Введение в курс по Социальной инженерии от “Inject School”

Урок 1.

День 1.

Тема: Что такое Социальная инженерия, далее СИ, история СИ.

.

Социальная инженерия - это совокупность приемов, действий, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату с использованием психологии и социологии.

Под термином социальная инженерия (СИ) подразумеваются сразу несколько понятий. Первое относится к социологии и обозначает совокупность методов, изменяющих человеческое поведение, обеспечивающих контроль над окружающими, их действиями. Эти подходы ориентированы на изменение организационных структур, так как самым уязвимым местом любой системы является человеческий фактор.

В каком-то роде социальная инженерия – это наука, а в сфере информационной безопасности под термином подразумевается незаконный метод получения информации. На сегодняшний день известными приемами пользуются мошенники, пытаясь добраться до «лакомого куска» – конфиденциальной или ценной информации.

По сути это метод управления действиями человека. Метод основан на выявлении слабостей человеческого фактора, такие как страхи, привычки, чувство долга, и т.д. и является очень разрушительным. Прием, когда хакер атакует не компьютер, а человека, работающего с компьютером, называется социальной инженерией. Социальные хакеры — это люди, которые знают, как можно "взломать человека", запрограммировав его на совершение нужных действий.

По масштабу действий и потенциальной разрушительной способности СИ способна нанести ущерб крупным корпорациям, целым странам, всему миру, но также в руках мирного социального инженера способна помочь достичь успеха в бизнесе и карьере, дипломатических отношениях.

Таким образом, резюмируя вышесказанное, можно утверждать, что термин "Социальная инженерия" является социологическим и обозначает совокупность организационных структур, определяющих человеческое поведение, и обеспечивает контроль над ним. В начале 21 века понятие было популяризировано, хотя методы для сбора фактов и манипуляции людьми были известны задолго до века компьютерной эры.

Методы СИ применялись и в глубокой древности, но в сфере компьютерной безопасности был популяризован компьютерным преступником, ныне консультантом по безопасности Кевином Митником, который утверждал, что самое уязвимое место в любом системе безопасности – это сам человек.

Кевин Митник — известный хакер, которому противостояли лучшие эксперты по защите информации из ФБР, и осужденный в 90-х годах правосудием США за проникновение во многие правительственные и корпоративные секретные базы. По мнению многих экспертов, Митник не обладал ни значительной технической базой, ни большими познаниями в программировании. Зато он обладал искусством общения по телефону в целях получения нужной информации и того, что сейчас называют "социальной инженерией".

То же самое можно сказать и о его книгах - никаких особенных откровений там нет. Вполне

возможно, что Митник это все прекрасно знает, более того, к сожалению, он ничего из того, что действительно знает, не рассказывает. Ни в своих выступлениях, ни в книгах. Что, наверное, в общем-то, и неудивительно, т. к. ФБР взялось тогда за него очень плотно. Было и множество объяснений, и запрет на работу с ЭВМ в течение нескольких лет, и тюремное заключение. Не стоит удивляться тому, что после таких перипетий он стал весьма законопослушным человеком, и не будет не то какие-то секретные базы похищать, но даже и о не секретных вещах станет говорить с большой осторожностью.

В результате таких недоговорок социальная инженерия представляется этаким шаманством для избранных, что не так. Более того, есть еще один важный момент. Во многих описаниях атак пропускаются целые абзацы, если не страницы. Если взять конкретно схемы некоторых, наиболее интересных атак, и попытаться их воспроизвести согласно написанному, то, скорее всего, ничего не выйдет. Потому что многие схемы К. Митника напоминают примерно такой диалог.

- Вася, дай пароль, пожалуйста!

- Да на! Жалко мне, что ли для хорошего человека.

Разбор же этой "атаки" напоминает примерно следующее: "Вася дал социальному хакеру, потому что он с рождения не умел говорить "Нет!" незнакомым людям. Поэтому основной метод противодействия социальным инженерам - это научиться говорить "Нет"". ...Может быть, эта рекомендация и подходит для Америки, но, что не для России, где большинство скорее не умеют говорить "Да", а "Нет" у всех получается весьма неплохо. Действительно, есть тип людей, которые органически не могут отказать другому человеку, но, во-первых, таких людей немного, а всех остальных нужно к такому состоянию подводить. А о том, как подводить, не сказано ни слова.

Вот примерно это и имеется в виду, когда говорят, что у Митника нередко пропускаются целые абзацы. Можно допустить, что первая фраза могла иметь место в начале, а вторая — в конце разговора. Но между ними было еще очень многое и самое интересное. Потому что, чтобы все было так просто, нужно человека погрузить либо в глубокий гипноз, либо вколоть ему "сыворотку правды". Но даже если это так и было, то об этом тоже нужно писать.

В жизни же происходит, как правило, по-другому. И пароли говорят, и базы выносят, не потому что не просто "нет" ответить не могут, а потому что "нет" отвечать бывает, ...очень не хочется. А для того, чтобы человеку, который владеет какой-то серьезной информацией, очень сложно было ответить "нет", нужно его подвести к такому состоянию. И порой социальному инженеру приходится работать с объектом достаточно долгое время, чтобы и довести его до нужного состояния.

Чем занимается социальная инженерия?

Методология управленческой деятельности может быть использована не только в корыстных целях (для мошенничества и хакерства). Социальная инженерия в жизни применяется для решения проблем на производстве, в сфере общественного взаимодействия. Конструируя различные ситуации, специалисты в этой области предугадывают возможные ошибки и варианты поведения людей. Деятельность включает в себя такие процедуры, как:

- анализ объекта деятельности;
- оценка его состояния в настоящем и будущем;
- разработка проекта нового состояния объекта;

- прогнозирование вариантов развития внутренней и внешней среды;
- реализация плана.

Очень известный пример СИ: Группа исследователей из врачей и медсестер трех больниц Среднего Запада проводила исследование, в котором психологи по телефону представлялись врачами и просили медсестер вколоть пациенту смертельную дозу лекарства.

Несмотря на то, что медсестры знали, что делали, в 95% случаев они беспрекословно выполняли команду (разумеется, их останавливали ассистенты на входе в палату.)

Социальная инженерия зародилась и получила наиболее широкое развитие в США. В послевоенный период мотивы социальной инженерии стали широко применятся в авиационной и оборонной промышленностях Северной Америки. Также СИ начала применяться в прикладных научных областях, а именно,- индустриальной социологии, военной социологии и психологии, исследованиях пропаганды и коммуникаций, групповой динамики.

До 1949 г. в стране действовала одна научная группа по социальной инженерии, к середине 60-х гг. их насчитывалось уже более 130. В настоящее время часть специалистов по СИ работает в сфере частного бизнеса. При университетах и колледжах США действуют курсы подготовки по социальной инженерии.

В России социальная инженерия долгое время находилась в тени идеологических стереотипов. Социальное прогнозное проектирование, стратегическое планирование, социальная инноватика, игровое моделирование - названия, за которыми скрывалось содержание Социоинженерной деятельности. В 1980-е годы СИ пережила период полноценного раскрытия - на предприятиях формировались исследовательские группы, организовывались масштабные исследовательские проекты.

Социоинженерный подход в настоящее время используется также и в бизнесе, журналистике как способ выяснения формирования общественного мнения.

Все методы современной социальной инженерии известны достаточно давно, и в основном пришли в нынешнюю социальную инженерию большей частью из арсенала различных спецслужб и разведывательных организаций.

Первый известный случай конкурентной разведки к VI веку до нашей эры, и произошел в Китае, когда китайцы лишились тайны изготовления шелка, которую обманным путем выкрали римские шпионы.

Для наглядности приведу еще один пример того, что же такое СИ:

В 1906 году в предместье Берлина безработный Вильгельм Фойгт купил на рынке изношенную форму прусского капитана и направился к ближайшим казармам. Там он встретил незнакомого сержанта с четырьмя гренадерами и приказал им захватить ратушу.

Фойгт забрал у сдавшегося бургомистра без малейшего сопротивления всю городскую казну - четыре тысячи марок. Затем он отдал распоряжение всем оставаться на своих местах еще полчаса, после чего уехал из города на поезде уже в гражданской одежде.

Английские газеты долго вспоминали эту историю, указывая с сарказмом на заведенные в Германии столь странные порядки, что человек в форме обладает непререкаемым авторитетом. Однако суть этой и массы подобных афер лежит гораздо глубже. Они всегда работают на уровне психологии людей, независимо от страны их проживания и актуальны по сей день. Именно из них выросла самая эффективная тактика сетевых атак на нейросеть, уютно расположившуюся между монитором и спинкой офисного кресла.

Примеров атак СИ на крупные банки и корпорации великое множество. Вот еще один из них. Происходило это в России, у одного известного и крупного банка, в многолюдном месте и световом дне остановился инкассаторский автомобиль, как только из машины вышли инкассаторы с мешками денег, подъехал черный тонированный фургон и оттуда "высыпалась" банда людей в масках и камуфляжах с автоматами, на спинах бойцов виднелась надпись "СОБР".

Инкассаторов без труда положили мордой в пол, а стоявший совсем рядом патруль полиции и наблюдавший всю эту картину невооруженным глазом, даже не дрогнул, и лишь один полицейский решил подойти к бойцам " СОБР а" и спросить, а что же происходит, на что получив ответ: « Не мешай, мы работаем», - полицейский пожал плечами и спешно удалился чтобы не мешать ребятам работать. Как вы уже догадались- никакой СОБР там не работал.

Историй связанных с применением СИ можно написать очень много, на самом деле СИ только тогда становится явной, когда люди знают что это такое. Для тех, кто умеет с ней работать, знает приемы СИ и умеет противодействовать.

Напоследок приведу еще один пример СИ:

Отдыхал я как-то в одном дорогом отеле на побережье моря. И разбирая свои вещи, вдруг увидел что распечатка билетов на самолет неправильная, там была абсолютно другая информация,
Чтобы исправить ситуацию мне нужно было скачать распечатку заново с сайта уже правильную, и где-то ее отксерокопировать на принтере, но его под рукой не оказалось.

В хороших отелях вам никогда не откажут в том, чтобы с вашей флешки взять распечатку и сделать вам ксерокопию. В моем случае т , разумеется мне тоже не отказали и совершенно без всяких опасений вставили мою флешку, и сделали распечатку. Опытные и знающие люди знают что этого делать категорически нельзя так как на флеш-карте может оказаться все что угодно, начиная от троянов, заканчивая скрытыми майнерами, получение доступа к компьютерной системе.

Точно также такие схемы работают и во многих других местах, например в сервисе распечатки фотографий. Вообще флешка является универсальным инструментом Социального хакера, часто хакер, выслеживая какую-либо жертву или же даже без оной, оставляет флеш карту или другой носитель информации в нужном ему месте, заранее зная, что человеческое любопытство победит, человек в 90% случаев даже если он знаком с методами информационной безопасности, все равно вставит эту флешку в свой компьютер, а если флеш карта была "обронена" прямо в отделении банка, под носом у "нерадивой" сотрудницы банка?

Исход один, - если у человека плохо работает файрвол (его личная осведомленность о компьютерной безопасности), он серьезно подвергает систему безопасности банка под удар, ибо любопытство распирает, а флешку нужно вставить и глянуть вот прямо сейчас. Даже такой вариант не стоит отрицать.

Вариаций использования СИ очень множество, и в обществе люди практически не имеют навыков и осведомленности о том каким образом на них могут влиять.

В последнее время социальная инженерия как наука динамично развивается, позволяя регулировать человеческое поведение и осуществлять контроль, но гораздо дольше она существует как методология атак. Профессионалы в этой области успешно обманывали людей на протяжении нескольких десятилетий, и всегда ставка делалась на человеческий фактор: любопытство, лень, страх. Чтобы не попасться в ловушку мошенников, нужно уметь распознавать основные приемы хакеров и понимать, что сведения, которые появляются в открытом доступе, могут быть использованы против тех, кто ими поделился.

Почему же многие исследователи считают, что социальная инженерия станет одним из основных инструментов хакеров XXI века? Ответ прост. Потому что технические системы защиты будут все больше и больше совершенствоваться, а люди так и будут оставаться людьми со своими слабостями, предрассудками, стереотипами, и будут самым слабым звеном в цепочке безопасности. Вы можете поставить самые совершенные системы защиты, и все равно бдительность нельзя терять ни на минуту, потому что в вашей схеме обеспечения безопасности есть одно очень ненадежное звено — человек. Настроить человеческий *брандмауэр,* иначе говоря *файрвол* (firewall), — это самое сложное и неблагодарное дело. К хорошо настроенной технике вы можете не подходить месяцами. Человеческий брандмауэр нужно подстраивать постоянно. Здесь как никогда актуально звучит главный девиз всех экспертов по безопасности: "Безопасность — это процесс, а не результат". Очень простой и часто встречающийся пример. Пусть вы директор, и у вас очень хороший сотрудник, который, по вашему мнению, ну уж никогда ничего никому не продаст и никого не продаст. В следующем месяце вы понизили ему зарплату, скажем, по тем или иным причинам. Пусть даже эти причины весьма объективны. И ситуация резко изменилась: теперь за ним глаз да глаз, потому что он места себе не находит от обиды, он уже вас убить готов, что уж тут говорить о каких-то внутрикорпоративных секретах.

Что для того, чтобы заниматься обеспечением безопасности, особенно в части настройки "человеческих файрволов", нужно обладать устойчивой нервной и психической системой. Почему, вы поймете из следующей прекрасной фразы А. Эйнштейна, которую мы, вслед за Кевином Митником, не можем не повторить: "Можно быть уверенным только в двух вещах: существовании вселенной и человеческой глупости, и я не совсем уверен насчет первой".

И в заключение необходимо развеять один устойчивый миф о социальной инженерии. О том, что это что-то такое страшное, появившееся в 80-х годах прошлого века благодаря стараниям известного хакера К. Митника, и теперь никто не знает, как от этой новой напасти защищаться.

Социальная инженерия не представляет из себя ничего страшного и появилась не вчера, — то, что человеческий фактор всегда самое слабое звено известно человечеству давно. Методы социальной инженерии были известны задолго до Митника, за несколько столетий. Те же разведчики во все века в своей деятельности процентов на 80 использовали методы социальной инженерии. К. Митник лишь стал использовать методы манипуляций сознанием человека применительно к IT. Точно так же давно было известно, как противостоять методам социальной инженерии.. Это стандартные и известные большинству методы защиты, которые нужно просто четко выполнять, и тогда все будет нормально.

В данном курсе «Социальная Инженерия» описан арсенал основных средств современного социального хакера (трансактный анализ, методология социального инженеринга, основные приемы), рассмотрены и разобраны многочисленные примеры социального программирования. Две лекции курса будут посвящены НЛП. Нейролингвистическое программирование (НЛП) представляет собой способ использования знаний, полученных из различных областей: лингвистики, нейрологии и психологии – с целью склонить оппонента к принятию «нужного» решения. Управление нервными процессами происходит с помощью языковых средств. Принципы социальной инженерии, базовые техники и убеждения взяты из НЛП. На жертву воздействуют «в реальном времени», требуя немедленного принятия решения, обращаются к подсознательным установкам индивида. Потому мы обязательно коснемся основ нейролингвистического программирования. Также в рамках курса будет дан обширный материал по введению в типологию личности.

Предупреждение!

Вся информация, связанная с курсом, а также его содержание, примеры, техники выложены только с целью ознакомления и изучения. По своей сути, этот курс о роли человеческого фактора в защите информации.

Методы социального программирования могут быть полезны как специалистам в области компьютерной безопасности, так и простым пользователям ПК, поскольку именно они часто выбираются социальными хакерами в качестве наиболее удобных мишеней. Информация защищается людьми, и основные носители информации — тоже люди, со своим обычным набором комплексов, слабостей и предрассудков, на которых можно играть и на которых играют. Тому, как это делают и как от этого защититься, и посвящен данный курс.

Защититься от социальных хакеров можно только зная их методы работы. Моя цель, ознакомить вас с этими методами, чтобы обезопасить себя от взлома социальных хакеров. Я надеюсь, что курс может оказаться полезен многим не только в профессиональном, но и в жизненном плане, так как мы коснемся таких разделов, как типология личности. Ответственность за применение данных знаний и техник слушатель курса берет полностью на себя.

На сегодня все, друзья, надеюсь, что вводный урок вам понравился! Задавайте вопросы в чат!