Урок 2

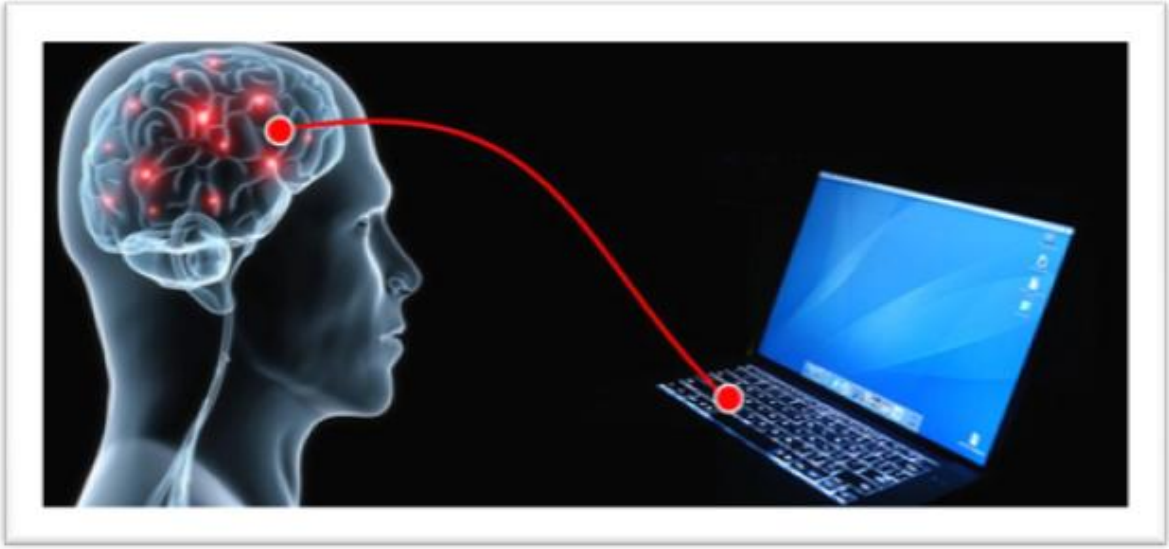
День 2

Тема лекции: «Основная схема воздействия в социальной инженерии. Что такое социальное программирование и его отличие от социальной инженерии».

Компьютерная система, которую взламывает хакер не существует сама по себе. Она всегда содержит в себе еще одну составляющую,- человека.

Образно говоря, компьютерную систему можно представить вот такой схемой.

Компьютерная система



ЧЕЛОВЕК *КОМПЬЮТЕР*

(способ взлома СИ) *(технические методы взлома)*

Задача хакера состоит в том, чтобы взломать компьютерную систему. Поскольку в нынешнее время системы технической защиты постоянно усложняются - все большую популярность для взлома этих систем получает социальная инженерия.

Хакеры применяют взлом первой составляющей компьютерной системы,- самого человека. По мнению специалистов угроза от взлома компьютерных систем с помощью СИ с каждым годом будет приобретать все большую популярность и все более совершенные методы СИ. Все просто. Методы СИ не требуют значительных финансовых вложений и больших знаний компьютерных технологий.

Как говорил Кевин Митник: «Для человеческой глупости нет патча». Людям присущи черты некоторых поведенческих наклонностей, которые можно использовать для манипулирования. Люди так и будут оставаться людьми, со своими слабостями, предрассудками, стереотипами и привычками, и будут самым слабым звеном в цепочке безопасности.

Вы можете установить свои компьютерные системы в помещении где даже нет выхода в внешний интернет, оборудовать помещения видеокамерами, любыми средствами защиты от утечки информации, подавители диктофонов, утечки через лазерный канал по вибрациям оконного стекла, вентиляцию, защищенную связь, перекрыть все способы съема информации ,- но человек все равно вынесет эту информацию за пределы вашего "супер" защищенного бункера.

Есть такое понятие как человеческий брандмауэр или файрвол,- это надежный метод защиты от утечки, но даже его настройка очень сложное и хлопотное мероприятие. Безопасность, - это процесс, а не результат.

Простой пример.

Как говорили во времена ВОВ: "Болтун-находка для шпиона".

Допустим вы большой начальник крупной корпорации с очень огромной капитализацией, ваша компания очень успешна и делает многомиллионную прибыль к примеру,- в индустрии или банковской сфере.

Есть конкуренты, которые спят и видят получить доступ к какой- либо интересующей их конфиденциальной информации, будь то маркетинговые стратегии компании, базы данных клиентов, важные переговоры и прочее, да все что угодно. И есть ваш сотрудник "Вася", которого вы отправляете в командировку на какую-то международную выставку, где он будет представлять на каком-нибудь стенде продукцию вашей компании. Вася работает на вас давно, и разумеется владеет достаточно большим объемом конфиденциальной информацией и секретами вашей фирмы. Вася знает о слабых и сильных сторонах компании, знает «все расклады», в том числе и «серые схемы», знает о контрактах, которые вскоре ваша компания собирается заключать, с какими компаниями, знает маркетинговые стратегии и многое другое.

И вот ваш сотрудник приехал на выставку и отвечает на разные вопросы интересующихся о компании, конечно же оглашая лишь ту информацию, которую он может оглашать, но к Васе подошла красивая, молодая, роскошная девица, как раз в "Васином" вкусе, а "Вася" то оказывается еще и одинок, и за разговором "Вася" уже понимает что он влюбился.

Все, господа... Вася на "крючке". Через 2-3 месяца ваша фирма пойдет ко дну...ну если не ко дну, то можно забыть о тех перспективах, которые были у вас до того как успешный "Вася" не влюбился.

Примеров такого рода может быть множество.

Или, к примеру "Вася" хороший сотрудник днем, а по субботам вечером ходит в гей-клуб. У многих людей при желании можно найти их слабые места, те места, которые они боятся афишировать. И узнав это, конкуренты могут "Васю" шантажировать, а иначе информация о том что "Вася"- гей разлетится по всем его друзьям и знакомым. Это называется вербовка.

Если в какой-то организации или структуре пропадает какая-либо конфиденциальная информация - будьте уверены, - кто-то сидит на "хвосте".

Все атаки социальных хакеров укладываются в одну очень простую схему. Разберем на примере схемы, где "Вася-гей".

1)Формулирование цели воздействия на объект . Целью в данной схеме является добыча хакером конфиденциальной информации о компании.

2)Сбор информации об объекте воздействия. Собирается информация о сотруднике "Васе"в ,социальных сетях, где просматриваются интересы, биография, любая информация об объекте.

3)Обнаружение наиболее удобных мишеней воздействия. В нашем примере удобной мишенью воздействия стала слабость "Васи" к мужскому вниманию.

4)Аттракция. Аттракция - это создание нужных условий для воздействия социоинженера на обьект. В данной схеме Аттракцией является шантаж "Васи" о разглашении его гей-тайны.

5)Принуждение к нужному действию . "Вася" сливает всю нужную информацию хакеру.

6)Нужный итог. Конкуренты получают ценнейшую информацию.

Социальная инженерия всерьез пересекается с таким понятием как "конкурентная разведка". Это сбор данных о какой-либо организации или структуре для выяснения каких-либо конфиденциальных тайн.

Одной из мишеней социальных хакеров также часто становятся базы данных каких-либо организаций. Зачастую на добычу таких данных уходят недели и даже месяцы, идет долгое внедрение в организацию, ее структуру. Хакер пытается все сильнее войти в доверие начальства, делая вид что работает на структуру, на самом деле собирая информацию о ней. Таким образом, очень часто пропадают также и секретные военные разработки и важная информация из кабинетов руководства страны.

Люди сами выносят ее оттуда и продают конкурентам или спецслужбам других стран.

Кроме социальной инженерии мы будем еще применять термин - Социальное программирование.

Социальную инженерию можно определить как манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации. Социальное программирование же может применяться безотносительно от какого-либо взлома, а для чего угодно, к примеру для обуздания агрессивной толпы или обеспечения победы какого-либо кандидата на выборах, или наоборот, для очернения кандидата и для того чтобы сделать толпу агрессивной.

Иногда кроме термина социальная инженерия употребляется также термин *обратная социальная инженерия.* Суть в том, что при обратной социальной инженерии вы человека напрямую ни к чему не принуждаете, а создаете такие условия, что он сам к вам обращается. К примеру, если вам нужно прийти в организацию под видом телефонного мастера, вы можете просто прийти и начать проверять телефонные коробки. Это в данной терминологии — социальная инженерия. А можно

поступить и по-другому. Вы создаете такую ситуацию, при которой в какой-то конкретной организации вас знают как телефонного мастера. После этого вы ждете, когда что-то случиться с телефонами, или сами делаете с ними что-то, и спокойно ждете, когда вам позвонят и попросят прийти. Это и есть обратная социальная инженерия. Таким образом, не вы сами куда-то ни с того ни с сего приходите, а вас просят прийти. Конечно, второй случай намного предпочтительнее, т. к. снимает с вас вообще все подозрения. Грамотные социоинженерные подходы именно так и строятся, поэтому этот термин мы считаем излишним, и его употреблять не будем.

Социальное программирование можно назвать наукой, которая изучает методы целенаправленного воздействия на человека или группу лиц с целью изменения или удержания их поведения в нужном направлении. Таким образом, по сути, социальный программист ставит перед собой целью овладение искусством управления людьми. Основная концепция социального программирования состоит в том, что **многие поступки людей и их реакции на то или иное внешнее воздействие во многих случаях предсказуемы.** Вещь, вообще говоря, очень интересная. Но в большинстве своем это действительно так. Общая схема методов работы социальных программистов представлена на рисунке ниже.

В социальном программировании разработка схемы воздействия идет с конца, т. е. от нужного итога.

Для наглядности приведу еще пример:

Допустим, есть большой чиновник, и у этого чиновника есть заместитель, который очень хочет на место этого чиновника попасть. К примеру, заместитель знает, что у чиновника есть тяга к алкоголю, и больное сердце. Заместитель начинает его тихонечко спаивать, в конце концов сосуды не выдерживают, инсульт, деревянный ящик. При этом начальник делает свой обычный стереотипный ход - он никогда не отказывается выпить, если ему предлагают зеленого змия

приятели и друзья. Хакер не заставляет его делать непривычных ему вещей, таких как подбить в опасный туристический поход по высокогорьям Тибета, тут как раз пешку надо заставлять ходить ладьей. Нет пешка будет ходить пешкой и выполнять свои привычные ходы- выпить на досуге. На похоронах заместитель рыдал как младенец, и потому остался близким другом семьи. Стал главой компании.

В социальном программировании разработка схемы воздействия идет с конца, т.е от нужного итога.

Общая схема методов работы социального программирования:

1)Формулирование цели воздействия на объект. Разработка итога. В нашем примере, - Заместитель хочет стать главой компании.

2) Исследование психофизических характеристик объекта воздействия с целью выбора наиболее подходящего способа воздействия. Собирается и изучается информация об объекте, его интересы, психофизиологические параметры, привычки, пристрастия. В нашем примере злоупотребление алкоголем действующим главой компании и при этом имеющаяся болезнь сердца или проблемы с печенью.

3)Разработка методов воздействия на объект и осуществление этого воздействия с целью достижения запланированного исхода. В в данной ситуации выяснилось, как я отмечал выше, что объект любит выпить, любит задушевные беседы и теплые компании, метод воздействия соответственно- алкоголь.

Приведем еще несколько примеров Социального программирования.

Есть несколько замечательных примеров того как работает социальное программирование, что это такое вообще, и как оно применяется на практике.

В одном из еще советских документальных фильмов был сюжет, где в одном из научных институтов велись исследования влияния социума на поведение людей и в сущности социального программирования. Безусловно, исследования прошли небезуспешно и для науки социальное программирование, в частности для исследований в сфере манипуляций сознанием общества были сделаны определенные выводы.

Было проведено несколько экспериментов со студентами института. Классная аудитория института психологии, научный сотрудник вызывает группу добровольцев из числа студентов в составе 10-15 человек, и просит их выйти из аудитории, через некоторое время из тех добровольцев по одному запускают в аудиторию. Перед вошедшим человеком ставят портрет мужчины лет 60, с обыкновенной среднестатистической внешностью, без всяческих проявлений эмоций.

Испытуемому говорят: « Это фото опасного преступника, составьте по фото его психологический портрет». И тут срабатывает метод "внушения" или скрытное социальное программирование. Испытуемый начинает говорить что-то вроде... «Нууу ,мне кажется он человек хитрый, подлый, коварный», и в таком духе под той же самой установкой испытуемые говорят про человека на фото, подобную информацию.

Далее заходит следующая "пятерка" испытуемых, и научный сотрудник дает установку:" Этот человек- великий ученый ". И в этой уже ситуации - характеристика шла обратная, люди повелись на установку.

Проводились еще несколько интересных экспериментов:

В научном классе располагалось несколько фотографий абсолютно разных людей, но похожих некоторыми чертами лица. Перед фотографиями садилась группа из человек 8-10 и им давалось задание: « Перед вами портреты разных людей, и сейчас в класс войдет еще один испытуемый, будет дано задание, определить есть ли на этих фотографиях, две фотографии одного и того же человека. Ваша задача вслух обсуждать, но без давления, попытаться доказать "новенькому испытуемому" что например на фото 2 и 4 один и тот же человек».

На самом деле, хоть там и были две похожие личности, но тем не менее это два абсолютно разных человека

Испытуемый после небольших колебаний, молча слушая доводы других людей, сам сделал вывод, что это действительно один и тот же человек, и даже сам после приводил аргументы.

Затем задача была усложнена значительно. Был уже другой испытуемый, другие фотографии, уверовал, что женщина на фото является мужчиной на другом фото. Фотографии были абсолютно не схожи, после испытуемый еще долго не мог поверить, что на фото абсолютно разные люди, даже разного пола.

Расскажу еще один пример из жизни моей подруги. В свое время она сдавала в институте экзамен по истории и стояла перед аудиторией вместе со своей группой. Подруга начала про себя повторять билеты и сказала вслух фразу, что после Франка-прусской войны Германии отошла часть Эльзаса и Лотарингии. На что вся группа рассмеялась в лицо, заявив, что такого слова как Лотарингия нет, есть слово Лотаргиния. Интернета в то время еще не было, учебники и лекции были дома и эту информацию подруга проверить не могла. Она начала лепетать о том, как это нет Лотарингии, а как же Карл Лотарингский? В итоге вся группа убедила подругу, что никакой Лотарингии нет, есть Эльзас и Лотаргиния, что отошли Германии. Моя подруга уверовала во мнение и авторитет толпы. Как назло ей достался как раз этот злосчастный билет. В тишине, сев к столу преподавателя, она произнесла на всю аудиторию- «Германии отошла часть Эльзаса и Лотаргинии». Преподаватель резко перебил и исправил – Лотарингии. В аудитории повисла зловещая тишина. Подруга была белая от гнева, что послушала мнение толпы и усомнилась в своих знаниях, когда двадцать человек утверждают обратное. Это яркий пример из области социального программирования, который мне рассказывала моя подруга, вспоминая институтские годы.

Еще один любопытный пример рассказала мне одна знакомая про ее гулящую от мужа подругу. Представим ситуацию. К дому подходит муж, жена сидит в машине вместе с любовником прямо перед домом. Муж открыв рот, смотрит на свою жену в машине с чужим мужчиной. Женщина выходит из машины, уходит за угол дома, машина уезжает. Муж разинув рот, продолжает стоять в шоке у подъезда. Жена как ни в чем не бывало, подходит к мужу и целует в щеку. На вопли мужа- «С кем ты была в машине и что все это значит??» жена крутит пальцем у виска и озабоченно спрашивает- все ли с ним в порядке?, что она только что вышла из за угла дома и в глаза не видела никаких машин и любовника. Главное спокойствие и уверенность в своих словах и действиях. В конечном итоге муж понял, что ему все привиделось.

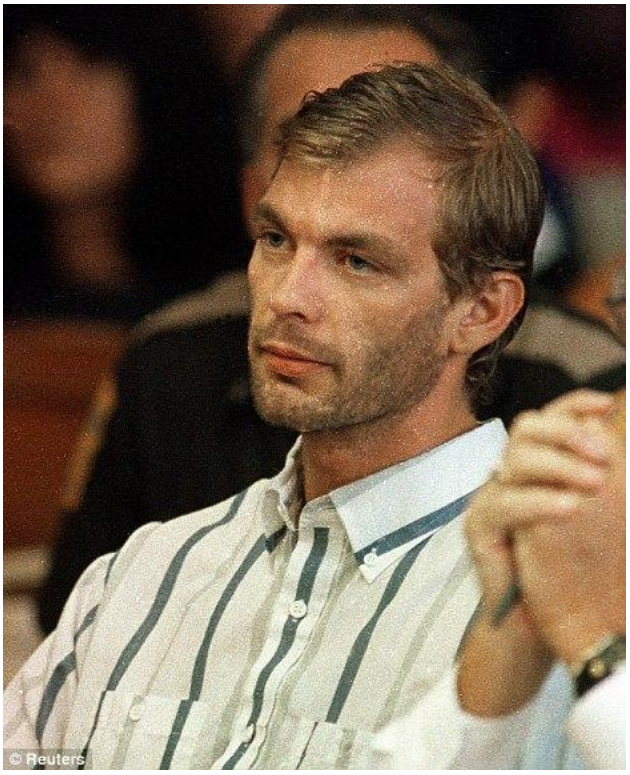
Еще известный пример того как работает социальное программирование:

В комнату заводят группу людей и ставят на стол перед ними две пирамидки, черную и белую, и говорят, - когда зайдет испытуемый, который не будет знать о нашем эксперименте, я всем задам вопрос - какого цвета пирамидки, вы все должны сказать что пирамидки обе белого цвета.

Когда заходил испытуемый, и очередь вопроса доходила до него, он тоже отвечал что пирамидки обе белого цвета.

Лабораторные задания к 2 уроку.

1) Задание к теме, *социальное программирование.*



Перед вами на фото, Джеффри Лайонел Дамер - американский серийный убийца, жертвами которого стали 17 юношей и мужчин в период между 1978 и 1991 годами. Ваша задача, - показать это фото вашим друзьям, знакомым, выдав за фото известного и успешного американского адвоката. Попросить описать по фото его основные ключевые качества, которые помогли стать ему настолько успешным адвокатом. Попросить составить максимально подробный психологический портрет.

Фото к лабораторному заданию будет прикреплено в отдельном файле.

2) Пример. У вас есть друг, у которого есть прокаченный с разным шмотом акк в игре. Это наиболее вероятный случай, что такой приятель или знакомый у вас есть. Ваша задача - зная его личные качества, интересы, увлечения, или слабые места убедить его отдать вам на время или насовсем его драгоценный акк. Подберите наиболее эффективный сценарий воздействия на

вашего друга. Например, информация о его девушке взамен на аккаунт, или даже расскажите ему что у вас есть интересная книга в формате Word о смежном увлечении вашего друга (к примеру ваш друг увлекается еще моделированием). Предложите ему крутую правдоподобную легенду, о редкой книге которая есть на вашей флешке, гипотетически на этой флешке может находится стиллер, который и добудет вам пароль от желаемой игры, или даже предоставит вам полный доступ к его компьютеру. Другу вовсе не обязательно реально скидывать вредоносное ПО на флешку, достаточно убедить его вставить ее в свой компьютер и открыть файл. Импровизируйте, и приводите свои примеры воздействия на объект по схеме воздействия СИ.

О полученных результатах по лабораторным работам жду вашего отчета в чате.

На этом урок закончен, задавайте вопросы в чат, приводите примеры из собственной жизни, когда вы сталкивались с понятием социальный инженеринг.