ОГЛАВЛЕНИЕ

ВСТУПЛЕНИЕ

В последние два десятилетия информационные технологии совершили настоящий прорыв. Появление гипертекста, IP-телефонии, головокружительное увеличение тактовых частот процессоров, а также пропускной способности каналов связи и многое, многое другое. Все это существенно усложнило процесс не только разработки, но и обслуживания ИТ-инфраструктуры. Появилась новая профессия – системный администратор.

Системный администратор является специалистом, обеспечивающим бесперебойную работу всей ИТ-инфаструктуры компании. Далеко не последнее место в работе сисадмина занимает обеспечение информационной безопасности корпоративных ресурсов.

Для обеспечения информационной безопасности администратору нужно как самому корректно устанавливать программное обеспечение, так и устанавливать обновления и исправления на уже использующееся ПО. Решение данных задач, особенно в крупных компаниях, требует зачастую много времени и большого числа специалистов, так как обычно в крупных компаниях обслуживанием системы телефонии, серверов электронной почты, веб-ресурсов и других систем занимаются разные специалисты. Но при этом каждая из этих систем должна быть построена с учетом требований по обеспечению информационной безопасности. Однако информационные системы, как правило, взаимосвязаны, например серверы электронной почты под управлением Microsoft Exchange должны входить в домен Active Directory, система IP-телефонии связана с почтовой системой, а веб-серверы связаны с серверами баз данных. Эффективное обеспечение информационной безопасности для таких интегрированных систем требует от соответствующего специалиста обширных технических знаний в смежных областях, так как иначе плохая защищенность одного элемента интегрированной системы может свести на нет все усилия по защите других ее элементов. Как говорится, прочность всей цепи определяется прочностью ее самого слабого звена.

Лучше всего непосредственно при построении корпоративной сети использовать наиболее жесткие настройки для всех ресурсов. Как правило, производители приложений и оборудования сами рекомендуют использовать наиболее защищенные режимы работы и подробно описывают их настройку (например, использование сложных паролей для входа пользователей в систему, защита электронной почты от нежелательных рассылок, отключение учетных записей пользователей по умолчанию и т. д.).

Однако типичной ситуацией является наличие какой-либо корпоративной инфраструктуры, которая строилась на протяжении нескольких лет различными специалистами, на разных моделях оборудования и приложений. В таких случаях корпоративные ресурсы по различным причинам содержат уязвимости и недостатки, связанные с информационной безопасностью.

У системного администратора, как правило, много работы. Особенно в небольших компаниях, где порядка 100 рабочих мест, полтора-два десятка серверов и один, максимум два человека должны все это обслуживать. В результате эти специалисты ежедневно заняты текущей работой, такой как решение проблем пользователей, замена картриджей в принтерах и бумаги в факсах, подготовка рабочих мест для новых пользователей и многой другой «текучкой». При этом зачастую задачи по обеспечению безопасной настройки программного обеспечения и оборудования, написания инструкций и политик по информационной безопасности для пользователей ставятся на задний план и, как правило, не выполняются. Причиной этого является как занятость системных администраторов, так и отсутствие у них соответствующих знаний и навыков для обеспечения информационной безопасности.

Для крупных компаний эта проблема не так актуальна, потому что, например, в крупных банках имеется отдел или даже департамент по обеспечению информационной безопасности. Соответственно, решением задач ИБ занимаются уже не системные администраторы, а администраторы по безопасности. При этом системные администраторы и администраторы по ИБ выполняют различные задачи: одни обслуживают ИТ-ресурсы и обеспечивают их функциональность, а другие обеспечивают безопасность ИТ-инфраструктуры. Администраторы по ИБ готовят политики и инструкции для системных администраторов.

Но в любом случае, независимо от того, кто отвечает за обеспечение информационной безопасности – системный администратор или администратор по ИБ, этому специалисту необходимо регулярно

производить оценку защищенности корпоративных ИТ-ресурсов, то есть производить аудит информационной безопасности системы.

Конечно, многие крупные организации предпочитают привлекать для осуществления проверки защищенности корпоративной информационной системы профессиональных аудиторов. Однако это имеет смысл только для крупных организаций, к которым предъявляются требования различных стандартов (ГОСТ, ISO и др.). Небольшим компаниям подобный аудит просто не по карману, и поэтому задача осуществления практического аудита ложится на системного администратора как на главного специалиста по корпоративной сети. К тому же такие проверки необходимо делать регулярно, что также накладывает дополнительные расходы.

В.1. Почему «защита и нападение»

Моя книга называется «Информационная безопасность: защита и нападение». С понятием «защита», я думаю, ни у кого вопросов не возникнет. Администратор ИБ должен осуществлять защиту корпоративных ИТ-ресурсов. А вот причем здесь нападение? Для того чтобы эффективно защищать что-либо, необходимо хорошо знать способы нападения, дабы уметь предугадывать действия нападающих и предотвращать их.

А теперь поговорим о том, как все это связано с тематикой данной книги. Для кого она предназначена? Эта книга предназначена прежде всего для системных администраторов и специалистов по информационной безопасности, которые хотели бы разобраться в практических аспектах защиты корпоративных ресурсов от различных угроз. Основной упор при написании книги я делал именно на практические аспекты, то есть здесь не будет «размышлений на тему». Вместо пространных размышлений я постарался сделать основной упор на практические способы решения проблем ИБ, то есть в книге будут описываться различные сценарии и настройки приложений и сетевого оборудования, работа со средствами по поиску уязвимостей и многое другое. Также мы поговорим о том, как нужно писать инструкции и политики по обеспечению ИБ, и коснемся законодательных основ обеспечения ИБ в контексте нормативных правовых актов Российской Федерации.

Итак, мы определились с тем, что эта книга является в определенной степени практическим руководством. Но у многих может возникнуть вопрос: а как насчет хакеров. Является ли эта книга руковод-

ством для компьютерных взломщиков? Отвечу так: в общем случае, для начинающего хакера данная книга может оказаться полезной в плане изучения основ ИБ, средств проникновения и защиты сетей и приложений. Однако использовать на практике для взломов конкретных систем приведенные в книге эксплоиты и утилиты вряд ли получится, так как за то время, пока писалась и издавалась данная книга, были выпущены заплатки и обновления, закрывающие эти уязвимости. Кроме того, многие приведенные примеры уязвимостей и некорректных настроек сознательно упрощены автором, для того чтобы дать читателю представление об общем типе подобных уязвимостей и средствах борьбы с ними, а не для того, чтобы научить проникать в чужие сети. Так что, юные исследователи компьютерных систем, если вы хотите узнать, как что работает в компьютерных системах, то эта книга для вас, но если вы хотите узнать, как взломать Пентагон, то тут она вряд ли сможет вам помочь.

Вот мы и подошли к основному вопросу, который рассматривается в моей книге, – поиску и устранению угроз безопасности информационной системы. Задача обнаружения и тем более устранения угроз безопасности информационной системы не является тривиальной. Как уже упоминалось выше, современные корпоративные сети состоят из множества различных устройств и приложений, и для обнаружения угроз необходимо иметь четкое представление о принципах работы данных систем, используемые протоколы, средства защиты и многое другое.

В своей книге я постараюсь уделить как можно больше внимания практическим аспектам информационной безопасности, применительно к техническим аспектам функционирования различных систем. То есть при рассмотрении вопросов, связанных с защитой локальной сети, я также расскажу об общих принципах функционирования различных сетевых протоколов и устройств. Возможно, для кого-то из читателей это покажется лишним напоминанием прописных истин, и он пропустит данные разделы, но мне все же хотелось бы, чтобы практический материал, приведенный в этой книге, был понятен даже начинающим специалистам.

Да, говоря о практике, замечу, что для выполнения многих примеров, описанных в данной книге, вам потребуется дистрибутив BackTrack Linux. Более подробно узнать об этом дистрибутиве вы можете в приложениях.

Надеюсь, я сумел привлечь внимание читателя. Теперь перейдем к обсуждению ряда теоретических основ информационной безопасности, без которых вам будет сложно понять дальнейший материал.

B.2. Социальная инженерия вместо пролога

Прежде чем начать обсуждение технических аспектов обеспечения информационной безопасности, нелишним будет рассмотреть некоторые вопросы, связанные с социальной инженерией. В частности, рассмотрим, какую информацию о сети своей потенциальной жертвы злоумышленник может почерпнуть из открытых источников, не прибегая к каким-либо специальным средствам и вредоносному программному обеспечению.

В любой корпоративной сети, как правило, используется множество разнообразных устройств и приложений. Активное сетевое оборудование (Cisco, DLink, Huawei), операционные системы (Windows, разнообразные Linux и Unix), веб-серверы (Apache, IIS, WebSphere), системы управления базами данных (MSSQL, MySQL, Oracle) и другие программные продукты – все это можно встретить в корпоративной сети даже средних размеров. Отдельной строкой идут средства информационной безопасности: антивирусы, межсетевые экраны, системы обнаружения вторжений. Конечно, системный администратор всегда должен хорошо знать свою сеть (хотя на практике часто бывает не совсем так). А вот потенциальным злоумышленникам знать о том, что используется в сети, совсем необязательно и даже крайне нежелательно.

B.2.1. Чем грозит наличие у злоумышленника знаний о вашей сети?

Идентификация сетевых ресурсов является важным подготовительным этапом перед осуществлением взлома. Если хакер знает, что ваш корпоративный портал работает под управлением IIS 7 или Windows Server 2008, то ему необходимо найти уязвимости, которым подвержены данные программные продукты. Для этого проще всего поискать в базах уязвимостей. В случае если найти ничего не удалось, то особо продвинутый взломщик может попытаться самостоятельно найти «лазейку», собрав у себя точную копию взламываемой системы и попытавшись самостоятельно проанализировать код. Для этого есть специальные инструменты, которых мы коснемся в этом разделе. Проведя анализ уязвимостей «офлайн», затем хакер сможет быстро провести атаку и внедрить в атакуемую систему вредоносный код.

Далее в этой книге мы еще будем подробно рассматривать вопросы, посвященные удаленному анализу сетевых служб. В этом разделе мы рассмотрим такой малоизученный, но тем не менее важный аспект, как социальная инженерия.

B.2.2. «Разбираем» XSpider

Ознакомившись с предыдущими абзацами, многие могут задаться вопросом: зачем мне все это нужно, у меня же есть специализированный сканер уязвимостей, например XSpider или MaxPatrol. Однако здесь стоит заметить, что коммерческие сканеры стоят недешево, и их, как правило, используют только для сканирования наиболее важных узлов в сети. Например, тех, что участвуют в обработке персональных данных, в соответствии с Федеральным законом № 152.

B.2.3. Социальная инженерия

Выше в этом разделе я попытался обосновать саму необходимость удаленного анализа сети для системных администраторов. Зная методы злоумышленников, легче от них защититься. Однако, говоря об информационной безопасности, все почему-то сразу вспоминают про антивирусы, межсетевые экраны и прочие технические средства. А вот про людей, работающих в компании, при этом часто забывают. А ведь массу полезной информации хакер может почерпнуть из общения с сотрудниками компании и из открытых источников, не прибегая при этом к помощи вредоносных программ и других технических средств. Кстати, уязвимости, связанные с человеческим фактором, не получится обнаружить с помощью XSpider.

Конечно, работа с персоналом – это прежде всего задача HR-департамента (отдела кадров). Служба персонала осуществляет прием сотрудника на работу, подписание соответствующих документов, ознакомление с различными правилами, политиками и регламентами. Однако сотрудники отделов ИТ и ИБ должны также участвовать в этом процессе. В компании должна быть разработана политика информационной безопасности.

B.2.4. Исходные данные

Прежде всего условимся о том, что известно злоумышленнику. Будем считать, что в самой компании у него нет никаких знакомых-инсайдеров, которые могут сообщить интересующую информацию.

Также условимся, что хакер не нарушает закона. Он не использует всевозможных средств прослушивания, «жучков», скрытых камер и прочего. В этом разделе мы не будем использовать никакие специализированные утилиты. Вся информация будет добываться исключительно из открытых источников.

Пусть он знает только название компании, сеть которой ему необходимо взломать. Кто-то посчитает, что этого недостаточно для того, чтобы начать взлом, и будет неправ.

Введя в поисковой системе название компании, злоумышленник быстро найдет ее официальный сайт. Вряд ли сейчас найдется хоть одна уважающая себя организация, у которой отсутствует свой сайт. А реклама, как известно, двигатель торговли, и для связи могут использоваться не только стандартные телефон и e-mail, но и более современные ICQи Skype. В контексте удаленного анализа сети нам наиболее интересны электронная почта и Skype.

Также на корпоративном портале, помимо контактной информации, как правило, есть раздел Вакансии. Начнем сбор информации с этого пункта.

B.2.5. Анализируем вакансии

В разделе Вакансии могут оказаться описания требований к соискателям, в том числе и для ИТ-специалистов. В случае если такого раздела нет, можно попробовать поискать вакансии данной компании на сайтах по поиску работы. В описании вакансии системного администратора очень часто указывается наименование оборудования, операционных систем и приложений, с которыми придется работать. Вот пример описания реальной вакансии в одной компании:

Сетевой администратор в большую компанию ~ 1000 человек. Филиалы компании в регионах по всей стране и бывшему СНГ.
Обязанности и требования:

- поддержка сетевых устройств: коммутаторов, маршрутизаторов и межсетевых экранов Checkpoint, Cisco, 3COM;
- мониторинг работы сетевых устройств и каналов связи на базе решений HPOpenView;
- обеспечение сетевого взаимодействия с филиалами;
- взаимодействие с провайдером услуг связи в процессе всего жизненного цикла предоставляемой услуги связи;
- обеспечение максимально быстрого восстановления работоспособности сетевой инфраструктуры.

Из этого на вид безобидного описания злоумышленник может сделать следующие выводы: в сети компании порядка 1000 машин, сеть географически распределенная, значит, используется VPN или арендованы каналы. В качестве средств защиты, скорее всего, используются Checkpoint, маршрутизация и коммутация на Cisco и 3Com. Для подключения к Интернету, вероятно, используются каналы связи только одного провайдера. Пока все достаточно размыто, осталось много вопросов.

Для их уточнения взломщику необходимо перейти к личному общению со специалистами. Для этого злоумышленнику проще всего воспользоваться той контактной информацией, которая предоставлена на сайте. Например, позвонить и поинтересоваться опубликованными на сайте вакансиями. Многие компании в целях экономии времени начальное собеседование проводят по телефону. Таким образом, специалисты по персоналу отсеивают явно не подходящих кандидатов. Злоумышленнику из общения с HR-менеджером вряд ли удастся получить много полезной технической информации, разве что уточнить количество пользователей и филиалов, да и то не всегда. Зато в процессе телефонного интервью злоумышленник может показать себя квалифицированным специалистом в требуемой области и быть приглашенным на собеседование.

На собеседования к квалифицированным кандидатам зачастую приглашают большое число специалистов (сетевых администраторов, инженеров по серверам, безопасников). Тут для злоумышленника большой простор для деятельности. В процессе дискуссии можно ненавязчиво узнать число филиалов. Кроме того, потенциального работника будут «гонять» прежде всего по тем технологиям, которые используются в корпоративной сети. Например, системные администраторы компании интересуются знаниями соискателя в области серверных операционных систем Windows и ActiveDirectory. Соискатель рассказывает про Windows 2003, затем про Windows 2008. Между делом упоминая RODC и преимущества его использования. На что собеседующие отвечают, что пока не все контроллеры используют Windows 2008. И уровень домена пока Windows 2003. Далее обсуждается тема миграции доменов, вследствие чего выясняется, что все филиалы находятся в одном домене. Поддомены не используются.

B.2.6. Беседа как источник информации

Далее в процессе собеседования «берут слово» сетевики и безопасники. Они спрашивают, с чем и как приходилось работать. Какие модели

оборудования использовались для межсетевого экранирования? Какие протоколы использовались для динамической маршрутизации? Какие корпоративные антивирусы знакомы соискателю? Внедрял ли он систему управления событиями безопасности?

B.2.7. Анализируем результат

В результате беседы выясняется, что в сети используется «зоопарк» решений. В некоторых филиалах применяются программные межсетевые экраны на базе Linux и iptables. В качестве коммутаторов в филиалах используются неуправляемые. Домен один для всех филиалов. Уровень домена Windows 2003. В филиалах установлены DC. Следовательно, все контроллеры домена равноправные, и взламывать можно сеть филиала, которая защищена хуже. Также было выявлено, что на данный момент централизованный мониторинг событий не ведется, и они только готовятся к внедрению ArcSight. Количество рабочих мест в филиалах было также уточнено.

В довершение всего начальник ИТ-отдела посетовал, что во многих филиалах отсутствуют системные администраторы и обслуживанием имеющихся систем занимается кто-то из бухгалтеров или менеджеров. Из этого можно сделать вывод, что уровень технической грамотности в филиалах намного ниже и атаку будет провести значительно легче.

Кстати, многие руководители ИТ-отделов любят проводить экскурсии в серверную для своих потенциальных работников. А еще зачастую собеседования проводятся непосредственно в тех же комнатах, где и сидят ИТ-специалисты. Очень часто в таких помещениях на стенах висят планы сети с IP-адресацией. За полчаса, которые обычно длится собеседование, профессионал запомнит данную схему.

Кроме всего прочего, у злоумышленника после беседы останутся контакты тех, с кем он беседовал. Это могут быть визитки или письмо с приглашением на собеседование. Чем больше имен, тем больше дополнительной информации сможет собрать злоумышленник.

Информацию о данных специалистах можно поискать в Интернете, а точнее в социальных сетях. Например, в сети Мой круг многие специалисты размещают свои резюме, где описывается их профессиональная деятельность. Ознакомившись с такими резюме, злоумышленник сможет получить более точное представление о том, в каких технологиях наиболее силен данный специалист. Например, если в сети используется ОС Linux в качестве межсетевых экранов, а все администраторы компании являются специалистами по Windows, то можно предположить, что iptables настроен нелучшим образом.

Вообще, социальные сети – это большое зло. Люди своими руками пишут досье на самих себя и выкладывают это всем на обозрение.

B.2.8. Немного о средствах связи

В случае, если попасть на собеседование не удалось. Допустим, компания не нуждается в технических специалистах. Злоумышленник может воспользоваться телефоном или Skype. Например, можно позвонить в компанию и попросить соединить с системным администратором. В случае если секретарь сплоховала и соединила, дальше под видом предложения о продаже расходных материалов и оргтехники попытаться выяснить используемое в сети оборудование и ПО. Способ, конечно, не самый эффективный, но лучше, чем ничего.

Дальше вспоминаем про Skype и ICQ. Посредством Skype злоумышленник может попытаться узнать IP-адрес корпоративного шлюза. Для этого хакер может попытаться отправить файл по Skype или ICQ. Далее с помощью пакетного анализатора можно отследить, на какой IP-адрес уходят пакеты. Правда, этот способ срабатывает не всегда, иногда в адресе получателя оказывается другой сервер Skype.

B.2.9. Электронная почта как источник информации о сети

Несмотря на то что данный материал посвящен социальной инженерии, мы постепенно переходим к техническим аспектам как к результату сбора информации. Ранее мы говорили о корпоративном портале, где обязательно должен быть контактный адрес электронной почты. Задача злоумышленника – отправив на этот адрес письмо, обязательно получить ответ. Затем необходимо открыть полученное письмо в исходном виде, включая заголовки.

```
Received: from mxfront29.mail.yandex.net ([127.0.0.1])
          by mxfront29.mail.yandex.net with LMTP id 6Axma6HQ
          for<xxxx@yandex.ru>; Wed, 1 Feb 2012 12:06:10 +0400
Received: from mx1.xxxx.ch (mx1.xxxx.ch [194.209.xx.xx])
          by mxfront29.mail.yandex.net (nwsmtp/Yandex) with ESMTP id 696C4lPv-696Wxxxx;
          Wed,  1 Feb 2012 12:06:10 +0400
X-Yandex-Front: mxfront29.mail.yandex.net
X-Yandex-TimeMark: 1328083570
X-Yandex-Spam: 1
```

Из приведенного заголовка можно узнать IP-адрес почтового сервера отправителя. Хотя этот адрес также можно выяснить и другим

способом, о котором мы поговорим далее. Также последние три строки сообщают о том, какая система использовалась в качестве антиспама. В данном случае это антиспам Яндекса.

Кстати, получить свойства письма можно в веб-интерфейсе бесплатной почтовой службы.

Иногда в свойствах почтовых сообщений может присутствовать более интересная информация, например внутренний IP-адрес отправителя. Вообще, NAT должен скрывать внутреннюю адресацию, так как эта информация тоже интересна злоумышленнику.

B.2.10. Доменное имя как источник информации

Еще одно техническое отступление от темы СИ, тем не менее связанное с ней. Располагая название корпоративного сайта, злоумышленник может собрать ряд интересующих его сведений с помощью общедоступного сетевого ресурса. Зайдем на страницу http://www.ripn.net/whois. В строке запроса необходимо указать доменное имя интересующей компании. Вот пример результата поиска информации по доменному имени:

```
Domain: mydomain.com
Type: CORPORATE
Nserver: a.ns.mydomain.com. 82.198.xx.xx
Nserver: ns4.nic.ru.
Nserver: b.ns.mydomain.com. 212.33.xx.xx
State: REGISTERED, DELEGATED
Org: Joint Stock Company…
```

Мы получили информацию о DNS-записях, зарегистрированных для данного домена. Можно воспользоваться еще одним, русскоязычным сервисом – leader.ru. На этом сайте в поле Whois необходимо указать доменное имя (рис. 1).

Здесь результат более интересный. Помимо тех сведений, которые нам выдал предыдущий портал, мы также получили сведения о диапазоне адресов, владельце и контактной информации, включающие в себя имя и фамилию ответственного, адрес электронной почты и телефон организации.

Полученные сведения можно использовать для сбора информации теми методами, которые описывались ранее в этом разделе. Например, поискать информацию об ответственном специалисте в социальных сетях.

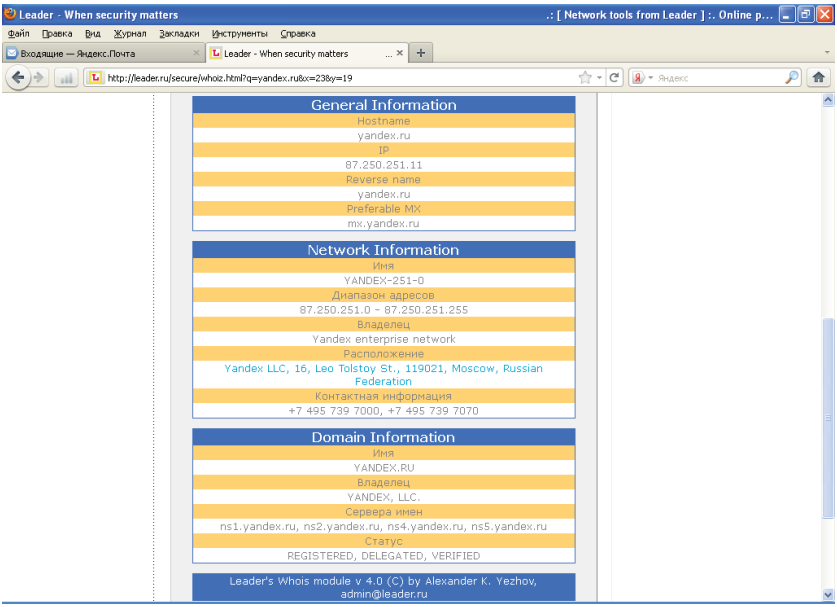

Рис. 1. *Результат работы*

B.2.11. Атака на клиента

До этого момента мы рассматривали ситуацию, когда злоумышленник приходил на собеседование для сбора необходимой информации. Однако возможна и обратная ситуация, когда компания-конкурент приглашает на собеседование сотрудника и различными способами пытается получить необходимую информацию.

Например, можно заманить на собеседование системного администратора и попросить для подтверждения его профессиональных навыков рассказать о топологии той сети, которую он обслуживает. Также можно попросить его показать те документы, которые приходилось разрабатывать. Таким образом можно тоже собирать информацию о сети для последующей атаки.

B.2.12. Срочный звонок

Вообще, социальная инженерия – это очень мощный инструмент, при правильном умении вести разговор (вспомните разведчика Штирлица) собеседник сам расскажет вам обо всем, что нужно.

Для начала приведу небольшую историю про известного взломщика Кевина Митника. Он умудрялся похищать информацию даже из тех сегментов сети, которые не были подключены к Интернету. Делалось это следующим образом. Допустим, отдел А имеет подключение к Интернету, а отдел Б той же компании не имеет. Митник, располагая адресной книгой компании, звонил сотруднику отдела Б, представляясь работником из А, и вежливо просил прислать ему факс с интересующей информацией, объясняя это тем, что он находится вне офиса и ему срочно нужны эти данные. Кто-то отказывал, но рано или поздно обязательно находился сотрудник (как правило, женщина), который выполнял просьбу хакера.

Несмотря на то что этой истории уже не один десяток лет, подобный способ получения информации до сих пор практикуется. Например, вам на мобильный телефон звонит некто, кого не очень хорошо слышно, представляется реально существующим сотрудником и просит сообщить, например, контактную информацию вашего руководителя или кого-либо из других сотрудников. Объясняется это тем, что звонящий находится вне офиса и ему срочно нужна данная информация. Многие в такой ситуации выполняют просьбу позвонившего. А ведь это может оказаться злоумышленник.

Правильным действием в подобном случае является вежливый отказ в предоставлении информации. Например, можно сказать, что вам плохо слышно, и попросить перезвонить попозже. Однако этого недостаточно. В идеале об этом звонке необходимо сообщить в службу безопасности компании. Если же таковая отсутствует или по каким-либо личным причинам вы не хотите к ним обращаться, то сообщите хотя бы своему непосредственному руководителю.

Кстати, та же служба безопасности часто проводит подобные «учения», звоня своим сотрудникам от имени неизвестных. Если требуемая информация была получена – сотрудника ждет наказание, в случае если ничего узнать не удалось, но при этом сообщили в службу безопасности, сотрудника поощряют. Многие сочтут такие провокации аморальными, однако этому методу обучают не только в учебных заведениях соответствующих силовых структур, но и на различных курсах по информационной безопасности.

Но, вообще, действия пользователей в подобных ситуациях должны быть четко прописаны в корпоративной политике безопасности, которую подписывает каждый сотрудник при принятии на работу.

B.2.13. Промежуточные итоги

На этом я завершаю тему анализа сети посредством социальной инженерии и, прежде чем перейти к рассмотрению вопросов, связанных с защитой от данного типа атак, предлагаю подвести промежуточные итоги. Замечу, что собранная информация будет активно использоваться для дальнейшего исследования сети в других разделах книги.

В результате анализа сети было выявлено следующее: используются домен ActiveDirectoryWindows 2003, известно точное число филиалов, количество пользователей в каждой из подсетей, IP-адресация и модели используемого оборудования.

Теперь поговорим о том, как можно попытаться защититься от описанных ранее угроз.

B.2.14. Защита от СИ

Защититься от атак, осуществляемых с помощью социальной инженерии, не так просто, как от технических. Дело в том, что здесь основная угроза исходит не от плохо защищенного оборудования или неправильно настроенного приложения, а от людей, работающих с этими системами. Необходимо в разумных пределах ограничить ту информацию, которую может получить злоумышленник посредством социальной инженерии.

Например, в случае телефонных звонков секретарь должна обязательно спрашивать, кто звонит и по какому вопросу. Это позволит отсечь часть попыток сбора информации. Хотя, конечно, более продвинутые злоумышленники без труда обойдут такой «фейс-контроль».

Что касается объявлений о вакансиях, публикуемых на корпоративном сайте, то лучше указать несколько различных технологий и моделей оборудования в качестве требований, для того чтобы усложнить взломщику задачу сбора информации.

Пример с собеседованием, конечно, является не самым распространенным вариантом сбора информации, так как большинство хакеров работают удаленно, и они скорее будут использовать сканеры портов и генераторы пакетов, чем общаться с представителями взламываемой организации напрямую. Однако не стоит забывать о таком способе сбора информации.