Л315. Типы отчетов в Kali Linux,

Анализ результатов исследования и документирование очень важны для профессионального тестирования на проникновение. Каждый запуск инструментов тестирования должен регистрироваться, а результаты работы каждого инструмента следует воспроизвести без искажений. Имейте в виду, что представление клиентам результатов тестирования — важная часть самого теста. Возможно, после принятия мер по устранению уязвимости потребуется дополнительное тестирование, с помощью которого будет проверено, насколько эффективны были меры по улучшению безопасности. Точное документирование выполненных вами действий поможет в будущем провести дополнительное тестирование.

Правильное документирование тестирования подразумевает запись всех выполненных действий и в случае возникновения у клиента инцидентов, не связанных с испытанием на проникновение, позволит отследить все шаги. Подробная запись ваших действий может быть очень утомительной, но, как профессиональный испытатель на проникновение, вы не должны упускать из виду этот этап.

Составление документации, подготовка докладов и их представление — главные задачи, которые должны реализовываться на постоянной основе. Эта глава содержит подробные инструкции, которые помогут вам в согласовании документации и составлении отчетности. Мы рассмотрим следующие темы.

- Проверка результатов, гарантирующая, что сообщаются только подтвержденные данные.
- Распределение отчетов по типам. Чтобы наилучшим образом отразить интересы соответствующих органов, участвующих в проекте тестирования на проникновение, типы отчетов следует обсудить с исполнительной, управленческой и технической точек зрения.
- Составление презентации. Раздел с презентацией должен содержать общие советы и рекомендации в таком виде, чтобы клиент мог понять приведенную информацию.
- Выполнение нужных процедур после тестирования. Здесь следует привести все меры и рекомендации, предлагаемые для устранения выявленных уязвимостей.

Они также должны быть включены в отчет, чтобы консультативная группа по восстановлению соответствующей организации могли их использовать. Данный вид деятельности является довольно сложным и по соображениям безопасности требует углубленного знания целевой инфраструктуры.

В последующих разделах вы получите полные сведения о том, как подготовить документацию, отчет и презентацию. Даже небольшая ошибка в отчете может привести к юридической проблеме. Созданный отчет должен соответствовать вашим выводам и показывать обнаруженные в целевой среде потенциальные недостатки. Если в требованиях клиента есть особые условия, их следует указать. Кроме того, в отчете нужно четко прописать методы работы злоумышленника, применяемые им инструменты и средства, а также список обнаруженных уязвимостей. Прежде всего вы должны сосредоточиться на слабых местах системы, а не на объяснении процедур, используемых для обнаружения этих слабых мест.

Технические условия

Требуется ноутбук или настольный компьютер с минимальным объемом оперативной памяти 6 Гбайт, четырехъядерный процессор и 500 Гбайт места на жестком диске. В качестве операционной системы используется Kali Linux 2018.2 или 2018.3. Она может быть установлена как на жесткий диск, так и в качестве виртуальной машины. Система также может загружаться с SD-карты или с USB-накопителя.

Документация и проверка результатов

В большинстве случаев, чтобы убедиться в том, что ваши результаты действительно пригодны для использования, потребуется глубокая проверка уязвимости. Усилия по минимизации последствий могут быть очень дорогостоящими, поэтому проверка уязвимости является критически важной задачей. В нашей практике уже было несколько ситуаций, когда люди просто запускали инструмент, получали результаты и представляли их непосредственно своим клиентам. Такая безответственность и отсутствие контроля может привести к серьезным последствиям и к краху вашей карьеры. Кроме того, неверные сведения, полученные от испытателя на проникновение, могут поставить под угрозу корректную работу самой системы клиента, так как он будет думать, что система защищена. Поэтому в тестовых данных не должно быть ошибок и несоответствий.

Ниже приведены несколько процедур, которые могут помочь вам в документировании и проверке результатов теста.

- **Записывайте все заметки.** Сделайте подробные заметки о каждом шаге, который вы сделали во время сбора информации, обнаружения, перечисления, сопоставления, эксплуатации уязвимостей, эскалации привилегий — на всех этапах процесса тестирования на проникновение.

- **Составьте шаблон заметок.** Сделайте шаблон заметок для каждого инструмента, который вы применяете. В шаблоне должны быть четко прописаны цель, варианты выполнения исследования и профили, выбранные для целевой оценки, а также должно быть место для записи соответствующих результатов тестирования. Кроме того, перед тем, как делать окончательный вывод по результатам работы каждого инструмента, повторите тест по крайней мере дважды. Таким образом, вы подтвердите результаты проведенных испытаний и застрахуете себя от всех непредвиденных ситуаций. Например, если вы сканируете порты с помощью инструмента Nmap, следует разработать шаблон со всеми необходимыми разделами, касающимися цели использования, целевого хоста, параметров выполнения и профилей (обнаружение службы, тип ОС, MAC-адрес, открытые порты, тип устройства и т. д.), и соответственно документировать результаты работы инструмента.
- **Гарантируйте надежность.** Полагаться на один инструмент (например, для сбора информации) неразумно. Это может привести к неточностям в вашем тестировании на проникновение. Мы настоятельно рекомендуем вам последовательно провести каждый тест с применением как минимум двух разных инструментов соответствующего профиля. Это обеспечит прозрачность процесса верификации, повышение производительности и уменьшение количества ложных срабатываний. Кроме того, где это возможно, стоит проверить некоторые условия вручную и использовать свои знания и опыт для проверки всех полученных результатов.

Типы отчетов

После сбора и проверки результатов теста и перед отправкой их целевой заинтересованной стороне вы должны собрать их в последовательный и структурированный отчет. Существует три различных типа отчетов; каждый из них имеет свои собственные схему и план, соответствующие интересам предприятия, участвующего в проекте тестирования на проникновение:

- исполнительный доклад;
- отчет для руководства;
- технический отчет.

Эти отчеты готовятся в соответствии с уровнем технических знаний и способностью клиента понять передаваемую пентестером информацию. Далее мы рассмотрим все типы отчета и основные элементы структуры отчетности, которые могут потребоваться для достижения вашей цели.

Отчеты должны соответствовать политике неразглашения, юридическим договоренностям и соглашению о тестировании на проникновение.

Исполнительный доклад

Исполнительный доклад представляет собой один из видов доклада об оценке. Это наиболее краткая форма доклада, содержащая с точки зрения бизнес-стратегии общую информацию о результатах тестирования на проникновение. Отчет подготовлен для руководителей уровня C в рамках целевой организации (CEO, CTO, CIO и т. д.). В нем должны быть такие основные разделы.

- **Цель проекта.** Определяет взаимно согласованные между вами и вашим клиентом критерии для проекта тестирования на проникновение.
- **Классификация рисков уязвимости.** В этом разделе объясняются уровни риска (критический, высокий, средний, низкий и информационный), отраженные в отчете. Эти уровни должны быть четко дифференцированы по степени тяжести и должны отражать риски нарушения безопасности.
- **Резюме.** В этом разделе кратко описываются цель и задачи тестирования на проникновение в соответствии с определенной методологией. Здесь также фиксируется количество обнаруженных и успешно эксплуатируемых уязвимостей.
- **Статистика.** Подробно описываются уязвимости, обнаруженные в инфраструктуре целевой сети. Они также могут быть представлены в виде круговой диаграммы или в любом другом интуитивно понятном формате.
- **Матрица рисков.** В этом разделе классифицируются все найденные уязвимости, определяются ресурсы, которые могут быть потенциально затронуты, и в сокращенном формате перечисляются рекомендации.

Это идеальный формат отчетности. Чтобы отчет был выразительным, при его подготовке следует иметь в виду, что вы не обязаны отражать технические результаты оценки, а должны предоставить фактическую информацию. Доклад должен занимать от двух до четырех страниц. Примеры докладов см. в разделе «Дополнительное чтение» в конце этой главы.

Отчет для руководства

Отчет для руководства, как правило, охватывает такие вопросы, как нормативное регулирование и оценка соблюдения всех норм безопасности. На практике исполнительный доклад следует расширить, включив в него ряд разделов, которые могут представлять интерес для руководителей и оказать помощь при возможном судебном разбирательстве. Ниже приводятся основные разделы доклада.

- **Достижение соответствия.** Содержит список известных стандартов и сопоставляет каждый из его разделов или подразделов с текущей ситуацией в области безопасности. В нем следует указать любые нарушения нормативных положений, которые были выявлены и которые могут непреднамеренно подвергнуть опасности целевую инфраструктуру и создать серьезную угрозу.

- **Методология тестирования.** Это описание должно быть кратким, но подробным, что поможет руководителям понять весь цикл тестирования на проникновение.
- **Предположения и ограничения.** Здесь описываются все ограничения и другие факторы, не позволившие испытателю на проникновение достичь определенной цели.
- **Управление изменениями.** Иногда это считается частью процесса восстановления. Однако данный отчет в основном содержит описание стратегических методов и процедур, которые обрабатывают все изменения в контролируемой ИТ-среде. Предложения и рекомендации, вытекающие из оценки безопасности и позволяющие свести к минимуму воздействие неожиданного события на сервис, должны соответствовать любым изменениям в процедурах.
- **Управление конфигурациями.** Основное внимание уделяется согласованности функциональной работы и производительности системы. В контексте безопасности нужно фиксировать любые изменения в системе, которые могут быть внесены в целевую среду (аппаратное, программное обеспечение, физические атрибуты и др.). Эти изменения должны контролироваться и учитываться для поддержания состояния конфигурации системы.

Ваша обязанность, как ответственного и грамотного испытателя на проникновение, — прежде всего уточнить все условия руководства и только после этого продолжать цикл испытаний. Это действие, безусловно, включает в себя индивидуальные беседы и соглашения о критериях оценки конкретных целей, в которых оговариваются все ограничения и рамки проводимого исследования, а также пути проведения испытания. Здесь следует обговорить все действующие на время проведения теста ограничения в исследуемой системе. Должны ли быть вносимые изменения постоянными и можно ли менять текущее состояние системы при внесении изменений в конфигурацию. На основании этих факторов формируется понимание текущего состояния безопасности в целевой среде, и после технической оценки можно давать какие-либо предложения и рекомендации.

Технический отчет

Доклад о технической оценке играет очень важную роль в решении вопросов безопасности, поднятых в ходе тестирования на проникновение. Отчет такого типа обычно разрабатывается для технических работников, которые хотят понять основные функции безопасности, обрабатываемые целевой системой. В докладе должны быть подробно описаны любые уязвимости, то, как их можно использовать, какое влияние они могут оказать на бизнес и как можно разработать решения для предотвращения любых известных угроз. Доклад о защите сетевой инфраструктуры должен соответствовать принципам безопасности «все в одном». До сих пор мы уже обсуждали основные разделы исполнительных и управленческих отчетов. В техническом докладе мы предоставляем всю вышеперечисленную информацию

в расширенном виде. Кроме того, в технический отчет следует включить специальные темы, которые могут вызвать особый интерес у технической группы целевой организации. Иногда такие вопросы, как цели проекта, классификация рисков уязвимости, матрица рисков, статистика, методология тестирования, допущения и ограничения, также являются частью технического отчета. Технический отчет состоит из следующих разделов.

- **Вопросы безопасности.** Вопросы безопасности, поднятые в процессе тестирования на проникновение, должны быть подробно прописаны. Поэтому для каждого применяемого метода атаки необходимо указать список участвующих в исследовании ресурсов и последствия этого исследования, исходные данные запроса и ответ, смоделированные данные запроса на атаку и ответ, предоставить ссылку на внешние источники для группы по восстановлению и дать профессиональные рекомендации по устранению обнаруженных уязвимостей в целевой ИТ-среде.
- **Карта уязвимостей.** Содержит список обнаруженных уязвимостей в целевой инфраструктуре, каждая из которых должна быть сопоставлена с идентификатором ресурса (например, IP-адресом и именем цели).
- **Карта эксплойтов.** Здесь предоставляется список успешно проверенных эксплойтов, которые работали против цели. Важно также упомянуть, был ли источник частным или публичным. Возможно, неплохо было бы рассказать об источнике кода эксплойта и о том, как долго он был доступен.
- **Передовой опыт.** В этом разделе следует показать все наилучшие разработки и оперативные процедуры безопасности, которых не хватило целевой системе при попытке проникновения. Например, в среде крупного предприятия развертывание системы безопасности пограничного уровня может эффективно заблокировать большинство внешних угроз еще до их проникновения в корпоративную сеть. В таких решениях не требуется техническое взаимодействие с производственными системами или устаревшим кодом.

В целом технический доклад позволяет соответствующим членам заинтересованной организации ознакомиться с реальной ситуацией на месте. Такой отчет играет важную роль в процессе управления рисками и, вероятно, будет использоваться для формулирования практических задач по восстановлению.

Отчет о тестировании проникновения в сеть

Так же как существуют различные типы тестирования на проникновение, существуют различные типы структур отчетов. Мы представили общую версию отчета об испытании на проникновение, который может быть дополнен соответствующими данными практически для любого другого типа тестирования на проникновение (например, веб-приложения, брандмауэра, беспроводной и обычной сети). В дополнение к списку, приведенному ниже, вам понадобится титульная страница,

где будет указано название компании, проводящей тестирование, тип отчета, дата сканирования, имя автора, номер редакции документа и краткая информация об авторских правах и конфиденциальности.

Ниже приводятся пункты отчета о тестировании на проникновение в сети:

- правовые положения;
- соглашение об испытании на проникновение;
- введение;
- цель проекта;
- допущения и ограничения;
- шкала рисков уязвимости;
- управляющее резюме;
- матрица рисков;
- методика тестирования;
- угроза безопасности;
- рекомендации;
- карта уязвимостей;
- карта эксплойтов;
- оценка соответствия;
- управление изменениями;
- передовой опыт;
- приложения.

Как вы можете видеть, мы объединили все типы отчетов в один полный отчет с конкретной структурой. Каждый из этих разделов может иметь собственные соответствующие подразделы, которые могут более подробно классифицировать результаты теста. Например, в приложениях могут быть перечислены технические детали и данные об анализе процесса тестирования, журналов деятельности, исходные данные из различных инструментов безопасности, детали проведенного исследования, ссылки на любые интернет-источники и глоссарий. В зависимости от запрашиваемого вашим клиентом типа отчета вы должны еще до начала испытаний понять все аспекты проводимого теста на проникновение.

Подготовка презентации

Для успешного проведения презентации полезно понимать технические возможности и цели заказчиков этого исследования. Вам нужно будет преподнести материал в соответствии с требованиями заказчика, иначе вы можете столкнуться с негативной реакцией. Ваша ключевая задача — заставить клиента понять потенциальные факторы риска, грозящие областям, которые вы тестируете. Например, специалистам на исполнительном уровне может не хватить времени на изучение всех деталей векторов атаки методами социальной инженерии, но им будет интерес-

но узнать текущее состояние безопасности и то, какие меры должны быть приняты для повышения уровня безопасности.

Хотя формальной процедуры для создания и представления результатов нет, вам необходимо придерживаться профессионального подхода, чтобы удовлетворить требования заказчиков. Вы обязаны изучить и понять целевую среду, оценить уровень квалификации технических специалистов и помочь им узнать вас, а также определить основные фонды организации.

Указание на недостатки текущего уровня безопасности и выявление всех уязвимостей поможет вам подготовить качественный и профессиональный отчет. Помните, что вы должны придерживаться полученных вами фактов и выводов, доказывать их на техническом уровне и соответствующим образом консультировать команду по восстановлению. Поскольку все это подразумевает непосредственное общение, настоятельно рекомендуем заранее подготовиться к ответам на любые вопросы, подкрепляя их фактами и цифрами.

Процедуры после тестирования

Меры по восстановлению, корректирующие шаги и рекомендации — это понятия, относящиеся к процедурам, проводимым после проведения испытаний. Во время этих процедур вы выступаете советником группы по восстановлению в целевой организации. В этом качестве вам может потребоваться взаимодействовать с различными специалистами с разным уровнем знаний и опытом. Поэтому имейте в виду, что ваш внешний вид и навыки работы в сети могут иметь большое значение. Кроме того, невозможно обладать всеми знаниями, требуемыми целевой ИТ-средой, особенно если вы не специалист в этой области бизнеса. В таких ситуациях без какой-либо поддержки со стороны группы экспертов довольно сложно обрабатывать и исправлять конкретный уязвимый ресурс. Мы разработали несколько общих правил, которые могут помочь вам в разъяснении важных рекомендаций вашему клиенту.

- Пересмотрите схему сети и проверьте условия эксплуатации на уязвимых ресурсах, которые указаны в отчете.
- Сконцентрируйтесь на схемах и данных защиты пограничного уровня, чтобы уменьшить количество угроз безопасности, прежде чем они одновременно нанесут удар по серверам и рабочим станциям.
- Атакам на стороне клиента или с применением методов социальной инженерии почти невозможно противостоять, но опасность такого нападения можно уменьшить. Для этого следует уделить особое внимание обучению сотрудников новейшим контрмерам.
- Для уменьшения негативных последствий от возможных атак необходимо четко выполнять рекомендации, которые предложил испытатель на проникновение.
- При необходимости воспользуйтесь проверенными и надежными сторонними решениями (IDS/IPS, брандмауэры, системы защиты контента, антивирусы, технологии IAM и т. д.).

- Используйте подход «разделяй и властвуй», чтобы отделить зоны защищенной сети от небезопасных или открытых объектов целевой инфраструктуры.
- Укрепляйте навыки разработчиков в кодировании безопасных приложений, которые являются частью целевой ИТ-среды. Оценка безопасности приложений и выполнение проверки кода могут повысить информационную безопасность организации.
- Применяйте меры физической безопасности. Реализуйте многоуровневую стратегию доступа с механическим и электронным контролем доступа, оповещениями о вторжении, мониторингом CCTV и идентификацией персонала.
- Регулярно обновляйте все системы безопасности, чтобы обеспечить конфиденциальность, целостность и доступность.
- Проверьте все документированные решения, представленные в качестве рекомендаций, чтобы исключить возможность вторжения или эксплуатации.

Использование структуры Dradis для составления отчетности по тестированию на проникновение

Система Dradis — это удобная система для составления отчетности. Запуск тестов и использование большого количества инструментов может быть очень увлекательным. Однако, когда дело доходит до организованной документации, этот процесс может показаться довольно скучным. Здесь следует учесть, что в отчет необходимо включить не только файлы результатов исследований, но и скриншоты этих результатов. Необходимо также документировать все команды, которые использовались во время исследования. Здесь вам может помочь фреймворк Dradis. Это программа с простым в использовании интерфейсом, которая поддерживает плагины для многих инструментов и позволяет легко настраивать контрольные списки.

Фреймворк Dradis можно найти в меню Kali. Для этого щелкните кнопкой мыши на строке Applications (Приложения), далее выберите 12 Reporting Tools (12 инструментов отчетности), а затем Dradis framework (фреймворк Dradis).

Dradis также можно запустить непосредственно из терминала, введя в командную строку команду `dradis` (рис. 14.1).

Оба предыдущих метода приводят к открытию веб-интерфейса Dradis в браузере. URL-адрес этого интерфейса — `127.0.0.1:3000/setup`. Введите пароль, который будут использовать все, кто обращается к серверу, а затем выберите Create shared password (Создать общий пароль).

Введите имя пользователя и пароль, а затем нажмите Let me in! (Впустить меня!). На экране появится панель управления Dradis CE (Community Edition). Dradis CE позволяет пользователю создавать в качестве методологии контрольные списки. Для создания методологии щелкните на строке Methodologies (Методологии) (на левой панели) или на строке +Add a testing methodology (Добавить методологию тестирования), которая находится в разделе Methodology progress (Прогресс методологии) в главном окне (рис. 14.2).

```
root@kali:~# dradis
[i] Something is already using port: 3000/tcp
COMMAND  PID   USER   FD   TYPE  DEVICE SIZE/OFF NODE NAME
ruby2.5 3039 dradis   12u  IPv6 1727348      0t0  TCP localhost:3000 (LISTEN)
ruby2.5 3039 dradis   13u  IPv4 1727349      0t0  TCP localhost:3000 (LISTEN)

UID        PID  PPID  C STIME TTY      STAT   TIME CMD
dradis    3039     1  0 Aug07 ?        Ssl    0:27 /usr/bin/ruby2.5 bin/rails se

[*] Please wait for the Dradis service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000

● dradis.service - Dradis web application
```

Рис. 14.1. Запуск dradis

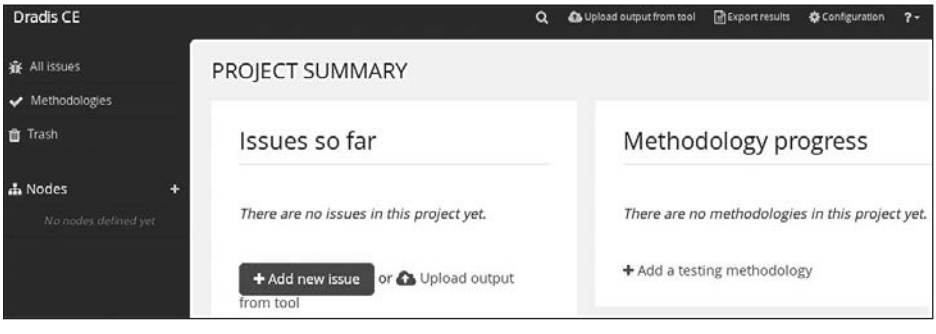

Рис. 14.2. Добавление методологии

Dradis дает пользователю возможность либо создать новую методологию, либо выбрать между другими пакетами соответствия (которые должны быть заранее загружены). Если вы для своей методологии хотите использовать определенный шаблон, можно выбрать пункт Download more (Загрузить больше), чтобы направить пользователя на страницу пакетов соответствия (https://dradisframework.com/academy/industry/compliance/) с различными имеющимися пакетами, включая следующее:

- инструмент аудита соответствия HIPAA;
- отчет Offensive Security Certified Professional (OSCP);
- руководство по тестированию OWASP v4;
- техническое руководство PTES.

Чтобы создать контрольный список для методологии, выберите параметр New checklist (Новый контрольный список) (рис. 14.3).

Дайте новому контрольному списку имя, а затем нажмите Add to Project (Добавить в проект). Будет создан пустой контрольный список с двумя заголовками разделов (рис. 14.4).

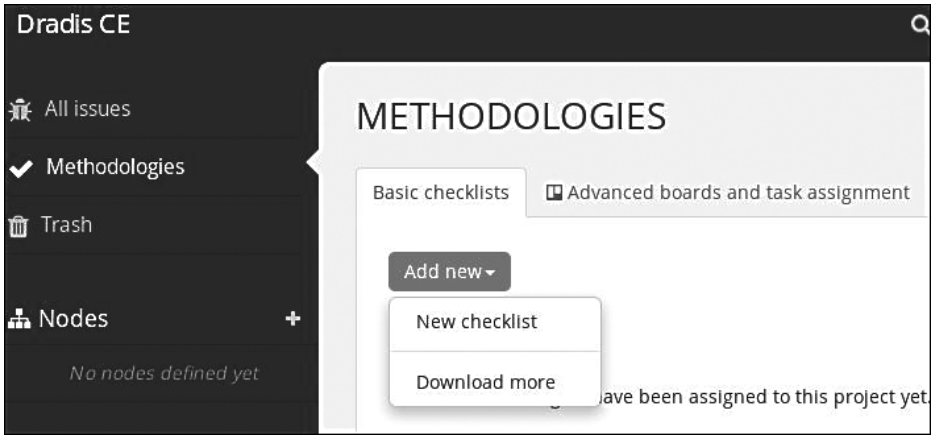

Рис. 14.3. Выбор контрольного списка

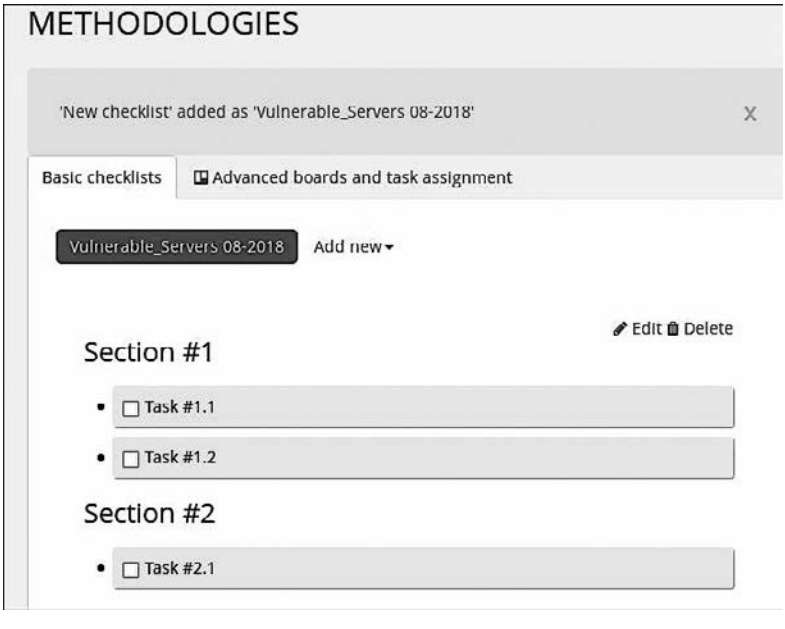

Рис. 14.4. Контрольный список создан

Чтобы изменить разделы и задачи, нажмите кнопку Edit (Изменить) и измените содержимое XML-кода. Для примера мы добавили `Scanning` в область `Section 1`. После завершения редактирования прокрутите список вниз, до нижней части XML-файла, и нажмите кнопку Update methodology (Обновить методологию) (рис. 14.5).

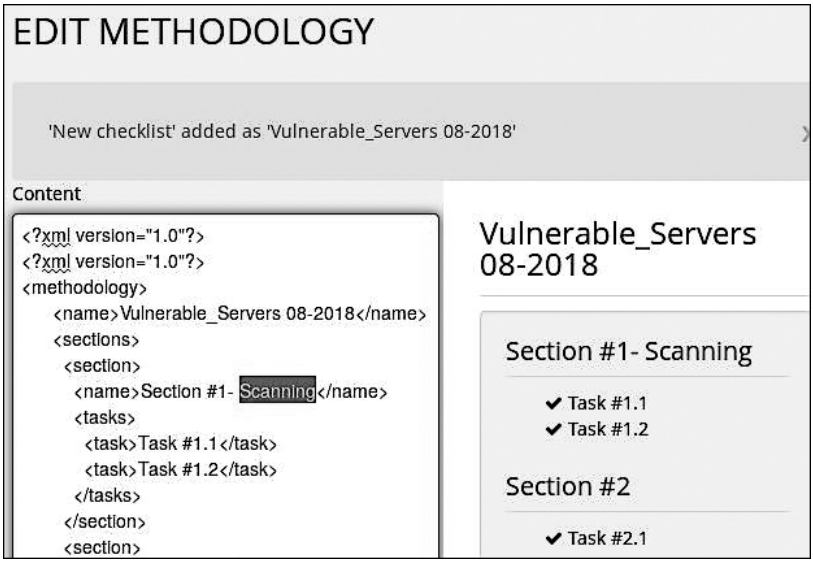

Рис. 14.5. XML-код изменен

На левой панели щелкните кнопкой мыши на Nodes (Узлы), чтобы добавить устройства, с помощью которых Dradis CE будет создавать отчет. Если вы работаете с несколькими узлами, введите IP-адреса узлов (по одному в строке) и для завершения нажмите кнопку Add (Добавить) (рис. 14.6).

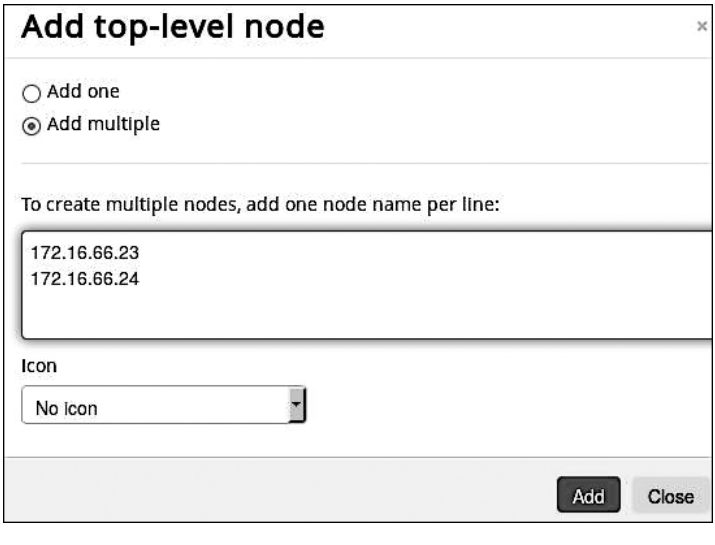

Рис. 14.6. Узлы добавлены

Чтобы открыть панель Nodes Summary (Сводка по узлам), в разделе Notes (Примечания) щелкните на отдельном IP-адресе. Слева откроется панель сводки по узлам. Здесь вы можете добавить данные, заметки, а также, если это необходимо, указать подузел (рис. 14.7).

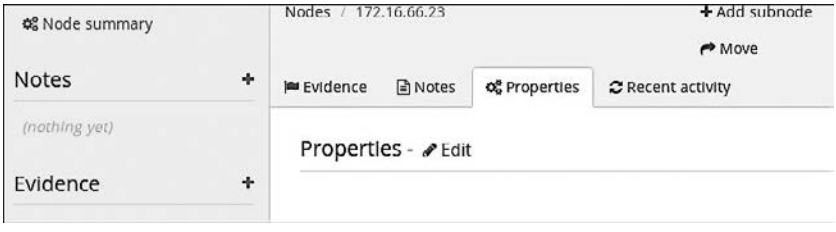

Рис. 14.7. Добавление данных

Dradis с помощью плагинов может работать с результатами работы таких инструментов, как Acunetix, Burp, Metasploit, Nessus, nikto, OpenVas, что упрощает процесс составления отчетов. В верхней части панели мониторинга нажмите Upload output from tool (Загрузить вывод из инструмента). Выберите инструмент и укажите файл для загрузки в Dradis, как показано на рис. 14.8.

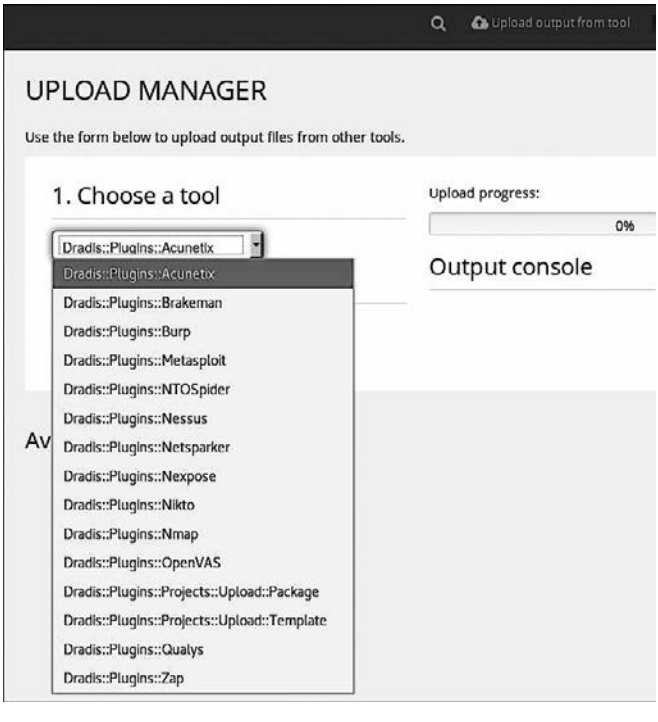

Рис. 14.8. Выбор инструмента для загрузки

Для завершения отчета нажмите кнопку Export results (Экспорт результатов) в верхней части панели мониторинга. Отчеты могут быть созданы в форматах CSV и HTML, а пользовательские отчеты — в форматах Word и Excel. Чтобы создать файл, выберите шаблон и нажмите кнопку Export (Экспорт) (рис. 14.9).

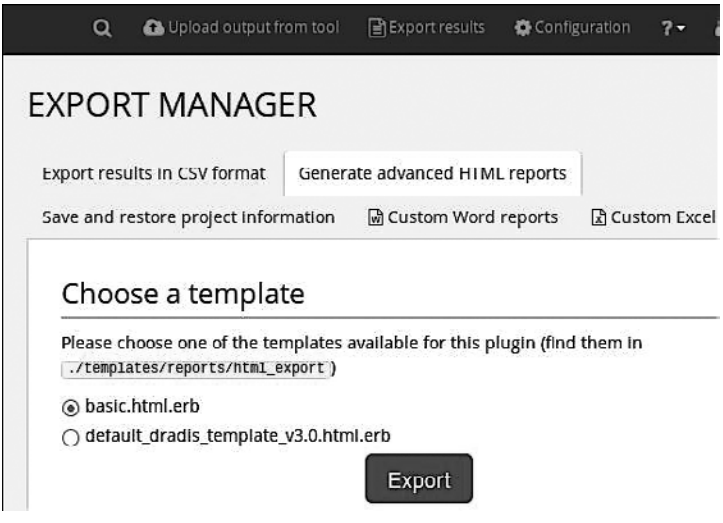

Рис. 14.9. Создание файла отчета

Инструменты отчетности по тестированию на проникновение

Dradis не единственный инструмент для создания отчетности, доступный в Kali Linux 2018. Если выбрать меню Applications (Приложения), а затем Reporting Tools (Инструменты отчетов), вы увидите другие доступные инструменты, такие как Faraday IDE, MagicTree и pipal (рис. 14.10).

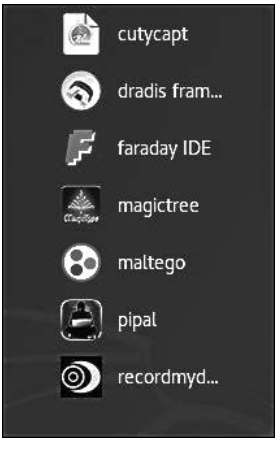

Рис. 14.10. Инструменты для создания отчетности

Faraday IDE

Faraday IDE — еще один инструмент, созданный для поддержания совместной работы с использованием примерно 40 встроенных инструментов для создания отчетов. Поддерживаемые плагины позволяют задействовать Metasploit, Nmap и Nessus. Faraday IDE поддерживает концепцию многопользовательского тестирования на проникновение в среде, функционирующей точно так же, как и при запуске инструментов в терминале по отдельности.

Для запуска Faraday IDE выберите меню Applications (Приложения), а затем щелкните на строке Faraday IDE. После загрузки интерфейса для начала работы с ним назовите рабочую область (рис. 14.11).

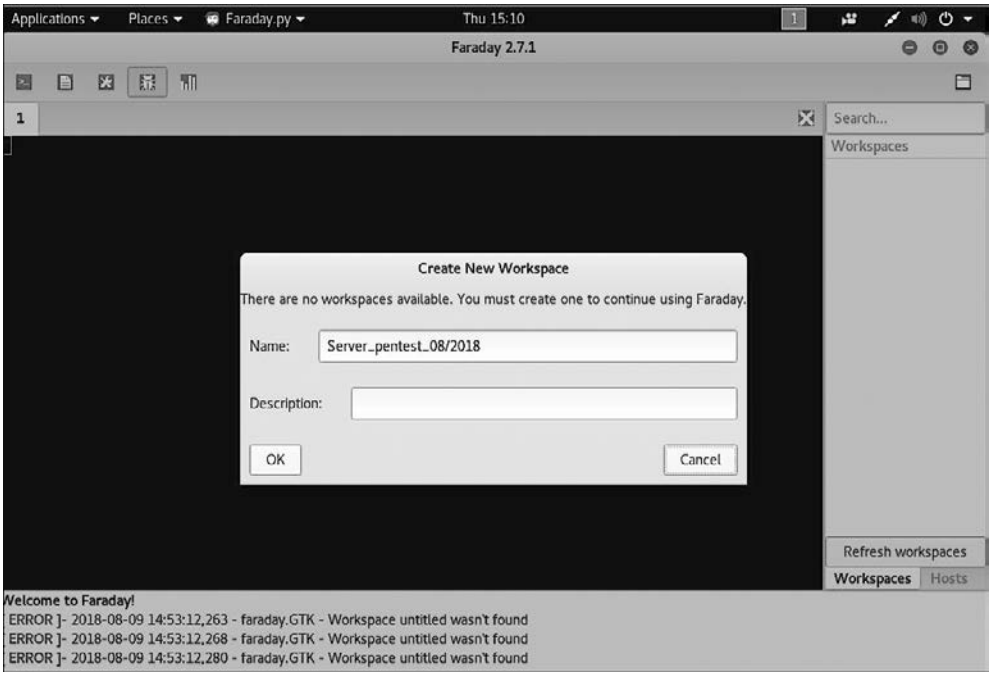

Рис. 14.11. Рабочая область названа

Более подробную информацию об установке и использовании Faraday IDE можно найти по адресу https://github.com/infobyte/faraday/wiki.

MagicTree

MagicTree — еще один инструмент, предназначенный для генерации отчетов и доступный в Kali Linux. Пользователей Nmap этот инструмент может особенно заинтересовать, так как он позволяет запускать сканирование Nmap непосредственно из самого приложения. Для запуска MagicTree выберите меню Applications (Приложения), а затем пункт Reporting Tools (Инструменты отчетов). Инструмент должен выглядеть примерно так (рис. 14.12).

Более подробную информацию об использовании Magic Tree можно найти по адресу https://www.gremwell.com/using_magictree_quick_intro.

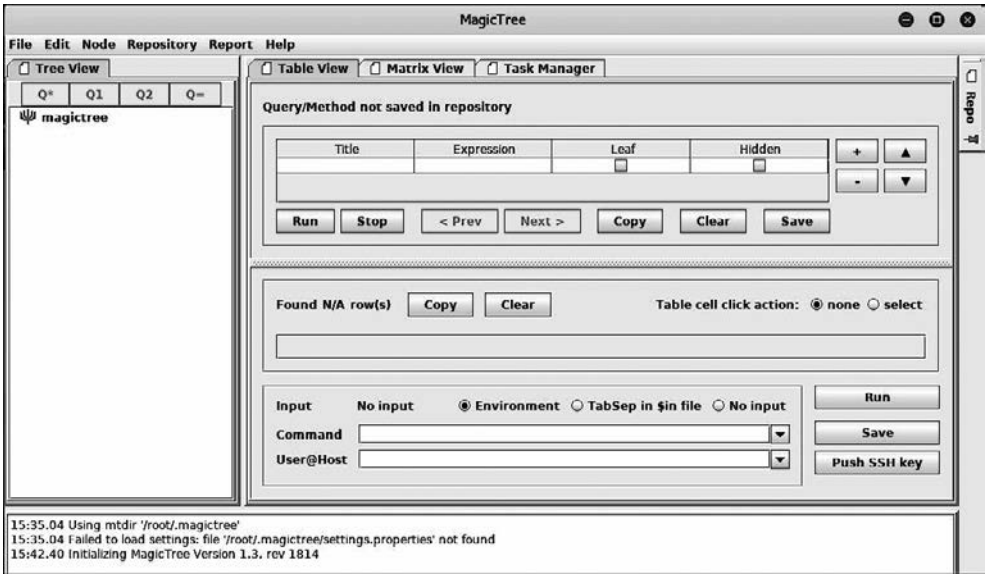

Рис. 14.12. Инструмент MagicTree запущен

Резюме

В этой главе мы рассмотрели основные шаги, позволяющие создать отчет на основании тестирования на проникновение, и обсудили главные особенности представления этого отчета клиенту. Сначала мы подробно разобрали методы документирования результатов с помощью конкретных инструментов и предложили для получения конечных результатов не полагаться на отдельные инструменты. Убедитесь, что при необходимости вы сможете вручную проверить результаты тестирования и что ваши навыки не устарели.

Затем мы рассмотрели инструменты для создания отчетности. При этом основное внимание уделялось фреймворку Dradis, а также Faraday IDE и MagicTree. Рекомендуем вам попробовать в работе каждый из этих инструментов.

Наконец, мы надеемся, что вам понравилась эта книга, и желаем всего наилучшего в вашей работе в сфере кибербезопасности и тестирования на проникновение.

Вопросы

1. Каковы три основных типа отчетов, представляемых клиентам, о тестировании на проникновение?
2. Какие значения отражает матрица рисков в исполнительном докладе?
3. В чем назначение карты уязвимостей?

4. В чем назначение карты эксплойтов?
5. Из чего состоит методология тестирования?
6. Как можно минимизировать атаки на стороне клиента или атаки методами социальной инженерии?

Дополнительные материалы

- Образец отчета о тестировании на проникновение: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf.
- Советы по написанию отчета о тестировании на проникновение: https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343.
- Примеры отчетов Nessus: https://www.tenable.com/products/nessus/sample-reports.
- Образец технического отчета о проникновении: https://tbgsecurity.com/wordpress/wp-content/uploads/2016/11/Sample-Penetration-Test-Report.pdf.