17. Zhang Sh., Zhang W., Gao Sh., Geng P., Xue X. Fiber-optic bending vector sensor based on Mach–Zehnder interferometer exploiting lateral-offset and up-taper. *Optics Letters*, 2012, vol. 37, pp. 4480-4482. doi: 10.1364/OL.37.004480.
18. Xu L., Jiang K., Wang S., Li B., Lu Y. High temperature sensor based on an abrupt-taper Michelson interferometer in single-mode fiber. *Applied Optics*, 2013, vol. 52, pp. 2038-2041. doi: 10.1364/AO.52.002038
19. Pu Sh., Dong Sh. Magnetic field sensing based on magnetic-fluid-clad fiber-optic structure with up-tapered joints. *IEEE Photonics Journal*, 2014, vol. 6, 5300206. doi: 10.1109/JPHOT.2014.2332476.
20. Yadav T.K., Mustapa M.A., Abu Bakar M.H., Mahdi M.A. Study of single mode tapered fiber-optic interferometer of different waist diameters and its application as a temperature sensor. *Journal of the European Optical Society*, 2014, vol. 9, 14024. doi: 10.2971/jeos.2014.14024.
21. Jung Y., Brambilla G., Richardson D.J. Efficient higher-order mode filtering in multimode optical fiber based on an optical microwire. *Asia Optical Fiber Communication and Optoelectronic Exposition and Conference*, Shanghai, China: OSA Technical Digest, 2008, pp. SuB4. doi: 10.1364/AOE.2008.SuB4
22. Xu M.G., Dong L., Reekie L., Tucknott J.A., Cruz J.L. Temperature-independent strain sensor using a chirped Bragg grating in a tapered optical fibre. *Electronics Letters*, 1995, vol. 31, pp. 823-825. doi: 10.1049/el:19950542.
23. Kim S., Kwon J., Kim S., Lee B. Temperature-independent strain sensor using a chirped grating partially embedded in a glass tube. *IEEE Photonics Technology Letters*, 2000, vol. 12, pp. 678-680. doi: 10.1109/68.849082.
24. Frazao O., Melo M., Marques P.V.S., Santos J.L. Chirped Bragg grating fabricated in fused fibre taper for strain and temperature discrimination. *Measurement Science and Technology*, 2005, vol. 16, pp. 984 – 988.
25. Kim S.-Ch., Kim S., Kwon J., Lee B. Fibre Bragg grating strain sensor demodulator using a chirped fibre grating. *IEEE Photonics Technology Letters*, 2001, vol. 13, pp. 839-841. doi: 10.1109/68.935821
26. Frazao O., Falate R., Fabris L., Santos J.L., Ferreira L.A., Araújo F.M. Optical inclinometer based on a single long-period fiber grating combined with a fused taper. *Optics Letters*, 2006, vol. 31, pp. 2960-2962. doi: 10.1364/OL.31.002960
27. Tao Qi, Shilin Xiao, Jie Shi, Lilin Yi, Zhao Zhou, Meihua Bi, Weisheng Hu. Cladding-mode backward-recoupling-based displacement sensor incorporating fiber up-taper and Bragg grating. *IEEE Photonics Journal*, 2013, vol. 5, 7100608. doi: 10.1109/JPHOT.2013.2274770
28. Karra S., Soumya M. Preparation of tapered optical fibers to utilize the evanescent field for sensing applications. *International Journal of Engineering Trends and Technology*, 2013, vol. 4, no. 3, pp. 442-446.
29. Ericsson FSU-975. User manual. Ericsson, 2001, pp. 76.
30. Listvin A.V., Listvin V.N., Shvyrkov D.V. *Opticheskie volokna dlya liniy svyazi* [Optical fiber for communication lines]. Moscow, LESARart Publ, 2003. 288 p.
31. Semenov A.B. *Volokonno-opticheskie podsistemy sovremennykh SKS* [Fiber-optic subsystem of modern SCS]. Moscow, Akademiya AyTi, DMK Press, 2007. 632 p.

Received 30.01.2017

УДК 004.7

МОДЕЛИРОВАНИЕ ЗАЩИЩЕННЫХ КАНАЛОВ ТЕЛЕКОММУНИКАЦИЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВИРТУАЛИЗАЦИИ

Васин Н.Н., Ирбахтин А.А.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: vasin@psuti.ru

В современных условиях работы телекоммуникационных систем возникают различного рода угрозы безопасности. Для того чтобы предупредить возможность их реализации, необходимы современные методы защиты. Для испытания методов защиты от возможных угроз наиболее целесообразным является метод моделирования. В работе рассматривается программно-аппаратный комплекс по моделированию защищенных каналов связи с использованием средств виртуализации. Описаны составные компоненты программно-аппаратного комплекса и их взаимодействие между собой. Рассмотрены два примера по использованию данного комплекса. Первый пример описывает передачу FTP-трафика по защищенному и незащищенному каналам связи. Этот пример показывает

важность наличия защищенных соединений в телекоммуникациях и методику моделирования с помощью средств виртуализации. Второй пример описывает моделирование DOS-атаки на сервер. Этот пример описывает возможность моделирования атак с помощью комплекса и проработку механизмов защиты от применяемых атак.

Ключевые слова: информационная безопасность, телекоммуникации, моделирование

Введение

В настоящее время вопросы контроля информационной безопасности сетевых устройств и серверов имеют большое значение. Сеть является первым барьером защиты, поэтому при построении и эксплуатации сетей необходим контроль уязвимостей в конфигурации устройств, а также уязвимостей программного обеспечения.

Тестирование сетей и выявление уязвимостей дает возможность предварительного усиления защиты сети и серверной части. Важным вопросом информационной безопасности является настройка защищенных каналов связи путем шифрования информационных и служебных передаваемых данных, а также проверки целостности принятых данных.

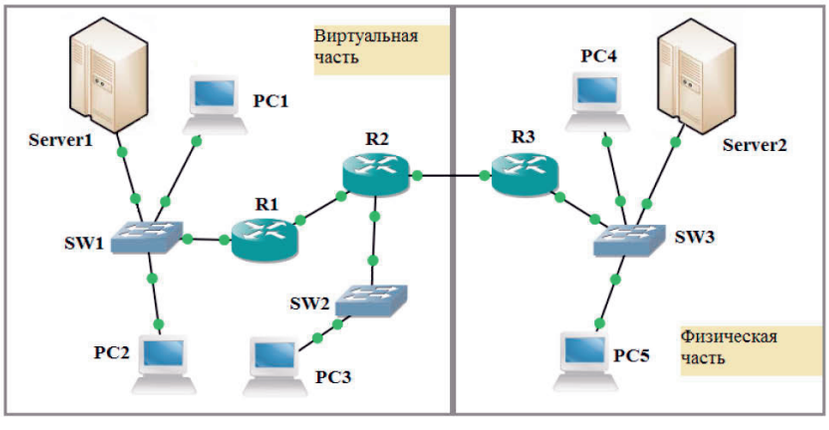

Рис. 1. Обобщенная структурная схема комплекса

Основа комплекса

Учитывая важность вышесказанных факторов, необходимо отметить, что важны и новые методы обучения студентов. Разработан программно-аппаратный комплекс по изучению и моделированию защищенных каналов связи. В состав комплекса входит эмулятор сетей GNS3 [1], система виртуализации VirtualBox [2], маршрутизаторы с ОС Vyatta [3], 6 маршрутизаторов Cisco серии 2800, 6 коммутаторов Cisco Catalyst 2900, сервер с ОС Ubuntu Server, рабочие ПК с ОС Ubuntu, ПК для анализа трафика с ОС KaliLinux, программа мониторинга и анализа трафика Wireshark [4].

Совокупность программных и аппаратных средств образуют универсальный комплекс, позволяющий моделировать и настраивать различные схемы передачи трафика по принципу «Клиент-Сеть-Сервер» как на реальном оборудовании, так и с помощью средств виртуализации. В дальнейшем к настроенным схемам передачи трафика можно применять различные методы защиты информации, например такие, как фильтрация трафика и шифрование каналов передачи: организация VPN по схемам «сеть-сеть», «хост-сеть», «хост-хост», организация TSL/SSL шифрования.

Принцип построения модели «Клиент-Сеть-Сервер» позволяет изучать протоколы сетевого уровня, при настройке части «Сеть», и протоколы верхних уровней, при настройке части «Клиент-Сервер», а также анализировать закономерности работы этих протоколов. Анализ передаваемого трафика служит основой для исследования и сравнения процессов, происходящих в каналах передачи информации, как использующих защиту, так и без нее.

Эмулятор сетей GNS3 в совокупности с системой виртуализации VirtualBox образуют основу платформы для виртуального моделирования, возможности которой ограничены системными ресурсами используемого ПК. Общая структурная схема построения модели на основе комплекса представлена на рис. 1.

Программа Wireshark [4; 10] широко распространенный инструмент для захвата и анализа трафика. Входит в состав ОС KaliLinux либо может быть установлена на любые другие ОС. Программа имеет возможность детального рассмотрения структуры пакета, что делает его

мощным средством для перехвата и анализа трафика. Анализ трафика происходит локально на хосте либо подключаясь в интересующие места, например с помощью коммутатора с настроенным зеркалированием портов.

Для более углубленного изучения и анализа безопасности моделируемой схемы используется ОС KaliLinux, которая позволяет тестировать ее компоненты на предмет возможных атак и выявлять причину их возникновения. Эти знания помогают в дальнейшем устранять выявленные уязвимости.

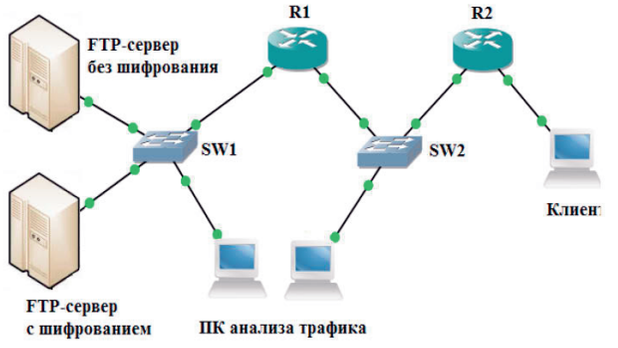

Рис. 2. Структурная схема модели для передачи FTP-трафика комплекса

В качестве первого примера рассмотрим сеть передачи данных по протоколу FTP с шифрованием по каналу VPN и без шифрования с открытым каналом передачи. Для этого построена модель, показанная на рис. 2. В качестве маршрутизаторов R1 и R2 используются программные маршрутизаторы с ОС Vyatta 6.6, основанные на ОС Linux. В качестве серверов используется ОС Ubuntu Server 14.04 [5-6]. Для мониторинга трафика использована ОС Kali Linux со встроенным анализатором трафика Wireshark. На коммутаторах используется зеркалирование портов или используются хабы. Таким образом, комплекс построен на базе свободно распространяемого ПО.

Примеры использования

Рассмотрим два примера по использованию возможностей применения моделирования:

– организация шифрованного соединения для FTP-трафика и показание эффективности шифрования;

– моделирование DOS-атаки с использованием утилит для взлома.

При настройке сети для маршрутизации использован протокол OSPF [3; 7-8], между маршрутизаторами R1 и R2 создан туннель IPSec [9]. На ОС Ubuntu Server установлена и настроена утилита vsFTPd [5], реализующая FTP-сервер. На FTP-сервере с шифрованием установлена и настроена утилита vsFTPd в комплексе с криптографическим пакетом для шифрования OpenSSL. Таким образом, сконфигурирован сервер с шифрованием FTP-данных по протоколу SSL [9]. Также для шифрования данных может быть использован и протокол TLS [9].

Для анализа передаваемого по сети трафика выполнены следующие действия:

– запущен Wireshark на ПК для анализа трафика;

– сделан FTP-запрос получения файла с ПК клиента на FTP-сервер. На FTP-сервер заранее помещены тестируемые файлы, например, изображения;

– анализ трафика, перехваченного ПК2 между маршрутизаторами R1 и R2, свидетельствует о том, что данные FTP-сессии недоступны для извлечения;

– ПК1 перехватывает FTP-сессию и данные, передаваемые между клиентом и сервером. С помощью опций Analyze > Follow TCP Stream Wireshark легко обнаруживает открытую FTP-сессию.

На рис. 3 изображен пример перехваченной FTP-сессии. Перехвачены управляющие команды протокола FTP, имя пользователя (USER alex), пароль пользователя (PASS 1234), передаваемый файл (PETR image_for_test.png).

Приведенные данные позволяют рассмотреть процесс инициализации сессии и передачу файла:

– ниже пакета с запросом на передачу PETR найден пакет FTP-DATA (см. рис. 4) и с помощью опций Analyze > Follow TCP Stream > Save сохранен передаваемый файл (image_for_test.png);

– передаваемый файл полностью соответствует файлу, заранее помещенному на FTP-сервер;

– проделаны аналогичные действия при запросе на FTP-сервер с шифрованием;

– перехваченные данные будут зашифрованы с помощью протокола SSL, что не исключит, но значительно затруднит их извлечение.

Приведенный пример наглядно показывает методику анализа трафика, используемого в комплексе, а также эффективность применения защищенных соединений и их важность в телекоммуникационных сетях.

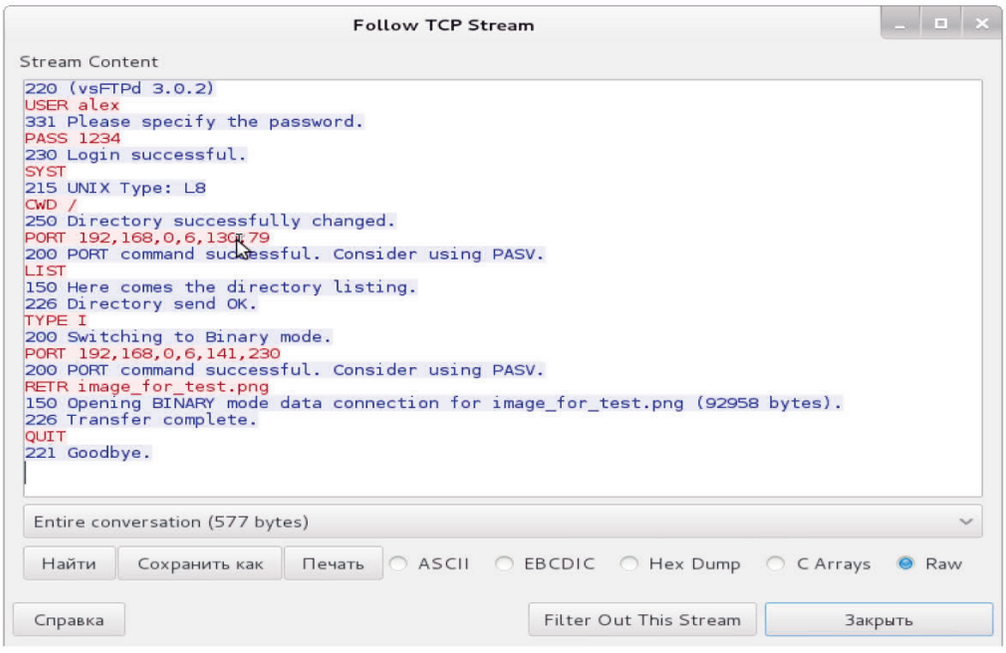

Рис. 3. Перехваченный FTP-запрос

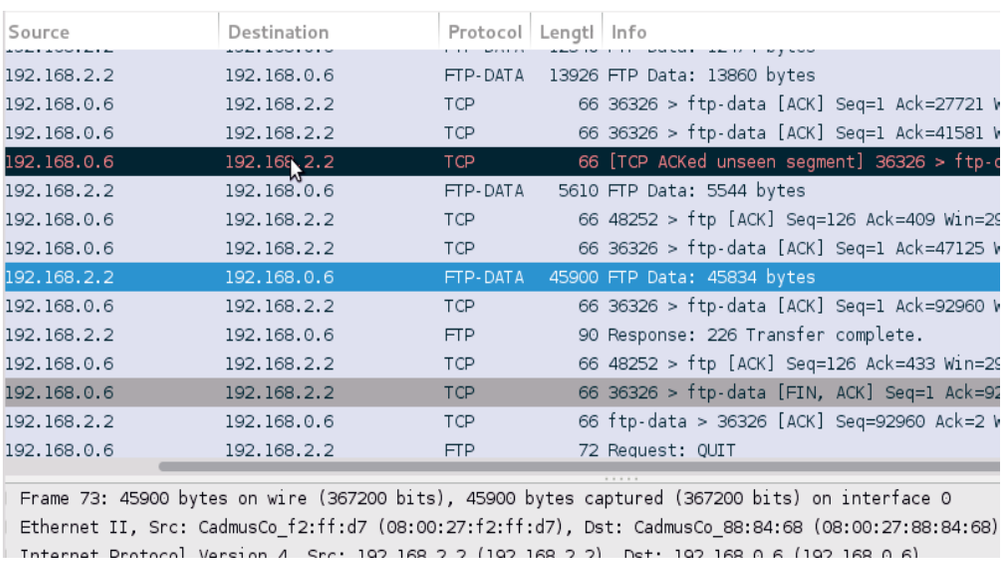

Рис. 4. Пакеты с FTP-данными (FTP-DATA)

Рассмотрим пример моделирования DOS-атаки. На рис. 5 показана схема сети, позволяющая смоделировать данную атаку. Сеть настраивается на протоколе маршрутизации OSPF [3; 7-8]. Сервер Server1 представляет собой хост, на который производится DOS-атака и который реализован на ОС Ubuntu Server с запущенным сервером Apache Server [11]. Таким образом, открыт доступ по HTTP [9] (см. порт 80). Хост PC2 является узлом, с которого производится атака, реализованный на ОС Kali Linux с установленными утилитами Slowloris[12] и Torshammer [13]. Хост PC1 является узлом мониторинга трафика с установленной программой Wireshark. Маршрутизатор R1 является шлюзом перед Server1, который реализован с помощью образа ОС Cisco ASA с настроенными функциями защиты от DOS-атак.

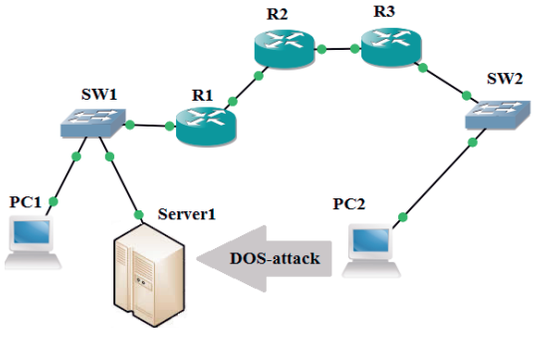

Рис. 5. Структурная схема моделирования DOS-атаки

Утилита Slowloris заставляет атакуемый сервер обслуживать большое количество открытых соединений путем непрерывной отправки незавершенных HTTP-запросов. В результате все потоки заняты обработкой запросов. Данная атака основана на уязвимости самих серверов и трудноразличима среди другого трафика. Особенно уязвимыми считаются серверы Apache.

Torshammer является утилитой, которая реализует уязвимость серверов к медленным POST-запросам. Медленные запросы основаны на генерации POST-запросов, которые затем долго дополняются, обычно посимвольно. В результате рабочие потоки зависают. Данная атака основана на уязвимости самого протокола HTTP. Данной уязвимости подвержены почти все серверы, и атака на ее основе тоже трудноразличима среди другого трафика.

Рассматриваемые атаки являются крайне опасными для серверов. Позволяют выбивать малые и средние сайты из рабочего состояния в считанные минуты, используя один компьютер. Запустив данные утилиты на хосте PC2, можно убедиться, что сервер Server1 пришел в неработоспособное состояние, то есть DOS-атака успешно реализована. Маршрутизатор R1, выполняющий роль межсетевого экрана, не эффективен против такого рода атак.

Таким образом, данные атаки невозможно предотвратить на уровне сети. Обнаружить такие атаки можно лишь с помощью систем мониторинга реального времени. Поэтому решение данных проблем неоднозначно. Одним из методов является установка на серверы специального ПО, контролирующего количество соединений и сбрасывающего зависшие через определенные промежутки времени. Еще одно решение защиты основано на правильной настройке менеджера тайм-аутов.

Сервер Apache защищается от атак медленного чтения за счет установки расширения Mod_security [14]. Но и данное решение не обеспечивает полной защиты. Mod_Security – модуль Apache, добавляющий возможности обнаружения и предотвращения вторжения на Web сервер. Модуль подобен IDS системе, которую часто используют для анализа сетевого трафика, за исключением того, что Mod_security работает только на HTTP уровне. Существуют и другие программные средства для защиты серверов от такого рода атак.

Заключение

Использование комплекса не ограничивается данными примерами. Комплекс предоставляет широкий спектр по изучению конфигурации сетей и серверов, конфигурации и тестирования защищенных соединений, моделированию различного рода атак и разработке соответствующих мер защиты от них.

Литература

1. GNS3. The software that empowers network professionals // URL: https://www.gns3.com (д.о. 20.09.16).
2. Oracle VM VirtualBox // URL: https://www.virtualbox.org (д.о. 20.09.16).
3. Brocade Vyatta Network OS // URL: http://www.brocade.com/en/products-services/ software-networking/network-functions-virtualization -os.html (д.о. 20.09.16).
4. Wireshark – Go deep // URL: https: //www.wireshark.org (д.о. 20.09.16).
5. Ubuntu documentation. FTP-сервер // URL: https://help.ubuntu.com/lts/serverguide/ftp-server.html (д.о. 20.09.16).
6. Ubuntu documentation. Сертификаты // URL:https://help.ubuntu.com/lts/serverguide/certificates-and-security.html (д.о. 20.09.16).
7. Васин Н.Н. Технологии пакетной коммутации. Часть 1. Основы построения сетей пакетной коммутации. Самара: Изд-во ПГУТИ, 2015. – 238 с.
8. Васин Н.Н. Технологии пакетной коммутации. Часть 2. Маршрутизация и коммутация в сетях пакетной коммутации. Самара: Изд-во ПГУТИ, 2015. – 261 с.
9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2011. – 944 с.
10. Chappell L. Wireshark Network Analysis. Second Edition. Protocol Analysis Institute, dba // Chappell University, 2012. – 461 с.
11. Apache Web Server Project // URL: http://httpd.apache.org (д.о. 20.09.16).
12. Slowloris (computer security) – Wikipedia // URL: https://en.wikipedia.org/ wi-ki/Slowloris_ (computer_security) (д.о. 20.09.16).
13. Torshammer – a slow-rate DDOS attack tool // URL: http://blog.nexusguard.com/slow-rate-ddos (д.о. 20.09.16).
14. ModSecurity: Open Source Web Application Firewall // URL: http://modsecurity.org (д.о. 20.09.16).

Получено 29.12.2016

Васин Николай Николаевич, д.т.н., профессор, заведующий Кафедрой систем связи (СС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. 8-846-332-08-05; E-mail: vasin@psuti.ru

Ирбахтин Александр Алексеевич, студент ПГУТИ. Тел. 8-927-777-56-11; E-mail: irbahtinsanek@mail.ru

MODELING SECURE CHANNELS OF TELECOMMUNICATIONS USING VIRTUALIZATION

Vasin N.N., Irbakhtin A.A.
Povolzchskiy State University of Telecommunication and Informatics, Samara, Russian Federation
E-mail: vasin@psuti.ru

In modern world upgrade of protect of communications channels is essential. Modeling is one of the methods for learning new methods of attacks and new methods of protect. We solved this problem by using a hardware-software complex for modeling. Complex for modeling works by using virtualization. Complex includes virtualization system VirtualBox, network simulator GNS3, routers Cisco, switches Cisco, operation systems KaliLinux, operation systems Ubuntu, program Wireshark, and program routers on the operation system Vyatta. In this paper, we consider two examples of use of the complex for modeling. The first example describes the transfer of FTP-traffic on open and secure channels. The second example describes the modeling of the DOS-attack on the server. These examples describe some modeling techniques, used in the complex. We modeled the operations of networks, servers, applications and attacked them. The identified vulnerabilities are closed by means of protective measures.

Keywords: information security, telecommunications, modeling

DOI: 10.18469/ikt.2017.15.1.04

Vasin Nicolai Nicolaevich, Povolzhsky State University of Telecommunication and Informatics, 23 Lev Tolstoy str., Samara 443010, Russian Federation; the Head of Department of Communication Systems, Doctor of Technical Science, Professor. Tel. +78463320805. E-mail: vasin@psuti.ru

Irbakhtin Alexander Alekseevich, Povolzhsky State University of Telecommunication and Informatics, 23 Lev Tolstoy str., Samara 443010, Russian Federation; student. Tel. +79277775611. E-mail: irbahtinsanek@mail.ru

References

1. GNS3 The software that empowers network professionals. Available at: https://www.gns3.com (accessed 20.09.2016).
2. Oracle VM VirtualBox. Available at: https://www.virtualbox.org (accessed 20.09.2016).
3. Brocade Vyatta Network OS. Available at: http://www.brocade.com/en/products-services/software-networking/network-functions-virtualization/ network-os.html (accessed 20.09.2016).
4. Wireshark - Go deep. Available at: https://www.wireshark.org (accessed 20.09.2016).
5. Ubuntu documentation. FTP server. Available at: https://help.ubuntu.com/lts/serverguide/ftp-server.html (accessed 20.09.2016).
6. Ubuntu documentation. Certifications. Available at: https://help.ubuntu.com/lts/serverguide/ cer-tificates-and-security.html (accessed 20.09.2016).
7. Vasin N.N. *Tekhnologii paketnoy kommutatsii. Chast' 1. Osnovy postroyeniya setey paketnoy kommutatsii* [Technology packet switching. Part 1. Foundations of packet switched networks]. Samara, PSUTI publ., 2015. 238 p.
8. Vasin N.N. *Tekhnologii paketnoy kommutatsii. Chast' 2. Marshrutizatsiya i kommutatsiya v setyakh paketnoy kommutatsii* [Technology packet switching. Part 2. Routing and switching in networks packet switching]. Samara, PSUTI publ., 2015. 261 p.
9. Olifer V.G., Olifer N.A. *Komp'yuternyye seti. Printsipy, tekhnologii, protokoly* [Computer networks]. St.Peterburg, Piter publ., 2011. 944 p.

10. Chappell L. *Wireshark Network Analysis. Second Edition. Protocol Analysis Institute, dba.* Chappell University, 2012. 461 p.
11. Apache Web Server Project. Available at: http://httpd.apache.org (accessed 20.09.16).
12. Slowloris (computer security) – Wikipedia Available at: https://en.wikipedia.org/ wiki/Slowloris_ (computer_security) (accessed 20.09.16).
13. Torshammer – a slow-rate DDOS attack tool. Available at: http://blog.nexusguard.com/slow-rate-ddos (accessed 20.09.2016).
14. ModSecurity: Open Source Web Application Firewall. Available at: http://modsecurity.org (accessed 20.09.2016).

Received 29.12.2016

ТЕХНОЛОГИИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

УДК 004.7

WEB APPLICATION OF ESTIMATING PROTECTION SYSTEM EFFECTIVENESS OF THE ENTERPRISE

Bakhareva N.F., Fedorov S.V.
Povolzhskiy State University of Telecommunications and Informatics,
E-mail: fstepan2010@gmail.com

This article describes the WEB-application algorithm that allows to automate the audit of the company and to generate recommendations for the protection of the company in accordance with the requirements of the legislation. Moreover, it deals with the principle of the database formation. The authors describe the database according to the thematic issues of the information security for all the selected groups, private indicators and reference base, which is the master system of the protection. It is also represented the system of the group assessment, performance information security and the current reporting security of the enterprise. In the result, the authors give an algorithm of the visualization of the audit results. Using this application will reduce the resource and time which can be spent on the audit.

Ключевые слова: audit; algorithm; group metrics; private metrics; information security; information system; polar coordinates; Cartesian coordinates

Introduction

The initial step in the constructing comprehensive information protection system in the enterprise is the audit of the information security, which comprises the determination of the baseline level of the information system security.

Nowadays, the information security audit represents one of the most actual and dynamically developing directions of the strategic and operational management in the field of the company's information security. The relevance of the performing the audit is caused by the necessity to ensure information security in the organizations of various forms of ownership.

From the perspective of the audit work, there are three principle steps:

– collecting information and data, interviewing workers and the study of organizational, administrative and technical documentation;

– the analysis of data;

– the recommendations development to harmonize the safety requirements and reporting documents (report or conclusion on the results of the audit).

To automate the audit, to reduce resource and time expenses for it's conducting and visualization of the results together with Information System Technology (IST) a software in PHP language has been developed. The database was created on the basis of MYSQL. JavaScript and a technology for displaying Canvas material were used for visualization of results.

The purpose of the project

Create a WEB-application, which allows to automate the company's audit and to form the recommendations for the system protection of the company in accordance with the requirements of the legislation. The diagram of the WEB-application operation is shown in Picture 1.

The basic tasks of the application

1. To get information about the company, its functioning and security which is realized in the course of specially organized interviews with senior