Урок 3.

День 3.

Тема: Основные области применения социальной инженерии. Начинаем работу по сбору информации об объекте.

Я выделяю следующие области применения.

- Общая дестабилизация работы организации с целью снижения ее влияния и возможностью последующего разрушения организации;
- Проникновение в сеть для дестабилизации работы основных узлов сети с какой либо целью;
- Воровство клиентских баз данных;
- Общая информация об организации, о ее сильных и слабых сторонах с целью последующего уничтожения данной организации тем или иным способом. Часто применяется для рейдерских атак;
- Финансовые махинации в организациях;
- Фишинг и другие способы кражи паролей доступа, доступ к персональным данным с целью кражи банковских данных;
- Информация о маркетинговых планах организации;
- Информация о наиболее перспективных сотрудниках с целью дальнейшего "переманивания" в свою организацию;
- Любая другая деятельность, связанная с получением конфиденциальной информации и разведкой;

Грамотная социнжинерная работа всегда начинается с вашей цели, к примеру,- это сбор информации об какой-то организации, человеке или структуре.

Что такое информация, ее сбор и анализ мы разберем ниже.

Информацию принято считать ценной только тогда, когда ее можно использовать, причем полезность информации зависит от ее полноты, точности , своевременности.

Следует конкретно различать и не путать : факты (данные),мнения (личностные, предположения) информацию (аналитически обработанные данные).

Информация обычно позволяет:

- ориентироваться в ситуации;
- четко планировать свои действия;
- отслеживать результат своих действий;
- уклонятся от неожиданностей;
- манипулировать отдельными людьми и группировками.

Информация обычно подразделяется:

- Тотальная . Дает общее обзорное представление об интересующем объекте, проблеме, мероприятиях.
- Текущая или оперативная. Держит в курсе изменяющихся событий.

- Конкретная. Заполняет выявленные пробелы в данных или отвечает на определенные вопросы.
- Косвенная. Подтверждает или опровергает некие предположения будучи стыкованной с последними только опосредованно.
- Оценочная. Растолковывает события и дает прогноз относительно развития ситуации в будущем.

Когда вы собираете информацию о каком либо объекте, проясните для себя следующие вопросы:

- Что нужно узнать?
- Где и в каком виде может быть желаемая информация?
- Кто ее может знать или достать?
- Как и в каком виде ее можно получить?

Четкие ответы на начальные вопросы обеспечат вам понимание последнего, техника решения которого зависит как от существующих внешних условий так и от ваших знаний, умений, воли, опыта, возможностей и изобретательности.

Получив исходную фактуру ее надо:

- Оценить по степени,достоверности,важности,секретности,стыкуемости,возможности использования.
- Интерпретировать в свете других данных и глубинной интуиции, выявив ее место в общей мозаике фактов.
- Определить нужна ли какая-то дополнительная информация.
- Эффективно использовать , учесть в своих планах, передать кому либо, придержать до следующего момента.

Информация бывает:

- Открытая, - более-менее доступная.
- Полузакрытая, - не засекреченная, но контролируема теми, кого она касается.
- Секретная, - ключевая информация, имеющая особый контроль и доступ.

Конфиденциальную информацию удается получить из весьма разнообразных источников, большую часть которых неискушенный человек попросту не принимает во внимание. Следует учитывать самые невероятные возможности, какими бы они не были.

Главными носителями секретной информации являются:

- знающие люди,- сотрудники организации, эксперты какой либо области;
- документы;
- средства беспроводной связи (телефоны)
- компьютеры, карты памяти.
- разные отслеживающие факторы, как поведение, разговоры, результаты действий.

Выйдя на тот или иной источник информации, просчитайте:

- его наличные и потенциальные возможности;
- допустимые пределы использования;
- степень его надежности;

- "Знающими лицами» в частности считаются те, кто бесспорно обладает или может обладать нужной информацией. К ним относятся эксперты, - это индивиды, чьи профессиональные знания и контакты, работа, хобби обеспечивают первоклассную ориентацию в разрабатываемом вопросе. Эксперт позволит вам по новому взглянуть на существующую проблему, выдаст базовые материалы, выведет на неизвестные ранее источники информации. Общая надежность получаемых при этом данных как правило высокая.
- «Внутренний информатор», - Осведомитель,- это человек из группировки объекта воздействия, завербованный и поставляющий информацию по материальным, моральным, и иным факторам. Ценность представляемых данных при этом существенно зависит от его возможностей и мотивов выдавать нужные сведения, верность такой информации при особом контроле может быть достаточно высока.
- "Горячий информатор"- Это любой знающий человек из сторонников объекта воздействия, также его контактеры, - друзья, партнеры, сотрудники, сослуживцы, проговаривающий информацию под влиянием активных методик воздействия в стиле жесткого форсированного допроса, пытки, шантажа, гипноза. Так как истинность сообщаемого в данном случае не гарантирована, такая импровизация приемлема только когда нет времени "нянчится" с другими источниками. Достоверность данной информации, как правило, высокая, но требует оперативной проверки.
- «Внедренный источник» - это свой человек тем или иным образом просочившийся в окружение объекта. Ценность предоставляемых сведений зависит от его индивидуальных возможностей и достигнутого уровня внедрения.
- «Легкомысленный информатор» или болтун - это человек объекта, проговаривающей интересные факты в деловой, дружеской, компанейской либо интимной беседе. Промелькнувшее случайное сообщение может быть как ложь, ценная информация, или намеренная дезинформация. Степень достоверности такой информации следует проверять.
- «Контактеры», - к ним относят людей, которые так или иначе, сталкиваются с объектом воздействия. Это могут быть друзья, родственники, партнеры, сослуживцы. Они также могут содействовать в подходе к объекту или же участвовать в прямом изъятии информации с объекта.
- «Союзник», - в данном случае подразумевается некая структура, общественная, криминальная, государственная, выступающая как противник или надзиратель объекта. Уровень надежности отдаваемой информации и материалов здесь зависит от насущных интересов, личных взаимоотношений и познаний источника.
- «Случайный источник», - иногда бывает, что какой-то индивид совершенно не рассматриваемый как потенциальный информатор вдруг оказывается носителем уникальной фактуры. Иной раз может обнаружится и доселе неизвестная информация,

контактер или союзник. Ввиду явной непредсказуемости на такого человека особо не рассчитывают, но случайно зацепив разрабатывают до конца.

В группу зафиксированных материалов входят:

- Официальные документы. К ним принадлежат личные дела и медицинские карты объекта, докладные, объяснительные записки и письма в разные инстанции, всевозможные задокументированные данные, собранные официальными структурами, такие как полиция, ЖКХ, отделы кадров об интересующем вас лице или организации. Эта информация является надежной но и она не исключает намеренную фальсификацию.
- Деловые бумаги и архивы. Это всевозможные договоры, отчеты, факсы, письма, методички, внутренние телефонные справочники, меморандумы и прочие бумаги, связанные с деловой активностью человека или организации. Они представляют собой первосортный источник конфиденциальной информации, позволяющий ориентироваться в делах объекта, прояснять его намерения и методы работы, прогнозировать поступки и возможности, выявлять партнерские связи. Достоверность информации преимущественно высшая.
- Носители цифровой информации, - компьютеры, флеш карты, планшеты, смартфоны. Достоверность информации предельно высшая, но нуждается в дополнительной проверке.
- Мусор. Выброшенные материалы в руках умелого социнженера может сослужить добрую службу. Причем добывать такие материалы иной раз сподручнее чем оригиналы.
- Страницы социальных сетей, чаты в различных мессенджерах и прочее. Данная информация требует дополнительной проверки.

Под отслеживающими факторами подразумевают акустическое (подслушивание), визуальное (слежка) и ментальное (анализирование) наблюдение за объектом.

- Подслушивание. Тайно подслушивать можно как деловые так и неформальные, дружеские и интимные разговоры. Благодаря этому удается узнавать потрясающие факты и выявлять перспективные цели организации, контакты человека, прояснять их цели и намерения. Скрытное подслушивание принято осуществлять с применением технических или программных средств прослушки, вредоносное ПО, а также контактные микрофоны, радиозакладки и прочее, но иной раз и без таковых, находясь близи беседующих.
- Тайное наблюдение. Наблюдать приходится как за объектом, так и за стационарным объектом. Скрытное наблюдение за человеком позволяет выяснить его контакты, связи, места встреч, маршруты, привычки, образ жизни, поведение, и все прочие детали необходимые при "разработке" объекта. Наблюдение за стационарным объектом в здании, офисе обеспечивает контроль посетителей и является стандартным в ходе поиска скрывающейся особы.
- Засекание слухов. Эти неподтвержденные сообщения циркулирующие в определенных контингентах людей полезны тем, что намекают на предполагаемые знания и ожидания среды ,- "слух снизу", а иной раз и на игры тех или иных сил, - слух сверху. В сущности они довольно достоверны, хотя часто бывают искажены. Кое-какую тщательно скрываемую информацию удается узнавать только из неясных слухов.

- Прояснение образа действий. Анализируя реакции объекта на слова и поведение различных людей, на обычные и экстремальные обстоятельства, можно довольно точно определить его цели и мотивы, силы и слабости, уровень подверженности чужому влиянию, информированность, ключевых партнеров, методы используемых действий. Все это дает возможность прогнозировать фактическое поведение человека или группы в самых разных ситуация, что в конечном счете позволяет эффективно ими управлять.

Взятие информации у объекта.

В качестве используемого объекта может выступать любое перспективное лицо,- член враждующей группировки, единичный игрок, контактер, союзник, обладающее любопытной информацией.

Личные мотивы выдачи информации.

Так как всякий индивид в демонстрируемом поведении направляется определенными побуждениями, понимание таковых дает возможность подобрать к нему ключи и получить желаемое.

О мотивах некоего субъекта узнают путем изучения его, причем следует учитывать и степень выраженности (очень сильно, довольно слабо) этих побуждений.

Характерные мотивы выдачи информации и возможные пути их утилизации таковы:

- Алчность. Обещание или же представление денег и иных материальных ценностей.
- Страх за себя. Шантаж, а порою и угроза либо факт грубого физического или утонченного психологического воздействия.
- Страх за своих близких . Явная угроза либо факт разнотипного насилия в духе похищения, избиения, изнасилования, кастрации, сажания на "иглу",убийства, и прочее.
- Фактор боли. Качественная пытка либо угроза интенсивного болевого воздействия.
- Сексуальная эмоциональность. Ловкое подсовывание сексуального партнера и различной порнографии с перспективой "расслабления",шантажа или обмена.
- Гражданский долг. Игра на законопослушности.
- Общечеловеческая мораль. Игра на порядочности.
- Национализм. Игра на глубинном ощущении некой национальной общности, ненависти, гордости, исключительности.
- Религиозные чувства. Побуждение ненависти к иноверцам , например.
- Тщеславие. Провоцирование желания объекта произвести определенное впечатление, показать свою значимость и осведомленность.
- Легкомыслие. Поведения человека в беззаботнейшем состоянии, неосмотрительности и болтливости. К этому же можно отнести задействование хронотопа явно повышенной доверчивости человека некое время и в определенное время, например в маршрутке.
- Помешательство на чем либо.
- Нескрываемый расчет получить взамен интересную информацию. Техника "за нос".

Разобравшись в психологии зондируемого объекта и отметив управляющие им мотивы, можно выйти на конкретные приемы и методики, способные "расколоть" объект.

Методы вербовки.

Сведения у перспективных информаторов можно получать либо разово, либо постоянно - проведя их вербовку.

Эффективными методами извлечения информации из объекта являются:

- Подкуп. Обещание или передача денег и иных материальных ценностей, как впрочем и содействие в чем либо.
- Шантаж. На реальное, сфабрикованное, на объекты уязвимости.
- Жесткая угроза либо факт физического или психологического воздействия.
- Специфический форсированный допрос. После предварительного похищения или "торможения".
- Пыткодопрос,- постепенное нагнетание ощущения и ожидания боли;
- Сексодопрос, обеспечение и эксплуатация непреодолимого сексуального желания;
- иглодопрос , вызывание наркотической ломки и обещание ее прекратить;
- наркодопрос, ввод особых наркотических средств и "раскалывание" при помрачнении сознания;
- гипнодопрос, введение в гипнотическое состояние, характеризуемое исчезание самоконтроля;
- Сексуальная подставка . Подведение интим-партнера для восприятия полезной информации, либо для содействия другим приемам эффективного влияния, вроде шантажа, допроса, уговаривания.
- Игра на эмоциях. Разжигание любви, ненависти, ревности, тщеславия и прочих ослепляющих чувств под напором которых "щекотливая фактура сообщается "сдуру","сгоряча" или "назло" кому-либо.
- Выуживание в "темную". Извлечение информации в ходе ловко проведенного допроса или разговора.
- "Промежду прочим". Поощрение состояния естественной или инспирированной болтливости.
- Игра на косвенных. Наблюдение за реакцией объекта на специально подготовленные вопросы.
- Блеф. Создание впечатления что вы знаете больше, чем на самом деле, в результате чего объект не видит дальнейшей необходимости скрывать что-либо, либо считает выкладывает информацию с целью самоутверждения.
- Параллель. Проведение темы явно способной вызвать у объекта некие ассоциации с тем, что вас интересует.
- Консультация . Просьба о содействии себе или кому либо после приведения объекта в состояние благодушия и дружелюбия.
- Целевой обмен информацией. Взаимообмен данными, следуя которому нужно дать минимум, а получить максимум, причем отдавать нужно те факты, утрата которых не принесет вам вреда.

- Убеждение. Умно скроенная беседа с эмоционально-логическим обоснованием полезности ознакомления вас с некоторыми сведениями.
- Фармакологическое воздействие. Применение химических препаратов создающих или усиливающих необходимое для проведения основного приема фоновое состояние, такое как болтливость, дружелюбие, страх, безволие, сексуальное возбуждение.

Сбор информации хакер всегда начинает после выявления конкретной цели воздействия, например,- это кража какой либо информации, паролей, секретных документов, денег и прочее. Далее следует тщательная информационная "разработка" объекта, составляется психологический портрет, собирается вся возможная информация из открытых источников, это могут быть в том числе социальные сети. Люди порой часто и совершенно бездумно выкладывают большое количество информации о себе и своем окружении в социальных сетях. Зачастую можно даже наткнутся на старые, давно забытые страницы, где может располагаться целый эшелон нужной вам информации, фотографии, места обитания, интересы, увлечения, друзья, место работы, телефоны и адреса электронных почт, никнеймы на других ресурсах.

Информация подвергается тщательной проверке и систематизации. Вы рисуете психологический портрет объекта. В зависимости от вашей начальной цели по отношению к объекту, составив его психологический портрет, вы определяете тип атаки или способ внедрения в периметр данного объекта. К примеру ваш объект явный поклонник социальной сети вконтакте, в наше время такой вид социоинженерной техники как Фишинг приобрел широчайшую популярность за счет распространения интернета, его доступности и наличия электронных устройств сейчас у каждого человека.

Согласно схеме воздействия социальной инженерии, в данной ситуации, вы определились с целью, к примеру, - это взлом страницы в вконтакте.

Далее вы собрали всю нужную информацию об объекте взлома, составили его психологический портрет и анализируете наиболее вероятный и действенный метод подхода к объекту. Например, можно завязать с объектом "случайный" разговор или переписку на какую-либо тему, которой объект выражено интересуется, поддерживая достаточно долгий контакт с объектом и постепенно входя в его доверие, вы производите аттракцию, вы начинаете непосредственную атаку, вы скидываете вашему объекту фишинговую ссылку, или файл содержащий в себе троян. Вы "прикормили" рыбку, и она клюнула.

В каждой серьезной и значительной атаке социального инжиниринга работает данная схема. Соберите информацию об объекте. Проанализируйте, какой вид атаки социальной инженерии наиболее подходит для данного объекта. Осторожно и постепенно внедряйтесь в периметр этого человека. Можно проводить и молниеносные атаки по времени, но, как правило, такие атаки наименее эффективны, человек может заподозрить что-либо, просто не клюнет на вашу наживку, или раскусит вас. Поэтому наиболее подходящий вариант атаки - это тщательная подготовка. Это не даст вам 100% гарантии успеха, но значительно повысит ваши шансы.

Что делать если информации об объекте негде достать, человек сохраняет анонимность. Разберем как пример взлом аккаунта в Телеграмм. Предположим, вы решили произвести взлом намеченной жертвы в Телеграмме для того чтобы прочитать его переписку, или провести через взломанный аккаунт дальнейшее развитие атаки на уже другой объект, "волк в овечьей шкуре".

В такой ситуации вы должны понимать, что раз вы совершенно не владеете информацией о вашей жертве, играйте на чувствах людей в целом, на их эмоциях. Все люди подвержены страхам, любовным интригам, жажде наживы. Проанализируйте те методы внедрения "стандартных" инъекций, основанных на эмоциях.

В любом случае, вам придется войти в периферию объекта, вам будет необходимо с ним завязать общение. Если это парень, представьтесь девушкой, играйте на чувстве флирта, создайте иллюзию вашей жертве, представившись какой-либо приятной особой для него. Постепенно входите в доверие объекта, и через некоторое время он попросит ваше фото. Отправляйте "фейковое" фото ему взамен, но при условии, что он отправит вам свое фото первый. В этом случае работает принцип социальной инженерии, вы играете на эмоциях человека, в данном случае объекту греет душу "новая" любовь или приятный флирт. Как правило, как минимум за короткий промежуток времени, вы сможете человека сначала деанонимизировать. В дальнейшем можете достать его номер телефона, реальное имя, страницу в вконтакте, как вариант.

Когда объект будет воспринимать вас своим, считайте что схема взаимодействия по СИ вами усвоена на отлично. Таким образом, вы подавляете файрвол объекта, вы внедрили свою инъекцию в его мозг и установили уровень доверия к вам на более менее приемлемый для успешной атаки. На такой стадии достаточно легко произвести взлом жертвы. В таких случаях можно выслать разрабатываемому человеку фишинговый сайт или троян, и не ощущая опасности от "любимого" человека или хорошего "друга" в большинстве случаев объект с радостью открывает нужные вам вкладки. Есть и более сложные методы взлома аккаунтов в Телеграмм. Узнав номер телефона нужного человека, вы можете заказать за определенную плату создание копии его сим-карты, для дальнейшего получения на нее смс и свободного доступа к его аккаунту. Правда в случае, если в аккаунте стоит двухфакторная авторизация, ничего у вас не выйдет.

После того как вы собрали нужную информацию об объекте, определили его психологический портрет, составьте на основе полученных и собранных данных несколько вариантов тем на какие вы будете общаться с вашей жертвой. Продумайте детали разговоров, возможно придумайте какие-то наводящие вопросы и все что может пригодится вам для дальнейшего внедрения. Но не увлекайтесь расспросами как в кабинете следователя, это отпугнет объект. Дайте вашему объекту иллюзию того, что он является душой вашей беседы. Постепенно, медленно, очень аккуратно продолжайте ваше общение, и точно также, прежде чем вы почувствуете что "клиент созрел", заранее продумайте план "контрольного выстрела".

Социальные сети располагают людей к неформальному общению с быстрым переходом на «ты», что в реальной жизни частенько было бы трудновыполнимо. Особенно это касается сайта знакомств. Будет большой удачей, если вы найдете на каком-нибудь сайте знакомств анкету вашей жертвы, тогда ваше знакомство точно не вызовет подозрений. Чем тщательнее подготовка к атаке, тем более вероятны ваши шансы на успех. Если атака идет через социальную сеть вконтакте, не поленитесь, изучив интересы вашего объекта, вступить в разные тематические группы, накидать на стену фото с котятами и няшными картинками, если ваш объект окажется любитель недалеких кукол и вам придется знакомиться от женского лица. Хотя, не забывайте, что жертва может потребовать с вами связаться по телефону, раз вы «близкий» друг, и отмазки от звонка могут вызвать подозрения. Вам всегда надо продумывать каждую мелочь.

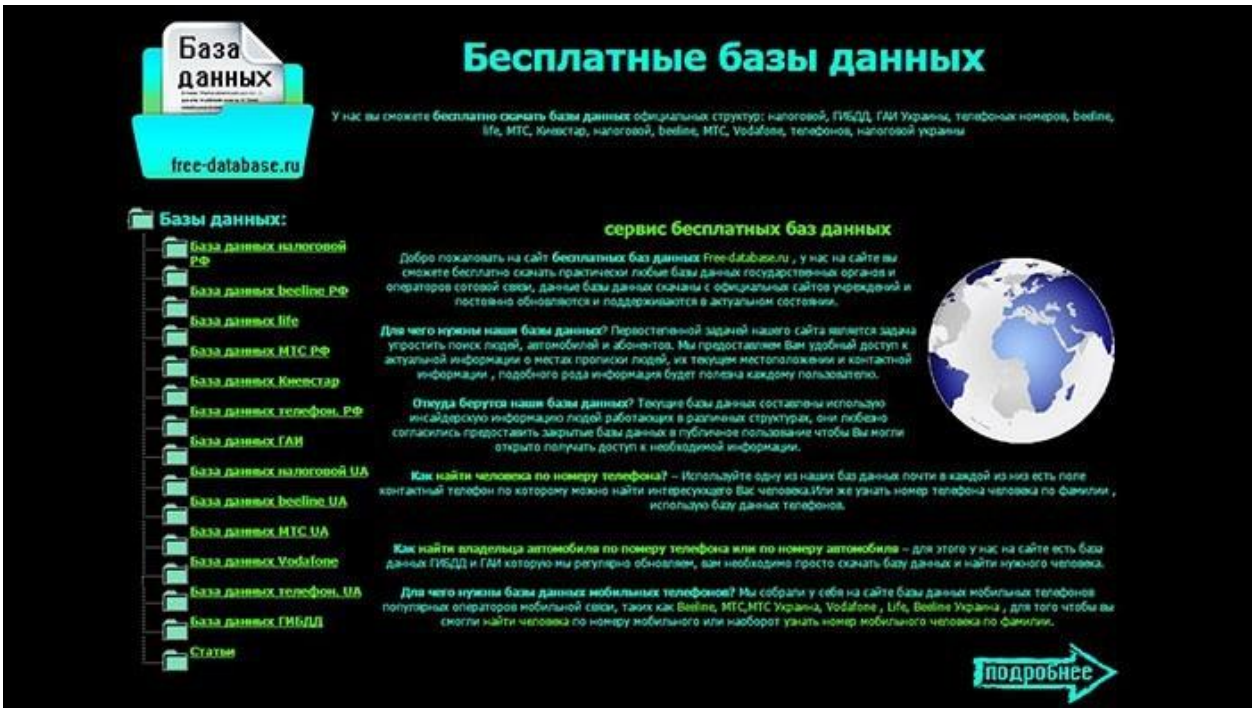
По сути аттракцию можно подразделить на несколько ступеней.

- Первая ступень - начальная аттракция. Вхождение в доверие, установление дружеских, партнерских, связей, установление положительной атмосферы общения.
- Вторая ступень - закрепление. Вы постепенно вводите свою инъекцию в объект. Идет прочное закрепление установленного контакта.
- Третья ступень - контрольный выстрел. Объект по вашему мнению готов?! наносите главный удар.

А далее, получение итога от атаки. Как правило если атака тщательно спланирована – то эффект превосходный. Приведу вам пример реального взлома одной из компаний нефтедобычи в одной из стран средней Азии. К слову скажу, такие компании имеют высочайший уровень безопасности своих систем, как правило такие системы не имеют выхода во внешний интернет, а все коды допуска, информация о работе внутренней системы находится под подпиской сотрудников о коммерческой и государственной тайны. Но произошел инцидент. Оператор ночной смены познакомился с одним человеком в сети за несколько месяцев до инцидента. Как повелось, на работе в ночную смену делать нечего, оборудование работает исправно, и в случае каких либо сбоев система оператора оповестит. Все казалось бы чудесно...но скучно...Оператор чтобы быстрее скоротать ночь на смене, сидел за своим компьютером в фейсбуке. Получив от своего хорошего "друга" или "волка в овечьей шкуре" ссылку на интересный сайт, заразил свой компьютер вредоносной программой. Социальный инженер получил базу данных паролей и логинов ночного оператора и подобрал их пароль к рабочей станции логину ночного оператора. После чего воспользовался привилегиями администратора в рабочей системе ночного оператора. Им были запущены необратимые последствия для всей системы, были поменяны условия работы всей системы. Как результат данной Социоинженерной атаки было снижение объемов переработки нефтепродуктов, достаточно долгий простой всего производства, многомиллионные штрафные санкции и нарушение сроков работы контрактов.

Технический сбор информации мы будем разбирать на специальном курсе, посвященном информационной безопасности. Одной из тем аудита информационной системы также является предварительный сбор информации об объекте, организации или сети. Могу дать краткий экскурс в чате, по требованию аудитории, конечно.

Также для пробивания информации по различным Базам данных сейчас работают множество детективных и темных сервисов. Они пробивают практически по всем организациям и структурам, могут вытянуть за определенные деньги практически любую информацию об интересующем вас объекте. Услуга очень актуальна и достаточно распространенная.



На рис. выше приведен пример одного из сайтов по пробиву информации.

На этом на сегодня все, друзья. Третий урок получился может не столь насыщенный, каким бы хотелось, множество информации уходит вглубь уже технического тестирования, и к теме СИ не имеет отношения. На следующих наших курсах мы постараемся тщательно разобрать другие виды сбора информации. Мы разберем различные сложные технические методы, такие как сбор информации по различным каналам утечки, такие как сотовая связь, лазерный съем информации с вибраций оконного стекла, IMSI-ловушки, цифровые отпечатки и прочее.

Лабораторное задание к 3 уроку.

На примере нашего сегодняшнего урока обозначьте для себя «жертву».

Соберите информацию о нем из различных источников, Вконтакте, Google, сайты знакомств, форумы, различные публикации, слухи о человеке от ваших знакомых или друзей.

Определитесь с объектом сбора информации, о котором знаете минимум информации к моменту выполнения данного задания. Соберите информацию по следующему шаблону:

1. ФИО;
2. Дата рождения и место;
3. Место и адрес проживания;
4. Место работы или род деятельности;
5. Семейное положение;
6. Хобби, увлечения, интересы;
7. Образование;
8. Предыдущие места работы и службы;
9. Номер мобильного и домашнего телефона;
10. Фамилии, имена членов семьи;

11. Места пребывания, досуга;
12. Наличие авто, недвижимости;
13. Контакты, связи, близкое окружение.

Данный список является максимально возможным, но на практике, вы сможете собрать, скорее всего, пару пунктов. Потренируйтесь на своих знакомых. Но имейте в виду, что сбор персональных данных о человеке, - это противозаконная деятельность. Потому информацию стоит брать для лабораторной работы только из открытых источников. Как в дальнейшем вы будете использовать знания, полученные на курсе, меня не касается, и ответственность я не несу. Но лабораторные работы я буду давать в рамках закона. Курс создан с целью ознакомления с **Социальной инженерией**, ее основными принципами и методами.