УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ТЕСТОВ НА ПРОНИКНОВЕНИЕ

Амиров Николай Гурамович, Кручинин Александр Владимирович
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, E-mail: kenobi@ukr.net

В работе проведен сравнительный анализ методик тестов на проникновение. Целью является выявления сильных и слабых сторон каждой методики. Сформулирована задача разработки методики, соотносящейся с требованиями, выдвигаемыми законодательством Украины.

Ключевые слова – тест на проникновение, пентест, методология.

ВВЕДЕНИЕ

С увеличением зависимости компаний любого направления деятельности от ИТ технологий, остро встает вопрос обеспечения информационной безопасности [1]. Одним из ключевых мероприятий в обеспечении информационной безопасности компании является тестирование на проникновение. Это позволяет удостовериться в надежности защиты от НСД и прочих угроз ИБ [4]. В Украине отсутствует единая утвержденная методика тестов на проникновение. В связи с этим предлагается провести анализ имеющихся методик для последующей разработки новой методики, подходящей для Украинских стандартов.

ОБЗОР МЕТОДИК ПРОНИКНОВЕНИЯ

1. Методология OSSTMM – The Open Source Security Testing Methodology Manual.

Является достаточно формализованным и хорошо структурированным документом для тестирования сети. Документ имеет так называемую «Карту безопасности» – визуальный показатель безопасности. На карте указываются основные области безопасности, которые включают в себя наборы элементов, которые должны быть протестированы на соответствие методике.

В документе присутствует подпункт «Методология» / «Тестирование технологии интернет-безопасности» / «Обзор сети» / «Тестирование Межсетевого экрана», где перечислена ожидаемая информация, которую может получить взломщик в результате удачной атаки или отсутствия нужной функции у средства защиты. Также описываются конкретные корректные реакции сети на атаки и их наличие, например, измерение времени отклика на пакет или проверка наличия потерь пакетов на маршруте к цели. Минусами методики считается формализованность и отсутствие дополнительного описания к требованиям [2].

2. Методология NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment.

Создана и поддерживается подразделением NIST – CSRC, центром по компьютерной безопасности, объединяющий специалистов федеральных служб, университетов, крупнейших ИТ-компаний США.

В разделе «Техники оценки уязвимостей цели», в качестве одной из техник описываются Тесты на проникновение, а именно Фазы и Логистика тестов. По данному документу тесты на проникновение, в дополнение к стандартным их возможностям, можно применять для определения:

- насколько хорошо система переносит реально существующие модели атак;
- примерного уровня сложности, который необходимо преодолеть атакующему;
- дополнительных мер противодействия, которые могли бы ослабить угрозы в адрес системы;
- способности защищающего систему на обнаружение атак и обеспечение соответствующей реакции на них [2].

3. Методология BSI – Study A Penetration Testing Model.

Разработана немецким подразделением «Federal Office for Information Security». В документе описывается проведение корректных испытаний системы на прочность. Подробно описываются не только сама методология тестов, но и необходимые требования, правовые аспекты применения методологии и процедуры, которые необходимо выполнить для успешного проведения тестов.

Приводится классификация тестов на прочность и определены ее критерии. В приложениях содержатся описание ПО, которое можно использовать для тестирования объектов, описанных в методике. Методика является достаточно подробной и старается предусмотреть все аспекты тестов на прочность, как технические, организационные, так и правовые [2].

4. Методология ISSAF – Information System Security Assessment Framework.

Разработан OISSG (Open Information Systems Security Group) для внутренних контрольных проверок.

Документ охватывает огромное количество вопросов, связанных с информационной безопасностью. Присутствуют главы, описывающие оценку безопасности межсетевых экранов, маршрутизаторов, антивирусных систем и много другого [2].

5. Методология OWASP (Open Web Application Security Project) Testing Guide.

OWASP (Open Web Application Security Project) – международное открытое сообщество, нацеленное на улучшение безопасности программного обеспечения. Каждый имеет право участвовать в OWASP, и все их материалы свободно распространяемы. OWASP Testing Guide представляет собой более широкую

методологию по сравнению с другими, т.к. дает указания не только по тестам на проникновение, но и по анализу вэб-приложений в целом (к примеру – исходного кода), поскольку эта методика фокусирует свое внимание именно на обнаружениях уязвимостей вэб-приложений [3].

6. Обзор методологии PTES – Penetration Testing Execution Standard – Technical Guidelines.

Стандарт, разработанный для объединения как бизнес требований, так и возможностей служб безопасности, и масштабирования тестов на проникновение. На первом подготовительном этапе подробно рассматриваются устанавливаемые каналы коммуникаций, правила взаимодействия и контроля, конкретные способы реагирования и мониторинга инцидентов. Далее выделены следующие этапы:

- сбор информации;
- моделирование угроз;
- методы анализа уязвимостей;
- эксплоитация – обеспечение обхода контрмер и обнаружение наилучшего пути атаки;
- пост-эксплоитация – анализ инфраструктуры, последующее проникновение в инфраструктуру, зачистка и живучесть.

Определена структура отчетов, составляемых по результатам тестирования [2].

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДИК ПРОНИКНОВЕНИЯ

В таблице 1 приведен фрагмент сравнительной таблицы методик по подробности описания и раскрытию каждого этапа проникновения по шкале от 0 до 10, где 0 – не раскрыто совсем, 10 – раскрыто максимально точно.

Для общей сравнительной оценки методик были предложены следующие критерии:

- описание информации, которую может получить взломщик – насколько четко в рамках методологии определены типы информации, которую возможно получить в результате взлома;
- описание целей тестирования на проникновение – насколько точно отражен ожидаемый результат при применении методологии;
- подробность описания методики;
- подробность описания пунктов;
- подробность описания классификации тестирования на проникновение;
- наличие классификаций уязвимости;
- подробность классификации уязвимостей;
- наличие списка рекомендуемых утилит для тестов;
- подробность описания использования утилит;
- восприятие;
- общая оценка методологии.

Фрагмент общей сравнительной таблицы методик приведен в таблице 2.

Таблица 1. Фрагмент сравнительной таблицы методик по подробности описания

Методологии / Этапы	OSSTMM	NIST SP 800-115	BSI	ISSAF	OWASP	PTES
Подготовка						
1. Утверждение с заказчиком режимов тестирования	7	1	0	5	0	7
2. Оформление и подписание договора	7	1	0	5	0	7
Выполнение тестов						
1. Сбор информации об объекте	1	4	8	8	8	7
2. Идентификация уязвимостей	1	3	8	8	8	8

Таблица 2. Фрагмент общей сравнительной таблицы методик

Методологии / Критерий	OSSTMM	NIST SP 800-115	BSI	ISSAF	OWASP	PTES
1. Описание информации, которую может получить взломщик	8	1	0	2	5	0
2. Описание целей тестирования на проникновение	4	5	10	1	10	5
3. Подробность описания методики	4	9	7	6	10	10

ВЫВОД

Используя результаты анализа можно приступить к разработке единой методики, удовлетворяющей требованиям украинского законодательства.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уязвимости веб-приложений [Электронный ресурс]:[https://habrahabr.ru/company/pt/blog/268779/].
2. Сравнительный анализ методик оценки межсетевых экранов [Электронный ресурс]: [http://ojs.ifmo.ru/index.php/IMS/article/viewFile/34/35].
3. OWASP Testing Guide v4.0 [Электронный ресурс]: [https://www.owasp.org/index.php/Category:OWASP_Testing_Project].
4. Тест на проникновение – Агентство Активного Аудита [Электронный ресурс]: [http://auditagency.com.ua/?r=blog&p=Pentest]