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

УДК_____

Хмельницкий
Алексей Олегович

Мониторинг и оценка защищённости веб-сайтов в сети Интернет

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 "Методы и системы защиты информации, информационная безопасность”

_____

Научный руководитель

Пулко Татьяна Александровна

кандидат технических наук, доцент

_____

Минск 2016

ВВЕДЕНИЕ

Важнейшей проблемой, определяющей темпы и будущее развитие Интернета, становится информационная безопасность. Глубокое проникновение компьютерных технологий во все сферы человеческой деятельности и многочисленные проблемы в их защите требуют более широкого внедрения защищенных информационных технологий. Уже сегодня информационные технологии являются «нервной системой» каждого развитого государства, которая позволяет функционировать остальным его подсистемам. А ядром всей информационной инфраструктуры становится сеть Интернет.

В настоящее время сеть Интернет объединяет миллионы компьютеров во всем мире. В тоже время архитектурные недостатки сетевых протоколов и многочисленные уязвимости в программном обеспечении сетевых платформ обуславливают невысокую в целом защищенность сети Интернет. Особенно остро проблемы информационной безопасности проявились в последние годы. Участившиеся атаки с помощью «сетевых червей» охватывают с каждым годом все большие количество компьютеров во всем мире и наносят значительный урон. А сетевые атаки хакеров на корневые DNS-сервера сети Интернет продемонстрировали реальную возможность внесения сбоев в инфраструктуру Интернета.

Одним из важнейших этапов обеспечения информационной безопасности является идентификация потенциальных рисков. Большинство ИТ-специалистов знают, насколько может быть опасна уязвимость в ОС и в приложениях. И чрезвычайно важно найти эти уязвимости прежде, чем ими смогут воспользоваться недоброжелатели. Для этой цели и были созданы сканеры безопасности.

Специалисты по IT-безопасности используют в своей работе специализированное аппаратное или программное обеспечение, сканирующее сеть и ее устройства на предмет обнаружения слабых мест в системе безопасности. Это и есть сканеры уязвимости, или по-другому — безопасности, сети. Они проверяют используемые приложения, ищут уязвимости, которыми могли бы воспользоваться взломщики, и предупреждают администратора о зонах риска системы. Грамотно используя сканер уязвимости сети, специалист может значительно усилить сетевую безопасность.

Таким образом, можно сделать вывод, что вопросы обеспечения безопасности веб-сайтов сети Интернет, а также выбор средств для осуществления этой безопасности, сейчас являются наиболее актуальными в плоскости глобальной сети.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует пункту «Средства технической и криптографической защиты информации» раздела 7 «Информационно-коммуникационные и авиакосмические технологии»приоритетных направлений научно-технической деятельности Республики Беларусь на 2016 – 2020 гг., утверждённых Указом Президента Республики Беларусь 22 апреля 2015г., № 166. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы заключается в исследовании возможности применения систем мониторинга и оценки защищенности веб-сайтов в сети Интернет для обнаружения и предупреждения уязвимостей.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать проблему обеспечения информационной безопасности в сети Интернет.
2. Рассмотреть современные способы мониторинга и оценки защищенности веб-сайтов в сети Интернет.
3. Разработать комплекс для анализа защищенности хостов в сети Интернет.
4. Провести апробацию разработанного комплекса.

Апробация результатов диссертации

Основные полученные результаты диссертационной работы докладывались и обсуждались на международной научно-технической конференции «Информационные технологии и системы 2015 (ИТС 2015» (Минск, Республика Беларусь, 2015 г.) и XIII Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Республика Беларусь, 2014 г.).

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав, заключения и библиографического списка.

Полный объем диссертации составляет 75 страниц машинописного текста. Диссертация содержит 29 рисунков на 22 страницах. Библиографический список занимает 3 страниц и состоит из 30 наименования использованных источников и списка собственных публикаций соискателя из двух наименований на одной странице.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 работы, в том числе 1 статья в сборнике материалов конференций, 1 статья в научном журнале.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приводится оценка современного состояния информационной безопасности в сети Интернет и использования сканеров уязвимостей для обнаружения слабых мест в системе безопасности, формулируются решаемые в магистерской диссертации задачи.

В первой главе приводится классификация сетевых атак, результаты международного исследования уязвимостей веб-сайтов сети Интернет, сравнение методов тестирования, исследование о защищенности веб-сайтов белорусских банков, государственная политика в области обеспечения информационной безопасности, законодательная база РБ по информационной безопасности.

Выводы к первой главе:

1) Рассмотрение видов сетевых атак показало, что, несмотря на развитость сети Интернет, их видов существует огромное множество, тем самым создавая действительно большую угрозу информационной защищенности.

2) Изучение международного исследования уязвимостей веб-сайтов сети Интернет подтверждает, что большое количество веб-сайтов содержат те или иные уязвимости (в исследовании все 40 из 40 веб-сайтов).

3) Сравнение методов тестирование показало, что отсутствие у атакующего доступа к исходным кодам не делает веб-сайт более защищенными.

4) Исследование о защищенности веб-сайтов белорусских банков, проведенное компанией ActiveCloud также показало, что, несмотря на то, что все банки используют на своих сайтах защищенный протокол SSL, далеко не все из них используют полных набор возможностей этого протокола, что делает эти веб-сайты отчасти уязвимыми.

5) В ходе анализа проблематики было установлено, что проблема сетевой безопасности в настоящее время актуальна как никогда, что обосновывает и подтверждает правильность выбора темы научного исследования.

Во второй главе приводится оценка защищенности веб-сайтов сети Интернет, обзор сканеров защищенности веб-сайтов, международный опыт создания безопасных веб-сайтов, способы создания безопасных веб-сайтов, методы защиты серверной стороны хоста, методы обеспечения безопасности кода защищенного хоста.

Выводы ко второй главе:

1) Рассмотрение способов оценки защищенности веб-сайтов показало, что сегодня имеется большое количество материалов, посвященных проведению анализа защищенности веб-сайтов.

2) Обзор сканеров защищенности веб-сайтов показал, что в настоящее время существует много разных решений по сканерам защищенности от ведущих IT компаний.

3) Исследование международного опыта создания безопасных веб-сайтов показал, что атаки злоумышленников постоянно эволюционируют и как следствие требуются новые методы защиты от них. Чтобы поддерживать актуальный уровень защищенности, существуют специальные проекты, посвященные безопасности веб-сайтов.

4) Анализ методов проектирование, создание и использование безопасных веб-сайтов показало, что только организация защиты на всех уровнях работы веб-сайтов (ОС, HTTP-сервер, серверный модуль Apache, MySQL сервер и т.д.), а также использование последних и актуальный версий ПО и соблюдения требования безопасности в разработанном коде могут позволить считать веб-сайт наиболее защищенным.

В третьей главеприводится техническое задание к разрабатываемую комплексу для анализа защищенности хостов в сети Интернет, архитектура моделируемого комплекса, анализ средств разработки и моделирование комплекса.

Выводы к третьей главе:

1) В ходе проектирования архитектуры моделируемого комплекса были выделены следующие модули: модуль сетевого сканирования, модуль дополнительного сканирования, модуль анализа результатов сканирования, хранилище уязвимостей, модуль первичного анализа, модуль поддержки принятия решений.

2) При анализе средств разработки были определены следующие компоненты разработки: Apache 2.3, PHP 5.6, PEAR, MySQL 5.3, Memcached.

3) Были смоделированы и разработаны следующие модули: ядро сканера, модуль сетевого сканирования, модуль дополнительного сканирования, модуль анализа результатов сканирования, модуль первичного анализа, модуль поддержки принятия решения.

В четвертой главепроисходит апробация работы комплекса для анализа защищённости хостов в сети интернет.

Выводы к четвертой главе:

1) Оценка уровня защищенности хоста Itransition.by показала, что был найден всего один потенциально подозрительный файл, что можно расценивать как высокий уровень защищенности.

2) В ходе апробации разработанного комплекса, была доказана его эффективность при оценке уровня защищенности хоста в сети Интернет.

В заключении приводятся основные результаты, полученные в ходе выполненных исследований.

ЗАКЛЮЧЕНИЕ

Целью данной работыбыло найти, обозначить и обобщить методы мониторинга и оценки защищенности веб-сайтов в сети Интернет, а также смоделировать свой комплекс для эффективной оценки защищенности хостов.

В ходе исследовательской деятельности была рассмотрена классификация современных сетевых атак в сети Интернет как таковых, изучен опыт международного исследования уязвимостей веб-сайтов сети Интернет, изучен опыт исследования о защищенности веб-сайтов белорусских банков, былпроведен обзор государственной политики в области обеспечения информационной безопасности ирассмотрена законодательная база РБ по информационной безопасности. Все это позволило четче обозначить проблему и понять пути движения к ее решению.

Для выявления путей решения обозначенной проблемы были рассмотрены способы оценки защищенности веб-сайтов в сети Интернет в настоящее время,был произведен обзор существующих сканеров защищенности хостов,изучен международный опыт создания безопасных веб-сайтов,были рассмотрены способы проектирования, создания и использования безопасных веб-сайтов, изучены методы защиты серверной стороны хоста и методы обеспечения безопасности кода защищенного хоста. Таким образом были выявлены современные способы мониторинга и оценки защищенности веб-сайтов в сети Интернет.

В рамках работы по созданию собственного комплекса для анализа защищенности хостов было сформировано техническое задание, разработана архитектура моделируемого комплекса, произведен анализ средств разработки и смоделирована модель разрабатываемого комплекса.

На завершающем этапе была проведена апробация разработанного комплекса для анализа защищённости хостов в сети Интернет, что позволило оценить его работоспособность на примере реального хоста. В итоге, в ходе апробации разработанного комплекса, была доказанаего эффективность при оценке уровня защищенности хоста в сети Интернет.

Предложенный в данной магистерской диссертации комплекс для анализа защищенности хостов в сети Интернет может быть использован при построении системы защиты информации любых предприятий, требованием для которых является обеспечение мониторинга и контроляуязвимостей работы веб-сайтов.

СПИСОК ОПУБЛИКОВАННЫХРАБОТ

1-А. А.О. Хмельницкий, О.В. Бобков, Т.А. Пулко, “Защита динамических веб-сайтов с помощью продукции компании CheckPoint на примере межсетевого экрана CheckPoint R77”, XIII Белорусско-российской научно–технической конференции, с.50, г.Минск, БГУИР 4–5 июня 2015 г.

2-А. О.В. Бобков, А.О. Хмельницкий, Т.А. Пулко, “Использование системы управления конфигурациями Ansible как инструмента для управления несколькими WEB-серверами”, с. 26 – 27, Международная научная конференция «Информационные технологии и системы 2015 (ИТС 2015)», БГУИР, Минск, Беларусь, 28 октября 2015 г.