УДК 004.7/.056

МОДЕЛИРОВАНИЕ ЗАЩИЩЕННОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ОРГАНИЗАЦИИ В СРЕДЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ CISCO PACKET TRACER 6.2

Кертов К.В., Болиев З.В., Шогенов А.А., Жилоков А.Х., Кучерова В.Ю.

ФГБОУ ВО «Кабардино-Балкарский государственный университет им. Х.М. Бербекова», Нальчик, e-mail: kazbek.kertov@mail.ru

В данной работе проведено моделирование локальной вычислительной сети организации в среде имитационного моделирования Cisco Packet Tracer 6.2. Были описаны основные преимущества использования данного программного продукта. В реализованной модели узлам сети организации был предоставлен выход во внешнюю сеть, имитирующую сеть Интернет посредством технологии преобразования сетевых адресов PAT. Данная технология была рассмотрена с точки зрения безопасности сети организации. Были рассмотрены преимущества виртуальных локальных сетей VLAN и целесообразность их реализации. После завершения этих работ была выявлена уязвимость сети, которая является довольно актуальной для сетей большинства крупных организаций. Возможность реализации выявленной угрозы хакером, получившим несанкционированный доступ к сети организации, была смоделирована в виде атаки, представляющей собой ICMP-запросы из внешней сети Интернет. После успешной реализации данной атаки было осуществлено пресечение выявленных уязвимостей сети с помощью списков контроля доступа ACL.

Ключевые слова: локальная вычислительная сеть, технология преобразования сетевых адресов (PAT), виртуальная локальная сеть (VLAN), ICMP-запросы, списки контроля доступа (ACL)

MODELING OF THE PROTECTED LOCAL NETWORK OF THE ORGANIZATION IN THE MEDIA OF IMITATION SIMULATION CISCO PACKET TRACER 6.2

Kertov K.V., Boliev Z.V., Shogenov A.A., Zhilokov A.Kh., Kucherova V.Yu.

Kabardino-Balkarian State University, Nalchik, e-mail: kazbek.kertov@mail.ru

In this paper we simulate the local computer network of the organization in the Cisco Packet Tracer 6.2 simulation environment. The main advantages of using this software product were described. In the implemented model, the nodes of the organization's network were provided with an outlet to an external network that mimics the Internet using PAT's network address translation technology. This technology was considered from the point of view of network security of the organization. The advantages of virtual local area networks VLAN and the feasibility of their implementation were considered. After the completion of these works, a network vulnerability was revealed, which is quite relevant for the networks of most large organizations. The ability to implement the detected threat by a hacker who received unauthorized access to the organization's network was modeled as an attack that represents ICMP requests from the external Internet. After the successful implementation of this attack, the identified network vulnerabilities were curbed using ACL access control lists.

Keywords: local computer network, Port Address Translation technology (PAT), Virtual Area Local Network (VLAN), ICMP – requests, Access Control Lists (ACL)

Постановка задачи моделирования и ее связь с актуальными научными и практическими исследованиями

В современном мире локальная вычислительная сеть (ЛВС) играет ключевую роль в функционировании и развитии бизнес-процессов организации. В связи с этим одной из наиболее широко обсуждаемых тем в сетевой индустрии является безопасность сетей. Безусловно, проблематика безопасности всегда оставалась важной, но наблюдаемое в последнее время стремительное расширение масштабов в области применения сети Интернет приводит к возникновению все новых и новых проблем с безопасностью сетей. В прошлые годы в большинстве компаний не применялись постоянные соединения с глобальной сетью, т.е. с сетью, через которую можно попытаться проще всего получить несанкционированный доступ к внутренней сети организации. В настоящее время во множестве компаний поддерживаются постоянные соединения с сетью Интернет, поскольку определенная часть их доходов основана на использовании средств доступа к сети. Тем не менее повсеместное подключение к интернет-среде увеличивает опасность проникновения извне и появляются дополнительные предпосылки нарушения защиты информации. В связи с этим вопрос безопасности локальной вычислительной сети организации становится чрезвычайно актуальным [1].

Согласно статистическим данным, хакерские атаки из сети Интернет с каждым годом растут в экспоненциальном виде. Основная часть данных атак направлена на локальную вычислительную сеть, что грозит целостности информационных и финансовых активов организации. Защита на должном уровне ЛВС, в свою очередь, может от-

носительно обезопасить весь поток данных, циркулирующих в системе. Исследование безопасности локальной вычислительной сети методом имитационного моделирования и дальнейшая реализация таких моделей в реальной сети организации позволяет реагировать на актуальные виды угроз и имеет практическую значимость.

Целью данной научной работы является выявление имеющихся потенциальных угроз информационной безопасности и уязвимостей сети организации методом имитационного моделирования. Проведя исследования в данной области, построена модель ЛВС, которая соответствует следующим общепринятым требованиям:

- масштабируемость;
- гибкость;
- простота внедрения;
- надежность;
- безопасность.

Научная новизна данной стати заключается в том, что реализация сетевых атак и средств их блокирования методом имитационного моделирования позволяет решать прикладные задачи в области обеспечения безопасности ЛВС. Статья посвящена иллюстрации результатов моделирования защищенной локальной вычислительной сети организации в среде Cisco Packet Tracer 6.2 [2].

Моделирование локальной вычислительной сети организации и осуществление доступа во внешнюю сеть Интернет

Защита ЛВС организации в первую очередь начинается с выявления имеющихся угроз безопасности системы. Далее следует выбрать необходимые программно-аппаратные средства защиты, в соответствии с политикой информационной безопасности организации. В основе политики информационной безопасности организации лежат соответствующие нормативно-правовые акты в области обеспечения безопасности.

Рассмотрим пример модели ЛВС организации (рис. 1). Приведенная модель не является эталонной и не содержит результатов комплексного и всестороннего моделирования защищенной локальной вычислительной сети. Она может быть изменена в зависимости от схемы ЛВС организации. В частности, могут быть изменены: топология, количество сетевого оборудования и количество конечных узлов сети. Данная модель спроектирована в среде имитационного моделирования Cisco Packet Tracer 6.2. Пакет Cisco Packet Tracer – это инструмент, предоставляющий возможность имитировать как работу некоторого набора сетевых устройств (маршрутизаторы, коммутаторы, точки беспроводного доступа, персональные компьютеры, сетевые принтеры, IP-телефоны и т.д.), так и сетевое взаимодействие между ними (распространение пакетов по сети). Так, данное программное обеспечение методом имитационного моделирования позволяет выявить те или иные недостатки ЛВС организации в области информационной безопасности или устранить различные неполадки, возникающие в сети организации. Данный метод моделирования защищенной ЛВС может быть реализован как для средних, так и для крупных сетевых комплексов [3].

В рассматриваемой модели ЛВС организации реализована технология виртуальной локальной сети (Virtual Local Area Network – VLAN). Данная технология реализована на коммутаторе Switch. Основное назначение виртуальной локальной сети – это создание нескольких логических подсетей в одной физической подсети. Так, после введения определенных конфигурационных команд в командной строке коммутатора, пользователи User_1, User_2, User_3 стали находиться в подсети 192.168.2.0/24 во VLAN 2, а сервер Server – в подсети 192.168.3.0/24 во VLAN 3. Данная технология уменьшает объем широковещательного трафика, что позволяет значительно увеличить пропускную способность сети. Помимо этого, технология виртуальной сети дает возможность ограничить доступ определенных пользователей, находящихся в ЛВС организации, к тем подсетям, к которым доступ для них запрещен. Также, в данной модели создана модель внешней сети Интернет, в которую входит маршрутизатор Provider и WEB-server. В маршрутизаторе Provider интерфейсам fastEthernet 0/0 и fastEthernet 0/1 присвоены IP-адреса из диапазона публичных IP-адресов 213.234.10.1/32 и 213.234.20.1/32 соответственно. Серверу WEB-server был присвоен IP-адрес 213.234.10.1/30, который также является публичным IP-адресом.

Технология преобразования сетевых адресов (Port Address Translation – PAT) позволяет отображать несколько частных адресов в один публичный IP-адрес. Это дает возможность не только временно решить проблему нехватки IP-адресов версии 4, но и позволяет пользователям сети организации выходить в сеть Интернет со своих частных IP-адресов. Так, в рассматриваемой нами модели была реализована данная технология трансляции сетевых адресов PAT на маршрутизаторе Router. Тем самым пользователи User_1, User_2 и User_3 получили доступ к внешней сети Интернет со своих частных IP-адресов [4].

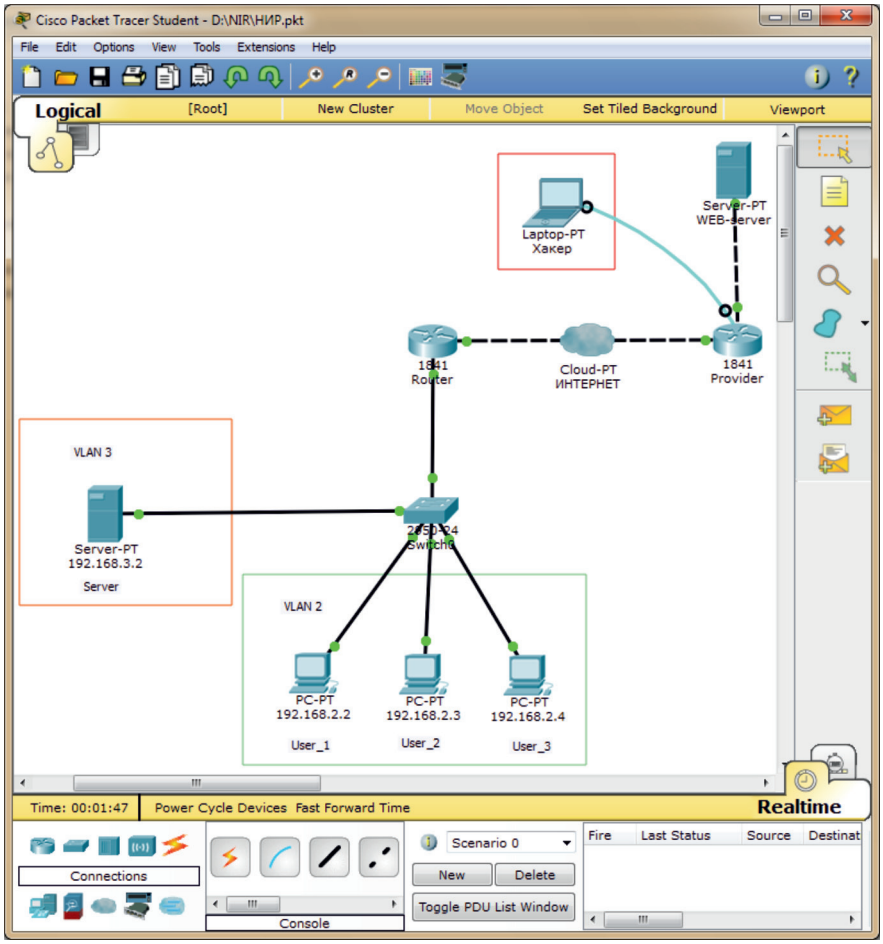

Рис. 1. Пример модели ЛВС организации

Моделирование атаки из сети Интернет и пресечение данной атаки посредством списков контроля доступа ACL

Реализация технологии PAT фактически создает межсетевую защиту между внутренней ЛВС организации и внешней сетью Интернет. Это означает, что компьютер потенциального злоумышленника из внешней сети не сможет подключиться к компьютеру пользователей организации, так как внутренние IP-адреса организации не транслируются в сеть Интернет. Однако смоделируем ситуацию, в которой злоумышленник (хакер) осуществил несанкционированное подключение к внешнему маршрутизатору (рис. 1). В таком случае он может с легкостью прописать маршруты во внутреннюю сеть организации на внешнем маршрутизаторе Provider. При этом хакер может взять достаточно большой диапазон сети – 192.168.0.0 с маской подсети 255.255.0.0, так как данные IP-адреса очень часто используются для узлов ЛВС различных организаций. Смоделируем данный вид атаки посредством протокола управления сообщениями Интернет (Internet Control Massage Protocol – ICMP), т.е. ICMP-запросов (рис. 2). Мы видим, что атака прошла успешно, 100% ICMP-запросов получили ответы (на рисунке подчеркнуто красным) [5].

Защиту ЛВС организации от атаки из внешней сети Интернет можно осуществить посредством настройки списков контроля доступа (Access Control List – ACL), которая является одним из наиболее важных инструментальных средств в программном обеспечении Cisco IOS, использующихся в осуществлении продуктивной стратегии информационной безопасности. Эти списки определяют правила, которые могут использоваться для фильтрации в сети некоторых пакетов. Данное утверждение означает, что списки управления доступом IOS могут стать ключевым инструментальным средством обеспечения безопасности, составляющим часть общей стратегии безопасности, независимо от того, нужно ли просто ограничить доступ к серверу с конфиден-

циальной информацией, допуская к этим сведениям только санкционированных сотрудников, или требуется предотвратить проникновение из сети Интернет потенциальных злоумышленников, которые могут, например, нарушить работу веб-сервера электронной коммерции.

Так, технология ACL является важнейшим базовым средством осуществления безопасности сети на основе фильтрации пактов, проходящих через маршрутизатор. Тем самым несанкционированный трафик сети блокируется. Технология ACL была реализована на внутреннем маршрутизаторе Router в рассматриваемой модели ЛВС организации. Для этого в командной строке CLI маршрутизатора был введен следующий набор команд (рис. 3).

Команды deny ip any 192.168.2.0 0.0.0.255 и deny ip any 192.168.3.0 0.0.0.255 позволяют отбрасывать пакеты, которые были сгенерированы из внешней сети Интернет, в данном случае для подсетей 192.168.2.0/24 и 192.168.3.0/24. Следует отметить, что данные команды нужно вводить в соответствии с количеством подсетей в ЛВС. Это позволяет обезопасить внутреннюю локальную вычислительную сеть организации от внешних целенаправленных атак. Немаловажным преимуществом технологии списков контроля доступа ACL является то, что пакеты, которые генерируются в ЛВС организации при выходе в сеть Интернет, при прохождении через маршрутизатор помечаются определенных образом и благополучно получают ответы. После введения вышеупомянутых наборов команд еще раз проведем моделирование атаки хакера, подключенного к маршрутизатору Provider посредством ICMP-запросов из внешней сети Интернет (рис. 4). Как мы видим, данная атака оказалась безуспешной, ни один из ICMP-запросов не получил ответы (подчеркнуто синим).

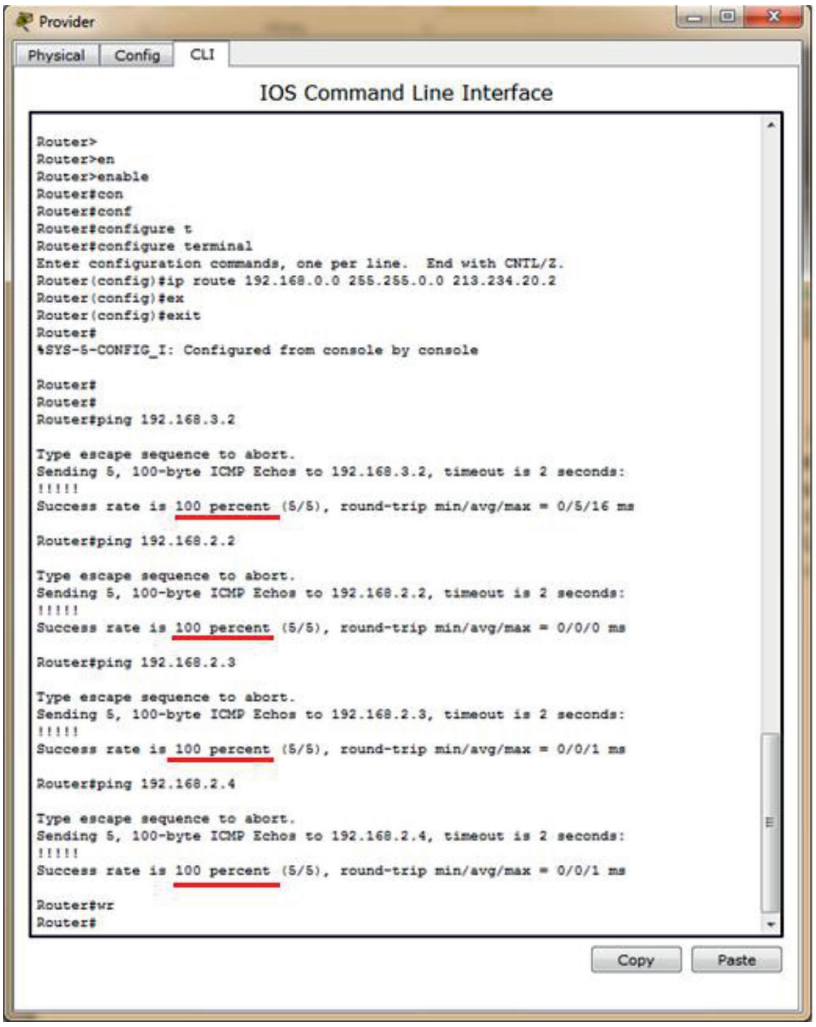

Рис. 2. Моделирование атаки в виде ICMP-запросов

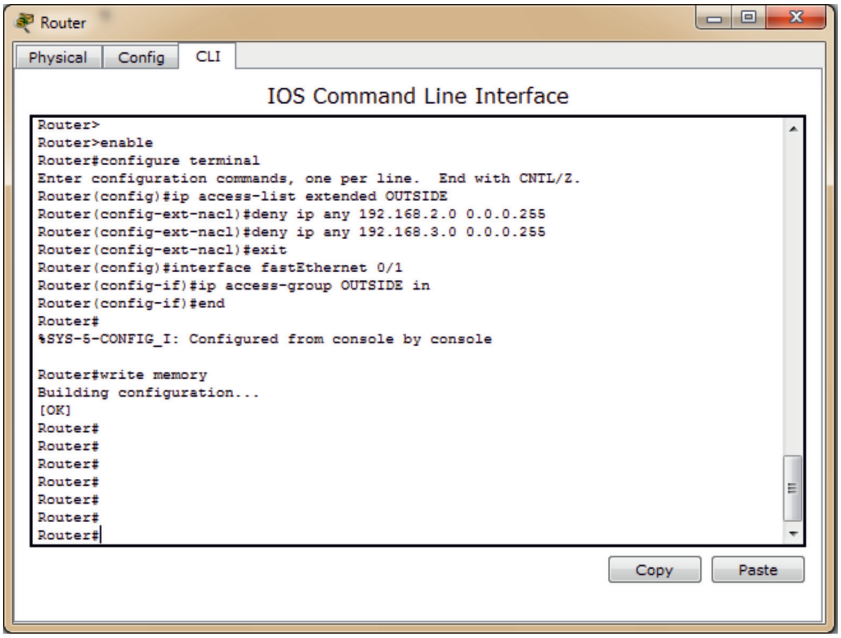

Рис. 3. Команды для реализации технологии ACL

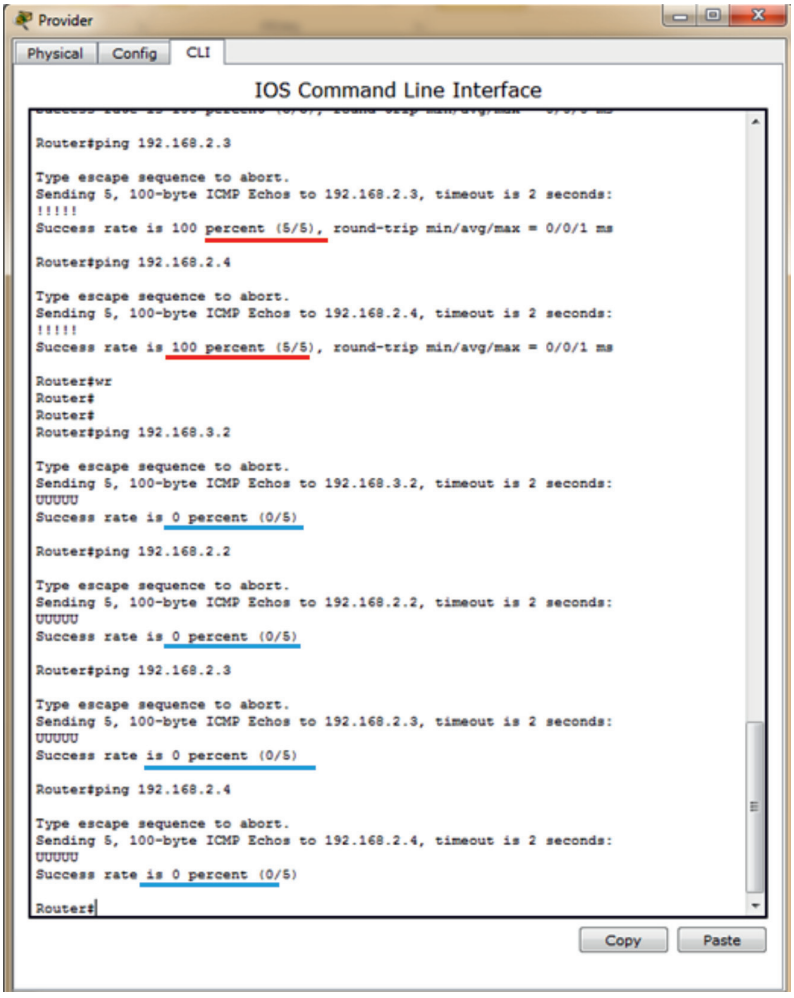

Рис. 4. Моделирование атаки в виде ICMP-запросов после настройки ACL

Приводя количественную оценку полученных результатов моделирования, следует отметить, что изначально сеть была скомпрометирована на 100% (рис. 2), после реализации технологии ACL (рис. 3) сеть стала полностью защищенной в плане фильтрации внешнего трафика и тем самым оценка сетевых атак составила 0% (рис. 4) [6].

Выводы и перспективы дальнейших исследований

Моделирование в среде имитационного моделирования Cisco Packet Tracer 6.2 наглядно продемонстрировало функционирование сетевых устройств и их взаимодействие; позволило обеспечить узлам сети доступ во внешнюю сеть Интернет, провести успешную хакерскую атаку, а также выявить имеющиеся уязвимости ЛВС организации и купировать их. Данная атака была успешно произведена в силу имеющихся уязвимостей сети, что на практике является частым явлением. На основе выявленных недостатков было решено осуществить фильтрацию трафика, проходящего через маршрутизатор Router, используя технологию управления списками контроля доступа ACL. Были описаны основные преимущества данной технологии и целесообразность ее внедрения в сетевую инфраструктуру. Обеспечение безопасности ЛВС методом имитационного моделирования и дальнейшая реализация таких моделей в реальной сети организации позволяет реагировать на актуальные виды угроз информационной безопасности, что обуславливает важность и перспективность проведения исследований в данном направлении.

Список литературы

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2011 – 320 с.

2. Андрончик А.Н. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков; под общ. ред. Н.И. Синадского. – Екатеринбург: Изд-во Урал. ун-та, 2014. – 180 с.

3. Одом У. Официальное руководство по подготовке к сертификационным экзаменам CCENT/CCNA ICND1, 2-е изд.: Пер. с англ. – М.: ООО «И.Д. Вильямс», 2010. – 672 с.: ил. – Парал. тит. англ.

4. Уэнстром М. Организация защиты сетей Cisco.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 768 с.: ил. – Парал. тит. англ.

5. Леммл Т., Одом Ш., Уоллес К. CCNP: Маршрутизация. Учебное руководство. – М.: «Лори», 2015 – 444 с.

6. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2, 2-е изд.: Пер. с англ. – М. : ООО «И.Д. Вильямс», 2011. – 736 с.: ил. – Парал. тит. англ.