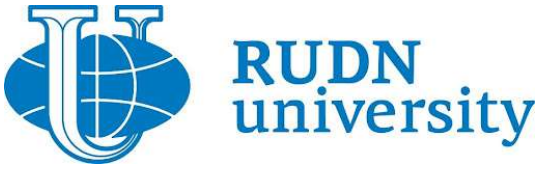
Социальная инженерия

Информационная безопасность

Доборщук В.В., НФИбд-01-18



20 сентября 2021

Содержание

Введение **3**

Теория и определение понятий **4**
Историческая справка 5

Виды социальной инженерии и используемые техники **7**
Техники и термины социальной инженерии 7
Претекстинг 7
Фишинг 7
Троянский конь 8
Дорожное яблоко 8
Кви про кво 8
Виды социальной инженерии 8

Защита пользователей от техник социальной инженерии **10**
Антропогенная защита 10
Техническая защита 10

Список использованных источников **12**

Введение

Даже самая совершенная система защиты бесполезна, если ей управляет психологически неустойчивый, наивный или доверчивый человек. Помните анекдот о диссертации на тему “зависимость скорости перебора паролей от температуры паяльника (утюга)”? Многие почему-то забывают, что в роли объекта атаки может выступать не только машина, но и ее оператор. Причем, оператор зачастую оказывается слабейшим звеном в системе защиты.

На хакерском жаргоне атака на человека называется социальной инженерией (social engineering) и в своем каноническом виде обычно сводится к звонкам по телефону с целью получения конфиденциальной информации (как правило, паролей) посредством выдачи себя за другое лицо.

Собственно, подобные приемы не новы и известны еще со времен глубокой древности. Остается только удивляться тому, что за истекшие тысячелетия человечество так и не научилось противостоять мошенникам и отличать правду ото лжи. Еще удивительнее то, что арсенал злоумышленников не претерпел никаких принципиальных изменений. Напротив, с развитием коммуникационных технологий их задача значительно упростилась.

Общаясь по Интернет, вы не видите и не слышите своего собеседника, более того, нет никаких гарантий, что сообщение действительно отправлено тем адресатом, имя которого стоит в заголовке. Атакующий может находиться и в соседней комнате, и в соседнем городе, и даже на соседнем континенте! Все это значительно усложняет идентификацию личности, поиск и доказательство причастности злоумышленника к атаке. Стоит ли удивляться огромной популярности социальной инженерии среди молодежи?

К счастью, подавляющее большинство мошенников действует по идентичным или близким шаблонам. Поэтому, изучение приемов их “работы” позволяет распознать обман и не попасться на удочку. Автором этой статьи собрана обширная коллекция хакерского арсенала, наиболее популярные “экспонаты” которой представлены ниже. Конечно, на исчерпывающее руководство по обеспечению собственной безопасности данная публикация не претендует, но общее представление о методиках хищения денег или информации все же дает.

Теория и определение понятий

Социальная инженерия заключается в том, чтобы обманом заставить пользователей предоставить точку входа для вредоносных программ. Жертва предоставляет конфиденциальную информацию или невольно устанавливает вредоносное ПО на свое устройство, потому что злоумышленник выдает себя за законного участника [1].

Сегодня социальную инженерию зачастую используют в интернете, для получения закрытой информации, или информации, которая представляет большую ценность.

Социальная инженерия - совокупность подходов в прикладных социальных науках, ориентированных: - на изменение поведения и установок людей; - на разрешение социальных проблем; - на адаптацию социальных институтов к изменяющимся условиям; - на сохранение социальной активности.

Злоумышленник получает информацию, например, путем сбора информации о служащих объекта атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего.

Злоумышленник может позвонить работнику компании (под видом технической службы) и выведать пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе. Очень часто этот трюк проходит.

Имена служащих удается узнать после череды звонков и изучения имён руководителей на сайте компании и других источников открытой информации (отчётов, рекламы и т. п.).

Используя реальные имена в разговоре со службой технической поддержки, злоумышленник рассказывает придуманную историю, что не может попасть на важное совещание на сайте со своей учетной записью удаленного доступа.

Другим подспорьем в данном методе являются исследование мусора организаций, виртуальных мусорных корзин, кража портативного компьютера или носителей информации.

Данный метод используется, когда злоумышленник наметил в качестве жертвы конкретную компанию.

Социальная инженерия — относительно молодая наука, которая является состав-

ной частью социологии, и претендует на совокупность тех специфических знаний, которые направляют, приводят в порядок и оптимизируют процесс создания, модернизации и воспроизведения новых («искусственных») социальных реальностей. Определенным образом она «достраивает» социологическую науку, завершает ее на фазе преобразования научных знаний в модели, проекты и конструкции социальных институтов, ценностей, норм, алгоритмов деятельности, отношений, поведения и т. п. Занятия сориентированы на вооружение слушателей прежде всего методологией аналитико-синтетического мышления и знаниями формализованных процедур (технологий) конструкторско-изобретательской деятельности. В характеристике формализованных операций, из которых складывается это последнее, особое внимание обращается на операции сложной комбинаторики. Игнорирование принципа системности в операциях комбинаторики нанесли и продолжают наносить большой ущерб на всех уровнях трансформационных процессов, которые происходят в нашем обществе. Последовательные знания принципиальных требований к указанным операциям дают основания к предотвращению ошибочных извращений в реформационной практике на ее макро-, мезо- и микроуровнях.

Историческая справка

Несмотря на то, что понятие социальной инженерии появилось недавно, люди в той или иной форме пользовались ее техниками испокон веков. В той же Древней Греции и Риме в большом почете были люди, могущие навешать на уши любую лапшу и убедить собеседника в «очевидной неправоте». Выступая от имени верхов, они вели дипломатические переговоры, а, подмешивая в свои слова вранье, лесть и выгодные аргументы, нередко решали такие проблемы, которые, в противном случае, невозможно было решить без помощи меча. В среде шпионов социальная инженерия всегда являлась главным оружием. Выдавая себя за кого угодно, агенты КГБ и ЦРУ могли выведать самые страшные государственные тайны.

В начале 70-х гг., в период расцвета фрикинга, некоторые телефонные хулиганы забавлялись тем, что названивали с уличных автоматов операторам Ma Bell и подкалывали их на тему компетентности. Потом кто-то, очевидно, сообразил, что, если немного перестроить фразы и кое-где солгать, можно заставить тех. персо-

нал не просто оправдываться, а выдавать в порыве эмоций конфиденциальную информацию. Фрикеры стали потихоньку экспериментировать с уловками и к концу 70-х настолько отработали техники манипулирования неподготовленными операторами, что могли без проблем узнать у них практически все, что хотели.

Заговаривать людям зубы по телефону, чтобы получить какую-то информацию или просто заставить их что-то сделать, приравнивалось к искусству. Профессионалы в этой области очень гордились своим мастерством. Самые искусные социальные инженеры (синжеры) всегда действовали экспромтом, полагаясь на свое чутье. По наводящим вопросам, по интонации голоса они могли определить комплексы и страхи человека и, мгновенно сориентировавшись, сыграть на них. Если на том конце провода находилась молоденькая, недавно поступившая на работу девушка — фрикер намекал на возможные неприятности с боссом, если это был какой-то самоуверенный тюфяк — достаточно было представиться начинающим пользовотелем, которому все нужно показать и рассказать. К каждому подбирался свой ключ. С появлением компьютеров, многие фрикеры перебрались в компьютерные сети и стали хакерами. Навыки СИ в новой области стали еще полезнее. Если раньше мозги оператору пудрили в основном для получения кусочков информации из корпоративных справочников, то теперь стало возможным узнать пароль для входа в закрытую систему и скачать оттуда кучу тех же справочников или что-то секретное. Причем такой способ был намного быстрее и проще технического. Не нужно искать дыры в навороченной системе защиты, не надо ждать, пока Jack the Ripper угадает правильный пароль, не обязательно играть в кошки-мышки с админом. Достаточно позвонить по телефону и, при правильном подходе, на другом конце линии сами назовут заветное слово.

Осуждённый компьютерный преступник и консультант по безопасности Кевин Митник популяризовал термин «социальная инженерия», указав, что для злоумышленника гораздо проще хитростью выудить информацию из системы, чем пытаться взломать её.

Виды социальной инженерии и используемые техники

Техники и термины социальной инженерии

Все техники социальной инженерии основаны на особенностях принятия решений людьми, называемых когнитивным базисом. Они также могут быть названы особенностью принятия решения человеческой и социальной психологий, основанной на том, что человек должен кому-либо доверять в социальной среде воспитания.

Претекстинг

Претекстинг — это действие, отработанное по заранее составленному сценарию (претексту). В результате цель должна выдать определённую информацию или совершить определённое действие. Этот вид атак применяется обычно по телефону. Чаще эта техника включает в себя больше, чем просто ложь, и требует каких-либо предварительных исследований (например, персонализации: дата рождения, сумма последнего счёта и др.), с тем, чтобы обеспечить доверие цели. К этому же виду относятся атаки и по онлайн-мессенджерам, например, по ICQ.

Фишинг

Фишинг — техника, направленная на жульническое получение конфиденциальной информации. Обычно злоумышленник посылает цели e-mail, подделанный под официальное письмо — от банка или платёжной системы — требующее «проверки» определённой информации или совершения определённых действий. Это письмо обычно содержит ссылку на фальшивую веб-страницу, имитирующую официальную, с корпоративным логотипом и контентом, и содержащую форму, требующую ввести конфиденциальную информацию — от домашнего адреса до пин-кода банковской карты.

Троянский конь

Эта техника эксплуатирует любопытство, либо алчность цели. Злоумышленник отправляет e-mail, содержащий во вложении «клёвый» или «сексуальный» скринсейвер, важный апгрейд антивируса или даже свежий компромат на сотрудника. Такая техника остаётся эффективной, пока пользователи будут слепо кликать по любым вложениям.

Дорожное яблоко

Этот метод атаки представляет собой адаптацию троянского коня и состоит в использовании физических носителей. Злоумышленник может подбросить инфицированный CD или флэш в месте, где носитель может быть легко найден (туалет, лифт, парковка). Носитель подделывается под официальный и сопровождается подписью, призванной вызвать любопытство.

Пример: Злоумышленник может подбросить CD, снабжённый корпоративным логотипом и ссылкой на официальный сайт компании цели, и снабдить его надписью «Заработная плата руководящего состава Q1 2007». Диск может быть оставлен на полу лифта или в вестибюле. Сотрудник по незнанию может подобрать диск и вставить его в компьютер, чтобы удовлетворить своё любопытство, или просто «добрый самаритянин» отнесёт диск в компанию.

Кви про кво

Злоумышленник может позвонить по случайному номеру в компанию и представиться сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы. В случае, если они есть, в процессе их «решения» цель вводит команды, которые позволяют хакеру запустить вредоносное программное обеспечение.

Виды социальной инженерии

Социальная инженерия подразделятся на два основных вида:

— **социальная инженерия**,
— **обратная социальная инженерия**.

У этих двух видов общее только то, что они воздействуют на человека, но при этом их способы воздействия совершенно различны. Социальная инженерия может быть применима в любой обстановке, без предварительной подготовки, а люди, в отношении которых была направлена социальная инженерия, остаются в неведении настоящей ситуации, иногда и личностей.

Социальная инженерия успешно применяется не только для взлома и получения информации, как написано во многих книгах, но и в реальных ситуациях, для извлечения обыкновенной прибыли.

В обычной жизни мы не взламываем ежедневно компьютеры и сервисы, но почти ежедневно тратим деньги, которые нужно как-то зарабатывать. Разберем самый обычный пример из жизни. Есть одна компания, под кодовым названием фирма №1. Как и у любой хорошей фирмы у нее много сайтов, на которых представлен один и тот же товар или услуга. Поисковые системы, которые являются основным источником посетителей на сайт, пытаются сделать выдачу по определенному запросу как можно более разнообразной, чтобы получить еще больше посетителей, а, следовательно, денег.

Целью обратной социальной инженерии (reverse social engineering) является заставить цель саму обратиться к злоумышленнику за «помощью». С этой целью хакер может применить следующие техники:

— **Диверсия.** Создание обратимой неполадки на компьютере жертвы.
— **Реклама.** Злоумышленник подсовывает жертве объявление вида «Если возникли неполадки с компьютером, позвоните по такому-то номеру».

Защита пользователей от техник социальной инженерии

Антропогенная защита

Простейшими методами антропогенной защиты можно назвать:

— Привлечение внимания людей к вопросам безопасности.
— Осознание пользователями всей серьезности проблемы и принятие политики безопасности системы.
— Изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.

Данные средства имеют один общий недостаток: они пассивны. Огромный процент пользователей не обращает внимания на предупреждения, даже написанные самым заметным шрифтом.

Техническая защита

К технической защите можно отнести средства, мешающие заполучить информацию и средства, мешающие воспользоваться полученной информацией.

Наибольшую распространенность среди атак в информационном пространстве социальных сетей с использованием слабостей человеческого фактора получили атаки при помощи электронных писем, как то: e-mail и внутренняя почта сети. Именно к таким атакам можно с наибольшей эффективностью применять оба метода технической защиты. Помешать злоумышленнику получить запрашиваемую информацию можно, анализируя как текст входящих писем (предположительно, злоумышленника), так и исходящих (предположительно, цели атаки) по ключевым словам. К недостаткам данного метода можно отнести очень большую нагрузку на сервер и невозможность предусмотреть все варианты написания слов. К примеру, если взломщику становится известно, что программа реагирует на слово «пароль» и слово «указать», злоумышленник может заменить их на «пассворд» и, соответственно, «ввести». Так же стоит принимать во внимание возможность написания слов с заменой кириллических букв латиницей для совпадающих символов.

Средства, мешающие воспользоваться полученной информацией, можно разделить на те, которые полностью блокируют использование данных, где бы то ни было, кроме рабочего места пользователя (привязка аутентификационных данных к серийным номерам и электронным подписям комплектующих компьютера, ip и физическому адресам), так и те, которые делают невозможным(или труднореализуемым) автоматическое использование полученных ресурсов (например, авторизация по системе Captcha, когда в качестве пароля нужно выбрать указанное ранее изображение или часть изображения, но в сильно искаженном виде). Как в первом, так и во втором случае известный баланс между ценностью требуемой информации и работой, требуемой для ее получения, смещается, вообще говоря, в сторону работы, так как частично или полностью блокируется возможность автоматизации. Таким образом, даже имея все данные, выданные ничего не подозревающим пользователем, например, с целью массово разослать рекламное сообщение (спам), злоумышленнику придется на этапе каждой итерации самостоятельно вводить полученные реквизиты.

Список использованных источников

1. Кевин Митник, Вильям Саймон «Искусство обмана»: Компания АйТи; 2004
2. Крис Касперски «Секретное оружие социальной инженерии»: Компания Ай-Ти; 2005
3. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004. — 992 с.
4. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.
5. Гришина Н.В. – Организация комплексной защиты информации. – М: Гелиос АРВ, 2007. – 256.
6. Козиол Дж., Личфилд Д., Эйтэл Д., Энли К. и др. Искусство взлома и защиты систем. — СПб/ Питер, 2006. — 416 с: ил.