УДК 004.00

СРАВНЕНИЕ ЭФФЕКТИВНОСТИ МЕТОДОВ АВТОМАТИЗИРОВАННОГО КОНФИГУРИРОВАНИЯ БЕЗОПАСНОСТИ ВЕБ-СЕРВЕРА

Огурень Д.Ю. (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»)
Научный руководитель – кандидат технических наук, доцент факультета БИТ Менщиков А. А. (квалификационная категория "ординарный доцент")
(Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»)

Аннотация.

Данный доклад посвящен обзору и сравнению эффективности методов автоматизированной настройки и проверки безопасности веб-сервера. По итогу анализа существующих методов и их возможностей сформированы предложения по реализации нового метода, который будет наиболее эффективным.

Введение.

В ходе научного исследования была поставлена научная проблема: как автоматически проверить и исправить конфигурацию безопасности веб-сервера.

На данный момент существует большое количество рекомендаций по конфигурации безопасности веб-сервера вручную. Однако данный процесс требует много времени администратора и подвержен появлению ошибок вследствие человеческого фактора. Поэтому автоматизированные методы во многих областях науки считаются наиболее эффективными. Так, одним из самых эффективных способов безопасной конфигурации веб-сервера остается метод автоматизации данного процесса.

Основная часть.

Существует небольшое количество автоматизированных решений для настройки веб-серверов. При этом большинство решений либо слишком сложны, либо имеют существенные недостатки.

Среди лицензионных решений доступно корпоративное решение Lynis. Однако в нем много других функций, которые не требуются для настройки веб-сервера. В Lynis представлены такие функции как аудит безопасности, управление уязвимостями, обширная поддержка операционных систем Unix, macOS и многое другое. Еще одним его недостатком является то, что оно коммерческое и требует покупки лицензии.

Среди решений с открытым исходным кодом доступны решения JShielder и Ubuntu hardening. Оба решения не перезаписывают существующие конфигурации и не используют последние версии системы. При этом решение Ubuntu hardening solution включает в себя небольшой диапазон конфигураций по сравнению с решением JShielder.

Был найден усовершенствованный метод – функциональный скрипт автоматической конфигурации веб-сервера, который по сравнению с существующими решениями включает в себя: резервное копирование конфигурации; использование последних версий сервисов; перезапись существующих конфигураций с открытым исходным кодом, с требуемой сложностью и диапазоном конфигураций для основных потребностей. Однако недостатком данного метода является то, что данный скрипт покрывает не все возможные уязвимости, так как каждая система имеет свои особенности. Более того, заранее собранные конфигурации

уже прописаны в скрипте, что не дает возможности их автоматического обновления и приводит к уязвимостям при установке неактуальных конфигураций.

Следующий рассмотренный метод конфигурации веб-сервера – метод, в основе которого лежит эволюционный алгоритм. Такой метод может сгенерировать большое количество конфигураций за разумное количество времени. В данном алгоритме конфигурации представлены в виде хромосом, и алгоритм проводит эти хромосомы через ряд процессов отбора, скрещивания и мутации, которые должны приводить к еще более безопасным конфигурациям, чем предыдущее поколение. Однако существует большая вероятность выхода ошибочных результатов вследствие сложности и недостаточности показателей корректной мутации конфигураций.

Другой рассмотренный метод - инструмент PracExtractor не обеспечивает полную автоматизацию конфигурации безопасности веб-сервера, но при этом выполняет такую важную функцию как создание спецификаций на основе большого количества рекомендаций официальной документации. Инструмент PracExtractor может извлечь 338 рекомендаций и сгенерировать 173 спецификации с разумной точностью из двенадцати больших руководств по программному обеспечению. Помимо обнаружения проблем конфигурации системных администраторов, PracExtractor также может помочь обнаружить неправильные настройки параметров конфигурации по умолчанию.

Выводы.

Таким образом, было проведено сравнение существующих решений по автоматизации конфигурирования безопасности веб-сервера. На данный момент не выявлено лидирующего по эффективности метода. Все рассмотренные методы имеют свои недостатки, что делает поставленную научную проблему крайне актуальной. В дальнейшем запланировано проведение экспериментов в лабораторных условиях, как с найденными научными результатами работ, так и с коммерческими продуктами. Такой эксперимент позволит разработать новый метод автоматизированной настройки безопасности веб-сервера, который будет включать наработки существующих методов и состоять из двух этапов: первый – автоматический анализ существующих и обновленных конфигураций сервера, создание на их базе спецификаций; второй – создание по спецификациям исполняемого скрипта для установки конфигураций, выбранных администратором с учетом всех особенностей системы.

Огурень Д.Ю. (автор) Подпись

Менщиков А.А. (научный руководитель) Подпись