УДК 004.056

С.А. Туманов

Средства тестирования информационной системы на проникновение

Тестирование на проникновение имеет большое количество векторов атаки. Аудитору важно не упустить всевозможные варианты проникновения. В статье рассматривается формирование сценариев проникновения, в которых обозначается последовательность действий аудитора. Предлагается поэтапное выполнение теста на проникновение информационной системы.
Ключевые слова: тестирование на проникновение, разведка, аудит, информационная система.

В настоящее время ни одна современная организация в своей деятельности не может обойтись без информационных технологий. Множество бумажных носителей информации заменяются на цифровые. Процессы взаимодействия предприятия и клиента активно переводятся на режим «онлайн», в результате чего клиент получает необходимые данные с помощью информационных систем.

В 2014 г. Министерство внутренних дел РФ зарегистрировало в нашей стране приблизительно 11 тыс. преступлений в сфере телекоммуникаций и компьютерной информации. Об этом сообщил начальник Бюро специальных технических мероприятий МВД России Алексей Мошков в ходе «Инфофорума–2015» [1].

Согласно результатам отчета компании Symantec – NORTON REPORT 2013 [2]:

– 50% пользователей старше 18 лет становились жертвами кибератак или неприятных ситуаций в Интернете;

– более 1 млн пострадавших в день или 122 человек в секунду;

– $113 млрд – общая сумма прямых убытков всего за 12 месяцев.

Для того чтобы обезопасить собственною информационную систему ряд организаций регулярно проводят тестирование на проникновение – выявление возможных уязвимостей, используемых для создания сценария проникновения в информационно-вычислительную сеть предприятия. Тестирование на проникновение позволяет получить объективную оценку возможности (и насколько легко эту возможность использовать) осуществить несанкционированный доступ к ресурсам корпоративной сети или сайта.

Тестирование на проникновение (тест на преодоление защиты, penetration testing, pentest, пентест) – частный случай аудита информационной безопасности. Процесс тестирования на проникновение является моделированием реальных действий злоумышленника – поиск уязвимостей системы защиты и их последующая эксплуатация. Эта услуга позволяет получить независимую оценку и экспертное заключение о состоянии защищенности информации ограниченного распространения.

Главной целью тестирования на проникновение является выявление уязвимостей, которые могут быть успешно эксплуатированы злоумышленником [7]. Проникновение в информационно-вычислительную сеть заказчика не означает, что тестирование завершено. Даже после проникновения рассматриваются другие варианты атак, с помощью которых можно проникнуть в информационную систему (ИС).

Преимущества тестирования на проникновение:

– позволяет эффективно продемонстрировать возможность проникновения в ИС и выявить слабые места в обеспечении информационной безопасности;

– позволяет выделить критические проблемы безопасности, требующие непосредственного внимания;

– позволяет выделять финансовые и материальные ресурсы на обеспечение безопасности ИС на тех участках, на которых это требуется больше всего;

– тестирование подразумевает использование различных сценариев, учитывающих особенности ИС предприятия.

Недостатки тестирования на проникновение:

– аудитор связан временными и многими контрактными ограничениями в отличие от настоящего злоумышленника.

Информация выше, относящаяся к аудиту ИБ, является актуальной для тестирования на проникновение. Существует два основных типа тестирования на проникновение:

– внутреннее тестирование («White Box», модель «белого ящика») – тестирование проводится с расчетом на то, что злоумышленник действует внутри организации и знает схему ИС;

– внешнее тестирование («Black Box», модель «черного ящика») – тестирование выполняется из общедоступных сетей и моделирует поведение злоумышленника, нападающего из Интернета либо из-за границы контролируемой зоны заказчика.

В отличие от аудита ИБ тестирование на проникновение имеет классификацию по осведомленности сотрудников учреждения о проведении работ:

– режим «Black Hat» – о проведении тестирования знают только руководители службы ИБ. В таком режиме удается проверить уровень оперативной готовности к атакам сетевых администраторов и администраторов ИБ;

– режим «White Hat» – никаких мер сокрытия атакующих действий не применяется, аудитор работает в постоянном контакте с ИБ-службой заказчика.

Аудитор вправе использовать любые из возможных злоумышленником атак для достижения цели, если это не противоречит условиям пентеста. Список возможных атак довольно обширен, и без определенного сценария и информации сложно осуществить проникновение в систему [8, 9, 10].

Главное отличие злоумышленника от аудитора в том, что аудитор только обнаруживает уязвимости и пытается их использовать без компрометации информационной системы. Злоумышленник использует уязвимости для проникновения в информационную систему и последующего сбора компрометирующей информации организации. Аудитор ограничен договором, он не сможет сделать больше, чем прописано в его условиях.

Основные фазы тестирования на проникновение:

1. Разведка.
2. Внешнее сканирование.
3. Получение доступа.
4. Внутреннее сканирование.
5. Получение доступа к определённой информации (хостам).

В большинстве случаев тестирование прекращается на этапе 3, но если заранее не обговорены границы проведения аудита (либо необходимо протестировать сеть и от внутреннего нарушителя), то тестирование продолжается.

Разведка. Разведкой в тестировании на проникновение является сбор информации из открытых источников, необходимой для составления сценария атаки на целевую организацию. В некоторых случаях для более глубокого тестирования организация предоставляет большинство данных о своей IT-инфраструктуре аудитору. Аудитору остается только дополнить информацию и приступать ко второй фазе.

Понятие футпринтинга. В понятии тестирования на проникновение используется термин «футпринтинг» (англ. footprinting) – это определенная техника получения информации об информационных системах и лицах, которым эти системы принадлежат.

Этапы футпринтинга [3]:

поисковые системы;

1) сайт организации;
2) электронная почта организации;
3) Google;
4) WHOIS;
5) DNS;
6) сетевой;
7) социальная инженерия.

Рассмотрим каждый метод в отдельности, вычислим, какую важную информацию можно изъять с их помощью, а также выделим основные инструменты, которые использует каждый метод.

Поисковые системы. Поисковые системы – это веб-системы для поиска различной информации в Интернете. Основными поисковыми системами являются google.ru, yandex.ru, yahoo.com, bing.com.

Информация: физическое расположение объекта, контактные данные организации, предлагаемые услуги, информация о сотрудниках, возможна информация о закупках (в том числе и СЗИ) и т.д.

Применение: данная информация особенно важна для использования методов социальной инженерии. Помимо этого, физическое расположение играет большую роль, например, для сканирования вне контролируемой зоны Wi-Fi устройств организации и т.п.

Помимо поисковых систем, такие компании предоставляют в открытом доступе множество сервисов. Например, наиболее полезными из сервисов при составлении сценария проникновения являются данные со спутника.

Основные сервисы для извлечения информации о физическом расположении: Google Maps (maps.google.ru) – данные со спутника, а также режим «Street View»; Yandex Maps (maps.yandex.ru); Google Earth (earth.google.com); 2ГИС (2gis.ru).

Информация: всевозможная информация об объектах, находящихся возле здания организации. Особенно полезно при применении сценариев социальной инженерии.

Применение: множество сценариев применения. Например, если проводится социальная инженерия, можно попытаться выяснить, как пробраться в контролируемую зону, увидеть расположение некоторых объектов безопасности (камер) с помощью онлайн-ресурсов. Второй пример, это определение точек, с которых возможна атака на беспроводное оборудование заказчика (заброшенные здания, парковки и т.п., находящиеся в предельной близости к зданиям заказчика).

С помощью поисковых систем также можно найти информацию о внешних и внутренних URL организации. Довольно важная информация для проникновения из внешней сети.

Внешние URL – на таких указателях находятся общедоступные сервисы организации, например официальный сайт.

Внутренние URL – на таких указателях находятся сервисы, используемые для доступа внутри компании, либо используют идентификацию пользователей (доступ с определенных IP, доменов, логин/пароль). Помогают использовать определенные функции внутри компании. Большинство организаций используют распространенные форматы внутренних URL. Зная внешний URL организации, вы можете вычислить внутренние URL методом проб и ошибок, а также инструментами: Netcraft (netcraft.com); Link Extractor (www.webmaster-a.com/link-extractor-internal.php).

Информация: используемые веб-сервисы организации.

Применение: с помощью веб-сервисов можно углубиться в структуру предприятия. Очень часто находятся «заброшенные» веб-сервисы, к которым не составляет проблем получить доступ, а оттуда уже планировать дальнейшее проникновение.

Сайт организации. Второй этап в методологии «футпринтинга». Главная информация, которую получаем с сайта на этом этапе: используемое ПО и версия; используемая ОС; поддиректории и параметры сайта; имена файлов, пути, название поля БД или запросы; скриптовая платформа (php, asp, jsp и т.д.); контактные данные (администратора или команды поддержки).

На основе полученной информации решаем, будет ли сценарий основываться (и каковы шансы сделать это) на проникновении на веб-сайт заказчика.

Инструменты, которые можно использовать: Paros Proxy;Burp Suite; irebug.

Информация: получаем всю необходимую информацию о работе сайта.

Применение: с помощью данной информации можно обнаружить уязвимости в конфигурации сайта (например, не были скрыты от внешнего подключения критичные файлы).

Добавим некоторые методы исследования сайтов, которые облегчают задачу получения информации о веб-сайте.

1. Создание копии веб-сайта заказчика позволяет нам исследовать сайт в режиме «оффлайн»; хранить резервную копию сайта; создать копию сайта.

Инструменты, с помощью которых можно сделать копию: HTTrack Web Site Copier; SurfOffline; BlackWidow; Webripper и многие другие.

2. Просмотр архивов веб-сайта.

С помощью просмотров архивов веб-сайтов мы можем отслеживать, какие изменения проводились на нем. К примеру, была удалена интересная нам информация.

Инструмент: Internet Archive Wayback Machine (www.archive.org).

3. Мониторинг изменений на веб-сайте.

Существует автоматизированное ПО, позволяющее отслеживать изменения, произошедшие с сайтом. Мониторинг работает в таком режиме: запускаем отслеживание определенного сайта – если изменения произошли, ПО сохраняет новую и старую версию сайта, а также показывает, какие именно изменения затронули сайт [3].

Инструмент: WebSite-Watcher (www.aignes.com).

Электронная почта. Отслеживание сообщений электронной почты – метод, позволяющий получить определенную информацию о сетевой структуре заказчика из сообщения электронной почты.

Информация, которую возможно получить данным методом:

– IP-адрес хоста, почтового сервера;

– название провайдера;

– географическое положение сервера;

– длительность чтения письма;

– определение типа почтового сервера;

– проверить, проверялись ли ссылки, отправленные в сообщении;

– определение ОС получателя;

– проверить, переслали ли ваше сообщение другим персонам.

Большую часть этой информации можно получить, изучив заголовок сообщения. Заголовок содержится в каждом письме, включает информацию об отправителе, маршруте отправки, дате, теме и получателе.

Инструменты. Информацию можно получить, самому проанализировав заголовок письма, либо используя автоматизированное ПО, такое как Email Tracking Tools; eMailTrackerPro; PoliteMail; Email Lookup.

Инструменты для получения информации, не содержащейся в заголовке письма: Read Notify; TraceEmail; MSGTAG; Zendio; Pointofmail и т.д.

Google. Хотя Google – это поисковая система, процесс футпринтинга с его помощью отличается от процесса футпринтинга с помощью поисковых систем. Получение информации происходит с помощью применения расширенных операторов поисковой системы Google. Но не все так легко, система фильтрует чрезмерное применение расширенных операторов и блокирует доступ к их использованию.

Самые распространенные операторы Google:

– .Site – оператор позволяет находить только страницы, которые содержат определенный URL;

– allinurl – позволяет найти необходимые страницы или веб-сайт, ограничивая результаты, содержащие все условия запроса;

– inurl – позволяет ограничить результаты только страницы или веб-сайта, которые содержат условия запроса, которые вы указали в URL;

– allintitle;

– intitle;

– inanchor;

– allinanchor.

Таким образом, можно получить следующую информацию:

– сообщения об ошибках, которые содержат важную информацию;

– файлы, хранящие пароли;

– важные директории;

– страницы, содержащие логин-порталы;

– страницы, содержащие информацию о сети или уязвимостях;

– уязвимости сервера и оповещений.

Инструменты: Goggle Hacking Tool: Google Hacking Database (GHDB); Metagoofil; Goolink Scanner; SiteDigger; Google Hacks и т.д.

WhoIs. WhoIs является протоколом прикладного уровня типа «клиент-сервер», использующий базу данных регистраторов доменных имен, которая хранит информацию о регистрированных пользователях или владельцах интернет-ресурса. Информация, которую можно получить данным способом:

– доменное имя и диапазон IP адресов;

– персональную информацию владельцев домена;

– дату создания домена и срок истечения.

Применение: с помощью данной информации можно сузить зону адресов организации, использовать методы социальной инженерии, используя персональные данные владельца домена, и т.п.

Инструменты: SmartWhois; Country Whois; LanWhoIs; CallerIP; WhoIs Analyzer Pro.

DNS. DNS является протоколом прикладного уровня, служит для получении информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста в сетевых инфраструктурах. С помощью данного метода можно получить информацию [4].

– IP-диапазоны домена;

– IP-адреса почтовых серверов, DNS-серверов, WhoIs-серверов домена.

Существуют разные типы DNS-записей. Именно благодаря им можно получить интересующую информацию по инфраструктуре домена.

– A – запись адреса, связывает имя хоста и его IP адрес;

– AAAA – запись адреса IPv6;

– CNAME – каноническая запись имени, используется для перенаправления на другое имя;

– MX – указывает серверы обмена почтой данного домена;

– NS – указывает DNS-сервер данного домена;

– SOA – начальная запись зоны указывает, на каком сервере хранится эталонная информация о данном домене, содержит контактную информацию лица, ответственного за данную зону.

Применение: сужаем зону интересующих адресов.

Инструменты: nslookup; DIG; myDNSTools и т.п.

Сетевой футпринтинг. Этот этап футпринтинга связан с получением информации о сети. В основном сбор информации на этом этапе происходит, когда аудитор находится в локальной сети проверяемой организации. Информация, которую возможно получить: диапазоны сетей; определение ОС; составление карты сетей;

Необходимо знать, что приватными сетями являются: 10.0.0.0/8; 176.16.0.0/12; 192.168.0.0/16.

Именно эта адресация используется в локальных сетях. Отличие в том, что маски могут быть разными. Благодаря этой информации есть шанс определить, какая адресация используется в сети организации.

Важным аспектом в сценарии проникновения является построенная схема сети. Без нее трудно скоординировать действия и определиться, какими путями проникать дальше. Главным инструментом для построения схемы сети является утилита trace route. Утилита использует разные протоколы передачи данных в зависимости от ОС.

Принцип работы: отправление пакетов указанному узлу, показывая информацию о промежуточных устройствах (маршрутизаторах) в сети.

Инструменты с расширенными возможностями: Path Analyzer Pro; VisualRoute 2010 и т.д.

Социальная инженерия. Социальная инженерия – использование методов несанкционированного доступа к информационным ресурсам, основанных на особенностях психологии человека. Является абсолютно нетехническим процессом, при котором злоумышленник, используя психологические слабости людей и их природу, «выманивает» у жертвы конфиденциальную информацию. Поэтому социальный инженер в первую очередь должен отлично разбираться в психологии человека.

Для того чтобы использовать этот метод, необходимо получить доверие уполномоченного пользователя. Это может быть администратор компонентов, связанных с ИС организации или пользователь с расширенными привилегиями в ИС.

Информация, которую можем получить: контактные данные; об уязвимостях ИС; об установленных СЗИ; данные пользователь/пароль; сервисы ИС и т.п.

Дополнительные методы социальной инженерии: подслушивание, подглядывание, информация из мусорных баков, а также социальные сети.

В некоторых методологиях социальные сети выделяют в отдельный этап футпринтинга. С помощью социальных сетей можно получать информацию как с помощью социальной инженерии, так и с помощью обычных методов. Ниже приведена схема, какую информацию может извлечь злоумышленник из информации, находящейся в социальных сетях (рис. 1).

Основные социальные сети, используемые многими пользователями и компаниями: Facebook; Вконтакте; LinkedIn; Twitter; одноклассники и т.д.

Дополнительную угрозу безопасности несет в себе интеграция друг с другом различных сервисов, например Foursquare (сервиса, позволяющего отмечать на карте свое местоположение и делиться этой информацией с друзьями) и Twitter (онлайн-сервис для ведения микроблогов) [5, 11].

С помощью объединения методов социальной инженерии и социальных сетей мы можем узнать IP-адрес жертвы. Выходим с лицом на контакт в социальной сети с помощью специальных сервисов (например, http://www.myiptest.com), передаем жертве сформированную ссылку, отправляем его пе-

реадресацией на другой сайт, а сами получаем IP-адрес жертвы. Этот способ возможен, если жертва плохо разбирается в информационных технологиях.

Этапы футпринтинга. Тестирование на проникновение с помощью футпринтинга используется для поиска публично доступной информации об организации в Интернете. Вполне возможно, что аудитор сможет найти приватную информацию с помощью публичных ресурсов.

Рис. 1. Схема получения информации из социальных сетей

Для того чтобы обеспечить максимальную область тестирования с помощью футпринтинга, необходимо следовать этапам [4]:

Шаг 1: Получение необходимых разрешений.

Если аудитор хочет попытаться получить информацию с помощью методов, не обговоренных в договоре с заказчиком, необходимо получить разрешение у ответственных лиц.

Шаг 2: Определение масштаба футпринтинга.

Под масштабами подразумевается, какие ИС заказчика будут протестированы. В основном эта информация указана в договоре либо аудитор сам определяет границы.

Шаг 3: Проведение футпринтинга с помощью метода поисковых систем.

Шаг 4: Проведение футпринтинга веб-сайта.

Шаг 5: Проведение футпринтинга электронной почты.

Шаг 6: Проведение футпринтинга с помощью Google.

Шаг 7: Проведение футпринтинга с помощью WhoIs.

Шаг 8: Проведение футпринтинга с помощью DNS.

Шаг 9: Проведение сетевого футпринтинга.

Шаг 10: Проведение социальной инженерии.

Шаг 11: Документирование всей информации, которую удалось найти.

Аудитор может на свое усмотрение менять порядок либо вообще убирать определённые этапы. Этот список шагов необходим для того, чтобы обеспечить максимальную область действия футпринтинга. Таким образом, в данной статье представлены базовые средства проведения теста на проникновение информационной системы.

Литература

1. 3DNews. Новости Software [Электронный ресурс]. – Режим доступа: http://www.3dnews.ru/909160, свободный (дата обращения: 05.05.2015).

2. Журнал Информационная безопасность. – 2013. – №5. – С. 32–33.

3. Steve D.F. Ethical Hacking and Countermeasures v8 Module 02: Footprinting and Reconnaissance (CEHv8), EC-Council. – Albuquerque, New Mexico: USA, 2014. – 261 p.

4. Steve D.F. Ethical Hacking and Countermeasures v8 Module 04: Enumeration (CEHv8), EC-Council. Albuquerque, New Mexico: USA, 2014. – 516 p.

5. Петренко С.А. Инсайд / С.А. Петренко, Н.М. Михайлов // Защита информации. – СПб., 2014. – Т. 1500, №2. – С. 33.

6. Penetration Testing A Hands-On Introduction to Hacking [Электронный ресурс]. – Режим доступа: http://www.nostarch.com/pentesting, платный (дата обращения: 02.04.2015).

7. Бондарчук С.С. Проблема информационной безопасности производства наноэлектроники/ С.С. Бондарчук, Д.Д. Зыков, Р.В. Мещеряков // Доклады ТУСУРа. – 2010. – №1(21). – С. 93–94.

8. Рубанов С.А. Гибридная система обнаружения вторжений на базе нечеткого классификатора с использованием жадного и генетического алгоритмов / С.А. Рубанов, И.А. Ходашинский, Р.В. Мещеряков // Вопросы защиты информации. – 2013. – № 4 (103). – С. 67–72.

9. Ходашинский И.А. Методы нечеткого извлечения знаний в задачах обнаружения вторжений / И.А. Ходашинский, И.В. Горбунов, Р.В. Мещеряков // Вопросы защиты информации. – М.: ФГУП ВИНИ, 2012. – № 1. –С. 45–50.

10. Ануфриева Н.Ю. Оценивание результативности работы центра информационного обслуживания / Н.Ю Ануфриева, Р.В. Мещеряков, Г.А. Шевцова // Изв. вузов. Приборостроение. – 2012. – Т. 55, № 11. – С. 63–66.

11. Мещеряков Р.В. Концептуальные вопросы информационной безопасности региона и подготовки кадров / Р.В. Мещеряков, А.А. Шелупанов // Труды СПИИРАН. – 2014. – № 3(34). – С. 136–159.

Туманов Сергей Андреевич
Ст. преподаватель каф. защиты информации НГТУ
Тел.: 8-923-104-27-27
Эл. почта: Serg-tum@mail.ru

Tumanov S.A.

Penetration testing tools for information systems

Penetration testing has a various vectors of attack. The auditor should not miss potential ways of penetration. In the article we consider the methodology of creating scenarios of penetration testing, which denotes the sequence of actions of the auditor. The tester should perform this methodology for the best result.
Keywords: penetration testing, reconnaissance, footprinting, information security audit.