ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

САХНО Виталий Викторович
магистрант
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

В современном мире вопросы безопасности информационных систем, хранящих информационные ресурсы, приобретают важное значение. Вместе с тем и текущие задачи аудита информационной безопасности компаний, часто, ограничиваются проверкой их на соответствие требованиям по информационной безопасности. Но при таком подходе к аудиту безопасности, остается неясным устойчивость систем защиты объектов к реальным атакам. Для проверки данной устойчивости на атаки, объекты подвергаются процедуре тестирования, а именно – тестированию на проникновение.
Ключевые слова: тестирование, аудит, информационная безопасность, атака, требования.

Тестирование на проникновение представляет собой одну из методик нахождения уязвимых областей системы для вторжения и нарушению целостности, достоверности и конфиденциальности со стороны злоумышленников. Процесс тестирования проникновения заключается в целенаправленной санкционированной атаки на систему или ее компонент, способные обнаружить ее слабые места и пробелы в строении защиты информации от сторонних проникновений.

Тестирование на проникновение еще может быть применена в качестве дополнения к другим методам проверки для оценки эффективности защиты информации от различных типов атак. Таким образом, тестирование на проникновение – это проверка в реальном времени, которая может проводиться как вручную, так и с использованием инструментов автоматизации; в результате чего, система и ее компоненты подвергаются воздействию контролируемых и злонамеренных атак для выявления уязвимостей в системе защиты информации [1].

Также одной из методик тестирование на проникновение является анализ конфигурации. В любом компоненте информационной системы будь то операционная система или СУБД содержится много настроек, которые и определяют уровень защищенности системы. Правильно выбранные настройки можно найти в документации ГОСТах или в статьях экспертов, делящихся своим опытом [2].

Анализ конфигурации может проводиться вручную и с использованием автоматизированных средств, но и в том, и в том случаи подразумевается нахождение административного доступа к проверяемой системе. Данная методика представляет собой самый безопасный вариант анализа защиты информации, но и также самый долгий.

Для создания комплексного подхода тестирования защиты информации целесообразно брать какую-либо последовательность действий от лица злоумышленников и разнообразить это применением эффективного инструментария, которые не могут позволить себе настоящие хакеры.

Комплексный процесс тестирования защиты информации можно разделить на следующие этапы, сравнимы с реальным нападением злоумышленника [3]:

1) поиск цели;
2) поиск уязвимости;
3) проверка и использования уязвимости;
4) расширение привилегий.

Первый этап. Данного этапа может и не быть в проекте по тестированию защиты информации, потому что список целей мы получаем от заказчика.

На данном шаге необходимо изучить следующие цели:

– сайты, связанные с заказчиком, а именно: адреса электронной почты, структуру организации и т. п.;

– сайты вакансий: в описаниях вакансий иногда встречается описание используемых технологии;

– сайты поставщиков ИТ-услуг.

Второй этап. После выявления целей, переходим к поиску уязвимостей. Мы делаем это с помощью сканеров уязвимостей (OWASP Zar, W9scan, Wapiti и т. п.), но также используем и ручной поиск уязвимостей [4]. Заключающим действием на данном этапе получается список потенциальных уязвимостей, который еще предстоит проверить на проникновение.

Третий этап. После того как мы составили список потенциальных уязвимостей, мы проверяем их на возможность использования в своих целях. Существует множество уязвимостей, которые могут быть выявлены только в случаи их использования: SQL-инъекции или XSS, слабый пароль [5]. На данном шаге мы с вами:

– используем эксплойты;
– перехватываем трафик (ARP-poisoning);
– подбираем пароли;
– проверяем на возможность SQL-инъекции/XSS.

В результате данного этапа мы выявили, какие из обнаруженных нами ранее уязвимостей «работоспособны»

Четвертый этап. После получение доступа к какой-либо системе, мы пытаемся понять, к чему получили доступ и можно ли его увеличить в рамках одной.

Таким образом, ранее рассмотренный подход позволяет обнаруживать максимальное количество реальных уязвимостей в системе защиты информации, с помощью инструментов, находящихся в открытом доступе.

СПИСОК ЛИТЕРАТУРЫ

1. *Галимова Е.Ю., Коваленко А.Н.* Метод выбора между ручным и автоматизированным тестированием, основанный на свойствах программного продукта. Вестник Донского государственного технического университета. 2016. – № 16(4). – С. 134-139. – URL: https://doi.org/10.12737/22160.
2. *Макаренко С.И.* Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. – 2018. – № 1. – С. 1-29. DOI: 10.24411/2410-9916-2018-10101.
3. Тесты на проникновение // Positive Technologies. 2018. – URL: https://www.ptsecurity.com/ru-ru/services/pentest/ (дата обращения: 08.02.2021).
4. Чем искать уязвимости веб-приложений: сравниваем восемь популярных сканеров // Positive Technologies. 2018. – URL: https://habr.com/ru/company/tomhunter/blog/456892/ (дата обращения: 08.02.2021).
5. *Щеглов А.В., Храмов В.Ю.* Способ разработки тестовых удаленных информационно-технических воздействий на пространственно-распределенные системы информационно-технических средств // Сборник студенческих научных работ факультета компьютерных наук ВГУ ФГБОУ ВО «Воронежский государственный университет». – Воронеж, 2016. – С. 203-210.

PENETRATION TESTING

SAKHNO Vitaly Viktorovich
undergraduate
Don State Technical University
Rostov-on-Don, Russia

In the modern world, the issues of security of information systems storing information resources are becoming important. At the same time, the current tasks of the audit of information security of companies are often limited to checking them for compliance with information security requirements. But with this approach to security auditing, it remains unclear the resistance of object protection systems to real attacks. To check this resistance to attacks, objects are subjected to a testing procedure, namely, penetration testing.
Key words: testing, audit, information security, attack, requirements.