УДК 0.004 **Информационные технологии**

Дьяченко Никита Владимирович, *магистрант*
Донского государственного технического университета

РОЛЬ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В современном взаимосвязанном цифровом пространстве, где угрозы кибербезопасности продолжают усложняться, защита конфиденциальных данных и обеспечение целостности информационных систем стали главным приоритетом для организаций по всему миру. Среди арсенала методов кибербезопасности тестирование на проникновение выделяется как важнейший метод выявления уязвимостей и повышения общей безопасности. В этой статье рассматривается роль тестирования на проникновение, подчеркивается его значение для упреждающего выявления слабых мест и усиления защиты от киберугроз.

Ключевые слова: киберугроза, тестирование, защита конфиденциальных данных, целостность информационных систем.

Annotation: In a modern interconnected digital space, where the threats of cybersecurity continue to become more complicated, protecting confidential data and ensuring the integrity of information systems of became the main priority for organizations around the world. Among the arsenal of cybersecurity methods, testing for penetration is distinguished as the most important method for identifying vulnerabilities and increasing overall security. This article discusses the role of testing on penetration, emphasizes its significance for the proactive identification of weaknesses and increasing protection against cyberosis.

Keywords: cyberosis, testing, protection of confidential data, integrity of information systems.

Введение

Тестирование на проникновение — это белый взлом компьютерной системы руками опытного хакера по официальному договору, с официальным отчетом на выходе.

В результате тестирования на проникновение исполнитель работ раскрывает все выявленные уязвимости, а также дает рекомендации по их устранению. Результаты отражаются в отчете проведения тестирования на проникновение.

Отчет проведения тестирования на проникновение содержит информацию о всех обнаруженных уязвимостях, а также о способах их эксплуатации. В отчете также приводятся рекомендации по устранению обнаруженных проблем и повышению безопасности системы.

Важными составляющими отчета являются:

1. Введение: краткое описание цели и характеристик тестирования на проникновение.

2. Методология: описание используемых методов и техник при проведении тестирования.

3. Результаты тестирования:

- Общий обзор системы: предоставляется информация о структуре и основных компонентах системы.

- Обнаруженные уязвимости: детальное описание каждой обнаруженной уязвимости, включая их тип, уровень критичности и потенциальные последствия.

- Эксплуатация уязвимостей: описание шагов, которые исполнитель выполнял для получения доступа к системе или для проведения атаки.

- Доказательства успешной эксплуатации: предоставление доказательств, подтверждающих факт наличия уязвимости и возможность успешной атаки.

4. Рекомендации по устранению уязвимостей: предоставление рекомендаций по улучшению безопасности системы и защите от подобных атак.

5. Заключение: подведение итогов тестирования и общая оценка системы.

Отчет проведения тестирования на проникновение является конфиденциальным документом, который предоставляется заказчику и определенным лицам или организациям, роли которых могут быть связаны с безопасностью системы, например, администратором системы или командой по устранению уязвимостей.

Заключение

Роль тестирования на проникновение в информационной безопасности заключается в проверке уязвимостей и защищенности информационных систем и сетей. Это процесс, который проводится специалистами по безопасности с целью выявления и исправления уязвимостей, а также оценки эффективности существующих механизмов защиты.

Важность тестирования на проникновение заключается в обеспечении безопасности информационных систем от внешних атак, внутренних угроз и несанкционированного доступа. Тестирование на проникновение позволяет идентифицировать уязвимости и недостатки в системах защиты, которые могут быть использованы злоумышленниками для несанкционированного доступа к конфиденциальной информации или совершения вредоносных действий.

Результаты тестирования на проникновение могут быть использованы для принятия мер по усилению защиты информационных систем, проведения исправлений и обновлений, а также повышения осведомленности пользователей о возможных угрозах и методах защиты.

Тестирование на проникновение может включать различные методики, такие как сканирование уязвимости, анализ безопасности кода, физическое тестирование, социальное инженерство и другие. Важно отметить, что такие тестирования должны проводиться только с согласия владельцев системы или сети, чтобы предотвратить любые возможные негативные последствия.

Таким образом, роль тестирования на проникновение в информационной безопасности заключается в обеспечении безопасности информационных систем и сетей путем обнаружения и исправления уязвимостей и недостатков, которые

могут быть использованы злоумышленниками для несанкционированного доступа или злонамеренных действий.

Библиографический список:

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: РИОР: ИНФРА-М, 2016.

2. Суханов А. В. Подход к построению защищенных информационных систем // Информационные технологии. – 2009. – № 6. – С. 57–61. 23.

3. Шеннон К. Работы по теории информации и кибернетике. – М.: ИЛ, 1963.