Психология глазами хакера.  
Начнём с хакеров.) Целью хакера является получение несанкционированного доступа для осуществления цели. Упрощённо говоря взлом(далее будем говорить упрощённо))  
Вот теперь перейдём к рассмотрению психологии в этом ключе(т.е. исходя из тех же целей и устанавливая аналогии). И так, для начала надо получить некоторое представление о том с чем имеем дело.  
При взломе человеков, мы имеем дело с психикой. Это ОС человека. Эта система во многом аналогична компьютерным ОСям, имеет гибридное ядро(подсознание), оболочку(сознание) с утилитами(умения, навыки и тп) и сторонним софтом (модели поведения).  
Основаниями гибридного ядра служат наноядро и микроядро(глубинные области бессознательного, между собой имеют довольно сложную взаимосвязь), "поверх которого" лежит модульное ядро(бессознательное и предсознательное).  
  
Далее перейдём непосредственно к взлому системы. Рассмотрим виды взлома.  
Тут два основных направления:   
мгновенный(он же кидок, мошенничество, обман и т.п.) - единоразовая акция предпринимаемая с конкретной целью  
(заполучение чего либо: вещи, денег или информации), при профессиональном исполнении объект  
не узнаёт о факте взлома. при ламерском исполнении понимает впоследствии, когда взломщик уже свинтил.  
долговременный имеет два подвида: временный и постоянный.  
1. временный взлом основан на построение выгодных отношений/налаживание отношений - применяется в областях бизнеса и для продвижения по карьерной лесницы. Состоит в построении отношений и их использовании для получения различных выгод(как правило помощь в чём либо), доступ существуют до тех пор пока сохраняются отношения или взаимная выгода.  
2. постоянный взлом (основан на действиии базовых протоколов) - наиболее широкий доступ к информации, сохраняется до дезактивации(смерти) терминала.  
  
Теперь перейдём к принципам взлома. Для осуществления взлома используются:  
баги психики, недостатки, общий базовый протокол.  
Баги и недостатки относятся к уязвимостям ОС.  
Уязвимости психики.  
Баги это деффекты системы, они же грехи(отставить панику, никакой религии, чисто прагматический аспект: грех от слова погрешность или деффект), ошибочные программы(модели поведения) компоненты глупости. Все они имеют преимущественно вредоносный характер(по крайней мере на данный момент). Стоит отметить, что в некоторых случаях несут пользу обладателю, но она пренебрижимо мала.  
Их происхождение мы сейчас рассматривать не будим, и сразу перейдём к тому как их использовать. К уязвимостям такого рода относятся все неадкватные составляющие мышления. Базовые баги: гордость(в крайнем случае гордыня), тщеславие, зависливость, ревнивость, высокомерие. Комплексные: фанатизм во всех формах(религиозный, политический-патриотизм, националистический, социальный-присущий определённой соц-группе, например футбольный), стыд, жалость, совесть, стеснение, и т.п. Простые: всевозможные мании(маниакальные стремления, они же страсти),: жадность, скупость, расточительность, стремление к богатству, азарт и т.п.  
Недостатки психики – это слабые компоненты психики. Сами по себе это полезные утилиты, они являются уязвимостями лишь в силу недостаточного развития. К ним относятся трусость, скованность, разгильдяйство(отсутствие организации), доверчивость, лень, безволие, низкий уровень самообладания, невежество и т.д.  
Тут стоит отметить допущенные в общественном мнении ошибки и возможные заблуждения. Трусость в народе противопоставляется смелости – это не верно. В действительности трусость – недостаток, низкий уровень смелости(то-есть характеристика, показатель уровня, а не собственная величина). То же самое со скованностью(низкоразвито� �ть социальных навыков), разгильдяйством, ленью, доверчивостью, невежеством(низкая осведомлённость).  
Так же не стоит путать трусость со страхом. Страх чувство которое испытывают все(почти) здоровые люди. Трусость – состояние, когда человеком владеет страх, обусловлено низким уровнем смелости. Смелость – способность контролировать страх.  
Использование уязвимостей.  
Сейчас повыходило множество околопсихологических книг о манипуляциях, в которых рассматриваются конкретные методики. И продолжают выходить новые. Но все их перечитывать не стоит, более чем достаточно и половины одной из них.  
Не стоит их все скрупулёзно перелистывать по следующим причинам:  
1.Там рассматриваются конкретные методики. Это значит, что если баг будет несколько другим - данный метод уже не сработает.  
2.Помимо того, что багов очень много, они в общем случае встречаются в частичном или изменённом виде.  
3.Видоизменение бага, делает методику менее эффективной, а в крайнем случае нерабочей напрочь.  
4.Слишком большой объём информации, в котором нет необходимости, загромождает память и затрудняет доступ.  
Поэтому эффективнее знать общие принципы и уметь выявлять уязвимости и устанавливать их характеристики, а уж составить методику конкретного взлома - дело техники, надо отметить нехитрое).  
Так-что самое главное это знать - что из себя представляет уязвимость и уметь её оценить.

Говоря в общем баги представляют из себя неразумную модель поведения(реакцию на информацию). Т.е. они выполняются бесконтрольно, при задействии бага, человек не способен адекватно оценивать ситуацию(а в некоторых случаях и вообще), воспринимать обстановку, и принимать решения. Человек уже ничего не решает и не способен выбирать. Его действия целиком задаются внешними условьями. Человек полностью зависит от данного обстоятельства.  
Использование багов делится на несколько методик. Это замануха(прямая, скрытая либо косвенная), провокация, склонение, скупка, давление.  
Для использования багов-страстей применяется замануха.. Прямая замануха представляет из себя совокупность целевой ситуации, в которую должен прийти человек(ситуация-клетка) и приманки. Приманка - реальная или мнимая перспектива получения того, что соответствует страсти взламываемого. Цель – вынудить сделать человека какое-либо действие служащие интересу взломщика. Стоит отметить, что зачастую жертва даже отдалённо понимая, что её эксплуатируют не может сопротивляться.  
Замануха широко применяется в интернете и всех видах мошенничества. Те самые «2000$ в день, заработок в интернете» «вышла новая игра, узнайте прямо сейчас» и прочие сообщения, где просят перейти по ссылке – ни что иное, как прямая замануха в простейшей форме. Другой пример – игра в напёрстки. В более сложной форме организуется какое-либо предприятие сулящее приманку, но для её достижения требуется совершить действие нужное взломщику.  
Скрытая замануха, это когда приманка не видна, а только подразумевается. Применяется в торговле. Так построена реклама, к примеру – когда продают, йогурт говорят о красоте и здоровье, счастливой жизни которую якобы получит покупатель, приобретя товар. Применений этой разновидности немного, потому для нас она особого интереса не представляет.  
Косвенная замануха используется для получения информации. Организуется какое-то совместное дело, сулящее приманку. Предлагается человеку в нём поучавствовать(ответ известен), но для его осуществления требуется знать кое какие-вещи(та самая инфа), которую он и выкладывает.  
Если составить цепочку из заманух из человека можно выжать всё. Главное не упустить момент когда нужно удалится.   
Цепочка осуществляется сложением из ряда ситуций, в каждой следующей из которых он получает приманку большего объёма, что подкрепляет его интерес.  
Скупка(он же подкуп) – ситуация когда напрямую диктуется условие, выполняя которое человек получает желаемое. Человек может быть куплен с потрахами(как говорится). Идя за приманкой, некоторые, переступают все свои принципы, оставляют все свои стремления и цели становясь в итоге марионеткой в чьих-то руках. Отличается от заманухи честностью. Объект понимает зачем он выполняет действия, и получает приманку в заявленном размере.  
При любой из методик использования страстей нужно потратится на приманку(либо трата средств либо труда). Но в большинстве случаев, да что там – во всех, страсти имеют довольно мелочные объекты стремления. Так, что суть использования простых багов сводится к скупке по дешёвке – заполучение чего-либо ценного(ваша цель) в обмен на дешёвку(приманку).  
Комплексные баги помимо заманухи дают возможность осуществлять ещё провокации и склонения.  
Провокация посылание сигнала несущего определённую информацию, вызывающую заданную, строго-определённую реакцию. Используется в основном при эксплуатации фанатизма, хотя т.о. можно использовать и совесть с жалостью.   
К примеру пользуясь фанатизмом можно втянуть человека в разговор(спровоцировать разговор), вызвать агрессивные действия, столкнуть лбами, поссорить(развалить группу), привести человека в какое-либо место, либо вынудить какое-либо действие(мыть полы нужно потому-что так ты угодишь Богу)).   
Склонение – вынуждение человека сделать, что либо не желаемое, либо не соответствующее его интересам. В основном применяется для эксплуатации совести, жалости, стеснения и стыда, реже фанатизмов(ты ведь хочешь помочь своей стране/команде/святой церкви, или -//- для тебя ничего уже не значат?). Методика заключается в том чтобы сначала создать ситуацию задействующую данный баг, затем предложить вариант её решения.   
Например в плане совести, сначала подстраивается деяние вызывающее муки совести(или же можно убедить что одно из деяний аморально), а затем предлагается действие «искупающее вину», естественно с вашим интересомhttps://freehacks.ru/images/smilies/wink.png Пример простейшей игры на жалости – попрашайки в метро.  
Заманухи в случае эксплуатации комплексных багов аналогичны прямым заманухам, но в качестве приманки используется что-либо связанное с объектом почитания – авторитетом(в случае фанатизмов) или благовидностью(совесть и т.п.). К примеру замануха на действие выглядит как: таким образом ты поможешь стране/команде/церкви. Либо же заманухой может служить объект связанный с авторитетом(к примеру мячь с закорючкой игрока, который ника не улучшит жизнь обладателя, в связи с чем объективной ценности не представляет, можно толкнуть при этом довольно дорого). Приманка для заманухи на совесть, должна быть сформирована так, чтобы совестливый человек не мог поступить другим образом(да как ты можешь ни помочь в том-то, ты же «хороший» человек), с жалостью и стыдом аналогично.  
Базовые баги дают широчайший набор возможностей для эксплуатации, это все перечисленные выше(кроме давлений) и в дополнение специализированные методики. Можно водить человека по заданному пути.  
Примером специализированной методики игры на гордости является лесть.  
Эксплуатация недостатков.  
Большинство способов сводится к склонению и давлению. Особняком стоит обман(использования невежества).  
При давлении используется усиленная подача информации на слабую утилиту, до тех пор пока система не откроет доступ.   
Пару примеров:  
Наиболее ярко видно это при эксплуатации трусости. Это прямое силовое воздействие всех мастей: устрашение(в первую очередь), угрозы, избиение. Впрочем все они так или иначе представляют собой устрашение.  
Давление при эксплуатации доверчивости состоит в общении и словесных заверениях до получения доверия.  
Эксплуатация недостатка самообладания состоит в расшатывание человека пока он не потеряет контроль, а затем контроль уже берётся в свои руки.  
  
Общие сведения об уязвимостях.  
Взаимосвязь уязвимостей. Баги и недостатки взаимосвязаны напрямую, хотя зависимость и не линейная(даже не фенкциональная). Недостатки создают благодатную почву для возникновения багов. Но множество недостатков не гарантирует множество багов, они создают лишь почву, а попадут ли на неё семена – дело случая. И в то же время если достаточно много недостатков, то недостающие баги можно внедрить(я это не поддерживаю, потому-что таким образом ты губишь человека. мало какая цель может оправдывать такие средства, но тем не менее такая возможность имеется). Кстати говоря, по видимому часть багов являются искуственно создаными вирусами.  
Баги же сжирают огромные ресурсы системы, тем самым вызывая появление и углубление недостатков – тут линейная зависимость.  
Взаимосвязь эксплуатации. Недостатки облегчают и упрощают использование багов, делают взлом по ним более доступным. Чем больше недостатков(слабостей, слабых мест) и чем они глубже, тем проще использовать баг. Обратное неверно, в случае единичных багов(т.е. до тех пор пока они не сжирают большую часть терминальных ресурсов). То есть наличие бага, не облегчает взлом по недостатку.  
  
Особенности эксплуатации: чем больше и глубже уязвимость(будь то баг или недостаток) тем проще осуществляется взлом. Если уязвимости небольшие то для осуществления взлома нужно умелое(а в некоторых случаях мастерское) исполнение и придётся приложить много усилий. Взлом будет трудоёмок. А при глубоких обширных деффектах всё делается без особого труда.  
  
Поиск уязвимостей. Проверка системы на уязвимости может быть осуществлена несколькими методами.  
Непосредственный анализ оболочки и модульного ядра. Эти части ОСи доступны непосредственному наблюдению, что даёт возможность увидеть уязвимости. Для применения этого метода требуется достаточно высокий уровень умения, в силу чего доступен он не столь многим людям.  
Тестирование. Осуществляется путём посыла на терминал небольших пакетов, каждый из которых содержит информацию на определённую уязвимость. Те из них на которые получен отклик покажут и наличие уязвимости. Таким образом прощупывается вся система, а потом планируется атака. Пакеты должны быть именно небольшими, выглядящими как случайности, чтобы не спугнуть объект. Так же есть вариант с созданием определённых ситуаций(испытание).  
  
Другие виды воздействий.  
Несколько отличаются по осуществлению Ddos-атаки на психику ¬– то есть воздействие на ОС с целью вывести ресурс из строя либо полностью либо в определённом плане.  
Псевдо-ddos-атака это воздействие целью которого лишить человека деловой активности, помешать осуществить какое-либо дело. Осуществляется по средством взлома-заманухи. Суть состоит в отвлечение объекта на приманку. Отвлекаясь на приманку человек упускает дело, ему становится не до него. Осуществляется путём дразниловки приманкой, которая то приближается оказываясь прям под носом, то вновь уходя в даль. Время от времени предоставляя мелкие кусочки(чтобы сильнее разжечь интерес).  
Собственно ddos-атака, осуществляется путём давления(взлом по недостаткам). Суть заключается в длительном перегружающем воздействие на слабую утилиту, что лишает объект деловой активности полностью.  
Гипноз стоит несколько обособлено. Он похож на методику – давление. Основан на перегрузке внимания. То есть псевдоуязвимостью является недостаточность силы внимания.   
Принцип осуществления – подача столь большого потока информации, что внимание не успевает его обрабатывать, и система повисает. Но в отличие от компа, мозг никогда не отключается полностью. Гаснет только сознание(оболочка с утилитами и софтом, в которой и находятся все системы безопасности). Взломщик получает доступ к модульному ядру и непосредственно задаёт команды. Чем то сходно с загрузкой в безопасном режиме но не совсем. На гипнозе подробно останавливаться не буду, так как сам этим методом не владею. Защита от гипноза будет рассмотрена ниже(ей я владею и практиковал).  
Взлом «на лоха». Используется для получения информации, осуществлятся может двумя способами. Первый – берёшь и говоришь общие фразы утвердительным тоном, так как будто ты, что то знаешь. Говоришь их уверенно и напористо. На все вопросы отвечаешь столь-же общими фразами, подталкивающими к нужному действию(выложить всё). Все фразы должны быть сформулированы в утвердительной форме. Далее как только пациент произносит, что либо за что можно зацепится – хватаемся и раскручиваем его.   
Выглядит примерно так(опущю начало разговора, и начну от момента начала взлома):  
-Ну что, рассказывай.  
- Чего рассказывать?  
-Ага, типо не помнишь?  
-Да, реально, вроде нечего рассказывать.  
-дурочку выключи, не помнит, она. Было ведь на этой неделе. Такое и через год не забудишь.  
-А ты про поездку?  
-А про что-же ещё, чё думала я не знаю!? Мне всё рассказали. Ну и как прошло?  
Ну и далее человек всё рассказывает. Оценивая этот метод с позиций разума, вероятность успеха должна быть процентов 10, но на практике получается 100%(9/9). Данные были получены различные и порой неожиданные. Этот способ практиковал лишь в шутку(потому и неожиданные).  
  
И в заключение стоит сказать, что взламывая ОСи необходимо, прежде всего, пропатчить свою систему. Убрать все уязвимости, чтобы защитится от ответного воздействия в случае если оно возникнет. Так ведь делают и хакеры, заботясь о том, чтобы их не вычислили – так что всё аналогично).  
И вторая причина убрать уязвимости – если в системе слишком много уязвимостей это затрудняет(в крайнем случае делает невозможным) взлом другой ОСи. Каким образом это происходит сейчас рассматриваться не будет. В общем для осуществления каждого взлома есть свои системные требования.  
Это помимо, общего снижения производительности.  
Так-же, как и всем людям, переступающим закон, хакерам в частности необходимо позаботится об такой уязвимости как «трусость». По той простой причине, что мусора, как и все силовые структуры ведут взлом именно по ней. Если вас взломают вы не только усугубите своё положение, но и возможно навредите другим, таким-же как вы. Взлом приведет к предательству близких вам людей, и падению себя в своих же глазах(это помимо объективного). Неправильно когда из-за дел одно человека, страдают другие.  
Взлом по уязвимостям применяется для осуществления мгновенного взлома( и не важно на сколько длителена общая продолжительность контакта, результаты взлома так или иначе кратковременны). То есть всё вышеперечисленное относится к мгновенному взлому.  
Пы. Сы. Если кто-то вас обманул, будьте ему благодарны, он вскрыл и наглядно показал уязвимость в вашей системе.

Временный взлом осуществляется, как говорилось ранее, путём построения взаимовыгодных отношений. Основан на действии негласного правила общения: взаимоодолжения(то есть когда ты помогаешь человеку, он подразумевает себя должным, это правило обычно не осознаётся. Порой даже отрицается, но оно есть и оно работает) Взаимовыгодные не значит равнозначные – но так или иначе выгоду получают оба участника. Если один из участников перестаёт получать выгоду то очень скоро рушаться отношения и как следствие - Access deniedhttps://freehacks.ru/images/smilies/wink.png.   
Применяется для получения помощи(то есть действий или открытой, но редкой информации – профессиональных консультаций) или установления деловых отношений.  
В осуществлении прост до безобразия – установление выгодных отношений, построенных на том чтобы давать человеку, то что его интересует(подкармливать). То есть сделать так, чтобы отношения с тобой человеку были выгодны(в начеле в одностороннем порядке, то есть вложения со стороны взломщика). Выгода не обязательна материальная, есть так-же такие формы выгоды как приятность общения(человек получает удовольствие от общения), помощь в различных ситуациях(подвезти жену до больнице, помочь комп настроить/отремонтировать), осуществление совместных дел(взаимодействие) и т.д. Выгода может быть как равноценной так и неравноценной(взломщик получает больше).  
Доступ существует до тех пор пока существуют отношения и взаимная выгода. Так к примеру, при долгой(долгая это значит годы) разлуке размер помощи существенно снижается(ограниченный доступ). При плавном(без ссор) разрыве отношений прекращается полностью.  
Недостаток этого вида взлома – ограниченность доступа к информации, но в некоторых случаях он и не нужен. Другой недостаток заключается в низкой прочности связей. На взломанного человека нельзя положиться, как только у него появятся более выгодные варианты, отношения будут разорваны. Так же не стоит ждать помощи в сложной, подразумевающей разлуку ситуации(тяжёлая болезнь, пленение и прочее).  
  
Мгновенные и временные взломы, лично мне не нравятся, особо меня не интересуют и по вполне объективным причинам.  
Мгновенные взломы это ламерские взломы. Они не требуют ни особого мастерства, ни специальных знаний. Это низкий уровень. Овладеть им довольно просто. Но особого внимания он не стоит, потому-что занимаясь делом низкого уровня, и сам остаёшься на низком уровне. Для взломщика нет перспектив развития ни как личности, ни как взломщика.  
Помимо безинтересности исполнения, они низки и с точки зрения результата. Он хоть и превосходит затраченные средства, всё равно мелочен. Вы получаете мелочь за свой труд.  
Кто-то, возможно, скажет что информация может быть очень ценной. А вот тут есть но. Если человек работает с ценной информацией, то у него достаточные профессиональные навыки чтобы не допустить взлом по уязвимостям.  
А вот умение находить уязвимость – штука очень полезная и нужная. Вот это пожалуй и есть то единственное, почему стоит ознакомится с мгновенным взломом на практике. Это касается только начинающих взломщиков.  
Временные взломы, с точки зрения искусности исполнения не отличаются от мгновенных. То есть, тоже безыскусны. Они правда несколько посложнее, но в основном за счёт длительности проведения(нужно сохранить ситуацию на длительный срок). Результат, за щёт постоянства, длительности и большем удобстве пользования ощутимо крупнее. Но всё-же на мой взгляд, не особо значителен.  
Ну и теперь остался последний вид взлома – постоянный взлом. Этот вид, на мой взгляд, наиболее интересен, сложен. В связи с этим развивает самого взломщика. Этот вид взлома самый результативный. Результаты данного взлома самые значительные. Тут уже безо всяких взглядов – объективный факт.  
Ну что-ж перейдём к рассмотрению самого взлома.  
Взлом осуществляется за счёт базовых протоколов наноядра – протокола развития и протокола организации.  
Взлом возможен при наличие несоответствия возраст/развитие. Наиболее распространённое несоответствие – взрослый/подросток и молодой/подросток(около 75-85% российского населения). Изредко встречается несоответствие – взрослый/ребёнок.  
Применяется в случаях когда нужно создать устойчивую надёжную группу(к примеру для осуществления сложного дела), а подходящего контингента больше нету.  
Если сказать по простому, когда нужен профессионал высокого уровня и широкого профиля, а вокруг одни чмошники, бездари и слюнтяи(утрирую конечно). Суть подхода состоит в том, чтобы из «дурака» сделать «героя».

Осуществляется он по следующему алгоритму:  
1. Устанавливается контакт с терминалом. В это время осуществляется выявление уязвимостей.  
2. Первичный взлом. Тут мы получаем предварительный доступ к терминалу, далее оглашаем(наглядно) список его уязвимостей. Если необходимо этому предшествует демонстрация.  
3. Получение формального согласия на взлом. Тут управление терминалом переходит в наши руки.  
4. Пропатчивание системы, устранение уязвимостей: удаляем баги, обновляем утилиты, устанавливаем новые утилиты и дополнительный софт. На этом этапе открывается доступ к информации и к середине процесса взломщик уже имеет полный доступ к информации терминала.  
5. Обучаем его работе с новым софтом и отдаём управление обратно. На этом взлом завершён.  
Теперь шаги подробно.  
Ну, касаемо первого шага, думаю понятно зачем он нужен. Осуществляется теми-же методиками, что и временный взлом: налаживание общения, заинтересовывание, помогание и т.д. Уязвимости устанавливаются в основном путём непосредственного анализа оболочки и модульника. Некоторые псевдотестированием(анали� � поведения в происходящих жизненных ситуациях).  
Шаг второй – решающий момент, основа подготовительного этапа взлома. Заполучив доверие в первом этапе, идёт продолжение банкета. Здесь человеку обрисовывается перспектива лучшей жизни и то от чего зависит её достижение. Обозначаются другие варианты жизни.  
Так же на этом этапе необходим заполучить уважение(порой к нему добавляется ещё и почтение). Осуществляется путём демонстрации своих преимуществ, и преимущества своей жизни. Преимуществ того, что предлагается тому что есть сейчас. В этом собственно и заключается взлом. После чего показываются причины, сложившейся ситуации(заключающиеся в уязвимостях). Даётся полный, адекватный и обоснованный расклад по уязвимостям.  
С третьего шага собственно и начинается сам взлом, им же заканчивается подготовительный этап. С момента получения согласия управление терминалом переходит в руки взломщика. Поначалу частично, а затем почти полностью.   
Но согласие должно быть именно формальным, сам вопрос задаётся в тот момент, когда у человека осталась только одна дорога – согласится. То есть по факту выбора здесь не предоставляется. Ответ известен заранее(правда, только взломщику).  
Необходимость формального согласия сложно обосновать в рамках рациональной логики. Факт её необходимости получен при анализе исходников наноядра. Так-что не могу сказать зачем но, оно нужно, так эффективнее протекает взлом(знание из того-же источника).  
Я всегда его получал, и впредь не собираюсь этот шаг обходить стороной.  
Осуществляется этот этап следующим образом. Перед самым моентом получения согласия, человеку выкладывается на стол всё, что собрано вами ранее. Всё, на что взломщик кусочно обращал его внимание ранее, излагается чётким связным текстом. Это лучшие перспективы, уязвимости мешающие их достичь, методы реализации желаемого, обосновывается выгодность мероприятия(взлома), после чего уже делается предложение принять участие в деле. Приняв предложение человек отдаёт своё формальное согласие.  
Стоит отметить, что с основами изложенного он должен быть ознакомлен ранее. Человек должен понимать о чём говорит взломщик. На этом шаге детали мозаики, которые человек видел ранее, взломщик просто собирает в картину, добавляя новые детали для полноты картины.  
Четвёртый этап – самый длительный. Перестройка ОС и её компонентов длительный и трудоёмкий процесс.  
И так вначале осуществляем одновременно, парралельно снос багов(в отличие от сайтов в ОСи человеков это целостные программы) и обновление(улучшение утилит).  
Снос багов осуществляется путём их наглядного показа, демонстрации их вреда и заданий на сопротивление им(на разумный контроль) с ведением постоянного их детектирования.  
Устранение недостатков производится путём целенаправленной развивающей тренировки. На неё подаётся предельная нагрузка, но не выше, чтобы не сломать систему. Подача нагрузки осуществляется с осознанием человека. То есть человек понимает суть мероприятия.  
Патч системы осуществляется путём работы с базовыми функциями(самообладание, воля, выдержка, разумный подход к принятию решений, развитие ума и разума).  
Обновление утилит – обучение навыкам требуемым в перечне предстоящих дел.  
Софт меняется посредством обоснования необходимости, выгодности нового подхода, затем обучение, затем введение в привычку посредством периодического повторения.  
По мере осуществления четвёртого этапа снижаем контроль осуществления выполнения заданий, оставляя их на самостаятельную проработку. В начале нужно контролировать выполнение каждого задания. Затем некоторые задания даются, но контроль за ними не осуществляется. Постепенно понимая пользу от предложенного начинает оценивать, результат и осуществлять выполнение самостоятельно. Под конец задания просто даются и никакой контроль не ведётся. Они выполняются полностью самостоятельно и контроль не требуется.  
По мере проведения этого этапа, открывается доступ к информации терминала, где-то к середине взломщик уже имеет полный доступ к информации. Это по видимому происходит по двум причинам. По причине того, что с информацией и она просто необходима. Вторая причина – рост доверия(когда человек понимает, что всё идёт ему на пользу, а уже полученная информация воспринимается адекватно и не придаётся огласке).  
Шаг пятый. Обучение работы с софтом особо не отличается от изложенного в шаге четвёртом. Единственная особенность – тут показываются методы работы с собственной оболочкой, и методы обзора модульного ядра.  
Взлом не нужно завершать самому. Одныжды человек скажет – остановись мгновение, ты прекрасно. Это всё конечно хорошо, но с меня хватит. Тут уже выражаешь своё формальное согласие(потому-что он не спрашивает, а объявляет о своём решении) и одобрение. Затем человеку предлагается дружба и совместное занятие тем самым делом, ради которого всё это затеивалось. Он соглашается. Всё взлом завершён, получен достойный верный, честный, способный компаньон/партнёр/соратник/сообщник. Доступ к управлению с этого момента завершается(оно и не надо, управление это тяжёлый труд и лишний геморой). Доступ к информации сохраняется в полном объёме и по видимому, пожизненно(не довелось проверить.  
Системные требования взлома: значительное превосходство взломщика над взламываемым по умственным и волевым характеристикам, освоение взломщиком разума как минимум на начальном уровне, минимальный возраст развития – молодость, отсутствие глубоких и обширных багов.  
При наличие большого числа багов в ОСи взломщика, взлом так-же неосуществим.

НЛП-ж

Нет -ж.   
нлп - ближе к гипнозу. Введение команд задаётся путём расположения слов в тексте.  
Один из приёмов: фраза команда разбивается по отдельным словам. затем составляется связный текст, таким образом, чтобы слово из фразы команды было каждым третьим в тексте. таким образом вся фраза попадает в ближайшее подсознание(при удачном раскладе).  
  
Там частью банальные манипуляции, просто обобщены и найдены корни, частью банальные древние как мир методы(очевидные), частью смешанная методика из разных областей.