Сравнительный анализ методик оценки межсетевых экранов

А.Г. Богораз, О.Ю. Пескова

Южный федеральный университет
poy@tgn.sfedu.ru

Аннотация

В статье рассмотрены основные российские и зарубежные методики оценки защищенности информационных систем в приложении к анализу межсетевых экранов. Описаны основные шаги методик, проведено их сравнение по различным показателям.

Введение

При современном уровне развития информационно-вычислительных сетей (и зачастую их главенствующей роли в технологической цепочке обработки информации) вопросы обеспечения сетевой безопасности являются критически важными для работоспособности всей информационной системы. Одним из основных средств защиты от внешних воздействий являются межсетевые экраны (МЭ, в другой терминологии – файерволы, брандмауэры), предназначенные для контроля и фильтрации трафика, проходящего через них.

Межсетевые экраны подразделяются на различные типы по своим функциональным возможностям, поддерживаемым протоколам, видам фильтрации и так далее. Но вне зависимости от типа МЭ существует большое количество программных и аппаратных решений различных производителей, и потребителю бывает трудно выбрать систему, наиболее адекватно и эффективно решающие задачи по защите конкретной сети от несанкционированного доступа. Информация о межсетевых экранах, доступная непосредственно от производителя, чаще представляет собой рекламу. Для осознанного выбора желательно получить четкое (стандартизированное) описание качественных характеристик продукта, его достоинств и недостатков, надежности и уязвимых мест.

На данный момент не существует методологии, нацеленной именно на специализированное тестирование межсетевых экранов. Для оценки качества МЭ приходится пользоваться более общими методиками.

Для корректного сравнения методологий следует понимать, что данные методики рассматривались только с точки зрения отношения к тестированию межсетевых экранов.

Интернет и современное общество: сборник научных статей XVI Всероссийской объединенной конференции IMS-2013, Санкт-Петербург, 9 - 11 октября 2013 г.

1. Классификация методик тестирования защищенности в приложении к тестированию межсетевых экранов

Классифицируем рассматриваемые методики по двум типам: методики тестирования информационной безопасности организации и методики проведения тестов на проникновение. Термин «тестирование на проникновение/ прочность» (pentest - «пентест») представляет собой метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника.

Анализировались следующие методики тестирования информационной безопасности организации:

- OSSTMM – The Open Source Security Testing Methodology Manual;
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment;
- ISSAF — Information System Security Assessment Framework.

Эти методики создавались как методики комплексного тестирования информационной безопасности организации.

Анализировались следующие методики проведения тестов на проникновение:

- методика Positive Technology;
- методика Digital Security;
- BSI — Study A Penetration Testing Model;
- PTES — Penetration Testing Execution Standard — Technical Guidelines.

Данные методики изначально создавались для проведения корректного тестирования на прочность. Тестирование на проникновение является одним из главных и важнейших инструментов проверки безопасности. Но в то же время нельзя утверждать, что методики проведения тестов на проникновение описывают только то, что относится к технологии тестирования на прочность, его требованиям, задачам и целям. В зарубежной литературе понятие «пентестинг» является гораздо более широким, чем инструмент для проведения технического тестирования сети. В случае наших методик, «пентестинг» понимается как комплексная попытка проникновения с задействованием всех возможных уяз-

вимостей, не только технических, но и тех, что относятся к социальной инженерии, и многих других. Поэтому можно сказать, что сравнение данных стандартов является вполне корректным, несмотря на их формально различные классы.

2. Российские методики анализа защищенности

2.1. Методика Positive Technology

Следует отметить, что российские методики, по большей части, являются копиями зарубежных методик.

Единственная методика, разработанная в России — методика Positive Technology [5]. Positive Technology — одна из ведущих российских компаний в области информационной безопасности. Компания специализируется на комплексном аудите ИБ, оценке защищенности прикладных систем и веб-приложений, тестировании на проникновение и внедрении процессов мониторинга ИБ.

В качестве целей проведения тестов на проникновение указываются:

- обоснование необходимости проведения работ по повышению защищенности;
- получение независимой оценки уровня безопасности информационной системы.

При планировании тестов определяются границы и режимы проведения тестов. Проведение тестов может быть как с уведомлением персонала объекта, так и без него.

Достаточно часто в ходе работ, тесты разбиваются на 2 фазы: внешнюю, при которой аудиторы работают с минимальными знаниями о системе, и их целью является «пробить периметр», и внутреннюю, когда периметр успешно «пробит», аудиторы начинают оценку защищенности сети, уже координируя свои действия с администраторами системы.

В компании определены три вида тестов на проникновение:

- технологический;
- социотехнический;
- комплексный.

Для оценки критичности обнаруженных уязвимостей используется методика Common Vulnerability Scoring System (CVSS), что позволяет использовать результаты тестирования на проникновение в качественных и количественных методиках анализа риска.

Данную методику можно применять на этапе оценки продукта для возможности использования на предприятии.

2.2. Методика Digital Security

Методика Digital Security — методика NSA INFOSEC, доработанная специалистами фирмы Digital Security [2]. Компания Digital Security — ведущая российская консалтинговая компания в области аудита ИБ. Модифицированная ее специалистами методика включает в себя этапы:

1. Утверждение с заказчиком режима тестирования. Определяется уровень информированности исполнителя о тестируемой системе и уровень информированности Заказчика о проведение теста на проникновение.
2. Подписание договора.
3. Выполнение теста на проникновение. В рамках теста на проникновение аудиторы проводят полный анализ всех деталей исследуемого объекта, выбирают подходящие сценарии атак, с учетом человеческого фактора, возможно, разрабатывают уникальное для каждого конкретного случая программное обеспечение для попытки проникновения в информационную систему.

Помимо технологических проверок в процессе внешнего теста на проникновение проводится тестирование возможности проникновения в информационную систему с использованием методик социальной инженерии путем почтовой рассылки на адреса электронной почты пользователей специализированно сформированного сообщения.

По результатам проведения тестирования на проникновение создается отчет, содержащий детальное описание проведенных работ, все выявленные уязвимости системы и способы их реализации. Отчет также содержит конкретные рекомендации по устранению данных уязвимостей.

Данную методику также можно применять на этапе оценки продукта для возможности использования на предприятии.

3. Зарубежные методики анализа защищенности

3.1. OSSTMM – The Open Source Security Testing Methodology Manual [3]

Является достаточно формализованным и хорошо структурированным документом для тестирования сети. Удобен, если необходимо провести полноценную проверку и стандартизацию 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:

1. Информационная безопасность.
2. Тестирование процесса безопасности.
3. Тестирование технологии интернет-безопасности.
4. Тестирование безопасности каналов связи.
5. Тестирование безопасности беспроводных технологий.
6. Тестирование физической безопасности.

Как таковой, классификации уязвимостей в документе нет, однако указано определение термина «уязвимость» как ограничения безопасности — это дефект или ошибка, которая запрещает доступ авто-

ризованным пользователям или процессам к активам, но разрешает привилегированный доступ неавторизованным людям или процессам к активам, или позволяет прятать активы или скрывать себя же в их пределах.

В документе присутствует подпункт «Методология»/«Тестирование технологии интернет-безопасности»/«Обзор сети»/«Тестирование МЭ», где перечислена ожидаемая информация, которую может получить взломщик в результате удачной атаки или отсутствия нужной функции у средства защиты.

В методике указано, что МЭ должен обладать конкретными функциями и возможностями, и перечислено свыше 30 типов тестов для их контроля. 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.

Данную методику можно использовать как на этапе оценки продукта для возможности использования на предприятии, так и на этапе разработки для проверки отдельных возможностей и функций. Также методику можно использовать как шаблон разработки, — какие стандартные функции должны обязательно присутствовать в конечном продукте.

3.2. NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment [7, 8]

Создана и поддерживается подразделением NIST — CSRC, центром по компьютерной безопасности, объединяющий специалистов федеральных служб, университетов, крупнейших ИТ-компаний США. Центр публикует с начала 1990-х годов Стандарты (FIPS) и более детальные разъяснения/рекомендации (Special Publications) в области информационной безопасности. Рекомендациям (Special Publications), созданным CSRC, присваивается код 800.

В документе присутствуют такие разделы как:

- обзор тестирования и экспертизы безопасности;
- обзор методов;
- определение цели и техники анализа;
- техники оценки уязвимостей цели;
- планирование оценки безопасности;
- выполнение оценки безопасности;
- пост-тестовые мероприятия.

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.

Выделяются следующие фазы тестов на проникновение:

1. Планирование.

На данном этапе определяются правила, утверждается и документируется управление, определяются тестируемые цели. Задается основа для успешного тестирования на проникновение.

2. Исследование.

Данный этап включает в себя 2 части.

Первая часть — старт тестирования и сохранение собираемой и сканируемой информации. Для идентификации потенциальных целей проводится определение сетевых портов и сервисов.

Вторая часть — анализ уязвимостей. Производится сравнение сервисов, приложений, ОС сканируемого хоста с базами уязвимостей (автоматический процесс для сканеров уязвимостей) и с собственными знаниями аудитора об уязвимостях. Аудитор может использовать свои собственные базы - или открытые базы уязвимостей — для ручного определения уязвимостей. Ручная обработка позволяет выявить новые уязвимости, но существенно замедляет процесс.

3. Атака.

Этап проверки ранее определенных уязвимостей путем их эксплоитирования. Если атака удачна, то уязвимость проверяется и определяются меры понижения угроз безопасности.

4. Отчет.

Производится во время 3 вышеописанных фаз. Во время фазы «Планирование» разрабатывается план оценки. Во время фаз «Исследование» и «Атака» сохраняются записываемые лог-файлы и создаются периодические отчеты для системных администраторов или менеджмента. В заключение теста, создается отчет, как правило, для описания уязвимостей, указания оценок рисков и представления указаний по смягчению обнаруженных недостатков.

В главе «Логистика тестов» описываются различные рекомендации по типам тестирования: перед проведением наружного тестирования желательно провести внутреннее, чем отличается внутренне тестирование от наружного, рассматриваются некоторые организационные моменты тестов.

Также существует отдельный документ, регулирующий методологию работы с МЭ — NIST SP 800—41 Guideline on Firewalls and Firewall Policy. В пункте «Тесты» документа приводится список аспектов оценки МЭ:

а) Соединения. Пользователи могут устанавливать и поддерживать соединения;

б) Наборы правил, настройка разрешений и запретов на передвижение трафика по сети;

в) Совместимость приложений. МЭ не мешают стандартной работе приложений;

г) Менеджмент. Администратор может конфигурировать и управлять МЭ эффективно и безопасно;

д) Журналирование. Журналирование и функции управление данными настраиваются в соответствие с политикой и стратегией организации;

е) Производительность. МЭ должен обеспечивать адекватную производительность при нормальной и пиковой нагрузках;

ж) Безопасность выполнения. МЭ может содержать уязвимости, которыми может воспользоваться атакующий;

и) Взаимодействие компонентов. Компоненты МЭ должны работать вместе должным образом;

к) Синхронизация политик. При большом количестве запущенных МЭ запускающих синхронизированные политики или группы правил, необходимо тестировать синхронизацию при различных сценариях;

л) Дополнительные возможности. Также должны быть протестированы для утверждения их корректной работы.

Данную методику можно использовать как на этапе оценки продукта для возможности использования на предприятии, так и на этапе разработки для проверки отдельных возможностей и функций. Также методику можно использовать как шаблон разработки — какие стандартные функции должны обязательно присутствовать в конечном продукте..

3.3. BSI — Study A Penetration Testing Model [1]

Разработан германским 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. Присутствуют такие разделы, как:

- введение и объекты обучения;
- it-безопасность и тесты на проникновение;
- классификация и объекты тестов на проникновение;
- правовые вопросы;
- общие требования;
- методология тестов на проникновение;
- выполнение тестов на проникновение.

Согласно этому документу, существует 3 типа методов, с помощью которых можно нанести IT-системе вред или подготовить атаку:

- атаки через сеть;
- социальная инженерия;
- обход физических мер безопасности.

Определены 5 процедур, которые необходимо выполнить для проведения тестов на прочность:

- поиск информации о целевой системе;
- сканирование целевой системы на предмет наличия сервисов;
- идентификация системы и приложений;
- исследование уязвимостей;
- эксплоитирование уязвимостей.

Приводится классификация тестов на прочность и определены ее критерии.

Документ также описывает пять фаз тестов на прочность:

1. Подготовка

С помощью клиента определяются объекты тестирования. Тесты должны выполняться с учетом всех правовых аспектов. Аудитор должен быть уверен, что тесты не нарушают каких—либо законов или договорных обязательств. Процедура и ее риски должны быть обсуждены и задокументированы.

2. Разведка

После первой фазы, аудитор может начинать собирать информацию о цели. Это фаза пассивного тестирования на прочность. Цель — получить полный и детальный обзор установленных систем, включая области открытые для атак и известные недостатки безопасности.

3. Анализ информации и рисков.

Для успешной, прозрачной и экономически эффективной процедуры, собранная информация должна быть проанализирована перед началом активного тестирования на проникновение. Анализ должен включать в себя определение целей тестов на проникновение, потенциальные риски системы и время, необходимое для оценки возможных проблем безопасности для последующих активных тестов.

4. Попытки активного вторжения.

Данная фаза влечет высокий уровень риска и должна проводиться с должным вниманием. Однако, только эта фаза может показать, какова опасность предполагаемых уязвимостей, выявленных в ходе разведывательной фазы.

5. Окончательный анализ.

Конечный отчет должен содержать оценку уязвимостей в виде форм потенциальных рисков и рекомендации устранения уязвимостей и рисков. Отчет также должен гарантировать прозрачность тестов и раскрытие уязвимостей.

6. Документирование. Во время всех вышеописанных фаз происходит журналирование, запись, обработка и выработка рекомендаций.

В приложениях содержатся описание ПО, которое можно использовать для тестирования объектов, описанных в методике.

Данную методику рекомендуется использовать для тестирования конечного продукта. Она является достаточно подробной и старается предусмотреть все аспекты тестов на прочность, как технические, организационные, так и правовые.

3.4. ISSAF — Information System Security Assessment Framework [6]

Разработан Open Information Systems Security Group — OISSG для следующих инструментов менеджмента и внутренних контрольных проверок:

а) Оценка политик и процедур информационной безопасности организации для отчетности об их соответствии индустриальным IT—стандартам,

применимым законам, а также нормативным требованиям;

б) Выявление и оценка зависимости бизнеса от инфраструктуры IT-услуг;

в) Проведение оценки уязвимостей и тестов на проникновение для выделения уязвимостей в системе, которые могут привести к потенциальным рискам информационных активов;

г) Указание моделей оценки по доменам безопасности;

д) Нахождение и устранение неправильных конфигураций;

е) Идентификация и решение рисков, связанных с технологиями;

ж) Идентификация и решение рисков, связанных с персоналом или бизнес-процессами;

з) Усиление существующих процессов и технологий;

и) Предоставление лучших практик и процедур для поддержки инициатив непрерывности бизнеса.

Документ охватывает огромное количество вопросов, связанных с информационной безопасностью. Присутствуют главы, описывающие оценку безопасности МЭ, роутеров, антивирусных систем и много другого.

В главе «Методология тестов на проникновение» представлены 3 фазы, которые необходимо осуществить для корректного проведения тестов на проникновение:

1. Планирование и подготовка.

Получение начальной информации, планирование и подготовка к тестам. Перед тестированием сторонам необходимо будет подписать формальное соглашение, которое обеспечит основу для задания и взаимную правовую защиту. В нем также будет указаны взаимодействующие команды, точные даты, время тестирования, пути эскалации и другие мероприятия.

2. Оценка.

На этом этапе производится выполнение тестирования на проникновение. Предусмотрены следующие девять уровней:

1). Сбор информации.

Для сбора информации в основном используется Интернет. Получаемая информация делится на 2 группы: техническая (DNS/WHOIS) и нетехническая (поисковые системы, группы новостей и т.д.). На данном этапе абсолютно любая информация является полезной: брошюры компаний, визитные карты, объявления в газетах и т.п. Данный этап критичен, так как позволяет выделить точек, которые могут быть уязвимы, и сфокусироваться на них.

2). Сетевое картографирование.

После сбора информации в интернете о целевом объекте применяется более технические подходы к определению сети и ее ресурсов. Информация о сети, полученная на первом уровне, используется для расширения знания о возможной топологии сети целевого объекта.

3). Идентификация уязвимостей.

Перед этой стадией, аудитор определяют объекты и способы тестирования. В процессе тестирования аудитор будет выполнять следующие мероприятия:

a) Идентификация уязвимостей сервисов с помощью определения реакции почтовых сервисов.
b) Выполнение сканирования на предмет поиска известных уязвимостей. Информация об известных уязвимостях берется из открытых баз данных уязвимостей.
c) Выполнение ложной позитивной и ложной негативной проверок (например, сопоставляя уязвимости друг с другом и с ранее полученной информацией).
d) Подсчет обнаруженных уязвимостей.
e) Оценка возможного воздействия (классификация найденных уязвимостей).
f) Идентификация путей атак и сценариев эксплоитирования.

В документе определяется 2 типа рисков: Технический риск и риск Бизнеса. В свою очередь каждый из них делится на 3 вида: Низкий, Средний, Высокий.

4). Проникновение;

5). Получение доступа или расширение привилегий;

Получение минимальных привилегий доступа возможно через доступ к непривилегированным аккаунтам с помощью следующих способов:

a) Подбор комбинаций логин/пароль (bruteforce, атака со словарем);
b) Поиск пустых или стандартных паролей в системных аккаунтах;
c) Эксплоитирование стандартных настроек поставщика (параметры конфигурации сети, стандартные пароли и т.д.);
d) Поиск публичных сервисов, допускающих определенные операции в системе (запись/создание/чтение файлов).

Конечной целью аудитора является получение доступа к аккаунту Администратора.

Часто в системах разрешены только аккаунты с минимальным количеством привилегий. В этом случае выполняется составление карты локальных уязвимостей, производится разработка или получение корректного эксплоита, затем он тестируется в изолированной среде и применяется к компроментированной системе.

6). Дополнительные тесты, например, получение зашифрованных паролей для их последующего оффлайнового взлома, сниффинг трафика и его анализ и т.д.

7). Компроментация удаленных пользователей/сайтов;

8). Поддержка доступа;

9). Скрытие следов.

Также присутствует глава «Оценка безопасности МЭ», где описывается, какие бывают МЭ, каким функциями они должны обладать и защиту от чего они не могут предоставить.

Непосредственно методология включает в себя 4 этапа:

1) Определение МЭ:

2) Определение общих неправильных конфигураций:

3) Тестирование общих атак на МЭ:

4) Тестирование продукта по специфическим вопросам.

Также в главе прилагается подробные рекомендации по тестированию. Описаны не только утилиты, которыми можно провести тестирование, но и указания по их использованию и какие реакции можно получить в результате тестирования с определенными параметрами.

Данную методику рекомендуется применять для проверки конечного продукта или проверки общей надежности сети.

3.5. PTES — Penetration Testing Execution Standard — Technical Guidelines [4]

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:

1. Сбор информации
2. Моделирование угроз
3. Методы анализа уязвимостей
4. Эксплоитация — обеспечение обхода контрмер и обнаружение наилучшего пути атаки
5. Пост-эксплоитация — анализ инфраструктуры, последующее проникновение в инфраструктуру, зачистка и живучесть.

Определена структура отчетов, составляемых по результатам тестирования.

4. Результаты сравнения методик

В целом, результаты сравнения методологий по фазам тестов на прочность можно проиллюстрировать следующей картой (рис.1)

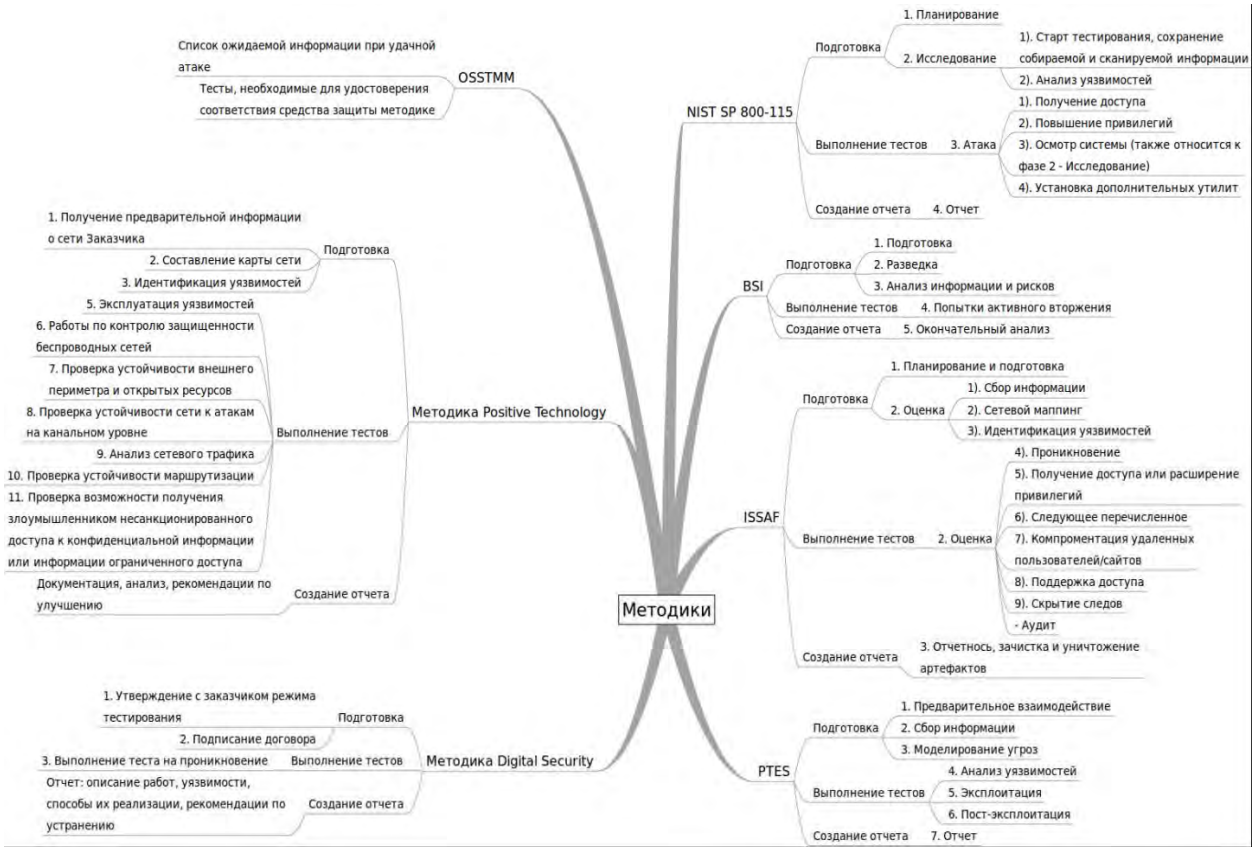

Рис. 1. Сравнение методологий по фазам тестов на прочность

В таблице 1 приведено сравнение методик по подробности описания пунктов. Для этого возьмем подпункты, предлагаемые всеми методиками, и рассмотрим, насколько подробно они упоминаются в каждой методике с помощью системы бальных оценок от 0 до 10. Пункты будут разделяться на 3 стандартных фазы: Подготовка, Выполнение тестов и Создание отчета.

В таблице 2 приведено сравнение методик по определенным критериям с помощью аналогичной системы бальных оценок от 0 до 10.

Таблица 1. Сравнение методик по подробности описания подпунктов

Методика / **Фазы**/Пункты	**Positive Technology**	**Digital Security**	**OSSTMM**	**NIST SP 800-115**	**BSI**	**ISSAF**	**PTES**
Подготовка							
1. Утверждение с заказчиком режимов тестирования	3	5	7	1	0	5	7
2. Оформление и подписание договора	3	6	7	1	0	5	7
Выполнение тестов							
1. Сбор информации об объекте	3	5	1	4	8	8	7
2. Идентификация уязвимостей	5	5	1	3	8	8	8
3. Анализ информации и рисков	3	4	1	2	8	8	8
4. Попытки активного вторжения	5	4	1	5	8	8	8
5. Обеспечение возможности последующих вторжений	0	0	0	0	0	8	8
Создание отчета							
1. Зачистка артефактов	0	0	1	5	4	5	8
2. Создание отчета	5	3	7	4	8	6	9
3. Анализ и рекомендации по устранению найденных уязвимостей	3	3	2	4	8	4	9
4. Описание рисков	3	0	1	3	8	4	9

Таблица 2. Сравнение методик по выбранным критериям

Методика / **Критерий**	**Positive Technology**	**Digital Security**	**OSSTMM**	**NIST SP 800-115**	**BSI**	**ISSAF**	**PTES**
1. Описание информации, которую может получить взломщик в случае отсутствия МЭ	0	0	8	1	0	2	0
2. Описание функций, которыми должен обладать МЭ	0	0	0	7	0	7	0
3. Описание аспектов оценки МЭ	0	0	0	7	0	2	0
4. Описание целей тестирования на проникновение	5	3	4	5	10	1	5
5. Подробность описания методики	2	4	4	9	7	6	10
6. Подробность описания пунктов	3	2	1	8	8	8	4
7. Наличие списка атак, которые необходимо реализовать для удостоверения соответствия МЭ методике	0	0	9	0	3	6	0
9. Подробность описания классификации тестирования на проникновение	1	1	7	3	10	1	5
10. Наличие классификации уязвимостей	0	0	0	6	0	5	3
11. Подробность описания классификации уязвимостей	0	0	0	2	0	4	2
12. Наличие списка рекомендуемых утилит для тестов	0	0	0	8	8	7	0
13. Подробность описания использования утилит	0	0	0	0	3	8	0
14. Восприятие	3	4	5	5	9	5	6
15. Общая оценка методики	3	3	6	7	8	6	5

По результатам анализа данных методик была предложена авторская методика тестирования, назначением которой является оценка уровня защиты, предоставляемой межсетевым экраном. Методика предназначена для стендового тестирования, однако, может использоваться для тестирования в рабочей системе заказчика.

Литература

[1] BSI — Study A Penetration Tesing Model / Germany, Bonn. 111 p. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile (дата обращения: 16.08.2013).

[2] Digital Security: N1 в аудите безопасности [Электронный ресурс] // Digital Security [сайт]. URL: http://dsec.ru/consult/test/#why (дата обращения 16.08.2013).

[3] Herzog P. OSSTMM — The Open Source Security Testing Methodology Manual. USA, New York, 13.12.2006. 129 p. URL: http://www.isecom.org/research/osstmm.html (дата обращения: 16.08.2013).

[4] Nickerson C. и др. The Penetration Testing Execution Standard / Chris Nickerson, Dave Kennedy, Chris John Riley, Eric Smith, Iftach Ian Amit, Andrew Rabie, Stefan Friedli, Justin Searle, Brandon Knight, Chris Gates, Joe McCray, Carlos Perez, John Strand, Steve Tornio, Nick Percoco, Dave Shackelford, Val Smith, Robin Wood, Wim Remes, Rick Hayes. 30.04.2012 [Электронный ресурс]. // Penetration Testing Execution Standarts [сайт]. URL: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (дата обращения 16.08.2013).

[5] Positive Technologies — безопасность, консалтинг, compliance management [Электронный ресурс] // Positive Technologies [сайт]. URL: http://www.ptsecurity.ru/services/pen/technological (дата обращения 16.08.2013).

[6] Rathore B. и др. ISSAF — Information System Security Assesment Framework / Rathore B., Brunner M., Dilaj M., Herreragh O., Brunati P., Subramaniam R., Raman S., Chavan U. 30.04.2006. 1264 p. URL: http://www.oissg.org/issaf02/issaf0.1-5.pdf (дата обращения 16.08.2013).

[7] Scarfone K., Hoffmann P. NIST Special Publications 800-41 Guidelines on Firewall and Firewall Policy. USA, Gaithersburg, 09.2009. 48 p. URL: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf (дата обращения 16.08.2013).

[8] Scarfone K., Souppaya M., Cody A., Orebaugh A. NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment. USA, Gaithersburg, 09.2008. 80 p . URL: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf (дата обращения 16.08.2013).

Comparative analysis of methodologies for assessment of firewalls

A.G. Bogoraz, O.Y. Peskova

The article describes the main Russian and foreign security assessment techniques in the annex of information systems to the analysis of firewalls. The main steps of techniques are described, and the various indicators are compared