ПОДГОТОВКА К CISSP: ТЕЛЕКОММУНИКАЦИИ И СЕТЕВАЯ БЕЗОПАСНОСТЬ

***Дорофеев Александр Владимирович**, CISSP, CISM, CISA*

Публикация продолжает серию наших статей по подготовке к сдачи экзамена на статус сертифицированного специалиста по информационной безопасности (Certified Information Systems Security Professional). В статье рассмотрен домен, посвященный телекоммуникациям и сетевой безопасности.

***Ключевые слова**: сертификация специалистов, CISSP, сетевая безопасность, телекоммуникации.*

PREPARING FOR CISSP: TELECOMMUNICATIONS AND NETWORK SECURITY

***Alexander Dorofeev**, CISSP, CISM, CISA*

Publication continues the series of our articles devoted to preparation for the CISSP (Certified Information Systems Security Professional) exam. In this article we will review the domain Telecommunications and network security.

***Keywords**: expert certification, CISSP, network security, telecommunications.*

В предыдущих статьях [1-4] мы довольно подробно разобрали аспекты менеджмента информационной безопасности, которыми специалист, готовящийся сдать экзамен CISSP, должен владеть на хорошем уровне. Еще одной очень обширной темой, в которой требуется разобраться, является сетевая безопасность. Мы рассмотрим, как подготовиться по всем областям данного домена и особенно заострим внимание на сетевых атаках.

В первую очередь специалист по информационной безопасности должен хорошо понимать базовые концепции построения компьютерных сетей: представлять модели сетевого взаимодействия OSI и TCP/IP, знать назначение и принципы работы основных сетевых протоколов. Для профессионалов, которые уже успешно забыли университетский курс «Компьютерные сети» и не сталкиваются с этими вопросами каждый день у себя на работе, рекомендуем пролистать классические учебники, написанные Олиферами [5] или Таненбаумом [6].

Помимо знания протоколов различных уровней, готовящемуся к сдаче экзамена нужно четко представлять себе назначение компонентов компьютерной сети и сетевых средств защиты, таких как: коммутатор, маршрутизатор, межсетевой экран, системы обнаружения и предотвращения вторжений и т. п.

Отдельного внимания в данном домене заслуживают различные сетевые атаки, которые мы сейчас и рассмотрим. Для того чтобы хорошо разобраться для каких целей, какая атака применяется, лучше всего рассмотреть их в контексте методологии взлома, которая применяется в частности и для проведения тестирования защищенности систем (тестирование на проникновение).

Перед тем, как погрузиться в разбор шагов, которые проходит хакер для проникновения в чужую сеть, давайте рассмотрим, какими бывают эти самые хакеры.

«Белая шляпа» (white hat) – эксперт по информационной безопасности, обладающий навыками взлома информационных систем и использующий их для выявления уязвимостей систем с целью их устранения. Таким образом, «белой шляпой» является эксперт-аудитор, оказывающий услуги по техническому аудиту систем, таких специалистов еще называют «этичными» хакерами (ethical hacker).

«Серая шляпа» (grey hat) – специалист, работающий на тех, кто платит. Он может выступать как в роли аудитора, так и в роли настоящего злоумышленника, решившего преступить закон.

«Черная шляпа» (black hat) – злоумышленник, зарабатывающий себе на жизнь криминальным ремеслом по взлому систем.

Синонимами слова «hacker» могут быть также такие термины, как «cracker» (взломщик) и «phreaker» (хакер, взламывающий системы телефонной связи).

Цели хакеров

Основными целями злоумышленника, как правило, является получение доступа к определенной информации (например, электронная переписка интересующих лиц) или доступ (желательно административный) к какой-либо системе (например, клиент-банк).

Данный подход используется и в ходе проведения тестов на проникновение, когда перед экспертами ставятся аналогичные задачи.

Инструменты

Что касается инструментария, используемого злоумышленниками, то на сегодняшний момент он довольно широк: от отдельных свободно распространяемых утилит, до полноценных фреймворков и комплексов.

В целом, можно отметить, что требования к уровню квалификации специалиста по использованию хакерского инструментария постоянно снижаются. Если еще в середине 2000-х чтобы провести эксплуатацию уязвимости нужно было найти исходный текст эксплойта, исправить в нем специально внесенную ошибку (защита от «дурака») и суметь скомпилировать и получить исполняемый файл, то сейчас доступны фреймворки эксплойтов с графическим интерфейсом, требующие от пользователя лишь общего представления об этапах проведения атаки: выбор цели, эксплойта, полезной нагрузки и т. п.

Среди комплексов тестирования защищенности мировым стандартом де-факто является сборник Kali Linux[1], представляющий собой загружаемый носитель или образ с ОС Linux, содержащий сотни предустановленных утилит для взлома. В России НПО «Эшелон» разрабатывает похожий комплекс тестирования защищенности «Сканер-ВС». Комплекс успешно прошел сертификацию ФСТЭК России и Минобороны России и применяется для «боевого» контроля состояния защищенности информационных систем.

На ряд инструментов мы сошлемся в процессе рассмотрения соответствующих этапов методологии взлома.

Обзор методологии взлома

Для того чтобы понять приемы, используемые хакерами для взлома систем, достаточно использовать аналогию с физическим проникновением на чью-либо территорию с целью кражи материальных ценностей.

Как поступает вор? В первую очередь он проводит разведку, целью которой является сбор информации об интересующих его ценностях и тех мерах, которые предпринял законный владелец для защиты своих активов. Собрав информацию и выявив бреши в защите периметра, вор проникает на территорию, чтобы забрать добычу. Злоумышленник не хочет быть пойманным и предпринимает всевозможные попытки по сокрытию своих следов.

Аналогичная последовательность выдерживается и в случае компьютерного взлома, но иногда с одной особенностью: так как речь идет об информационных активах, то кража не ведет к исчезновению их у владельца, и соответственно, у злоумышленника может возникнуть желание не один раз похитить что-то ценное, а установить постоянный и комфортный доступ к системе, которым он может пользоваться когда угодно.

Итак, давайте выделим этапы проникновения:

1. Сбор информации (разведка);
2. Выявление уязвимостей;
3. Эксплуатация и проведение атак;
4. Обеспечение комфортного доступа;
5. Расширение зоны влияния;
6. Сокрытие следов

Сбор информации

Какую информацию собирает хакер для того, чтобы оказаться внутри корпоративной сети определенной организации?

Во-первых, информацию об ИТ-инфраструктуре: IP-адреса, доменные имена, используемое программное и аппаратное обеспечение. Во-вторых, информацию о сотрудниках: имена, контактные данные (как личные, так и рабочие), увлечения и т.п.

В качестве источников данной информации могут выступить:

- сайт организации;
- базы данных регистраторов доменных имен;
- сайты поставщиков, работающих с данной организацией (интересуют пресс-релизы о завершенных проектах);
- сайты социальных сетей, в особенности профессиональных, на которых люди, по сути, размещают свои резюме;
- сайты для поиска работы/сотрудников (интересуют описания вакансий).

В результате злоумышленник получает представление о цели, имеет перечень интересных ИТ-ресурсов, и имена сотрудников организации.

1 http://www.kali.org/

Отдельно необходимо упомянуть о так называемой социальной инженерии (social engineering). По сути, это использование такой науки как психология во вред человеку. Хакеры стараются с помощью различных психологических приемов спровоцировать человека на необходимое действие, например, прямо или косвенно раскрыть информацию.

Классикой жанра является выход на ИТ-администратора через профессиональный форум. Так, например, зная имя человека, его «кличку» в интернете (как мы знаем, у большинства ИТ-специалистов есть свой единственный и неповторимый ник) злоумышленник вступает с жертвой в дискуссию на техническом форуме. Администратор может искать на форуме решение какой-либо технической проблемы и наш злоумышленник может помочь ее решить, но поможет так, чтобы решить и свою задачу по получению доступа в желанную компьютерную сеть. Например, администратору может быть передана какая-либо самописная программа, устраняющая проблему, а заодно и выполняющая «нужные» злоумышленнику действия.

Выявление уязвимостей

Что такое уязвимость мы уже определяли ранее в наших статьях – это некий недостаток, позволяющий угрозе реализоваться. В случае сетевой безопасности хорошими примерами уязвимостей являются:

- использование паролей по умолчанию для администрирования систем (например, admin:admin);
- ошибки переполнения буфера, допущенные программистами в ходе разработки, ведущие к тому, что произвольный код может быть выполнен на удаленной машине;
- отсутствие фильтрации вводимых пользователем данных;
- и т. п.

Существуют различные классификации и реестры уязвимостей. Хороший обзор по данной теме приведен в статье Маркова А. С. и Фадина А. А. [7].

Специалист, готовящийся сдать экзамен для получения статуса CISSP должен также знать такое понятие, как уязвимость «нулевого дня» (zero day). По сути, это уязвимость, о которой еще ничего не знает вендор и для закрытия которой отсутствует соответствующее исправление (patch). Информация об уязвимости «нулевого дня» и реализация программы, эксплуатирующей данную уязвимость, являются товаром на хакерском черном рынке. Цена подобного товара варьируется от нескольких тысяч долларов до нескольких десятков тысяч[2].

Среди специалистов можно встретить мнение, что реальный взлом возможен только с использованием известных узкому кругу лиц уязвимостей. На самом деле в реальной ИТ-инфраструктуре современного предприятия уязвимости могут не закрываться годами. Почему? Потому что установка исправления может вызвать сбой в работе систем и негативно повлиять на деятельность организации. Для того чтобы такой риск снизить, солидные компании внедряют довольно дорогостоящий процесс тестирования обновлений перед их распространением.

В практике автора был случай, когда в одной известной российской компании ряд серьезных уязвимостей, обнаруженных в ходе проведенного тестирования на проникновение, «прожили» в системе целый год после ознакомления ответственных или безответственных ИТ-специалистов.

Для взлома систем нужна информация о версиях программных решений, получив которую можно найти данные о характерных для конкретного продукта уязвимостях. Как правило, такую информацию можно встретить в двух местах: специализированных базах данных уязвимостей и сайтах вендоров.

Узнать версию программного продукта можно различными способами. Например, многие сетевые сервисы при обращении к ним демонстрируют так называемый баннер, содержащий данные о версии. Именно такой подход используется в известном сканере портов NMAP[3]. Иногда версию можно определить аналитическим путем. Например, можно найти пресс-релиз компании-разработчика или интегратора, создавшей интернет-портал, который необходимо взломать злоумышленнику. В пресс-релизе зачастую есть вся необходимая информация об использовавшихся технологиях, а сопоставление даты выхода этой новости с информацией о датах релизов соответствующего продукта, позволяет без труда определить, какие именно версии использовалась. Зная версию продукта, злоумышленник может найти соответствующую информацию об уязвимостях и доступных эксплойтах.

Настоящий хакер осуществляет данные действия вручную, и применяет различные приемы для обеспечения скрытности своей деятельно-

2 http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

3 http://nmap.org/

сти: использование прокси-серверов, кэша поисковых машин и т. п. Данный процесс можно автоматизировать с помощью специальных сканеров безопасности, основная масса проверок которых заключается в выявлении версии и поиске информации в постоянно обновляемой собственной базе данных уязвимостях.

Применение сканеров безопасности связано с большим объемом очень специфического сетевого трафика, который всегда вызывает подозрения у систем обнаружения вторжений. Поэтому подобные сканеры любят этичные хакеры, и не любят неэтичные.

Эксплуатация уязвимостей и проведение различных атак

Зная наверняка об имеющейся уязвимости или имея лишь предположение, хакер постарается ее проэксплуатировать. В первую очередь, конечно, злоумышленник будет искать готовые и проверенные в деле эксплойты, при необходимости разработает сам или попросит это сделать компетентного коллегу.

Одной из составляющих эксплойта является так называемая «полезная нагрузка» (payload). Это тот функционал, который запускается на удаленной машине, чтобы дать злоумышленнику, то, что ему нужно. Как правило, это:

- получение командной строки на удаленной машине с правами администратора;
- внедрение кейлоггера (keylogger) для записи вводимых пользователями удаленной машины данных;
- создание учетной записи с заданным паролем;
- и т. д. и т. п.

Одним из самых популярных фреймворков для разработки и использования готовых эксплойтов сейчас является Metasploit Framework[4].

Помимо эксплуатации различных программных уязвимостей одной из самых действенных атак на протяжении нескольких десятилетий остается атака на слабые пароли, так как пароли выбирает самое слабое звено – человек.

Специалист, обладающий статусом CISSP должен хорошо разбираться в различных вариациях подобных атак. В первую очередь необходимо отметить, что бывают интерактивные атаки на пароли (online password cracking) и так называемые оффлайн-атаки.

Интерактивные атаки заключаются в том, что злоумышленник имеет доступ к функционалу авторизации и последовательно вводит пары логин-пароль и анализирует успешность авторизации. Одной из самых качественных утилит для проведения подобной атаки является THC-HYDRA[5]. В случае оффлайн-атак у злоумышленника есть хэш-значения паролей, и подбор осуществляется без взаимодействия с системой, из которой они были извлечены.

По способу формирования паролей различают метод «грубой силы» (bruteforce) и «по словарю» (dictionary attack). В первом случае пароли формируются на основе заданных правил. Например, злоумышленник издалека видел, как пользователь вводил пароль и запомнил, что в пароле есть только латинские буквы и цифры, а длина его 7-9 символов. Задавая подбор именно по этим параметрам, вероятность успешного подбора резко увеличивается. Атаки «по словарю» позволяют попытать счастья и проверить, не использует ли пользователь распространенный пароль. Последние утечки паролей явно показывают, что многие пользователи предпочитают выбирать клавиатурные пароли (такие как «qwerty», «qazwsxedc»), номера телефонов, даты, имена и т. п. Известной утилитой подобного плана является John The Ripper[6].

Необходимо, отдельно упомянуть о нескольких моментах, связанных с хэшами паролей. Если известен хэш пароля, то не всегда его нужно взламывать, иногда для авторизации его достаточно просто «подложить» системе (атака «pass the hash»). Если у злоумышленника есть доступ к хэшам и возможность подмены (например, получен доступ к веб-приложению на уровне базы данных), то можно просто заменить хэш на тот, который расчитан для известного пароля. Хэши паролей не обязательно нужно считать «на ходу», можно сначала их сгенерировать на заданных наборах символов, а в ходе атаки лишь осуществлять поиск, данный вид атаки называется атакой с применением радужных таблиц (rainbow tables).

Еще одним интересным видом атак является атака «человек по-середине» (man-in-the-middle). В качестве самой распространенной иллюстрации рассмотрим атаку ARP-spoofing. Как мы знаем, протокол ARP позволяет сопоставить физические MAC-адреса устройств их IP-адресам с помощью соответствующих ARP-таблиц, хранящихся у участников сетевого взаимодействия.

4 http://www.metasploit.com/

5 https://www.thc.org/thc-hydra/

6 http://www.openwall.com/john/

Смысл атаки заключается в том, что в таблицы машины-жертвы и ресурса, с которым идет интересный для злоумышленника сетевой обмен (например, шлюз по умолчанию, контроллер домена) вносятся изменения, заставляющие включить в процесс коммуникации посредника: компьютер злоумышленника. Хакер посредством использования сниффера извлекает необходимые данные из трафика: имена учетных записей, пароли, хэши паролей и т.п. Самой известной программой, с помощью которой можно реализовать данную атаку является Cain&Abel.

Отдельно стоит обсудить атаки, связанные с web-приложениями: межсайтовый скриптинг (Cross Site Scripting - CSS) и SQL-инъекция (SQL injection).

В случае CSS на страницы веб-сайта внедряется скрипт, который исполняется в браузере пользователя при просмотре данной страницы. Это может произойти, например, из-за ошибки программиста, не реализовавшего корректную фильтрацию данных, вводимых пользователем, например, при публикации пользователем сообщения на форуме. Подобные атаки сейчас используются для проведения атак на машины пользователей, так например, скрипт может определить версию браузера и подобрать подходящий эксплойт для его автоматического взлома.

SQL-инъекция заключается в том, что из-за ошибки в фильтрации данных или в архитектуре web-приложения у злоумышленника появляется возможность через веб-интерфейс напрямую взаимодействовать с базой данных приложения посредством SQL-команд.

Обеспечение комфортного доступа

После того, как система взломана и у хакера есть к ней доступ (например, он может посылать команды операционной системе) его задачей становится обеспечение комфортного стабильного доступа. Он может его обеспечить себе, получив пароль легитимного администратора или установив так называемый руткит (rootkit). Под руткитом подразумевается специально разработанное приложение или набор приложений, которые дают возможность злоумышленнику иметь скрытный административный доступ к системе. Таким образом, деятельность злоумышленника остается скрытой для стандартных средств мониторинга ОС.

Расширение зоны влияния

Расширение зоны влияния можно продемонстрировать на следующих двух примерах.

Злоумышленник получил доступ к веб-серверу на уровне операционной системы. Такой доступ позволяет ему найти конфигурационные файлы веб-приложений, запущенных на данном сервере и извлечь из них пароли для доступа к базам данных, размещенных на других серверах. Имея доступ на уровне базы данных зачастую можно получить и доступ к ОС, так как может быть оставлен включенным соответствующий функционал.

Второй пример связан с получением базы хэшей паролей пользователей контроллера домена. Хакер подбирает пароли к учетным записям пользователей (мы помним с вами, что это офлайн-атака). Вскрытые пароли злоумышленник проверяет на других системах и обнаруживается, что ряд пользователей используют одни и те же пароли для доступа к различным корпоративным ресурсам.

Сокрытие следов

Сокрытие следов может варьироваться от удаления журналов на взломанных машинах до взлома консолей управления и баз данных систем межсетевого экранирования, обнаружения вторжений и SIEM-систем.

DoS и DDoS-атаки

Особняком от рассмотренных атак стоят атаки типа «отказ в обслуживании» (Denial of Service – DoS) и их самый распространенный сейчас тип «распределенные атаки» (Distributed Denial of Service - DDoS).

Необходимо отметить, что DDoS-атаки связаны с отправкой большого объема трафика или запросов из различных источников на целевой узел. Например, злоумышленник дает команду зараженным компьютерам, находящимся в контролируемой им бот-сети (botnet) постоянно открывать определенную веб-страницу. Веб-сервер жертвы не справляется с таким количеством запросов и перестает отвечать на запросы.

Простая DoS-атака может быть инициирована лишь одним узлом. Некоторое время назад была популярна атака «медленный HTTP-запрос» (Slow HTTP POST). Атака реализовывается следующим образом: злоумышленник отправляет запрос веб-серверу, указывая в специальном заголовке большой объем данных, который должен принять веб-сервер. Веб-сервер готовится обработать данные и выделяет соответствующие ресурсы. Затем начинается передача данных, но она осуществляется очень медленно, что позволяет использовать ресурсы сервера намного дольше, чем это необходимо, и, как следствие, мешать обработке других запросов. Несколько тысяч таких соединений легко могли сделать веб-сервер недоступным.

Вместо заключения

Мы рассмотрели, что делает злоумышленник, взламывая системы, и познакомились с базовыми понятиями из этой области, необходимыми для успешной сдачи экзамена CISSP. На наш взгляд, чтобы хорошо освоиться с данной темой, лучше всего немного попрактиковаться и почувствовать себя настоящим хакером. Сейчас для этого не нужно пытаться взламывать чужие сайты, а можно просто воспользоваться виртуальным образом ОС, подготовленным для обучения тестированию защищенности, например, таким как Metasploitable 27. Настоящий профессионал в области информационной безопасности должен четко представлять, что происходить по ту сторону баррикад.

Литература:

1) Дорофеев А. В. Статус CISSP: как получить и не потерять? //Вопросы кибербезопасности. 2013. № 1(1). С. 65-68.
2) Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67-73.
3) Дорофеев А. В. Менеджмент ИБ: управление рисками // Вопросы кибербезопасности. 2014. № 2(3). С. 66-73.
4) Дорофеев А. В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3(4). С. 69-73.
5) Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2014. 4-е изд. 944 с.
6) Таненбаум Э., Уэзеролл Д. Компьютерные сети. СПб.: Питер, 2012. 5-е изд. 960 с.
7) Марков А. С., Фадин А. А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. №3. С. 56-61.
8) Шахалов И. Ю., Дорофеев А. В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. С. 4-14.

References:

1) Dorofeyev A. V. Status CISSP: kak poluchit i ne poteryat? Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 65-68.
2) Dorofeyev A. V., Markov A. S. Menedzhment informacionnoj bezopasnosti: osnovnye koncepcii, Voprosy kiberbezopasnosti, 2014, No 1(2). pp. 67-73.
3) Dorofeyev A. V. Menedzhment informacionnoj bezopasnosti: upravlenie riskami, Voprosy kiberbezopasnosti, 2014, No 2(3). pp. 66-73.
4) Dorofeyev A. V. Menedzhment informacionnoj bezopasnosti: perehod na ISO 27001:2013, Voprosy kiberbezopasnosti, 2014, No 2(3), pp. 69-73.
5) Viktor Olifer, Natalija Olifer. Komp'juternye seti. Principy, tehnologii, protokoly – 4-e izd, - Piter, 2014. – 944 p.
6) Andrew S. Tanenbaum, David J. Wetherall. Computer Networks Prentice Hall; 5 edition (October 7, 2010), 960 p.
7) Markov A. S., Fadin A. A. Sistematika ujazvimostej i defektov bezopasnosti programmnyh resursov,Zashhita informacii. Inside, 2013, No 3, pp. 56-61.
8) Shakhalov I. Yu., Dorofeev A. V. Osnovy upravleniya informatsionnoy bezopasnost'yu sovremennoy organizatsii, Pravovaya informatika, 2013, No 3, pp. 4-14.

7 http://sourceforge.net/projects/metasploitable/files/Metasploitable2/