КОНЦЕПЦИЯ ПОСТРОЕНИЯ МОДУЛЯ ЗАЩИТЫ WEB-ПРИЛОЖЕНИЯ НА ОСНОВЕ ИМИТАЦИИ И АНАЛИЗА СЕТЕВЫХ АТАК

Д.Н. Одинец, В.Л. Кулеш, Е.А. Алуев

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В настоящее время все большее число организаций обращают внимание на повышение надежности и безопасности своих web-приложений. Особенно это актуально для банковских компаний, имидж, а соответственно, и успешность работы которых, в первую очередь зависят от надежности и безопасности их web-приложений. Учитывая изложенное выше, разработка программного модуля защиты web-приложения на основе имитации и анализа сетевых атак сегодня является очень актуальной задачей.

Использование автоматизированного поиска уязвимостей web-ресурсов при помощи учета специфики исследуемых программ позволит предотвращать возможные атаки злоумышленников путем выявления, анализа и устранения уязвимостей web-приложения заблаговременно.

Предложена концепция обнаружения и защиты web-приложения от сетевых атак злоумышленников, на основе которой разработан кроссплатформенный программный модуль. Данный модуль работает на основе имитации сетевых атак и их анализе. Основное отличие созданного модуля от основных известных вариантов сетевых атак – поиск уязвимостей web-приложения в автоматизированном режиме.

Разрабатываемый программный модуль защиты web-приложения позволил выявлять следующие основные варианты уязвимости web-приложения:

– обнаружение, анализ и блокирование SQL-инъекций;

– обнаружение, анализ и блокирование возможности осуществления некорректной авторизации и управления сеансами;

– обнаружение, анализ и блокирование возможности межсайтового выполнения сценариев;

– обнаружение, анализ и блокирование возможности отказа в обслуживании.

Основу концепции составляют следующие алгоритмы:

– алгоритм сбора информации о целевом web-приложении;

– алгоритм сканирования приложения;

– алгоритм анализа результатов;

Такой подход дает возможность создать гибкую структуру программного модуля, что позволяет в дальнейшем модифицировать продукт путем добавления новые блоков и изменения старых без существенных вмешательств в общею схему работы всей взаимосвязанной системы.

В результате исследований получены записи логов для документирования фактов атак в виде списка и сохранения этой информации в файл. Каждая запись в этом списке является кортежем, содержащий тип атаки и временную метку атаки. Визуально это выглядит как [('DDoS', '2024-04-23 15:30:45'), ('SQL Injection', '2024-04-23 15:32:18'), ('Phishing', '2024-04-23 15:35:02')].