Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.41.42

Поклонский
Сергей Анатольевич

Защита информации хранимой на веб-серверах от несанкционированного доступа

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты, информационная безопасность

Научный руководитель
Охрименко А. А.
кандидат технических наук, доцент

Минск 2018

ВВЕДЕНИЕ

В современных условиях из-за широкого распространения различных типов сетей стала очень часто встречаться организация аппаратной части сетевого оборудования в виде серверов – устройств, выделенных и/или специализированных для выполнения с их помощью сервисного программного обеспечения. Сервера служат для большого диапазона задач: начиная от маршрутизации-фильтрации данных, заканчивая хранением активных приложений. В большинстве случаев физически сервер находится удаленно, и совершать над ним какие-либо манипуляции крайне проблематично. Поэтому в большинстве серверов для решения данной проблемы используется протокол SSH (Secure SHell).

SSH является протоколом для удаленного безопасного входа и других сетевых сервисов в недостаточно надежно защищенной сети.

С каждым годом вопрос безопасности в сетях становиться все острее. Многие специалисты, хоть как-нибудь связанные с работой в сети, много слышали о различных угрозах, и если не знают твердо, то, по крайней мере, подозревают, какие последствия могут быть при получении злоумышленниками конфиденциальной информации. Часть специалистов нуждается в программном инструменте, который с одной стороны, было бы легко и удобно пользоваться, а с другой стороны этот инструмент был бы достаточно безопасным для работы с конфиденциальной информацией.

Мы поддерживаем мнение о необходимости увеличения ресурсов человечества в сфере информационных технологий путём реализации программного обеспечения с открытым исходным кодом, что даст возможность интернет-сообществу использовать его по своему усмотрению, добавлять новую функциональность, корректировать работу старой, вносить предложения по улучшению программного продукта и обращаться к его разработчику напрямую. На наш взгляд, это оптимизирует работу многих людей, занятых в сфере информационных технологий и позволяет улучшить отрасль в целом.

Таким образом, задача создать приложение, отвечающее вышеописанным требованиям, является актуальной задачей.

На данный момент не существует программного обеспечения совмещающего в себе возможности работы с протоколом SSH, обладающего свойством кроссплатформенности и при этом имеющего оконный графический интерфейс, обеспечивающий низкий порог вхождения, позволяющий пользователю с минимальным количеством специальных знаний возможность использовать программный продукт.

Данное программное средство будет спроектировано учитывая возможности расширения и будет предоставлять основные функции для обеспечения его жизнеспособности. В целях развития проекта, его программный код будет опубликован на хостинге с использованием GPL лицензии, вследствие чего получит свободное распространение.

Непосредственно соискателем было выполнено проектирование архитектуры программного средства; выбор, максимально удовлетворяющих условиям задачи, инструментов; организация репозитория с открытым доступом, и реализация минимально жизнеспособного продукта.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016-2020 гг., утверждённых Постановлением Совета Министров Республики Беларусь 12 марта 2015г., №190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Цели и задачи исследования

В настоящее время web-серверы весьма распространены и многообразны, многие бизнес-процессы основаны на их эксплуатации, а их безопасность и устойчивость напрямую влияет на доходы и репутацию компаний. Из-за возможности получения прибыли от хищения/модификации обрабатываемой веб-серверами информации они являются целью для множества злоумышленников. Целью настоящей работы является обеспечение информационной безопасности сервера компании LHIPSbel.

Для достижения поставленной цели в диссертации поставлены и решены следующие задачи:

– собрана и проанализирована информация об используемом компанией оборудования и программных средствах;

– собрана и проанализирована информация об наиболее вероятных уязвимых местах в аппаратной и программной среде компании, выявлены наиболее критичные угрозы;

– сформулирован и обоснован наиболее подходящий метод нейтрализации отобранных угроз – реализация программного средства;

– разработана функциональная и информационная модель предметной области для реализации ПС;

– спроектировано и реализовано ПС LHShell.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на следующих научно-технических конференциях:

– «Современные средства связи: XIX Международная научно-техническая конференция (16–18 сентября 2017 года, Минск, Республика Беларусь)» и 54-я научной конференции аспирантов, магистрантов и

студентов БГУИР по направлению: Информационные системы и технологии (4 мая 2017 года, Минск, Республика Беларусь).

– XXIII МНТК «Информационные системы и технологии» (ИСТ–2017), Нижний Новгород (2017 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р. Е. Алексеева, 2017, а также на постоянно действующем семинаре «Проблемы информатики, радиоэлектроники и защиты информации», том 3, заседание 22.09.2017. Под редакцией Г. В. Сечко / ООО «Стримцентр».

Опубликованность результатов диссертации

По результатам диссертации опубликованы 2 печатные работы - публикации [1А-2А].

Теоретическая и практическая значимость.

Теоретическая значимость работы заключается в теоретическом обосновании метода мониторинга уязвимостей с использованием существующей базы данных угроз, метод заключается в программном анализе уязвимостей выявленных существующим программным средством LHWebSecure (LWHS) и сопоставлении полученных результатов с базой данных Web Secure Standard (WSS) с выдачей предложений по повышению уровня защищённости. Практическая ценность заключается в разработке программного продукта обеспечивающего реализацию этого метода и предоставляющего пользовательский интерфейс.

Личный вклад магистранта в выполненную работу.

Работа полностью выполнена лично магистрантом на базе его исследований, проводимых на кафедре ЗИ БГУИР. Вклад научного руководителя А.А. Охрименко и научного консультанта Г.В. Сечко заключается в постановке задач исследования, определении возможных путей их решения и обсуждении полученных результатов. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в настоящей диссертационной работе результатов.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе «Общие сведения об используемом серверном оборудовании» представлено серверное оборудование компании. Также описаны используемые программные средства и дополнительное ПО, специфика которого накладывает определённые условия по выполнению работы. Продемонстрирована настройка сервера и его возможности. Дано подробное описание настройки протокола прикладного уровня ssh.

Во второй главе «Анализ информационной безопасности серверного оборудования по результатам эксплуатации» проведен анализ существующих аналогов программных средств, а также проведён отбор угроз информационной безопасности серверного оборудования по результатам эксплуатации. Даны определения используемой терминологии и представлены показатели уязвимости по метрике CVSS. На основе анализа отобранных угроз выбран наиболее действенный метод парирования – создание программного средства, реализующего собственный протокол прикладного уровня в рамках клиентского приложения с возможностью управления и найстроки.

В третьей главе «Моделирование предметной области программного средства» представлены модели наиболее сложных алгоритмов процесса реализации. Проведена разработка функциональной и информационной моделей, на основе которых, разработана спецификация требований. Представлен алгоритм работы программы.

В четвёртой главе «Техническое проектирование программного средства» проиллюстрирована организация данных, концептуальный прототип программного средства. Приведена физическая структура программы. Предоставляется описание основных модулей и методов работы ПС. Представлена диаграмма классов. Обоснован выбор средств разработки, в частности языка программирования Java, среды разработки ПО IntelliJ IDEA.

В пятой главе проведён анализ качества разработанного программного средства LHShell, дано описание процесса обнаружения и регистрации ошибок , представлены тестовые примеры и результаты их выполнения.

В процессе разработки диссертационной работы, помимо решения поставленной задачи путем создания программы, выполняющей требуемые действия, проведена работа по написанию сопутствующей технической документации. Техническая документация содержит описания реализации функций, совокупность диаграмм и схем, справочную информацию.

ВЫВОДЫ

В настоящей диссертации:

1) Выбрана предметная область анализируемых программных средств. В неё вошли клиентские приложения для работы с протоколом SSH.

2) Проанализированы многие возможные угрозы информационной безопасности персональных компьютеров. С точки зрения наибольшей значимости для информационной безопасности и одновременной наименьшей стоимости парирования угроз отобрана для последующей работы – угроза потери информации посредством атаки на уязвимость используемого компанией протокола ssh .

3) Определён наиболее действенный способ парирования выбранной угрозы.

4) Обоснован выбор и выбраны инструментальные средства для разработки программного средства. Ими выбраны язык программирования – Java, средство разработки – IntelliJ IDEA, сборщик проекта – Apache Maven.

5) Разработаны:

а) функциональная модель программного средства, включающая его контекстную диаграмму и декомпозицию контекстной диаграммы.

б) информационная модель программного средства, включающая его логическую схему данных.

в) алгоритмы функционирования программного средства – алгоритм авторизации и алгоритм работы модуля проверок.

6) проведено тестирование программного средства на ошибки.

В процессе эксплуатации программного средства происходит его модернизация. Программа обладает свойствами расширяемости, ведется работа по улучшению программного продукта.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1А. Поклонский, С. А. Исследование результатов тестирования информационной безопасности веб-сервера vCenter Server 5.5. / С. А. Поклонский, А. Н. Прузан // Информационные системы и технологии : 53-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» : материалы конференции по направлению 8 / редкол. : А. А. Охрименко, В. И. Пачинин, Г. В. Сечко. – Минск : БГУИР, 2017. – С. 71.Сборник статей VI межд. заоч. НТК. Ч.1 / Поволжский гос. ун-т сервиса/. – Тольятти: Изд-во: ПВГУС, 2016 (публикация).

2А. Постоянно действующий семинар «Проблемы информатики и защиты информации», Минск, 15.09.2016. Поклонский С. А., Шантур Е. А. Обзор угроз информационной безопасности веб-серверов и методов их парирования // Программирование и защита информации. Сборник трудов постоянно действующего семинара «Проблемы информатики и защиты информации», том 2, заседание 22.12.2015, доп заседание 15.09.2016. Под редакцией В.Л. Николаенко, А. А Охрименко, Г. В. Сечко / Институт информационных технологий Белорус. гос. ун-та информатики и радиоэлектроники: рукопись деп. в БелИСА 01.11.2016, № 201630. – 155 с. – С. 93–119.