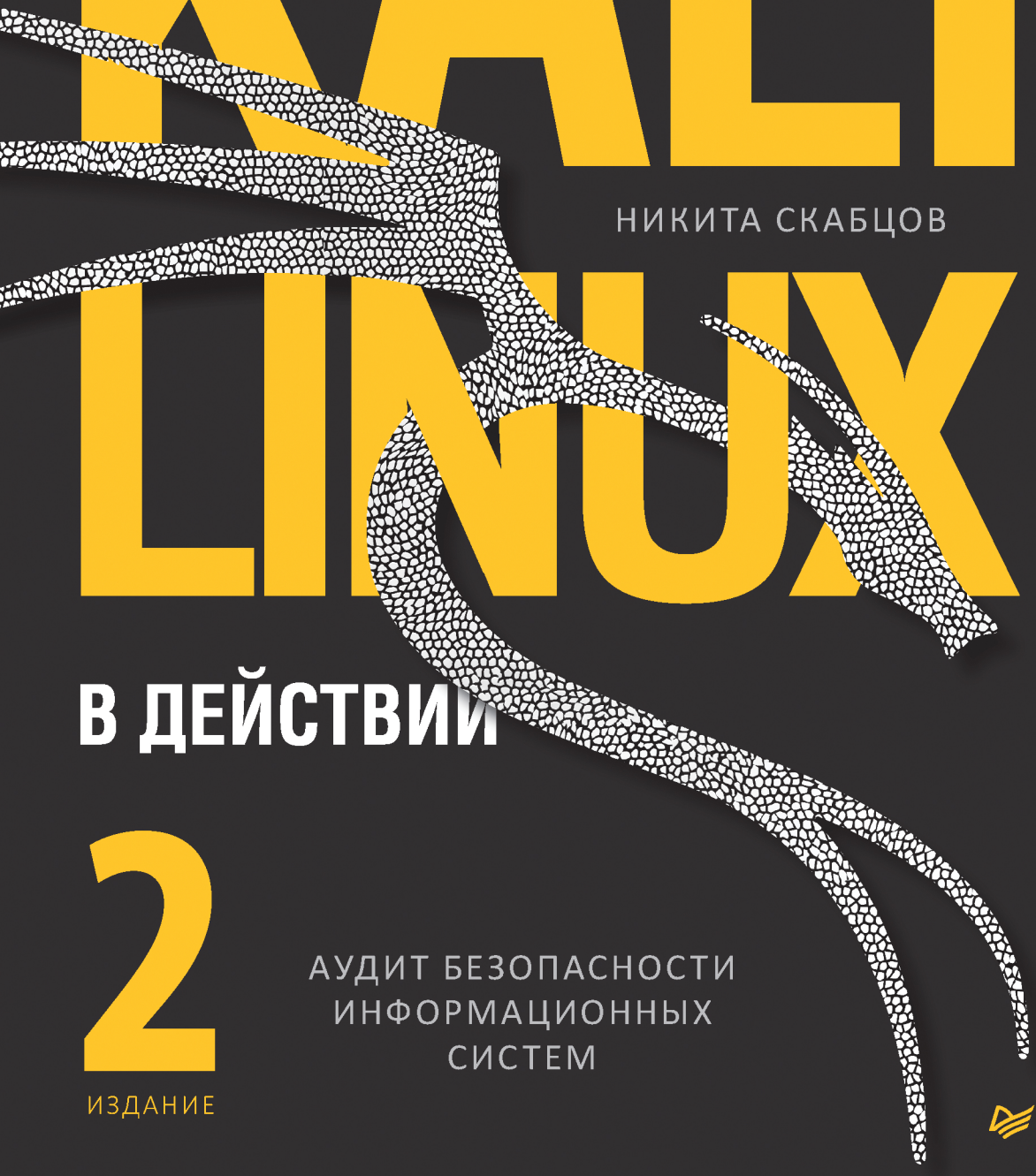
KALI LINUX

НИКИТА СКАБЦОВ

В ДЕЙСТВИИ

2 ИЗДАНИЕ

АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ



ББК 32.973.23-018-07
УДК 004.56.53

Никита Скабцов

С44 Kali Linux в действии. Аудит безопасности информационных систем. 2-е изд. — СПб.: Питер, 2024. — 384 с.: ил. — (Серия «Библиотека программиста»).

ISBN 978-5-4461-2154-0

В этой книге рассматриваются методы обхода систем безопасности сетевых сервисов и проникновения в открытые информационные системы. Информационная безопасность, как и многое в нашем мире, представляет собой медаль с двумя сторонами. С одной стороны, мы проводим аудит, ищем способы проникновения и даже применяем их на практике, а с другой — работаем над защитой. Тесты на проникновение являются частью нормального жизненного цикла любой ИТ-инфраструктуры, позволяя по-настоящему оценить возможные риски и выявить скрытые проблемы.

Может ли взлом быть законным? Конечно, может! Но только в двух случаях — когда вы взламываете принадлежащие вам ИС или когда вы взламываете сеть организации, с которой у вас заключено письменное соглашение о проведении аудита или тестов на проникновение. Мы надеемся, что вы будете использовать информацию из данной книги только в целях законного взлома ИС. Пожалуйста, помните о неотвратимости наказания — любые незаконные действия влекут за собой административную или уголовную ответственность.

Вы последовательно пройдете все шаги, необходимые для проведения аудита безопасности информационных систем и тестов на проникновение: от общих понятий, рассмотрения стандартов и необходимых действий перед проведением аудита до методов проникновения в информационную систему и закрепления в ней. Каждая глава книги подкреплена реальными примерами и содержит практическую информацию по применению тех или иных методов.

Книга адресована читателям, имеющим опыт работы в сфере информационных технологий и знакомым с работой основных сетевых сервисов как на Linux-, так и на Windows-платформах, а больше всего будет полезна системным администраторам, специалистам по ИТ-безопасности, всем тем, кто желает связать свою карьеру с защитой информации или аудиторской деятельностью.

Во втором, дополненном и переработанном, издании информация была полностью обновлена и соответствует современным реалиям.

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ISBN 978-5-4461-2154-0

Изготовлено в России. Изготовитель: ООО «Прогресс книга». Место нахождения и фактический адрес:
194044, Россия, г. Санкт-Петербург, Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.
Дата изготовления: 02.2024. Наименование: книжная продукция. Срок годности: не ограничен.
Налоговая льгота — общероссийский классификатор продукции ОК 034-2014, 58.11.12 —
Книги печатные профессиональные, технические и научные.
Импортер в Беларусь: ООО «ПИТЕР М», 220020, РБ, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс: 208 80 01.
Подписано в печать 08.12.23. Формат 70×100/16. Бумага офсетная. Усл. п. л. 30,960. Тираж 1000. Заказ 0000.

Оглавление

02 Методология

Существует множество методик проведения тестов на проникновение. Хотя их знание, безусловно, не гарантирует вам успешного взлома целевой ИС, однако крайне повышает шансы на это. К тому же, следуя методике, вы будете уверены, что сделали все возможное для качественного проведения работ и вам не будет стыдно представить отчет заказчику.

К сожалению, во многих случаях аудиты безопасности проводятся на скорую руку, без должной подготовки и применения необходимой методики, что снижает качество выполняемой работы и, следовательно, подвергает угрозе ИС заказчика. Тесты на проникновение должны производиться с применением эффективной методики, которую при необходимости вы можете изменять и подстраивать под требования заказчика, исходя из специфики выполняемой работы.

В данном разделе будет представлен краткий обзор нескольких популярных методик. Не пожалейте времени на их подробное изучение — это значительно облегчит вашу работу и позволит выполнять ее еще более профессионально.

Стандарт оценки безопасности информационной системы

Данный стандарт разрабатывается и поддерживается группой безопасности открытых информационных систем (OISSG). Стандарт оценки безопасности информационной системы (ISSAF) представляет собой постоянно рецензируемый документ, содержащий информацию о том, как проводить тесты на проникновение. Сильной стороной ISSAF является показ связи между различными задачами проекта и инструментами для их достижения. Несмотря на то, что разработчики не отдают предпочтения тому или иному программному обеспечению, в своей работе вы так или иначе будете использовать большую часть предложенного ими.

Первая фаза — планирование и подготовка

В этой части описываются шаги, которые необходимо сделать перед началом работ: обмен вводными данными, планирование ресурсов и подготовка. В первую очередь вам необходимо заключить договор о выполнении работ, он должен быть подписан обеими сторонами. Данное соглашение будет являться основой для проведения дальнейших работ. Также вам необходимо спланировать даты, время проведения тестов, технические детали и другие необходимые условия. Этот этап, помимо прочего, включает в себя уточнение списка контактных персон с обеих сторон, организацию собрания для обсуждения необходимых деталей проведения будущих работ, согласование ранее намеченного плана.

К сожалению, на данный момент эта фаза не описана настолько подробно, насколько нам хотелось бы. Однако учитывая, что свежие версии данного фреймворка не выходили достаточно давно, вряд ли мы увидим их в ближайшее время.

Вторая фаза — аудит ИС

Несмотря на довольно неинформативную первую часть, вторая часть ISSAF проработана достаточно хорошо. В ней подробно описываются шаги, которые необходимо сделать для качественного проведения аудита. Одной из сильных ее сторон является уровень детализации. Тут представлены не только сами инструменты для выполнения тестов, но и примеры их использования. Даже если вы не знакомы со спецификой ИБ-аудита, в некоторых случаях вы сможете провести вполне удачную серию тестов, используя только приведенные примеры.

Помимо описания самих программ, примеров их запуска и использования, в ISSAF также трактуются полученные результаты, что, несомненно, расширит ваши знания даже после простого прочтения. Это не самый лучший вариант проведения аудита, но для тех, кто только знакомится с областью ИБ, он вполне подойдет.

Обратите внимание на то, что в данном фреймворке до конца не раскрывается весь потенциал тех или иных инструментов. Также здесь не описаны все возможные интерпретации полученных данных — это и понятно, ведь их очень много, да и авторы не преследовали такой цели.

В представленном ISSAF фреймворке каждый этап описывается как слой, ниже приводится краткое описание каждого из них:

- сбор информации (использование интернета для поиска всей доступной информации о цели с помощью как технических, так и нетехнических методов);
- картирование сети (идентификация всех систем и ресурсов целевой ИС);

- идентификация уязвимости (действия, выполняемые специалистом для обнаружения уязвимостей в целевой ИС);
- проникновение (получение несанкционированного доступа путем обхода методов защиты и попытка получения как можно более высоких привилегий в системе);
- получение доступа и повышение привилегий (попытка получить более высокие привилегии после успешного взлома системы или сети экспертом);
- продолжение проникновения (получение дополнительной информации о процессах в подконтрольной системе с целью ее дальнейшего использования);
- компрометация удаленных пользователей/сайтов (использование доверительных отношений и связей между удаленными пользователями и системами предприятия);
- поддержание доступа (использование скрытых каналов и руткитов для сокрытия присутствия специалиста в системе или обеспечения постоянного доступа к скомпрометированному ресурсу);
- сокрытие следов (устранение всех признаков взлома путем скрытия файлов, очистки журналов, обхода проверок целостности и антивирусного ПО).

Указанные этапы взлома применяются по отношению к следующим типам ресурсов: сети, хосты, приложения и базы данных.

Сетевая безопасность

ISSAF с различной степенью детализации предоставляет подробную информацию о различных типах оценки безопасности сетевых устройств. Во фреймворке представлена справочная информация по различным темам, примеры стандартных конфигураций, список используемых средств для проведения атак и ожидаемые результаты. Указанная информация будет интересна не только новичкам, но и специалистам с опытом работы в сфере ИБ. Ниже приведены некоторые темы, освещаемые данным фреймворком:

- взлом паролей;
- оценка безопасности коммутатора;
- оценка безопасности маршрутизатора;
- оценка безопасности файервола;
- оценка безопасности системы обнаружения вторжений (IDS);
- оценка безопасности виртуальной частной сети (VPN);
- оценка безопасности антивирусной системы;
- безопасность сети хранения данных (SAN);
- оценка безопасности беспроводной локальной сети;
- безопасность пользователей интернета;

- безопасность AS 400;
- безопасность Lotus Notes.

Не стоит пугаться большого объема информации, необходимости в доскональном прочтении всего стандарта нет. Самое главное — знать, что в нем содержится, и тогда, столкнувшись во время проведения тестов с незнакомой вам системой, вы будете представлять, где получить о ней информацию. Стоит еще раз упомянуть, что, к сожалению, данный стандарт давно не обновлялся и не покрывает весь спектр существующего ПО, но до сих пор содержит много актуальной информации.

Безопасность хостов

В ISSAF описаны вопросы, касающиеся безопасности самых популярных операционных систем, среди которых Unix/Linux, Windows, Novell Netware. Предоставлена и информация о веб-серверах.

Обязательно обратите внимание на раздел, посвященный веб-серверам. В современном мире веб-серверы используются не только для размещения страниц в интернете, сейчас многие производители используют их для создания графических интерфейсов управления устройствами.

Так как стандарт давно не обновлялся, некоторые описанные типы операционных систем давно не используются, а самые свежие разработки в него не включены. Однако упомянуть о нем все же необходимо, ведь многие крупные предприятия в целях экономии продолжают использовать устаревшее ПО (так, некоторые банкоматы продолжают работать под управлением Windows NT).

Безопасность приложений

На самом деле разделить тестирование приложений и баз данных достаточно сложно. В наши дни многие приложения активно используют базы данных того или иного типа, так что, получая к ним доступ, вы получаете и доступ к базе данных. В рамках фреймворка рассматриваются следующие типы атак: атаки на веб-приложения, SQL-инъекции, аудит исходного кода, аудит бинарных файлов.

Безопасность баз данных

В данном разделе описаны специфические методы, применимые именно к базам данных: удаленный взлом баз данных, манипуляция процессами, полный аудит баз данных.

Социальная инженерия

В данном разделе описываются методы социальной инженерии. Все описанные методы довольно старые, но к большому сожалению, уровень грамотности

пользователей не вырос слишком значительно, а специалисты по ИБ не уделяют этому вопросу должного внимания. В связи с этим практически все описанное можно успешно применять и в наше время.

Третья фаза — отчетность, избавление от следов пребывания

В данном разделе описаны необходимые шаги, которые следует выполнить по завершении аудита ИС. Они включают подготовку и передачу данных лицам, указанным на первом шаге, а также вопросы конфиденциальности полученных данных. В отношении этого раздела следует сказать, что он также недостаточно подробен.

Отчет

Данный фреймворк описывает два вида отчетов — устный и письменный. Первый стоит использовать в случае нахождения критической уязвимости, которая, на ваш взгляд, должна быть устранена немедленно. Информацию о таких случаях также необходимо внести в финальную версию письменного отчета.

По мнению разработчиков, финальный отчет должен содержать следующую информацию:

- данные об организационных мероприятиях;
- цели проведения работ;
- используемое ПО;
- используемые эксплойты;
- даты и время тестов;
- все полученные данные;
- список найденных уязвимостей;
- рекомендации по устранению найденных уязвимостей, ранжированные в порядке приоритетности.

Финальный отчет рекомендуется не перегружать огромным количеством данных. Не включайте все в основной документ, вынесите что-то в приложение. Так вы предоставите всю необходимую информацию, а результат вашей работы будет выглядеть намного лучше.

Очистка следов пребывания

В этом разделе идет речь о необходимости удалить любые файлы и ПО, созданные вами в исследуемой ИС. Если по каким-то причинам вы не можете сделать это самостоятельно, в вашем отчете нужно представить подробную инструкцию о том, как это могут сделать администраторы ИС.

Руководство по методике тестирования безопасности с открытым исходным кодом

Руководство по методике тестирования безопасности с открытым исходным кодом (OSSTMM) — стандарт, разработкой которого занимается организация ISECOM (Institute for Security and Open Methodologies), старающаяся придерживаться строго научного подхода. Первую версию стандарта представили в 2000 году, и он поддерживается до сих пор.

OSSTMM был разработан с целью создания стандартизированной методики для аудита ИС, которая была бы открытой и общедоступной. Этот стандарт обеспечивает набор инструкций и рекомендаций для проведения тестов на проникновение, включая оценку уязвимостей, анализ рисков, собственно тесты и проверку безопасности приложений.

Он охватывает широкий диапазон тестов на безопасность, среди которых проверка сетевых устройств, физической безопасности, методы социальной инженерии, тестирование приложений, оценка безопасности беспроводных сетей и тестирование на проникновение.

Более того, OSSTMM предлагает методику, позволяющую оценить эффективность системы безопасности и провести оценку соответствия ее требованиям. Это помогает организациям оценить уровень своей защищенности и принять меры для улучшения безопасности своих ИС и приложений.

Каналы

Каналы в OSSTMM — это категории информационных ресурсов, которые могут быть подвержены угрозам и атакам. В OSSTMM представлены семь каналов, проверяемые при проведении аудита ИС:

- канал сетевого доступа: маршрутизаторы, коммутаторы, файерволы, VPN и другие сетевые устройства;
- канал приложений: веб-приложения, приложения для мобильных устройств, приложения для рабочих станций и т. д.;
- канал операционных систем: Windows, Linux, Unix и т. д.;
- канал физической безопасности: здания, серверные залы, шкафы для хранения оборудования и другие физические объекты;
- канал социальной инженерии: проверка сотрудников на подверженность фишингу, обману, мошенничеству и т. д.;
- канал беспроводной связи: Wi-Fi, Bluetooth, NFC и т. д.;
- канал телекоммуникаций: телефонные системы, VoIP, видеоконференции и т. д.

При проведении тестирования на безопасность необходимо проверять все эти каналы, чтобы убедиться, что все информационные ресурсы организации защищены от потенциальных угроз и атак.

Модули

В OSSTMM есть модули, которые представляют собой повторяющиеся процессы в рамках теста на проникновение. Эти модули используются во всех каналах OSSTMM. Реализация каждого модуля может быть разной в зависимости от целевой системы или сети. Каждый из модулей предлагает специализированные подходы для каждого канала, однако их связывают общие принципы, которые мы рассмотрим ниже.

Подготовка

Первая фаза OSSTMM — это фаза ознакомления и подготовки, которая включает в себя определенные шаги. Цель этого этапа состоит в том, чтобы подготовить основу для проведения тестирования безопасности и разработать план действий, который будет использоваться во время тестирования.

Описываются следующие действия:

- **Определение целей тестирования.** Является первым и важным шагом в проведении аудита. Цели тестирования в зависимости от требований заказчика могут меняться, но обычно включают в себя поиск и оценку уязвимостей, проверку соответствия политикам и процедурам безопасности, а также тестирование способности системы обнаруживать и предотвращать атаки.
- **Выбор методики тестирования.** OSSTMM предоставляет широкий спектр методик тестирования безопасности, а выбор конкретной зависит от целей тестирования и типа тестируемой информационной системы.
- **Подготовка тестовой среды.** Этот этап включает в себя создание копии рабочей среды организации, которая будет использоваться для проведения тестирования безопасности. Во время этого этапа происходит создание виртуальных машин, настройка тестовых устройств и т. д.
- **Оценка рисков.** Позволяет идентифицировать потенциальные угрозы, которые могут повлиять на проведение аудита и работу целевой ИС. Включает в себя разработку плана действий для их предотвращения.
- **Планирование тестирования.** Включает в себя определение сроков и бюджета, распределение ресурсов, назначение ответственных за проведение тестирования и определение тестовых сценариев.
- **Сбор информации.** На этом шаге проводится сбор информации о целевой ИС. Обычно это подразумевает сбор информации об инфраструктуре, используемых технологиях, политиках безопасности и т. д.

Сбор информации

Во время этой фазы тестирования происходит активный поиск информации об объекте, который нужно протестировать. Это может быть сбор информации о компьютерной сети, операционной системе, приложениях, уязвимостях и т. д. Сбор информации включает в себя использование открытых источников —

сайтов, социальных сетей, форумов, — а также сканирование портов и анализ протоколов.

Ко второй фазе относятся следующие действия:

- **Определение целей тестирования.** Целью может быть, например, проверка степени защищенности сети или приложения.
- **Определение диапазона тестирования.** Оговариваются системы и приложения, которые будут тестироваться. Диапазон может включать в себя все приложения и сети организации, а может ограничиваться только конкретными участками информационной системы.
- **Сбор информации о целевой системе.** Может включать в себя сбор открытой информации, такой как доменные имена, IP-адреса, информация о серверах, базах данных, приложениях и т. д.
- **Определение методов атаки**, которые будут использоваться для взлома системы.
- **Оценка рисков.** Необходимый этап, на котором оцениваются риски, связанные с тестированием системы. Этот этап позволяет определить, какие действия могут повлечь за собой нежелательные последствия, например повреждение данных или нарушение работы системы.

Эта фаза особенно важна для тестирования безопасности, поскольку она позволяет тестировщикам получить ценную информацию, необходимую для понимания объекта тестирования, а также для идентификации уязвимостей и потенциальных точек входа для атаки. Она также может помочь определить, какие методы тестирования безопасности будут наиболее эффективными в дальнейшей работе.

Анализ уязвимостей

Цель третьей фазы в OSSTMM состоит в том, чтобы провести тестирование системы на наличие уязвимостей, оценить их критичность, провести атаки на систему, оценить эффективность защиты и определить меры по улучшению уровня безопасности. На данном уровне выполняются следующие шаги:

- **Идентификация уязвимостей.** Проводится их поиск в информационной системе.
- **Оценка уязвимостей.** Проводится с целью определить, какой уровень угрозы они представляют для информационной системы.
- **Классификация уязвимостей.** Проводится по их типу и уровню угрозы, что позволяет определить приоритеты для последующих шагов во время аудита информационной системы.
- **Проверка эффективности защитных мер.** Оценка эффективности защитных мер, которые были реализованы для предотвращения атак, может включать в себя проверку наличия и правильной настройки механизмов аутентификации, контроля доступа, межсетевых экранов и т. д.

- **Проверка соответствия политикам и процедурам безопасности.** Включает в себя проверку наличия и правильной настройки систем регистрации событий и другие процедуры.

Эксплуатация уязвимостей

Фаза является одним из ключевых и важных этапов аудита безопасности. На этой фазе специалисты осуществляют проверку возможности эксплуатации обнаруженных уязвимостей в целях получения контроля над системой или доступа к защищаемым ресурсам. Цель этого этапа — определить реальную уязвимость системы и оценить риски. Основные шаги:

- **Подбор утилит и инструментов для эксплуатации уязвимостей.**
- **Эксплуатация уязвимостей.** Специалисты пытаются использовать обнаруженные уязвимости для получения доступа к системе или защищаемым ресурсам.
- **Повторная проверка системы.** Производится, чтобы убедиться, что эксплуатация не привела к нежелательным последствиям или не была обнаружена защитными механизмами.

Повышение привилегий и расширение доступа

На этом этапе осуществляется проверка возможности повышения привилегий и расширения доступа. Основные шаги:

- **Анализ среды и определение потенциальных уязвимостей.** Проводится с целью выявить потенциальные уязвимости и недостатки, которые могут быть использованы для повышения привилегий и расширения доступа.
- **Подбор инструментов и методов**, которые будут использоваться для повышения привилегий и расширения доступа.
- **Попытка повышения привилегий.** Специалисты пытаются повысить свой уровень доступа, чтобы получить больше прав в контроле над системой или защищаемыми ресурсами.
- **Попытка расширения доступа.** Имеет целью получить доступ к защищаемым ресурсам, которые были недоступны на более низком уровне доступа.

Оценка рисков и управление ими

Цель этого этапа — оценить потенциальные риски, связанные с безопасностью информационной системы, и определить меры по их устранению или снижению. Основные шаги:

- **Идентификация систем и уязвимостей.** Проводится анализ ИС с целью определения ее наиболее ценных элементов, требующих защиты, а также определение уязвимостей, которые могут быть использованы злоумышленниками.

- **Определение потенциальных угроз.** Определяются не только потенциальные угрозы, которые могут нанести ущерб ИС, но и вероятность их эксплуатации.
- **Оценка уровня риска.** Может основываться на различных критериях, таких как вероятность, возможные последствия, доступность и т. д.
- **Разработка мер по снижению рисков**, включая технические и организационные.
- **Повторная оценка рисков.** Позволяет убедиться в эффективности реализованных мер по снижению рисков.

Другие методики

Как уже было упомянуто, в сфере информационной безопасности существует множество методик, которые могут применяться для обеспечения защиты информационных систем и данных. Приведем некоторые из них:

- ISO 27001 (International Organization for Standardization) — международный стандарт для управления информационной безопасностью. Определяет требования к управлению рисками и обеспечению безопасности информационных систем и процессы для их реализации;
- OSSTMM (Open Source Security Testing Methodology Manual) — методика тестирования безопасности, описывающая процесс тестирования и определения уязвимостей информационных систем;
- NIST (National Institute of Standards and Technology) — федеральный стандарт США, определяющий рекомендации по управлению информационной безопасностью;
- PTES (Penetration Testing Execution Standard) представляет процесс тестирования безопасности с помощью проникновения специалистов в информационную систему для определения уязвимостей и разработки мер по их устранению;
- SDL (Security Development Lifecycle) описывает этапы разработки, включая оценку угроз, управление рисками и создание безопасных кодовых баз;
- Cyber Kill Chain описывает этапы атаки хакеров на информационную систему. Понимание того, какие приемы могут использоваться злоумышленниками, позволяет организациям разрабатывать меры по предотвращению атак;
- PCI DSS (Payment Card Industry Data Security Standard) — стандарт, разработанный владеющими платежными картами Visa, MasterCard, American Express, Discover и JCB компаниями для обеспечения безопасности личных данных в процессе их обработки, передачи и хранения. Хотя это не практическое техническое руководство по проведению тестов на проникновение, но оно позволяет получить достаточно полное представление о самом процессе тестирования.

Каждая методика имеет свои преимущества, а выбор той или иной зависит от конкретных потребностей организации и уровня безопасности, необходимого для ее информационных систем и данных.

03 Сбор открытой информации о цели

Итак, все организационные формальности улажены, вы заключили договор с компанией, собрали команду высококвалифицированных специалистов, определились с методикой и ролями, а теперь готовы приступить к аудиту.

Как уже говорилось, первый этап взлома любой ИС начинается со сбора максимального количества информации о цели. Получение данных из различных источников и веб-разведка являются неотъемлемой частью тестирования на проникновение и важным элементом проактивной защиты. Чем больше сетевых сервисов использует предприятие, тем больше цифровых следов оно оставляет в Глобальной сети, то же справедливо и для частных лиц: интернет помнит все. Понимание того, какую информацию можно найти, а также как ее обрабатывать и использовать, является ключевым моментом в деятельности как исследователя, так и специалиста по информационной безопасности.

В реальном мире специалисты, осуществляющие тесты на проникновения, до 90 % времени тратят именно на сбор и обработку данных о целевой системе. При работе с клиентом вы можете столкнуться с необходимостью не только найти уязвимые места в его инфраструктуре, но и предоставить информацию о том, как выглядит цифровой след организации в Глобальной сети. В ходе сбора информации может появиться необходимость ответить на следующие вопросы: какие домены предприятия отслеживаются в сети, есть ли сервисы, использующие уязвимые системы шифрования, есть ли общедоступные сервисы, использующие уязвимую конфигурацию (и многие другие).

Если задаться целью погрузиться с головой в мир изучения данных, стоит попробовать установить одну из созданных открытыми сообществами операционных систем, специально предназначенных для сбора и обработки информации: Buscador, Dora, CSI Linux и т. п.

Учтите, что практически никогда не удается получить всю информацию из одного-единственного источника. Данные приходится собирать из множества

различных мест (БД, HTML-код, новостные ленты и т. д.), чтобы впоследствии, как из кусочков мозаики, составить полную картину ИС организации.

На данном этапе выявляются слабые места сети, через которые возможно осуществить проникновение в систему. При правильном подходе можно выявить не только потенциально уязвимые места, но и возможные векторы атаки на обозначенную цель. В зависимости от размера организации объем собранной информации может варьироваться от десятка строк до сотен страниц текстовой информации. Важно не только собрать, но и грамотно обработать полученные данные.

Инструмент анализа каждый волен выбирать сам, будь то логические схемы, доска и маркеры или стикеры на стенах, — главное, чтобы в результате информация была обобщена и представлена в удобном и читабельном виде.

Что искать?

Для проведения успешной атаки нам пригодится **любая** доступная информация о предприятии.

Имея в своем распоряжении только название организации, обычно начинают сбор следующих данных:

- домены;
- сетевые адреса или сетевые блоки;
- место нахождения;
- контактная информация;
- новости о слиянии или приобретении;
- вакансии;
- ссылки на связанные с организацией веб-сервисы;
- различные документы;
- структура организации;
- сведения о сотрудниках.

Это только примерный список, продолжать его можно достаточно долго. Например, просмотрев вакансии предприятия, можно узнать, какие ИС используются внутри организации. Проанализировав же HTML-код домашней странички, можно найти ссылки на внутренние ресурсы.

От того, как проведен сбор информации, в будущем будет зависеть направление, тип и успешность атаки. Большая часть процесса сбора информации не требует специальных знаний — только умения пользоваться поисковыми системами. Зачастую они индексируют даже ту информацию, которую пытались скрыть от внешнего мира.

OSINT

С момента создания небольшого проекта, объединяющего несколько университетов США в одну информационную систему, до образования Глобальной сети прошло совсем немного времени. В наши дни доступ к Сети имеют миллиарды людей и в разы больше устройств со всего мира. С одной стороны, доступ к практически неограниченному объему информации и возможность самому создавать и публиковать различный контент принесли много благ современному обществу, однако есть и другая сторона медали. В современном информационном пространстве ведут незаконную деятельность множество преступных группировок, и технологии позволяют им осуществлять эффективную коммуникацию достаточно скрытно. Вторая проблема — это обычные люди, которые публикуют такую информацию, которая может принести определенный вред как им самим, так и организациям, где они работают, или даже странам, в которых они проживают. По примерным подсчетам, в этом году общий убыток от вышеописанных действий может достичь около 3 трлн долларов США. В связи с этим многие корпорации и государства начали активно инвестировать в OSINT (Open Source INTelligence, разведка по открытым источникам).

Аббревиатура OSINT обозначает всю публично доступную информацию. Хотя доподлинно неизвестно, когда впервые начали использовать этот термин, однако сейчас под ним подразумевается поиск и анализ данных, доступных в публичном пространстве. Считается, что США в период холодной войны стали одними из первых, кто широко применил такой подход. Справедливости ради стоит заметить, что не одни они занимались сбором и анализом доступной информации, это делало множество стран.

Приведем определение OSINT департамента обороны Соединенных Штатов: «Открытая разведывательная информация (OSINT) — это полученная из общедоступных источников и обработанная информация, распространяемая в соответствующей аудитории с целью удовлетворения конкретных потребностей разведки».

Впоследствии был создан национальный центр OSINT, задачей которого является сбор и анализ общедоступной информации как из онлайн-, так и из офлайн-источников. После серии терактов и принятия соответствующих законодательных актов эта организация была переименована и вошла в состав Центрального разведывательного управления.

OSINT выделяют из других методов поиска информации, так как все данные должны собираться только из открытых источников на законных основаниях, в том числе без нарушения авторских прав или вторжения в частную жизнь.

Во время поиска данных исследователи могут обнаруживать приватную информацию, доступ к которой не был ограничен должным образам. Таким путем, например, появлялась информация на известном сайте WikiLeaks. Использование такой информации противоречит философии OSINT и обозначается другим термином: NOSINT (Net-based Open Source INTelligence).

OSINT включает в себя множество источников информации, для поиска могут использоваться:

- интернет (форумы, блоги, сайты социальных сетей, сайты обмена видео, вики, записи Whois о зарегистрированных доменных именах, метаданные файлов, DarkNet-ресурсы, данные геолокации, IP-адреса, поисковые системы и все, что можно найти в интернете);
- традиционные средства массовой информации (телевидение, радио, газеты, книги, журналы);
- специализированные журналы, научные публикации, диссертации, материалы конференций, профили компаний, годовые отчеты, новости, профили сотрудников и резюме;
- фото и видео, включая метаданные;
- геопространственная информация (карты, коммерческие изображения продуктов).

OSINT широко используется хакерами и специалистами по информационной безопасности для сбора информации о конкретной цели в интернете. Он также считается ценным инструментом при проведении атак по типу социальной инженерии. Первый этап при любой методике тестирования на проникновение начинается с разведки (другими словами, с OSINT). Рисунок 3.1 показывает основные этапы тестирования на проникновение.

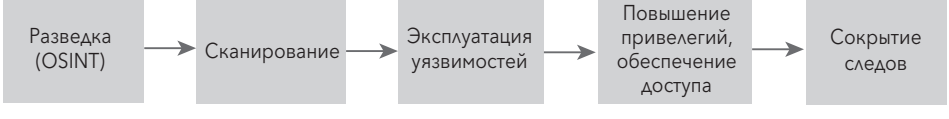


Рис. 3.1. Основные этапы тестирования на проникновение

Информацию OSINT можно собирать тремя основными методами: пассивным, полупассивным и активным. Выбор метода сбора зависит от контекста, а также от типа данных, которые вас интересуют.

Пассивный сбор данных. Это наиболее часто используемый тип сбора данных, потому что его основной целью является получение информации о цели только из общедоступных ресурсов. В этом случае ваша цель ничего не знает о вашей деятельности.

Этот вид поиска позволяет остаться анонимным и должен проводиться скрытно. С технической точки зрения этот тип сбора позволяет получить лишь ограниченную информацию о цели, потому что вы не отправляете никакого трафика на целевой сервер — ни прямо, ни косвенно. Основным недостатком данного типа является то, что вы можете получить устаревшую информацию.

Полупассивный сбор данных. Этот тип сбора данных подразумевает, что исследователь отправляет ограниченный трафик на целевые серверы для полу-

чения общей информации о них. Этот трафик максимально похож на типичный интернет-трафик, так как он не должен привлекать внимание к вашей деятельности. Вы проводите не глубокое исследование онлайн-ресурсов цели, а только их поверхностное изучение, не привлекая повышенного внимания со стороны администраторов целевой системы. Хотя этот тип сбора считается в некотором роде анонимным, но записи о ваших действиях все равно останутся в системных журналах; однако исследование необходимо проводить таким образом, чтобы эти записи нельзя было классифицировать как преднамеренный сбор информации.

Активный сбор данных. В этом сценарии вы напрямую взаимодействуете с системой, чтобы собрать информацию о ней. Цель может узнать о процессе сбора данных, поскольку осуществляющий его человек, скорее всего, использует инструменты автоматического сбора информации, работающие по определенному шаблону.

Такие инструменты позволяют получить информацию об открытых портах, наличии уязвимостей, приложениях и многое другое. Такой трафик будет выглядеть как подозрительный и оставит следы, которые могут быть найдены системой обнаружения вторжений (IDS) или системой предотвращения вторжений (IPS). Проведение атак по типу социальной инженерии в некоторых случаях также считается видом активного сбора информации.

Пассивный сбор данных

Мы начнем с рассмотрения инструментов для пассивного сбора данных. В этом разделе основной упор будет сделан на работу с такими поисковыми системами, как Google, и более специализированными — как Shodan.

Работа с поисковыми системами

Каждый день количество информации, находящейся в открытой части интернета, неуклонно растет. Можно быть полностью уверенным и в том, что также неуклонно увеличивается количество данных в темной и глубокой части Сети, но нам достоверно неизвестно, насколько быстро. Что же касается открытых данных, то согласно статистике, количество сайтов в сети уже превысило отметку в два миллиарда, а Google утверждает, что проиндексировал более сотни триллионов страниц (не путайте сайт и страницу — в данном контексте имеется в виду, что один сайт может содержать множество страниц).

В таком огромном количестве информации несложно и запутаться — как мы знаем, поисковые роботы постоянно сканируют страницы на наличие изменений и ссылок, затем, при необходимости, обновляют свою базу данных. В свою очередь, когда пользователь запрашивает какую-либо информацию, он обычно получает огромное количество результатов, которые представляют собой смесь видеофайлов, картинок, тестовой и другой информации.