодичностью более медленной шкалы RTO. Пропускная способность атакуемого снижается до нуля, в то же самое время средняя скорость атаки будет довольно низкой, что делает проблемным обнаружение подобной атаки.

Рассмотрим простую модель зависимости времени вывода из строя атакованной системы (это и будет периодом атаки) от ее полосы пропускания.

Для начала смоделируем на одиночном потоке трафика и одиночном потоке DoS-трафика. Допустим, атакующий отправил первый пик в момент времени t=0, тем самым выведя из строя удаленную систему. Обычный отправитель в это время получил таймаут и вынужден ждать окончания таймера повторной передачи пакета 1 сек и удваивать RTO. Если атакующий повторил атаку (снова вывел из строя систему) в промежуток времени от 1 до 1+2RTT, то он вынудит ждать стек TCP еще 2 секунды. Создавая подобные выводы из строя в моменты времени 3, 5, 17, ..., атакующий тем самым фактически вынудит прекратить предоставление TCP-сервиса, в то же самое время атакующий будет отправлять пики DoS-трафика с довольно низкой средней скоростью.

Приведенная ситуация эффективна для одиночного потока трафика, для нескольких входящих и выходящих потоков требуется периодичное (вместо экспоненциального, как указано для одиночного) создание ситуаций вывода из строя канала передачи по шкале RTO. Более того, в случае одинакового параметра minRTO (как рекомендует RFC 2988) у всех потоков, все потоки будут простаивать в таймауте более длительное время (в случае создания периодичных сбоев в канале).

Для атаки используются импульсы длительностью l и скоростью R с определенным периодом T. Как показано ниже, атака будет удачной при следующих условиях: скорость передачи R достаточна для получения таймаута в канале (т.е. сумма скоростей обычного и DoS-трафика должна превышать суммарную пропускную способность канала), длительность l по шкале RTT достаточна для получения таймаута на канале (и довольно мала, чтобы избежать обнаружения) и период T по шкале RTO выбран таким образом, что поток трафика, пытающегося после таймаута пройти в канал, получил очередной таймаут.

Для проведения будут использоваться отдельные узлы нашего стенда. В роли сервера жертвы с запущенным HTTP сервисом Apache2 используется host10-n10 с IP адресом 192.168.10.10/24. Атака проводиться с узлов других сетей. Атакующие машины host10-n12 и host10-n13. SlowLoris скрипт, написанный на языке Perl, реализующий низкоинтенсивную атаку на веб-сервис.

Запуск скрипта осуществляется командой:

```
#perl slowdos.pl -dns 192.168.10.10 -port 80 -timeout 100
                    -num 10000 –tcpto 5
```

Хост Main выступал в роли легитимного клиента и контрольного хоста для проверки доступности сервиса. Для проверки доступности атакуемой систему, используется утилита siege, которая позволяет получать информацию о доступности веб-сервера.

Запуск siege осуществляется командой:

```
#siege –c 10 –t 10M http://192.168.10.10/index.html
```

Параметр –c означает эмуляцию 10 одновременных клиентов. Параметр –t 10M означает запуск на 10 минут, по истечении которых производиться подсчет статистики.

В ходе эксперимента скрипт генерации подключений был запущен на атакующих хостах на 10 минут. С контрольной машины проводились попытки подключения к веб-службе с помощью автоматизированного средства siege. На рис. 2

видно зависимость доступности веб-сервиса от периодичности атаки. В идеальной модели без погрешностей на задержки в сети и производительность атакующих машин, а так же на потери в сети интернет, можно с уверенностью сказать, что атака проведена успешно без серьезных затрат на пропускную способность канала связи атакующих машин.

Рис. 2. График сравнения доступности атакуемой системы и потерь во время атаки

3.2. Моделирование низкоинтенсивной атаки на BGP. Для проведения экспериментов требуется выбрать сегмент сети, который будет хорошо демонстрировать поведение систем во время атаки. После ознакомления с параметрами всех узлов был выбран сегмент, показанный на рис. 3.

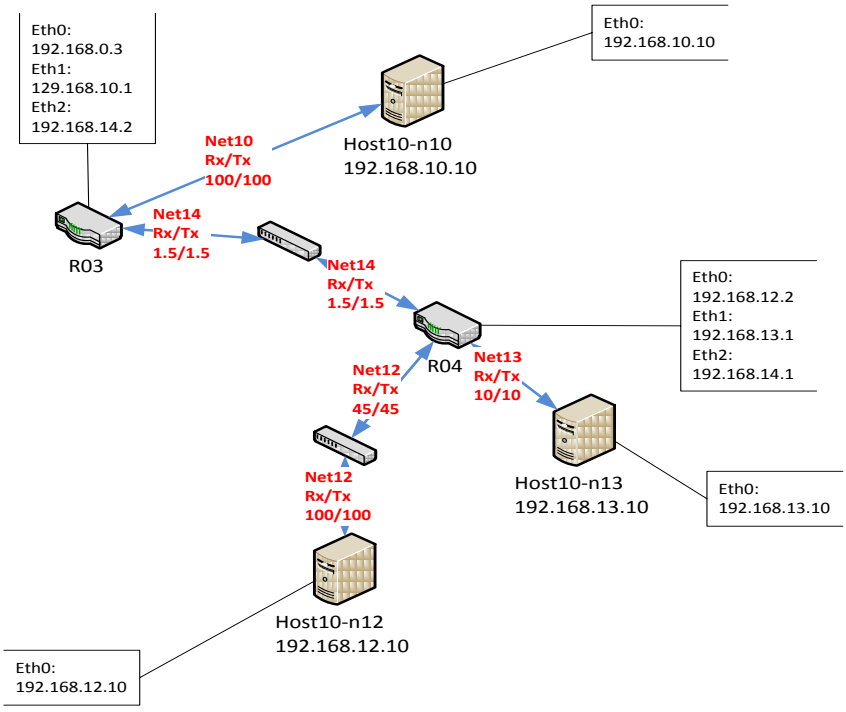

Рис. 3. Сегмент сети для моделирования атаки на BGP

Проверка пропускной способности канала проводилась с помощью утилиты iperf. Запуск производился на маршрутизаторе R04 и виртуальной машине Host10-n10 и Host10-n12.

Моделирование проводилось по двум сценариям:

1. Атака не посредственно на сервис Quagga, обслуживающий протокол BGP.
2. Проведение атаки на систему находящуюся за BGP-маршрутизатором, чтобы повлиять на общую пропускную способность канала связи маршрутизатора.

Атака сервиса Quagga. Для начала требуется попробовать инициировать соединение на порт 179 для установления соединения. Для этой задачи используется модуль scapy для python. Произведем отправку пакетов с TCP флагом SYN на атакуемый маршрутизатор, IP-адрес которого 192.168.14.1, с виртуальной машины 192.168.10.10.

```
    import time
    i = 1
    while i<10000:


       SYN=IP(dst="192.168.14.1",
src="192.168.10.10")/TCP(sport=179, dport=179, flags="S",
seq=40+i)
             SYNACK=sr1(SYN)
             ACK= IP(dst="192.168.14.1",
src="192.168.10.10")/TCP(sport=SYNACK.dport, dport=179,
flags="A", seq=SYNACK.ack, ack=SYNACK.seq + i)
       time.sleep( 5 )
       send(ACK)
       i += 1
```

Листинг 1 – Цикл соединения

Данный цикл отправляет пакет с флагом SYN и ждет ответа SYN-ACK, далее отвечает ACK пакетом с таймаутом в 5 сек (средний таймаут для состояния SYN-RECV).

Сразу после запуска в состояниях сетевых подключений видно как инициируется подключение и проходит все стадии, кроме стадии ESTABLISHED. Это происходит ввиду того, что сервис Quagga инициирует отправку пакета с флагом RST. Это логичная реакция сервиса на нелегитимное подключение. Стоит заметить, что при варьировании значения time.sleep() в диапазоне от 1 до 300 секунд, удаленная система завершала соединение на состоянии SYN-RECV. В итоге ни каких проблем с доступностью атакуемой системы выявлено не было (рис. 4).

В ходе анализа результатов эксперимента были сделаны выводы, что для проведения атак такого типа требуется написание полноценного программного обеспечения для эмуляции работы по протоколу BGP. Так же следует заметить, что для того, что бы устанавливалось полноценное соединение и началась передача данных, на основе которых было бы возможно провести атаку низкой интенсивности, сервер должен быть "плохо" сконфигурирован. При "плохой" конфигу-

рации любая автономная система сможет подключиться и начать обмен данными, в нашем случае таблицами маршрутизации. Как показала практика, сервисы такого рода имеют стандартные параметры такие, что запрещено любое внешнее взаимодействие. В спецификации протокола BGP существует понятие «соседей», что подразумевает с каким маршрутизатором требуется осуществлять обмен таблицами маршрутизации. Для разграничения доступа используются ACL списки, в которых явным образом необходимо указывать права доступа. Основными правами являются:

- разрешение на получение маршрутов от соседа;
- разрешение на скачивание маршрутов соседу.

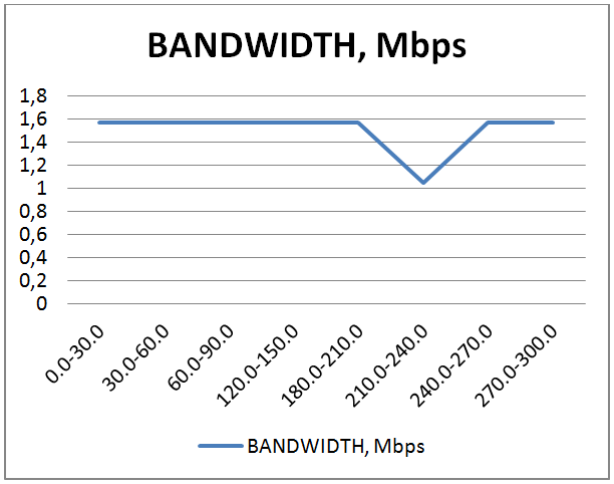

Рис. 4. Пропускная способность канала связи во время атаки

Таким образом, подобная атака может возникнуть только в случае халатности специалиста ответственного за данное программное обеспечение.

Низкоинтенсивная DoS-атака с маршрутизатором посередине. В эксперименте проводится атака на виртуальную машину, находящуюся за атакуемым маршрутизатором. Цель заключается в том, что бы маршрутизатор начал снижать пропускную способность канала при обработке проходящего трафика генерируемого при атаки низкой интенсивности.

Атакуемой машиной будет Host10-n10 с IP адресом 192.168.13.10. Маршрутизатор ответственный за сегмент сети где находится атакуемая машина – это R04. На виртуальной машине Host10-n10.

Запуск скрипта осуществляется командой:

```
#perl slowdos.pl -dns 192.168.10.10 -port 80 -timeout 100
                  -num 10000 -tcpto 5
```

Для наблюдения за состоянием пропускной способности канала связи на маршрутизаторе была запущена утилита iperf.

По истечении 5 минут видим результаты на рис. 5.

Пропускная способность канал маршрутизатора ни как не изменилась. Падение скорости на графике обусловлено тем, что в параметрах интерфейсов выставлены параметры потерь пакетов, для приближения к реальным условиям.

В ходе эксперимента было выявлено, что при малых размерах ботнета, проходящий трафик, генерируемый при атаке низкой интенсивности не влияет на пропускную способность канала связи граничного маршрутизатора.

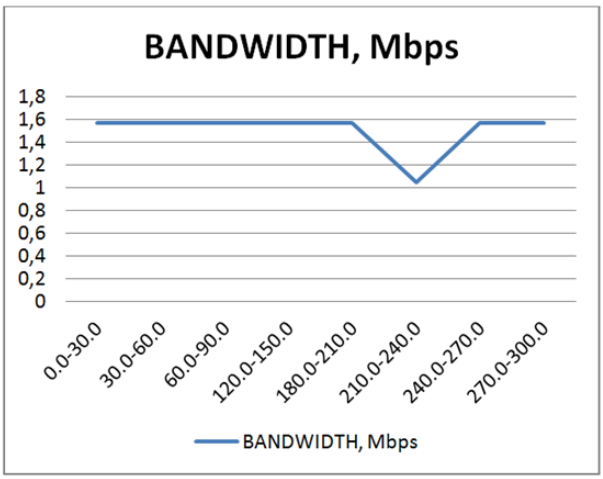

Рис. 5. Пропускная способность канала связи маршрутизатора во время атаки

4. Анализ экспериментальных данных. В результате проведенных экспериментов можно сделать следующие выводы. Во-первых, практически все проведенные атаки на системы, сконфигурированные «по умолчанию», прошли успешно. Причиной этому является то, что в таких случаях в системах, как правило, не сконфигурированы параметры для противодействия самым распространенным атакам. Исключением успешной атаки на сервис с конфигурацией по умолчанию является quagga. После того, как в результате повторяющихся атак были выведены из строя критичные узлы магистральных каналов связи, злоумышленникам удавалось провести атаки типа spoofing по причине небезопасной конфигурации маршрутизаторов.

Проведение низкоинтенсивной атаки на http-сервер сильно повлияло на общую пропускную способность. После начала атаки наблюдалось снижение пропускной способности канала связи (рис. 6), что приводило к снижению качества обслуживания клиентов http-сервером. Для сравнения на рис. 7 отображается график пропускной способности во время покоя.

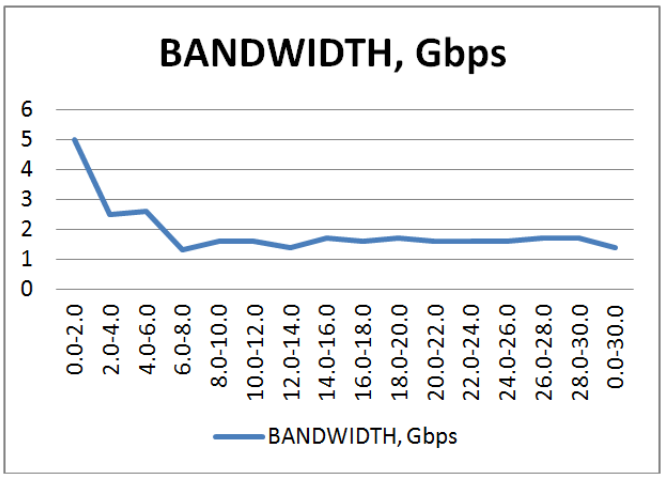

Рис. 6. График пропускной способности канала связи во время атаки

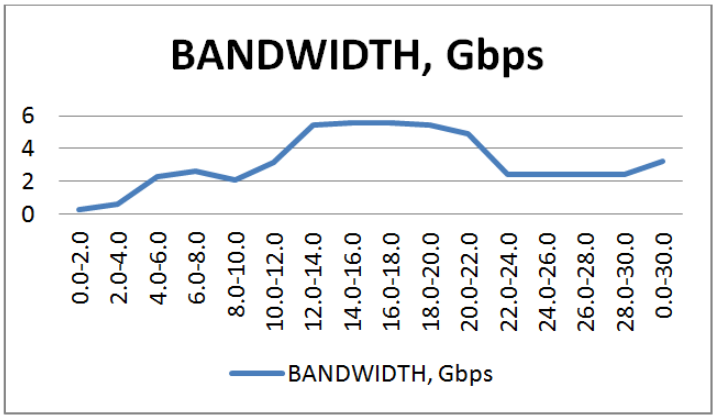

Рис. 7. График пропускной способности канала связи в состоянии покоя

На отметке времени начиная с 20.0–22.0 начинается «штатное» снижение пропускной способности, связанное с тем, что механизм контроля TCP Reno выбирает оптимальную скорость для передачи данных большого объема, при которой потери будут минимальны.

Выводы. Самыми важными экспериментами были атаки на BGP протокол. Так, в статье [7] описывалась модель проведения Low-Rate DoS-атаки на протокол BGP для нарушения маршрутизации в глобальных сетях, вследствие которой, может возникнуть лавинный эффект и резкое увеличение нагрузки на маршрутизаторы ответственные за один и тот же сегмент сети может привести к выходу из строя большого сегмента глобальной сети Интернет.

После проведения экспериментов стало ясно, что для успешной атаки такого рода требуется соблюдение большого количества условий, таких как ошибки конфигурирования, большое количество вычислительных ресурсов у атакующих и хорошо скоординированный сценарий атаки. Было установлено, что реализация данного сценария возможна только в сочетании с атакой «человек посередине».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Решение Cisco Systems «Clean Pipes» по защите от распределенных DOS-атак для операторов связи и их клиентов [Электронный ресурс]. – Режим доступа: http://www.cisco.com/ web/RU/downloads/CleanPipes_rus.pdf, свободный (дата обращения: 01.08.2013).
2. *Абрамов Е.С., Сидоров И.Д.* Метод обнаружения распределенных информационных воздействий на основе гибридной нейронной сети // Известия ЮФУ. Технические науки. – 2009. – № 11 (100). – С. 154-164.
3. *Лобанов В.Е., Оныкий Б.Н., Станкевичус А.А.* Архитектура системы защиты Грид от атак типа «отказ в обслуживании» и «распределенный отказ в обслуживании» // Безопасность информационных технологий. – 2010. – № 3. – С. 136-139.
4. Обзор DDoS-атак во втором квартале 2011 года. – [Электронный ресурс]. – Режим доступа: http://www.securelist.com/ru/analysis/208050712/ Obzor_DDoS_atak_vo_vtorom_ kvartale_ 2011_goda (дата обращения: 01.08.2013).
5. *Chee W.O. Brennan T.* OWASP AppSec DC 2010. HTTP POST DDoS. – [Электронный ресурс]. – Режим доступа: https://www.owasp.org/images/4/43/ Layer_7_DDOS.pdf (дата обращения: 01.08.2013).

6. *Abramov E.S., Andreev A.V., Mordvin D.V., Makarevich O.B.* Corporate networks security evaluation based on attack graphs // Proceedings of the 4th international conference on Security of information and networks (SIN '11)-ACM, New York, NY, USA, 2011. – P. 29-36.
7. *Aleksandar Kuzmanovic, Edward W. Knightly*. Low-rate TCP-targeted denial of service attacks and counter strategies // IEEE/ACM Trans. Netw. – 2006. – № 14 (4). – С. 683-696.
8. *Paxson V., Allman M., Chu H.K., and Sargent M.* Computing TCP's Retransmission Timer, RFC 6298, Proposed Standard, June 2011.

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

Тарасов Ярослав Викторович – ЗАО «Инфосистемы Джет»; e-mail: info@jet.msk.su; 127015, Москва, ул. Большая Новодмитровская, 14-1; тел.: +74954117601; директор по развитию.

Макаревич Олег Борисович – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: mak@tsure.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; зав. кафедрой.

Tarasov Yaroslav Viktorovich – Jet Infosystems; e-mail: info@jet.msk.su; 14-1, Large Novodmitrovskaya street, Moscow, 127015, Russia; phone: +74954117601; director of development.

Makarevich Oleg Borisovich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”; e-mail: mak@tsure.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; head the department.

УДК 004.056.5

В.Г. Миронова, А.А. Шелупанов

АНАЛИЗ РЕЖИМОВ РАЗГРАНИЧЕНИЯ И РАСПРОСТРАНЕНИЯ ПРАВ ДОСТУПОВ НА ОСНОВЕ ДИСКРЕЦИОННОЙ МОДЕЛИ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПОВ TAKE-GRANT

В функционирующих информационных системах обработки конфиденциальной информации используются два режима обработки данных – однопользовательский и многопользовательский. При многопользовательском режиме обработки данных целесообразно использование разграничения прав доступа пользователей к информации, поскольку это увеличивает уровень безопасности информации. Обеспечение безопасности информации, обрабатываемой как в электронном, так и бумажном виде начинается с режима разграничения прав доступов пользователей. Но не стоит забывать о том, что между пользователей и злоумышленником существует возможность передачи или распространения прав доступа к конфиденциальной информации. Существует несколько политик разграничения прав доступа к информации – дискреционная и мандатная. Анализ возможностей распространения прав доступов зависит от выбранной политики безопасности и позволяет выявлять каналы утечки конфиденциальной информации и способы ее распространения. Данные о каналах утечки информации и способах ее распространения позволяют проектировать и создавать надежную систему защиты информации.

Информационная безопасность; политика безопасности; модель; разграничение прав доступа.