УДК 004.02

А. Г. ТЕЦКИЙ, Д. Д. УЗУН

Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Украина

ИССЛЕДОВАНИЕ АТАКИ НА ПРОНИКНОВЕНИЕ НА СИСТЕМУ УПРАВЛЕНИЯ КОНТЕНТОМ С ПОМОЩЬЮ МАРКОВСКОЙ МОДЕЛИ

В статье рассмотрены варианты атаки на веб-ресурс, развернутый с использованием системы управления контентом. Описан типовой набор серверного программного обеспечения. Разработана марковская модель, учитывающая возможность уменьшения количества уязвимостей в системе. Модель включает в себя возможность использования методов атаки с помощью социальной инженерии и атаки на уязвимости. Целью атаки является получение доступа в панель администратора системы управления контентом. Предложен выбор характеристик модели для проведения моделирования.

Ключевые слова: *уязвимость, безопасность, атака на проникновение, марковская модель, система управления контентом.*

Введение

С развитием информационных технологий стремительно растет количество сайтов в сети Интернет. В настоящее время для создания сайта не нужно владеть языками программирования, достаточно лишь установить на хостинг наиболее подходящую по функционалу систему управления контентом (англ. CMS - Content Management System). Исследование безопасности таких систем представляет особый интерес, поскольку многие системы управления контентом имеют открытый исходный код и имеют модульную архитектуру, которая позволяет расширять функциональность сайта с помощью установки дополнительных компонентов (модулей, плагинов). Уязвимости могут быть найдены как в ядре CMS, так и в ее компонентах. Уязвимость в ядре какой-либо версии продукта ставит под угрозу все инсталляции данной версии и, зачастую, версии, которые были выпущены ранее. Помимо этого, источником уязвимостей может быть и другое ПО, обеспечивающее функционирования сайта. На рисунке 1 показан набор программного обеспечения LAMP, наиболее часто применяемый при создании Web-ресурсов.

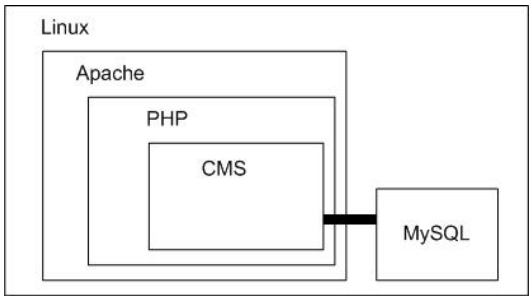

Рис. 1. Набор серверного программного обеспечения

Как правило, разработчики ликвидируют найденные уязвимости в последующих версиях продуктов или выпускают патчи для критических уязвимостей. Однако, далеко не каждый владелец сайта беспокоится об информационной безопасности своего электронного ресурса и не следит за своевременным обновлением используемой системы управления контентом. Широкое использование устаревших версий CMS позволяет производить массовые атаки на уязвимые сайты с помощью специально разработанных ботов [1].

Цель статьи – исследовать методы атаки проникновение на веб-приложение, разработать модель с учетом данных методов для последующего моделирования и расчета вероятности успешной атаки. Под успешной атакой понимается получение доступа к панели управления сайтом.

1. Обзор методов атаки

Практически все платформы для создания сайтов имеют панель администратора, через которую происходит управление ресурсом.

Существуют различные варианты для проведения атаки, ниже перечислены наиболее распространенные.

1. Атакующий знает логин и пароль администратора.

Узнать его можно разными способами – подсмотреть при авторизации, перехватить HTTP-пакет с авторизационными данными, заразить компьютер администратора соответствующим ПО, которое запомнит данные авторизации и отправит их атакующему. Это лишь несколько вариантов, не связанных с уязвимостями в исследуемой системе.

2. Атакующий знает логин администратора, пароль подбирается методом перебора по словарю.

Чем больше размер словаря, тем больше шансов на нахождение используемого пароля. Данный метод атаки эффективен при «слабых» паролях.

3. Использование уязвимости Local File Inclusion.

Ключевым моментом является получение содержимого конфигурационного файла, который содержит некоторые настройки, в том числе данные для подключения к базе данных. Атакующий подключается к БД и вручную добавляет нового администратора в таблицу пользователей. Остается только авторизоваться в панели управления сайтом под вновь добавленным пользователем.

4. Использование уязвимости SQL-injection.

В данном случае необходимо получить хэш пароля администратора из таблицы пользователей, после этого подобрать пароль по известному хэшу.

2. Создание модели

Для исследования влияния атаки на систему можно применять различные математические аппараты [2]. Так как вероятность любого состояния системы в будущем зависит только от её текущего состояния и не зависит от того, каким образом система пришла в это состояние, то процесс атаки можно считать марковским. В данном случае, уместным будет использование марковской цепи, поскольку атака рассматривается как некоторая система, состояния которой принадлежат некоторому дискретному множеству $Y=\{x_1, x_2, \ldots, x_n\}$, а переходы между состояниями происходят в моменты времени $t_0, t_1, ..., t_n$. Также рассматривалась возможность использования непрерывных цепей Маркова, однако неизвестно, будет ли время подвергаться экспоненциальному закону распределения [3].

Создаваемая модель содержит четыре непересекающихся между собой варианта атаки на систему управления контентом.

Изображенная на рисунке 2 модель имеет следующие состояния:

S_0 – начальное состояние системы. Переход в состояние S_i характеризуется выпуском патча, что влечет за собой уменьшение количества уязвимостей в системе. Допущением данной системы является то, что выпуск патча не добавляет новые уязвимости, а только уменьшает количество известных;

S_k – состояние системы, в котором выпущены патчи для всех обнаруженных уязвимостей;

$S_{a1} \ldots S_{an}$ – последовательность состояний, направленных на получение логина и пароля без эксплуатации уязвимостей;

$S_{b1} \ldots S_{bm}$ – последовательность состояний, направленных на получение пароля методом перебора;

$S_{c1} \ldots S_{cl}$ – последовательность состояний, направленных на получение логина и пароля с использованием уязвимости Local File Inclusion;

$S_{d1} \ldots S_{dp}$ – последовательность состояний, направленных на получение логина и пароля с использованием уязвимости SQL-injection;

S_z – система успешно атакована.

Переход из состояния S_z в S_0 фактически означает восстановление работоспособного состояния без выпуска патча. На практике это происходит после смены пароля администратора либо удаления администратора, который был добавлен атакующим в процессе атаки. Во избежание повторной атаки по уже известному сценарию, необходимо определить, каким именно путем был достигнут успешный исход атаки и принять соответствующие меры.

Для определения вероятностей пребывания системы в каждом из состояний необходимо составить уравнение для каждого состояния и решить полученную систему линейных алгебраических уравнений, выбрав соответствующие параметры модели λ и добавив условие нормировки.

$$S_0: \lambda'_0 P_0 + \lambda_{0a1} P_{a1} + \lambda_{0b1} P_{b1} + \\ + \lambda_{0c1} P_{c1} + \lambda_{0d1} P_{d1} + \lambda_0 P_l = 0, \quad (1)$$

$$S_k: \lambda'_k P_k + \lambda_{ka1} P_{a1} + \lambda_{kb1} P_{b1} + \\ + \lambda_{kc1} P_{c1} + \lambda_{kd1} P_{d1} = 0, \quad (2)$$

$$S_{a1}: \lambda'_{a1} P_{a1} + \lambda_{a1} P_{a2} = 0, \quad (3)$$

$$S_{an}: \lambda'_{an} P_{an} + \lambda_{an} P_z = 0, \quad (4)$$

$$S_{b1}: \lambda'_{b1} P_{b1} + \lambda_{b1} P_{b2} = 0, \quad (5)$$

$$S_{bm}: \lambda'_{bm} P_{bm} + \lambda_{bm} P_z = 0, \quad (6)$$

$$S_{c1}: \lambda'_{c1} P_{c1} + \lambda_{c1} P_{c2} = 0, \quad (7)$$

$$S_{cl}: \lambda'_{cl} P_{cl} + \lambda_{cl} P_z = 0, \quad (8)$$

$$S_{d1}: \lambda'_{d1} P_{d1} + \lambda_{d1} P_{d2} = 0, \quad (9)$$

$$S_{dp}: \lambda'_{dp} P_{dp} + \lambda_{dp} P_z = 0, \quad (10)$$

$$S_z: \lambda'_z P_z + \sum_{i=0}^{k} \lambda_{zi} P_i = 0. \quad (11)$$

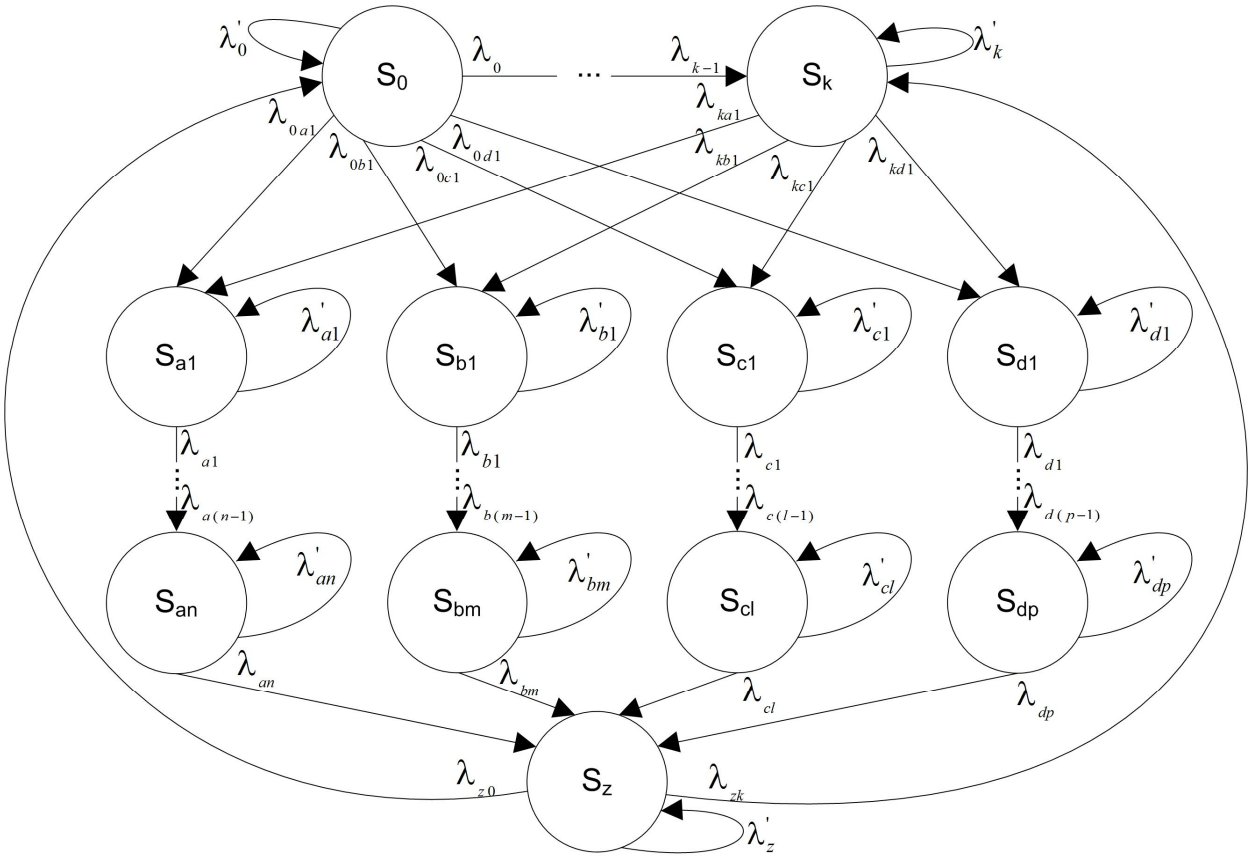

Рис. 2. Граф состояний при атаке на систему управления контентом

Заключение

Разработанная модель позволяет определить вероятность успешной атаки системы при использовании четырех различных методов атаки с целью получения доступа к панели управления сайтом. Отличием является то, что модель включает в себя методы атаки, как связанные с уязвимостями атакуемой системы, так и не связанные с ними. Учтена возможность выпуска патчей, которые не будут добавлять новые уязвимости.

К дальнейшим исследованиям можно отнести детализацию модели и проведение моделирования. При моделировании могут быть использованы статистические данные из источников [4-5]. Стоит понимать, что точной статистики взломов сайтов никто предоставить не сможет и используемые количественные значения являются лишь ориентировочными. Для методов атаки, использующих уязвимости в атакуемой системе управления контентом, статистические данные могут быть представлены достаточно точно; вероятности успешной атаки для методов, использующих социальную инженерию, должны варьироваться, поскольку они зависят от персонала, имеющего доступ к панели администратора.

Литература

1. Статистика: Компании по всему миру подвергаются вирусным атакам каждые три минуты [Электронный ресурс]. – Режим доступа к статье: http://www.securitylab.ru/news/439232.php. – 15.02.2016.

2. Майстренко, В. А. Безопасность информационных систем и технологий [Текст] / В. А. Майстренко, В. Г. Шахов. – Омск : Изд-во ОмГТУ, 2006. – 232 с.

3. Алексеев, О. Г. Марковские модели боя [Текст] / О. Г. Алексеев, В. Г. Анисимов, Е. Г. Анисимов. – М. : Министерство обороны СССР, 1985. – 85 с.

4. Статистика уязвимостей веб-приложений (2014 г.) [Электронный ресурс]. – Режим доступа к статье: http://www.ptsecurity.ru/download/WEB_APP_VULNERABILITY_2014.A4.RUS.242465.14.OCT.2015.pdf. – 15.02.2016.

5. Когда взломают ваш блог? или Немного статистики о взломах WordPress [Электронный ресурс]. – Режим доступа к статье: http://web-koshka.ru/wordpress/bezopasnost/stat-security.html. – 15.02.2016.

References

1. *Statistika: Kompanii po vsemu miru podvergayutsya virusnym atakam kazhdye tri minuty* [Statistics: Companies around the world are exposed to virus attacks every three minutes]. Available at: http://www.securitylab.ru/news/439232.php (Accessed 15.02.2016).

2. Maistrenko, V. A., Shakhov, V. G. *Bezopasnost' informatsionnykh sistem i tekhnologii* [Security of information systems and technologies]. Omsk, OmGTU. Publ. 2006. 232 p.

3. Alekseev, O. G., Anisimov, V. G., Anisimov, E. G. *Markovskie modeli boya* [Markov models of battle]. Moskow, Ministerstvo oborony SSSR Publ. 1985. 85 p.

4. *Statistika uyazvimostei veb-prilozhenii (2014 g.)* [Statistics of web application vulnerabilities (2014)]. Available at: http://www.ptsecurity.ru/download/WEB_APP_VULNERABILITY_2014.A4.RUS.242465.14.OCT.2015.pdf (accessed 15.02.2016).

5. *Kogda vzlomayut vash blog? ili Nemnogo statistiki o vzlomakh WordPress* [When your blog will be hacked? Or a few statistics about WordPress hacking]. Available at: http://web-koshka.ru/wordpress/bezopasnost/stat-security.html (accessed 15.02.2016).

Поступила в редакцию 15.02.2016, рассмотрена на редколлегии 14.04.2016

ДОСЛІДЖЕННЯ АТАКИ НА ПРОНИКНЕННЯ НА СИСТЕМУ УПРАВЛІННЯ КОНТЕНТОМ ЗА ДОПОМОГОЮ МАРКОВСЬКОЇ МОДЕЛІ

А. Г. Тецький, Д. Д. Узун

У статті розглянуті варіанти атаки на веб-ресурс, розгорнутий з використанням системи управління контентом. Описано типовий набір серверного програмного забезпечення. Розроблено марківську модель, що враховує можливість зменшення кількості вразливостей в системі. Модель включає в себе можливість використання методів атаки за допомогою соціальної інженерії та атаки на уразливості. Метою атаки є отримання доступу в панель адміністратора системи управління контентом. Запропоновано вибір характеристик моделі для проведення моделювання.

Ключові слова: вразливість, безпека, атака, марківська модель, система управління контентом.

RESEARCH OF PENETRATION ATTACK ON CONTENT MANAGEMENT SYSTEM USING MARKOV'S MODEL

A. G. Tetskyi, D. D. Uzun

The article describes the variants for an attack on a web resource deployed by using a content management system. The typical server software is described. The Markov model, which includes the possibility of reducing the number of vulnerabilities in the system, is developed. The model includes possibility to use methods of attack via social engineering and vulnerabilities. The aim of the attack is to gain access to the control panel of content management system. A choice of characteristics for simulation is proposed.

Key words: vulnerability, security, attack, Markov model, content management system.

Тецкий Артём Григорьевич – ассистент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: a.tetskiy@csn.khai.edu.

Узун Дмитрий Дмитриевич – канд. техн. наук, доцент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н. Е. Жуковского «ХАИ», Харьков, Украина, e-mail: d.uzun@csn.khai.edu.

Tetskyi Artem Grygorovych – Assistant Lecturer of Dept. of Computer Systems and Networks , National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine, e-mail: a.tetskiy@csn.khai.edu.

Uzun Dmytro Dmytrovych – Candidate of Technical Science, Assistant Professor of Dept. of Computer Systems and Networks , National Aerospace University named after N. Ye. Zhukovsky "KhAI", Kharkov, Ukraine, e-mail: d.uzun@csn.khai.edu.