Hacker Highschool

SECURITY AWARENESS FOR TEENS



Урок 1
Быть хакером

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

WWW.ISECOM.ORG - WWW.OSSTMM.ORG - WWW.HACKERHIGHSCHOOL.ORG - WWW.BADPEOPLEPROJECT.ORG - WWW.OSSTMMTRAINING.ORG

ВНИМАНИЕ

Проект Hacker Highschool является средством обучения и, как в любом обучающем средстве, существует опасность. Некоторые уроки, если ими злоупотреблять, могут привести к физической травме. Также дополнительные опасности могут быть там, где еще недостаточно исследований о возможных последствиях излучений от специфической техники. Студенты, использующие эти уроки, должны контролироваться, но и поощряться на изучение, попытки и занятия. Однако ISECOM не несет ответственность за то, как любая информация в этом документе может быть использована во вред.

Следующие уроки и книги являются открытыми и общедоступными в следующих статьях и условиях ISECOM:

Все работы проекта Hacker Highschool предназначены для некоммерческого использования с учащимися начальной школы, студентами младших курсов Highschool, и студентами высших из государственных образовательных учреждений, частных организаций или частично для домашнего обучения. Эти материалы в любой форме не могут быть использованы для продажи. Предоставление этих материалов любому классу, обучающей организации или лагерю, в которых взимается плата, категорически запрещено без лицензии, в том числе на уроки в колледже, университете, профессионально-технических занятиях, летних или компьютерных лагерях и тому подобное. Для приобретения лицензии посетите раздел ЛИЦЕНЗИИ на веб-странице в HHS http://www.hackerhighschool.org/licensing.html.

Проект Hacker Highschool является открытым сообществом и если Вы найдете достоинства в этом проекте, мы просим Вас поддержать нас путем приобретения лицензии, дарения или спонсорства.

Содержание

Сотрудники журнала

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Kim Truett, ISECOM
Marco Ivaldi, ISECOM
Shaun Copplestone, ISECOM
Greg Playle, ISECOM
Jeff Cleveland, ISECOM
Simone Onofri, ISECOM
Tom Thomas, ISECOM
Valentin Pashkov, русский перевод
Roman Sinchuk, русский перевод

ISECOM

Любовь к взлому

Предисловие от Pete Herzog

Из всего, что Вы, возможно, слышали о хакерах, правда — то, что они делают очень-очень хорошо - это обнаружение. Хакеры - мотивированные, находчивые и креативные люди. Они проникают в суть работы предмета до такой степени, что они знают, как взять его под свой контроль и переделать во что-то другое. Это позволяет им переосмыслить даже большие идеи, потому что они могут действительно докопаться до сути того, как все функционирует. К тому же они не бояться сделать одну и ту же ошибку дважды только из-за научного любопытства, чтобы посмотреть имеет ли эта ошибка всегда одинаковые результаты. Вот почему хакеры не воспринимают провалы как ошибки или трату времени, потому что каждый провал означает нечто новое, что может быть изучено. И все эти черты необходимы любому, кто хочет добиться прогресса.

> *Многие люди, которых называли хакерами, особенно со стороны средств массовой информации, или которые имели проблемы со "взломом", на самом деле не были хакерами.*

Хакеры — тип практического, экспериментирующего ученого, хотя возможно иногда термин "сумасшедший ученный" подходит больше, так как в отличии от профессиональных ученных, они уходят с головой в чувства, а не в формальные гипотезы. Это не обязательно плохо. Много интересных вещей были разработаны или придуманы людьми, которые не следуют стандартным соглашениям о том, что было известно или предполагалось правдой в то время.

Математик *Георг Кантор* предложил новые идеи о бесконечности и теории множеств, что вызвало возмущение среди многих коллег-математиков настолько, что один назвал его идеи "тяжелой болезнью", заражающей математику.

Никола Тесла – другой человек, считавшийся "сумасшедшим ученным" в свое время, знал больше всех о том, как ведет себя электричество. Он придумал, возможно, первый бесколлекторный двигатель, в котором проходила электроэнергия переменного тока, но в основном он известен, как эффект Тесла или катушка Тесла.

Также был *Игнац Филипп Земмельвайс*, который выяснил, что доктора должны мыть свои руки между лечением пациентов, чтобы заболевание не распространилось. Он заинтересовался, является ли распространение заболевания между пациентами его виной, поэтому он решил мыть руки между визитами к пациентам, и, конечно же, случаи заражения исчезли. Его идеи пошли против научной конвенции о том, что было известно в то время о микробах(ничего), а также удобства врачей, которые чувствовали, что будет слишком хлопотно сохранять руки в чистоте.

То, что Вы думаете, что Вы знаете о хакерах, это то, что они могут прорваться в чужие компьютеры и взять счета чужих людей. Они могут читать вашу электронную

почту без вашего ведома. Они могут смотреть через вашу веб-камеру без вашего разрешения и могут видеть и слышать Вас в предполагаемом уединении собственного дома. Это не соответствует действительности.

Некоторые хакеры видят сетевую безопасность как еще один вызов, поэтому они возятся с различными способами обмануть или одурачить систему, но на самом деле то, что они пытаются сделать – это перехитрить сетевые инсталляторы или конструкторы. Они узнают так много о сети, как только могут, где она берет инструкции, правила использования и как она взаимодействует с операционными системами и другими системами пользователей, которые имеют доступ к ней, и администраторами, которые управляют ей. Затем хакеры применяют все эти знания, чтобы испробовать различные способы для получения того, чего они хотят. Этот вид взлома может быть очень полезен в мире для понимания того, как обезопасить себя создать более совершенные технологии.

К сожалению, иногда взлом осуществляется преступниками и то, что они хотят, является незаконным и вредным. И о них, как правило, Вы читаете в новостях.

Хакер — это не тот, кто постит на чужую страницу, когда он выходит со своей странички в социальных сетях или **взламывает**(англ «shoulder-surfs») пароли, и затем запускает в своей учетной записи. Это не хакерство. Хакер также не тот, кто загружает **скрипт кидди**(англ «script kiddie») для взлома чужих электронных адресов. Это не хакеры; это просто воры и вандалы.

Взлом — это исследование. Вы никогда не пытались переделать что-то снова и снова различными способами, чтобы заставить его делать то, что Вам надо? Вы когда-нибудь открывали машину или устройство, чтобы посмотреть, как она работает, исследовать все компоненты, а затем внести необходимые изменения, чтобы увидеть насколько иначе стало работать? Это взлом. Вы взламываете всякий раз, когда Вы тщательно изучаете, как что-то действительно работает, для того, чтобы творчески использовать это так, как Вы хотите.

Просто так вышло, что способ, которым разработан интернет, а также огромное число различных приложений, систем, устройств и процессов делает его наиболее распространенным местом поиска хакеров. Вы можете сказать, что он был создан хакерами, поэтому это самая лучшая площадка для них. Но это не единственное место. Вы можете найти огромное количество хакеров практически в каждой области и индустрии, и все они имеют одно общую черту: они тратят время на изучение работы вещей, так что они могут заставить работать их по-новому. Они не смотрят на то, как сделан оригинал, но вместо этого видят больше и лучше потенциала, и взламываю для получения чего-то нового.

Не думайте, что Вы можете просто быть великим хакером. Только совершая потрясающие взломы с огромным смирением Вы может стать великим.

Взлом сам по себе не является незаконным. По крайне мере не больше, чем бросать камень — незаконно. Все это сводится к намерению. Если Вы бросили камень и ваши намерения — ранить кого-то, то это преступление. Если Вы не хоетли

никого обидеть, но кто-то пострадал, то это не может быть преступлением, но Вы понесете ответственность за свои поступки, и оплатите ущерб. В проекте ISECOM по подготовке хакеров **(Hacker Profiling Project)** было выявлено, что самый большой ущерб от взлома исходит от молодых, неопытных хакеров, повреждающих случайно чужое имущество. Это как бросать камни на улице просто для забавы, но в процессе появятся вмятины на машине и разбитые окна. Может быть, ущерб неумышленный, но Вы знаете, что Вы понесете ответственность и заплатите за это. Так что будьте осторожны, когда происходит взлом чужого имущества. Лучше взламывайте собственное имущество.

Взломать то, что Вы приобрели и чем владеете может быть незаконно. Есть хакеры, которые были наказаны за взлом собственных устройств и компьютеров. Есть хакеры, которые взломали программы, музыку и фильмы, которые они купили, и они были привлечены к ответственности за это. В частности, Вам может быть не разрешено легально взламывать программное обеспечение, которые Вы приобрели, даже если это только ради проверки, что оно достаточно безопасно, чтобы запускать на своем компьютере. Это происходит потому, что многие купленные вами вещи могут контактировать с контрактом или **Лицензионным Пользовательским Соглашением (EULA),** которое говорит о том, чего Вы не должны делать. И Вы соглашаетесь с этим, когда открываете или устанавливаете продукт, даже если Вы не можете прочитать его или даже не знаете об этом, пока не закроете или установите его. Имейте это в виду, когда Вы практикуете хакерские навыки на том, что Вы приобрели для собственного пользования.

Зачем быть хакером?

Рассмотрим, как ученые составили карту человеческого генома: они использовали метод, разработанный для декодирования паролей. Пароли обычно хранятся в зашифрованном виде, поэтому их трудно украсть. Иерархический шот-ган **брутфорсинг**(англ «brute-forcing») это метод расшифровки паролей путем **взлома**(англ «crack») их зашифрованной формы. Он ломает зашифрованный **хэш**(англ «hesh») пароля, преобразовывая несколько символов за раз, затем сшивает их обратно. Исследователи генома адаптировали эту технику, чтобы составить карту целых 3,3 миллиарда базовых пар генома человека.

Хакерство проявляется на кухне, когда повара используют жидкий азот в качестве охлаждающего агента, чтобы сделать идеальное мороженое, или когда они рубят помидоры, чтобы сделать картофель фри с томатным соусом вместо кетчупа или им просто нужно сделать что-то, для чего у них нет нужного оборудования...

Химики взламывают элементы и соединения на протяжении веков. От природы молекулы привередливы, когда речь заходит о том, как они ведут себя в различных условиях (на жаре, холоде, в горах, или глубоко в океане), так что химики должны хорошо разбираться в свойствах химических веществ, поэтому они могут пытаться взломать одно нужное вещество все вместе. Нигде это не проявляется более

очевидно, чем в изобретении новых лекарственных средств, когда сотни растений изучаются на предмет их химических свойств от корней до плодов, добываются и соединяются с другими для получения новых препаратов. Затем химики пробуют снова и снова, иногда годами, чтобы получить правильные комбинации и добиться нужных результатов.

Хакерство используется в бизнесе для понимания рынка или покупательского поведения некоторых типов потребителей. Бизнесмены тщательно исследуют силы, которые управляют интересующей их областью бизнеса, а потом пытаются изменить или повлиять на них так, что бы заставить делать то, что им нужно. Иногда они взламывают продукт, а иногда взламывают вас(при помощи рекламы и **прайминга**(англ «priming»), вещей, над которыми вы будете работать на уроках социальной инженерии).

Хакерство также становятся все более важной частью войны. Высококвалифицированные солдаты находчивы и изобретательны в достижении своих целей точно так же, как хакеры. Взломщики кодов, разведчики-аналитики и полевые офицеры используют то, что является базовыми хакерскими навыками, что бы понять, что имеет противник, что он делает и как извлечь пользу из недостатков его оборудования. Так как все больше стран полагается на компьютеры и сети, использование взлома в кибер-атаках и обороне стало важной частью национальных вооруженных сил и разведывательных операций. Национальные и международные органы безопасности даже приходят на хакер-конвенции, что бы нанять хакеров!

Настоящая причина быть хакером – это реальная власть. Вы можете делать действительно клеевые вещи, когда имеете мощные хакерские навыки. Глубинные знания дают Вам великую силу. Если Вы знаете, как что-то работает от «а» до «я», Вы можете взять это под контроль, значит в ваших руках настоящая власть. Более того, у вас есть силы защитить себя и тех, кто вам дорог.

Все больше и больше людей живут в онлайне, как в форме отношений, люди ищут работу и деньги, сделанные в Интернете. Информация может быть полезной – или несущей угрозу – а хакеры могут защитить себя лучше, чем кто-либо другой. Они могут исследовать то, что происходит с их данными. Они могут быть уверены, что общедоступно только то, что они хотят, да и просто чувствуют себя в безопасности. Это огромное конкурентное преимущество в школе, на работе и в жизни, так как малейшее негативное мнение в конечном итоге будет использовано против вас. Можете на это рассчитывать.

Взламывайте все, но не вредите никому.

Как взламывать

Рассказывать Вам, как взламывать — все равно что объяснять, как сделать сальто назад на бревне: каким бы не было подробным объяснение Вы не сможете сделать это с первого раза. Необходимо развивать навыки, чувства и интуицию через практику или иначе Вы будете падать плашмя на лицо. Но есть некоторые вещи, которые мы можем сказать Вам, чтобы помочь в этом и призвать Вас продолжать практиковаться.

Во-первых, Вы должны знать некоторые маленькие секреты о том, как хакеры на самом деле работают. Мы собираемся взять их из **Методик тестирования руководства,** или OSSTMM (www.osstmm.org). Хакеры напоминают его, и оно произносится, как "ау-стим". OSSTMM - это **Общедоступное Руководство по Методике Проверки Безопасности**, и хотя можно его читать, как инструкцию настроек DVD-плеера, он является основным документом, который многие хакеры-профессионалы используют, чтобы планировать и осуществлять свою атаку и защиту. Глубина этого руководства сравнима с реальными драгоценностями, которые откроют Ваши глаза.

Два способа получить желаемое

Например, Вам следует знать, что на самом деле есть только два пути получить что угодно: Вы сами берете его или есть кто-то, кто возьмет его и отдаст Вам. Это означает, что все захваты в мире требует **взаимодействия(англ «interactions»)** между человеком и вещью. Очевидно, верно? Но задумайтесь об этом. Получается, что все защитные механизмы должны пытаться остановить кого-то от взаимодействия с вещью, которую они защищают. Если Вы закроете всё в огромном сейфе, Вы не сможете пресечь все взаимодействия. Магазины должны расставить вещи на полки, чтобы покупатели могли потрогать их. Компаниям необходимо отправлять информацию клиентам через электронную почту, которая крепится к почтовым серверам и передает сообщения на другие почтовые сервера.

Всё это — взаимодействия. Некоторые из них происходят между вещами и людьми, знакомыми друг с другом. Мы называем эти взаимодействия **дарением(англ «Trusts»).** Когда взаимодействия происходят между незнакомыми людьми или системами, мы называем их взаимодействия **доступа(англ «Access»).** Вы можете воспользоваться доступом, и взять то что хотите, или Вы можете обмануть тех, кому данная цель доверяет, чтобы они взяли то, что нужно и отдали вам. Если Вы задумаетесь об этом на мгновение, то это означает, что безопасность подразумевает защиту чего-либо, как от тех, кто этот объект не знает, так и от тех, кто его знает и доверяет.

Упражнения

1.1 Какой тип взаимодействия используется в поисковых системах? Подумайте тщательно: какие-либо из них предоставляют Доступ? Доверие?

1.2 Приведите простой пример использования Доступа и Доверия для получения велосипеда, прикованного к стойке.

1.3 Приведите пример, как вы можете использовать Доступ или Доверие, что бы проникнуть в чужую электронную почту.

Пища для ума: Шпионаж

Использование взлома против иностранного государства, совершение преступных актов взлома и проникновения, нарушения границ, кражи, уничтожения с целью получения политического или военного информационного преимущества называется **шпионажем**. А когда взлом совершается зарубежным бизнесом против бизнеса другой страны, чтобы получить преимущество – это **экономический шпионаж**.

Взлом для получения частной и личной информации об отдельных людях, с целью застыдить их публично это **DoXing**. Если публичная информация добыта о целевом лице или компании для атаки, но не было совершено уголовных деяний, это называется **документ гриддинг**(англ «document gridding») или **OSInt**(анализ открытых ресурсов, англ «Open Source Intelligence»).

Взлом ради понимания действия корпоративных сетей, систем, приложений и устройств в качестве цели атаки без реального нарушения границ или вторжения в систему, известен как **сетевое наблюдение**(англ «network survey»).

Взлом с целью тщательного изучения конкурента без нарушения каких-либо законов (хотя то, что они делают можно назвать гадким или грубым) называется **конкурентной разведкой**.

Вы, наверное, умираете от желания услышать, какие жесткие и грубые вещи вытворяются в рамках закона. Возьмем пример причинения неудобства кому-нибудь для получения от него информации. Лгать ему – до тех пор, пока вы его не убили – легально (хотя есть законы запрещающие вызывать панику в общественных местах, например, кричать “Пожар!” в переполненном кинотеатре, когда его нет).

Допустим, хакер хочет знать, где компания планирует возвести новый завод. Он использует документ гриддинг что бы узнать, какие люди уполномочены принять это решение. Затем хакер звонит в их офис, что бы узнать в каких городах они бывали, и, возможно, какие заводы посещали. Но, естественно, это частная корпоративная информация, и никто ее не расскажет просто так, не поднимая тревогу. Поэтому хакеру нужно добыть информацию хитростью. Это не так сложно, если подойти к процессу с воображением.

Хакер: Здравствуйте, я доктор Джонс, и я звоню вам из школы по поводу вашей дочери Нэнси.

Цель: Серьезно? И что она натворила на этот раз?

Хакер: Ну, у нее было сильное носовое кровотечение, которое мы не могли остановить. Я бы хотел спросить, не подвергалась ли она воздействию каких-либо химических препаратов, химического производства или что-то в этом роде? Эти симптомы встречаются редко, за исключением людей, подвергающихся воздействию этих химических веществ. Вы можете мне что-нибудь рассказать?

Цель: (сливает информацию)

В большинстве своем это не является незаконным, но причиняет ненужное беспокойство. Не говоря уж о том, что заставляет родителя волноваться.

Взлом ради захвата всего мира

Взлом это не просто взаимодействия. Знаете что. Многие люди говорят, что политика это взаимодействия. Может быть. Но вы, вероятно, думали что взлом это нарушение безопасности. Иногда это так. А на самом деле это захват контроля над чем-нибудь и его изменение. Понимание взаимодействий, их значения в реальном мире, использование понятий, которые обсуждались ранее полезно, когда вы пытаетесь вникать, открывать или даже изобретать. Зачем вам это делать? Что бы быть вольными заставлять то, что находится в вашей собственности делать то, что вам надо. И удерживать других от изменения вашей собственности, что у других людей может называться безопасностью (но мы не эти люди).

> Иногда, когда вы покупаете что-нибудь, компания, которая вам это продала, пытается силой или хитростью убедить вас, что правила запрещают изменять или модифицировать этот предмет. И вы соглашаетесь с ними, до тех пор, пока принимаете факт того, что нарушение правил отберет возможность замены или ремонта товара. Так что взлом предмета не просто делает его вашим, а делает его вашим окончательно и неоспоримо. Для некоторых звучит страшновато, но в этом есть свои преимущества. Особенно если вы хотите удержать других от посягательств на ваше имущество.

Для многих и многих людей безопасность - значит поместить продукт в место под замок, сигнализацию, фаерволл или что-то, что теоретически сохранит его в целости. Но иногда все это работает не так хорошо, как должно, или добавляет своих проблем, которые увеличивают **поверхность атаки**(англ «Attack Surface»), тогда как продукты безопасности должны ее уменьшать. (Поверхность атаки это все пути и взаимодействия применяемые для атаки кого- или чего-либо.) удачи вам при получении улучшенного продукта в мире массового маркетинга, предоплаты, краудсорсинга и принципа «вы купили это «как есть», и с этим вам придется жить». Вот почему вы взламываете свою безопасность. Вам необходимо проанализировать товар и выяснить, как изменить его так, что бы он работал лучше. А потом вам может потребоваться взломать еще раз, чтобы компания-продавец не привела его к первоначальному состоянию!

Поэтому, когда вы думаете о хакерстве в плане нарушения безопасности, помните, что это лишь одна из областей применения, потому что если вы этого не умеете, возможно вам придется отказаться от некоторой свободы или конфиденциальности, которые вам не хотелось бы терять. (И да, мы понимаем что сейчас вас могут не заботить отдельные вещи которые вы делаете, говорите или постите, но у интернета память длинная, и ему все проще и проще становится напомнить другим о ваших делах. Что происходит в сети – остается в сети. Запомните это на будущее, даже если сегодня для вас это не имеет значения).

Теперь, когда вы получили представление о взаимодействиях, давайте рассмотрим их более детально. Вы знаете основные взаимодействия, такие как Доступ и Доверие, а вы слышали о **Видимости**(англ «Visibility»)? Это третий тип взаимодействия. Он такой же могущественный, как другие два. На языке полицейских он упрощенно звучит как возможность, а в хакерстве это больше чем знание существует ли что-то, что взаимодействует с предметом, или нет. Это взаимодействие приносит много новых техник безопасности, таких как обман, иллюзия и камуфляж, а так же совершенно

новые хакерские методы обхода таких мер безопасности, как обман, иллюзия и камуфляж!

Когда известного грабителя банков Джесси Джеймса спросили, зачем он грабит банки, он ответил: «Потому, что там есть деньги». Он имел в виду, что через Видимость он узнал, что у банков есть деньги, тогда как о других вещах он этого точно сказать не мог. Видимость: люди знают, какие активы они держат. Но не все имеет Видимость. По сути Приватность это противоположность Видимости, и это мощный способ не стать мишенью. Находитесь ли вы на опасных улицах, в джунглях или в интернете, в первую очередь сохраняйте низкий уровень Воздействия и избегайте Видимости, чтобы не быть атакованным.

Exercises

1.4 Интернет – популярное средство для создания мифов и увековечивания ложных историй, именно поэтому тяжело отличить правду от вымысла. Поэтому если вы хотите научиться быть хорошим хакером, заведите привычку проверять факты и узнавать правду. Вот почему сейчас вы пойдете и разузнаете, действительно ли Джесси Джеймс так сказал. И не довольствуйтесь ответом, найденным на первой же веб-странице, а покопайтесь немного.

Теперь, когда вы привыкли искать информацию, отыщите правду о следующих простых вещах:

1.5 Что значит слово «иглу» в инуитском языке, из которого оно происходит? Какие типы взаимодействий вы сейчас использовали, что бы отыскать ответ?The

1.6 Многие родители, не задумываясь, указывают на то, что сахар делает маленьких детей гиперактивными. Так ли это? Какое взаимодействие в действительности происходит в маленьких животах, когда дети едят много конфет или другой сладкой еды, которая заставляет их двигаться чересчур активно?

1.7 Вы могли слышать что сахар – причина кариеса, но какое на самом деле взаимодействие тут имеет место, и что есть реальная причина? Сахар это или нет? Дополнительные очки, если вы сможете сказать каким типом взаимодействия является чистка зубов в борьбе с реальной причиной кариеса и найдете название хотя бы одного химического вещества направленного на корень проблемы (*подсказка: флюорид неверно*).

Четыре пункта процесса

Взяв три типа взаимодействия вместе, Вы получите **Пористость**, основанную на поверхности атаки. И, как подразумевает слово, это поры или “дыры” в любой защите, которые должны быть, чтобы получились любые необходимые взаимодействия (а также любые неизвестные или ненужные). Например, магазину всё ещё необходимо разложить товары на полки, чтобы люди могли прикоснуться к ним, положить в корзину и купить их. Эти взаимодействия должны продать товары. Но владелец магазина может быть не в курсе сотрудников, которые тайком убирают вещи с погрузочной платформы — это и есть нежелательное взаимодействие.

Пористость — это то, что Вам нужно знать о защите себя или атаки целей. Но этого недостаточно, чтобы проанализировать, как их взломать. Чтобы сделать это, Вы должны знать о трех типах взаимодействия больше, чем Вы только что узнали. Есть еще один маленький секрет от OSSTMM и его называют **Четыре Пункта Процесса (FPP)**. В нем предоставлены четыре способа использования взаимодействий для

максимально глубокого анализа, по которому мы понимаем что нужно сделать, чтобы можно было наблюдать за предметом и видеть, что происходит.

Эхо процесс

Мы растем, открываем и изучаем вещи, взаимодействуя напрямую с ними. Маленькие дети тыкают высохшую белку палкой, чтобы убедиться, что она мертва. Это называется **эхо процесс(англ «echo process»).** Он является самой основной и незрелой формой анализа. Это как кричать в пещеру и слушать ответ. Эхо процесс требует направлять в цель различные типы взаимодействия Доступа, а затем отслеживать его реакцию, чтобы выяснить, каким образом Вы можете взаимодействовать с ним. Эхо процесс является причинно-следственным типом проверки.

Это необычный способ проверки чего-то, потому что, хотя это очень быстрая проверка, но она также не очень точная. Например, при использовании эхо процесса в тестировании безопасности, цель, которая не отвечает, считается безопасной. То же происходит, когда она не имеет Видимости. Но мы также знаем, что если что-то не реагирует на определенный тип взаимодействия, то не значит, что оно “безопасно". Если бы это было так, то другие животные не убивали бы опоссумов, когда те претворялись мертвыми, и любой мог спастись от медведя, просто упав в обморок от страха. Но это не правда. Избегание видимости может помочь Вам пережить некоторые типы взаимодействия, но, конечно, не все.

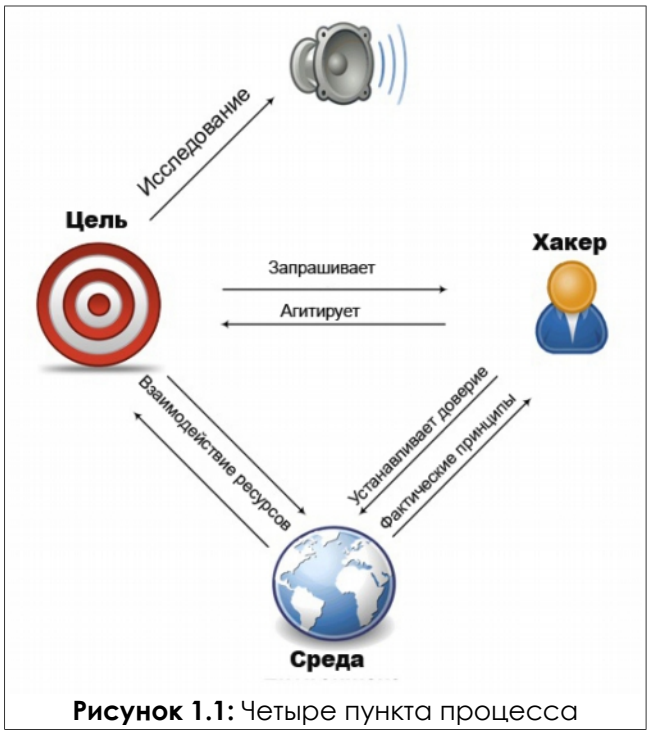

Рисунок 1.1: Четыре пункта процесса

К сожалению, в большинстве своем люди в повседневной жизни используют для исследования вещи только эхо процесс. Существует так много информации, утраченной из-за этого вида одномерного анализа, что мы должны быть благодарны отрасли здравоохранения, которая пошла дальше “Если я сделаю это, будет больно?” метода диагностики. Если бы больницы использовали только эхо процесс для определения состояния здоровья человека, то они редко по-настоящему помогали бы людям. Радует только, что время в комнате ожидания будет очень коротким. Вот почему некоторые врачи, большинство ученных и особенно хакеры используют четыре пункта процесса, чтобы убедиться, что они ничего не пропустили.

Четыре пункта Процесса нужны, чтобы Вы посмотрели на взаимодействия следующими способами

1. **Индукция**: Что можно сказать о цели по ее окружению? Как она ведет себя в этой среде? Если цель не находится под влиянием окружающей среды, это также интересно.
2. **Следствие**: Какие сигналы (излучения) цель посылает? Изучение любых треков или показателей этих излучений. Система или процесс, как правило, оставляет характерную черту взаимодействия с окружающей средой.
3. **Взаимодействие**: Что происходит, когда Вы мешаете цели? Этот пункт включает эхо тесты, в том числе ожидаемые и неожиданные взаимодействия с целью, чтобы вызвать ответные меры.
4. **Вмешательство**: Как далеко она отклонится, перед тем как сломается? Вмешайтесь в потребности цели, вроде электричества, или в её взаимодействия с другими системами, чтобы найти критические точки, при которых она может продолжать работу.

Вернемся к нашему примеру о больнице... четыре стадии FPP будут выглядеть следующим образом:

1. Функции **взаимодействия** — это эхо процессы, в которых врачи ощипывают пациентов, говорят с ними, проверяют их рефлексы на локтях и коленях и используют другие инструменты диагностики.
2. **Следствие** считывает **излучение** от пациентов, такие как пульс, артериальное давление и мозговые волны.
3. **Вмешательство** изменяет или вызывает напряжение гомеостаза пациента, поведение, обычаи или уровень комфорта, чтобы посмотреть, что происходит.
4. И, наконец, **индукция**, которая изучает среду, места, которые пациент посетил перед тем, как он заболел, и как они могут повлиять на пациента, если он, возможно, чего-то коснулся, принял внутрь или вдохнул.

Упражнения

1.8 Как Вы могли увидеть, Четыре пункта процесса позволяют более глубоко исследовать взаимодействия. Теперь Вы можете попробовать сами. Объясните, как Вы могли бы использовать Четыре пункта прогресса, чтобы узнать работают ли часы, и если они работают корректно, то сохраняется ли нужное время.

Что взломать

Когда вы что-то взламываете, необходимо установить базовые правила. Вам понадобятся язык и понятия, чтобы знать, что вы на самом деле взламываете. Область(англ «Scope») - слово, которое мы используем для описания всевозможных операционных сред, каждая из которых взаимодействует с вещью, которую вы хотите взломать.

Пища для ума: Классы и Каналы.

В профессиональной терминологии (которой пользуются и хакеры), область состоит из трёх Классов, которые подразделяются на пять Каналов:

Класс	Канал
Физическая безопасность(PHYSSEC)	Человеческий
	Физический
Безопасность спектра(SPECSEC)	Беспроводной
Безопасность коммуникаций(COMSEC)	Телекоммуникации
	Данные сетей

Классы это не то, о чем бы вам стоило слишком беспокоиться, но они являются официальными ярлыками, использующимися сейчас в охранной, правительственной и военной индустрии. Классы определяют область изучения, исследования или операции. Так что если вы ищете больше информации на любую тему, действительно полезно знать, как это называют профессионалы.

Каналы это обычное обозначение способов взаимодействия с активами. Нередко для взлома гаджета используется, "Четырех Точечный Процесс" для каждого канала. Да, выглядит довольно трудоемко, но подумайте, как это захватывающе, когда вы находите способ заставить что-то работать, который не числится ни в одном руководстве, или, еще лучше, даже неизвестен производителю!

Активом(англ «asset») может быть хоть что, имеющее ценность для владельца. Это могут быть физические объекты, такие как золото, люди, чертежи, ноутбуки, телефон с частотой сигнала 900Мгц и деньги; или интеллектуальная собственность, вроде личных данных, отношений, брендов, бизнес процессов, паролей и слов, сказанных по телефону с сигналом мощностью 900Мгц.

Зависимости(англ «dependencies») - это вещи вне активов владельца, не способные обеспечить свою самостоятельность**.** Не так много компьютеров генерируют для себя электричество, например. Даже если маловероятно, что кто-то отключит вам электричество, это все еще в области вашего действия.

Цель безопасности — **разделение**(англ «separation») между активами и их зависимостями и устранение угрозы.

Мы сказали, что безопасность это **функция разделения**. Существует четыре способа обеспечения разделения:

- Переместить актив, что бы создать барьер между ним и угрозой.
- Перевести угрозу в безопасное состояние.
- Уничтожить угрозу.
- Уничтожить актив. (Не рекомендуется!)

Когда мы взламываем, мы ищем места, где возможно взаимодействовать с целью, и где нельзя. Подумайте о дверях внутри здания. Некоторые из них необходимы работникам; другие — потребителям. Некоторые — для спасения от пожара. А некоторые вообще бесполезны.

Тем не менее, каждая дверь — это точка взаимодействия, которая помогает как при выполнении необходимых операций, так и нежелательных, таких как воровство. Когда мы выходим на сцену в роли хакеров, мы не знаем наперед причины(мотивы) всех этих точек взаимодействия, поэтому мы анализируем их с помощью Четырех Пунктов Процесса.

Рассмотрим, к примеру, парня, который хочет быть абсолютно защищенным от молнии. Единственный способ (будучи на планете Земля) — забраться внутрь горы, потому что молния совершенно точно не сможет проникнуть через всю эту грязь и камни. Если предположить, что ему никогда не потребуется выйти наружу, то его безопасность стопроцентна. Но если он начнет сверлить дыры в скале, молния будет иметь на одну точку доступа больше с каждой дырой, и пористость увеличится. OSSTMM разделяет понятия **обезопасить** себя от молнии, и **быть защищенным** от нее. Причина в том, что существует при большей пористости более вероятно, что хакер сможет изменить и взять под контроль то, что захочет.

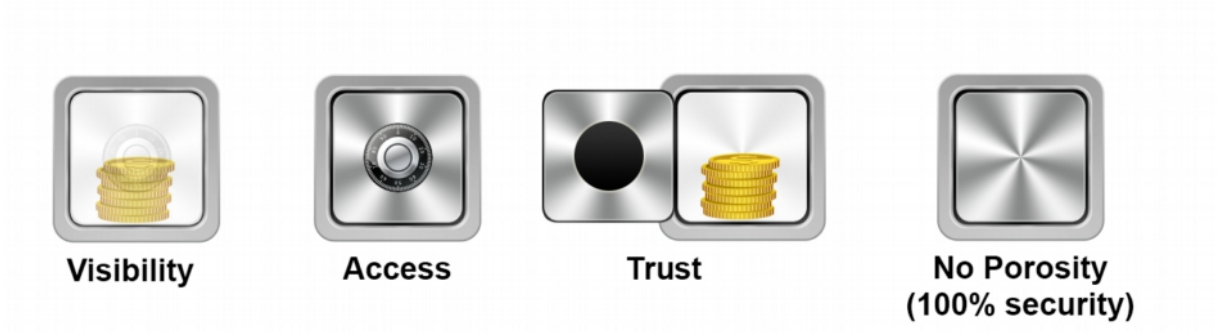

Рисунок 1.2: Пористость

Пища для ума: Пористость

Вот некоторые примеры, которые описывают, как поры могут быть расположены, классифицированы и определены в процессе взлома.

Понятие	Значение
Видимость	Когда полиция расследует преступление, ищут *средства*, *мотив* и *возможность*. Если актив видимый, он может подвергнуться атаке, а если невидимый, то он не может стать целью атаки, хотя его и можно обнаружить. Некоторые специалисты по безопасности любят говорить что **затемнение**(англ «obfuscation») — плохая защита, потому что оно не защищает, а лишь скрывает что-либо. Но это неплохая вещь особенно тогда, когда вам не нужен постоянный контроль безопасности. К этому эффекту **OSSTMM** предлагает небольшой драгоценный камень: "Безопасность не должна сохраняться вечно, а просто чуть дольше чем то, что могло бы заметить, что ее нет."
Доступ	Доступ — число различных мест, где происходит взаимодействие с внешней областью. Для здания это могут быть двери на улицу или окна, а для интернет-сервера — число открытых сетевых портов или сервисов, доступных на этом компьютере.
Доверие	Доверие - когда один объект свободно взаимодействует с другим объектом в пределах области. Доверие — причина того, что Вы не просите у своей матери удостоверение личности, когда она приходит обнять Вас. Это также то, почему Вы не подозреваете, что она отравила Вашу еду. Вы учитесь доверять вещам в своей области. Тогда однажды, если ваша мать будет захвачена инопланетной расой (а ля **Вторжение похитителей тел**) и действительно отравит Вашу еду, Вы съедите ее, ничего не подозревая. Таким образом доверие - и дыра в безопасности и обычная замена аутентификации, способ, которым можно подтвердить, является ли кто-либо тем, о ком мы думаем. Доверие - странная вещь, потому что она присуща только людям и высоко ценится в обществе. Без доверия мы никогда не были бы в состоянии свободно взаимодействовать. Но из-за доверия нас легко обмануть, одурачить, ограбить и оболгать. Исследование OSSTMM в области доверия показывает, что существует 10 причин доверять кому-либо, называемые **Критериями доверия**(англ «Trust Properties») и если все десять причин удовлетворены, тогда мы можем доверять без риска и беспокойства. Но то же самое исследование показывает, что большинству нужен только один выполненный критерий для ощущения безопасности, и действительно параноидальные или циничные люди удовлетворяются тремя причинами.

Ресурсы

Эффективное исследование изучения и критического мышления — ключевые навыки для хакеров. Взлом, в действительности, является творческим процессом, основанным больше на образе жизни, чем на уроке. Мы не можем научить Вас всему, что Вам необходимо знать, но мы можем помочь Вам понять, что Вам нужно знать. Потому что наука движется быстро, и то, что мы изучаем сегодня, может быть не актуально завтра. Гораздо лучше для Вас охватить традиции обучения хакеров, которые являются самой важной частью взлома и которые будут отличать Вас от **скрипт кидди**(англ. «script kiddie»)(хакерское слово, которое означает человека, который использует инструменты, не зная как или почему они работают).

Если Вы столкнетесь в этом уроке со словом или понятием, которое Вы не понимаете, очень важно, чтобы Вы посмотрели его значение. Игнорирование новых слов сделает трудным для Вас понимание концепции ближайших уроков. Вам будет предложено изучить тему, а затем предполагается использование информации, чтобы выполнить упражнения этого урока — но эти уроки не объяснят Вам, как выполнить исследование. Поэтому обязательно потратьте столько времени, сколько Вам необходимо, чтобы научиться использовать различные доступные ресурсы.

Книги

Вы можете быть удивлены, что мы не заостряем Ваше внимание только на Интернете, но книги являются отличным способом узнать о фундаментальной и фактической науке всё, что Вы хотите знать. Хотите узнать что-то из области информатики, например об аппаратных деталях Вашего компьютера? Ничто не поможет Вам больше, чем чтение книг по этой тематике. Основной проблемой книг о компьютерах является то, что они очень быстро устаревают. Секрет в том, что нужно научиться видеть фундаментальную структуру под тонкой оболочкой деталей. MS-DOS и Windows очень разные, но оба основаны на принципе Булевой логики, которая привела к компьютерам начиная с графини Ады Лавлейс, которая написала первые компьютерные программы в девятнадцатом веке. Безопасность и конфиденциальность частной жизни может быть изменена в последние 2500 лет, но **«Искусство войны»** Сунь-Цзы охватывает основополагающие принципы, которые все ещё применяются и сегодня. (Кстати, не существует более быстрого способа прослыть **n00b'ом,** чем процитировать Сунь-Цзы. Вы должны знать, как применять некоторые вещи, но не говорить о них. И цитирование «Искусства войны» доказывает, что Вы на самом деле не читали его, потому что Сунь-Цзы говорит, что нужно держать Ваши реальные знания в тайне.)

Даже при том, что информация, найденная в книгах, может не быть столь же современной как информация, поступающая из других источников, но сведения, полученные из книг, скорее всего будут лучше написаны, чем в большинстве других источников. Также иногда она являются более точной. Писатель, который тратит год на написание книги, скорее всего потратит время, чтобы проверить факт, чем кто-то, кто пишет объявления в блогах шесть раз в день. (Смотрите Разделы Журналы и Блоги для получения дополнительной информации.)

Но помните, точность не означает объективность. Источники автора информации могут быть предвзяты. “Книги по истории написаны победителями” (это цитата), и тоже самое верно, когда дело касается политики и социальных норм, которые могут убрать некоторую информацию из публикаций. Такое происходит со школьными учебниками, которые выбраны в рамках политического процесса и содержат только ту информацию, которая считается социально приемлемой для изучения. Так что не думайте, что Вы нашли золотую истину только потому, что Вы прочли это в книге.

Истина лишь в том, что любой человек может написать книгу, и любая книга может содержать различные версии истины.

Не смотрите на книгу и не отказывайтесь от нее из-за её размеров, прежде чем начнете её читать. Никто не читает большинство массивных книг, которые Вы видите, от корки до корки. **Думайте о них, как о доисторических веб-страницах.** Откройте одну на случайной странице и начните читать. Если Вы чего-то не понимаете, идите назад и посмотрите толкование (или перейдите к тому, что понятно для Вас). Переходите по книге взад и вперед, как будто Вы скачете от ссылки к ссылке на веб-странице. Этот тип нелинейных исследований гораздо более интересный и полноценный для хакеров, так как удовлетворяет Ваше любопытство больше, чем чтение.

И наконец, ценный навык, который извлекают из книг, - это способность хорошо писать. Это огромное преимущество, когда Вы пытаетесь понять и заняться новой областью знаний. Он также помогает снискать большее доверие других читателей, особенно тех, кто обладает властью.

Журналы и газеты

Журналы и газеты очень полезны для предоставления краткой и своевременной информации. Хотя эти типы публикаций могут быть бедны на детали. Также помните, что каждая газета или журнал имеют свою собственную аудиторию и свою повестку дня или тему, независимо от любых заявлений быть "справедливыми и беспристрастными". Знайте тему издания: журнал «Linux» не обязательно хороший источник информации о Microsoft Windows, так как Windows противоречит заявленной теме (конкурирующие операционные системы), и, честно говоря, читатели журнала «Linux» хотят читать о превосходстве Linux. Многие из специализированных журналов используют **подавление доказательств**,(англ. «cherry picking») техническими приемами выделяют только положительные аспекты чего-либо, что соответствует теме журнала, или негативные аспекты того, что не соответствует.

Будьте в курсе возможных погрешностей публикаций. Вот где Вам дают мнение, а не факты, или исключительные факты из истории под собственным мнением, и поэтому Вы не сможете составить личного мнения. Рассмотрите источник! Даже "нейтральное" периодическое издание может быть полно предубеждений и спекуляции, ведь это хороший способ сказать "основное предположение" , но на самом деле часто только "догадки" со стороны журналиста.

Существует огромное движение в области медицины за то, что должны быть опубликованы все медицинские и фармацевтические исследования (или, по крайней мере, все финансируемые государством), даже если они провалились, так врачи смогут сделать более осознанный выбор о применении лекарств или процедур. В то время, как текущие медицинские журналы публикуют "факты" с исследовательских испытаний, детали и обстоятельства по-прежнему туманны. Это

действительно важно, когда Вы имеете дело с предметами, которые основываются на имеющихся причинах. Причинная обусловленность требует, чтобы причина предшествовала и была причиной эффекта.

Другие приемы, используемые периодическими изданиями (как случайно, так и нарочно) — **неофициальные данные,** такие как мнения людей, опубликованные в качестве доказательств, независимо от того являются ли они экспериментами или нет; **авторитетное свидетельство,** в котором работники отрасли, представленные в качестве экспертов, высказывают свое мнение, или люди, которые являются органами власти в одной области предлагают свое мнение в другой, в которой они не имеют опыта; и, наконец, **спекуляция,** которая выдает что-то истинным, лишь потому что "все" считают, что это правда, хотя нет никаких фактических доказательств.

Лучший способ справиться с проблемами точности и скрытого плана — это хорошо и много читать. Если Вы читали об интересном вопросе в журнале, изучите его дальше. Возьмите одну сторону вопроса и ищите подтверждение; а затем возьмите другую и ищите уже опровержение. Некоторые культуры делают это по умолчанию. Искать другие стороны истории — часть их социальных привычек. Это действительно мощная культурная черта, особенно если Вы пытаетесь обеспечить успешную демократию.

Упражнения

1.9 Поищите в Интернете три онлайн журнала о взломе. Как Вы нашли эти журналы?

1.10 Все три журнала конкретно о компьютерном взломе? Что еще они предлагают, что может быть полезно в других сферах или в другом бизнесе?

Пища для ума: Спекуляция

Вот абзац из газетной статьи о грабеже. Можете найти здесь Спекуляцию? Отметьте подозрительные области:

Банк ипотечного кредитования Лэйк Мидоу был ограблен во вторник днем. Вооруженные бандиты в масках пришли за несколько минут до закрытия, и удерживали сотрудников банка в заложниках в течении часа, пока что-то не заставило их скрыться на внедорожнике последней модели. Как сообщалось, никто из заложников не пострадал.

Никто не мог идентифицировать бандитов, и по последующим моментам после ограбления полиция вынуждена была предположить, что работа выполнена профессионалами. Автомобиль был найден за банком в южной части густого леса у подножия гор Блюгрин. Полиция, вероятно, будет теперь искать опытных ранее судимых грабителей, состоящих в отношениях с людьми, проживающими в этой районе.

Со средним количеством в 57 сообщений об ограблениях ежедневно по всей стране, и населением графства Блугрин, обещавшим увеличиться до 50000 к следующему году, это может обратиться лавины банковских краж в этом регионе. «Кажется, это становится модным» - сказал комиссар полиции Смит.

Поскольку мы становимся более безразличными к спекуляции и остаемся не осведомлены о предвзятости статистических данных и результатов, в будущем все наших новости могли бы происходить от единственного журналиста, спекулирующего ими по мере происхождения. Из вышеописанного примера можно сделать только один реальный вывод: ограбление произошло вечером вторника. Теперь для наглядности, вот как бы выглядела заметка, если бы мы изменили всю спекуляцию, чтоб сделать ее более нелепой:

Справедливый банк ипотечного кредитования был ограблен во вторник вечером появившимися внезапно перед самым закрытием курицами, которые предупредили, что они могли бы удерживать сотрудников банка в заложниках в течении десяти лет, но прибыл воздушный шар, и они сбежали на нем. Как сообщалось, никто из заложников не был покрыт перьями.

Никто не мог идентифицировать бандитов, и по последующим моментам после ограбления полиция вынуждена была предположить, что работа выполнена профессионалами, и среди них был художник по костюмам в дополнение к опытному воздухоплавателю. Воздушный шар был найден за банком, летящим к югу от антарктической тундры. Полиция, вероятно, будет теперь искать опытных визажистов, у которых также есть связи с людьми, увлекающимися воздушными шарами.

Со средним количеством в 57 сообщений об ограблениях ежедневно по всей стране и сообщениями воздухоплавательной индустрии об увеличении продаж до 47 газилионов долларов к неопределенной дате в будущем, это могло стать началом лавины банковских краж с использованием воздушных шаров. «Кажется, это становится модным» - сказал комиссионер полиции Гордон.

При подавляющем использовании спекуляции и статистики во всех отраслях, неудивительно, что они и в индустрию безопасности вошли с такой мощью. В этой отрасли часто используется термин **FUD**, который является аббревиатурой от Страха, Неуверенности и Сомнений(англ «Fear, Uncertainty, and Doubt»). Вот как спекуляция и субъективный анализ степени риска используется для привлечения внимания и продажи идей безопасности. К сожалению, они успешно играют на примитивных человеческих страхах и растущей нечувствительности к спекуляции. Это привело к несоответствующим решениям поддержания безопасности, применяемым ненадлежащим образом и ложной уверенности во властях. Очевиден провал навыков критического мышления у населения, что эксплуатируется и коммерческим сектором и преступниками.

Поисковые системы

Google — хорошо известная, но не единственная поисковая система. Bing хорош в поиске простых запросов, а Yahoo — при выполнении полного исследования. Но знайте, что все эти веб-сервисы хотят знать о вас все, что могут, а возможно даже больше, чем им следует знать. Они запоминают все ваши поисковые запросы и вебсайты, на которые вы переходите.

Существуют системы, такие как AltaVista и DuckDuckGo.com, которые могут предоставить вам некоторую — и даже больше — анонимность. Это может быть полезно когда вы шарите по темным углам.

Вебсайты доступны для поиска, пока они онлайн, и обычно долгое время после. Обычно они сохраняются в виде **кэшированных страниц**(англ «cached pages»). В интернете кэш — это онлайн запись последней версии вебсайта, даже если сам сайт канул в небытие. Поисковые системы и архивы сайтов сохраняют эту информацию неопределенно долго, в понятиях интернета — «бесконечно». Перед тем как что-то разместить в интернете, полезно вспомнить, что оно потом никуда не денется. Никогда. Возможно, вам придется искать ссылку на сохраненную копию страницы. Google, например, обычно ставит пометку "кэш" рядом с обычной ссылкой на результат. Раздел «Кэш» помещали в выпадающее меню справа, и возможно, переместили в другое место к тому времени, когда вы это читаете.

Помимо поисковых систем, существуют также полезные общественные кэши в таких местах, как интернет-Архив http://www.archive.org. Вы можете найти версии целых веб-сайтов, кэшированных несколько лет назад, которые могут быть очень полезными для поиска информации, которая "исчезла".

Последняя заметка о веб сайтах: не думайте, что Вы можете доверять сайту просто потому, что он обнаруживается поисковой системой. Многие хакерские атаки и вирусы распространяются путем посещения сайта, загрузки невинно выглядящей программы, скринсейва или любого другого файла. Вы можете обезопасить себя, не загружая программы с неизвестных сайтов, и убеждаясь в том что ваш браузер работает в **песочнице**(англ «sandbox»). Но этого может быть недостаточно. Браузер — это окно в интернет, и, как через любое окно, плохие вещи могут проникнуть просто потому, что оно открыто. Вы можете даже не узнать об этом, пока не станет слишком поздно.

Упражнения

1.1 Существует много поисковых систем. Некоторые из них хорошо справляются с проникновением в **Невидимую сеть**(англ «Invisible Web»), область интернета, в которую тяжело проникнуть большинству поисковых систем, например некоторые закрытые базы данных. Хороший поисковик знает, как все их использовать. Некоторые сайты специализируются на отслеживании поисковых систем. Найдите пять поисковых систем, которыми вы раньше не пользовались, и о которых возможно даже и не слышали.

1.2 Есть также поисковые системы, которые ищут другие поисковые системы. Их называют метасистемами. Найдите одну из таких метасистем.

1.3 Введите запрос «безопасность и взлом» (включая кавычки) и запишите три первых результата. Чем отличаются результаты, когда вы НЕ используете кавычки?

1.4 Поиск темы очень отличается от поиска слова или фразы. В предыдущем задании вы искали фразу. Теперь вы будете искать идею.

Сделайте так: подумайте о фразе, которая может находиться на той странице, которую вы ищете. Если вы хотите, чтобы поисковая система выдала вам список журналов о хакерстве, вы не должны вводить запрос «список журналов о хакерстве». Не так уж много страниц будут содержать эту фразу! У вас будет несколько попаданий, но не так много.

Вместо этого вам надо подумать: «Если бы я был на месте журнала, какие типичные предложения я бы содержал?» введите следующие слова и фразы в поисковую строку и определите, какие из них обеспечивают лучший результат:

1. мой список любимых журналов о хакерстве

2. список профессиональных хакерских журналов

3. ресурсы для хакеров

4. хакерские журналы

5. хакерские журналы список ресурсов

1.5 найдите самый старый веб сайт Mozilla в интернет архиве. Для этого вам потребуется найти сайт “www.mozilla.org” на сайте архива http://www.archive.org.

1.6 Теперь совместим все вместе. Положим, вы хотите загрузить первую версию веб браузера Netscape. Используя поисковые системы и интернет архивы, посмотрите, сможете ли вы определить местонахождение и скачать первую версию этого браузера.

Веб-сайты и веб-приложения

Стандартом *де-факто* для обмена информацией в настоящее время является веб-браузер. В то время, как мы классифицируем все, что видим, как “веб”, всё больше и больше, что мы действительно используем — это “веб-приложения”, так как не все в Интернете — это сайты. Если Вы проверяете электронную почту, используя веб-браузер, или получаете музыку через службы веб-соединения, то Вы используете веб-приложения.

Иногда веб-приложения требуют право доступа. Это означает, что Вам необходимо имя пользователя и пароль, чтобы получить доступ. Наличие доступа, если у Вас есть законное право на доступ, называется **правом доступа**(англ. «privileges»). Взлом веб-сайта ради изменения страницы может означать, что у Вас есть доступ, но поскольку у Вас нет юридического права, Вы не имеете привилегированного доступа. Когда продолжите использовать Интернет, Вы увидите, что во многих местах доступ к привилегированным участкам предоставляют случайно.

Если найдете что-то подобное, хорошо бы сообщить об этом администратору сайта. Однако, остерегайтесь возможных правовых последствий. К сожалению, многие администраторы недовольны нежелательными отчетами о уязвимости.

Чтобы внести свой вклад и сделать Интернет более безопасным, а также защитить себя, Вы должны рассмотреть использование **анонимного прокси-сервера** (например, Tor или anonymous remailers, и т. д.) для рассылки отчетов об уязвимости администраторам. Но помните: все эти анонимные технологии имеют свои слабые места, и Вы можете быть не таким анонимным, как Вы думаете! (Не один хакер уже познал этот тяжелый путь)

Упражнения

1.11 Используйте поисковик, чтобы найти сайты, которые совершили ошибку, дав право доступа всем. Чтобы сделать это, будем искать папки, которые позволяют нам увидеть список содержимого ("перечень файлов в каталоге"), это, как правило, не должно быть разрешено. Для этого мы будем использовать некоторые уловки Google на http://www.google.com. Введите это в поле поисковика:

```
allintitle:"index of" .js
```

Просмотрите результаты и Вы сможете найти тот, который выглядит как список каталогов. Этот вид поиска известен, как взлом Google.

1.12 Сможете ли Вы найти другие типы документов этим методом? Найдите еще три каталога, которые содержат .xls файлы, .doc файлы и .avi файлы.

1.13 Есть другие варианты поиска, схожие с "allintitle:"? Как Вы можете найти их?

Электронный Журнал

Журнал, также известен, как **e-zine**, является потомком **фэнзинов**: небольшие, как правило, бесплатные журналы с очень маленькой аудиторией (менее 10,000 человек) которые часто издаются любителями и любительскими журналами. Фэнзин печатался на бумаге. Журналы в Интернете, такие как знаменитый **2600** или веб-журнал **Phrack,** пишутся волонтерами; часто это означает, что производители не редактируют содержимое на предмет нетехнических ошибок. Иногда резкие формулировки могут быть удивительны для тех, кто не знаком с этим жанром.

Такие журналы обсуждают очень резкие темы или программы, и, как правило, очень самоуверенные. Вместе с тем они чаще всего показывают и обсуждают две стороны вопроса, так как он обычно не заботятся о том, что они должен понравится рекламодателями и абонентам.

Упражнения

1.14 Поищите в Интернете три журнала на предмет взлома. Как Вы нашли эти журналы?

1.15 Почему Вы классифицируете их, как журналы? Помните, только потому что они продают его, как журнал или написали в названии "журнал" - нельзя сказать, что он является им.

Блоги

Блог можно рассматривать, как эволюцию журнала, как правило, в письменной форме одного человека. Блоги обновляются чаще, чем большинство печатных изданий или журналов, а также создают группы, связанные очень сильными темами. Также важно читать комментарии, как и «постить». Больше, чем в журналах, в блогах ответом часто служит немедленный и самоуверенный пост, с комментариями от всех участников. Это одна из ценностей блога.

Есть миллионы блогов в Интернете, но лишь небольшой процент из них являются активными. Информация большинства, однако, является все еще доступной.

Упражнения

1.16 Найдите в Интернете три блога о взломе.

1.17 Какие группы или сообщества связанны с ним?

1.18 Имеется в блоге безопасность, правоохранительные органы или академическая тема?

Форумы и Списки Рассылок

Форумы и **списки рассылки** разработаны средствами массовой информации, и они очень похожи на записи разговоров на вечеринке. Относитесь немного скептически к тому, что Вы там читаете. Разговоры часто отвлекают внимание, многое из сказанного — слухи, некоторые люди **троллят**, может вспыхнуть **большой базар**, и когда вечеринка закончилась, никто не уверен, кто что сказал. Форумы и списки рассылок похожи, потому что существует много способов помочь распространению неточной информации — иногда намеренно — и существуют пути способствовать анонимам. Поскольку вопросы и темы быстро меняются, чтобы получить всю информацию важно прочитать весь поток комментариев, а не только несколько первых.

Вы можете найти форумы практически на любую тему, и многие онлайн-журналы и газеты предлагают форумы для читателей, чтобы они написали отзывы на статьи, которые они издают. Поэтому форумы имеют бесценное значение для получения мнений о статье; независимо от того, скольким людям понравилось, обязательно найдутся недовольные.

Существует множество рассылок по специальным темам, но их трудно найти. Иногда самый лучший способ заключается в поиске информации по определенной теме, чтобы найти сообщество рассылок, которое занимается этой темой.

Как хакеру, Вам важно знать, что многие форумы и рассылки не найти с помощью основных поисковых систем. Хотя Вы и можете найти форум или рассылки с помощью поисковика, Вы не сможете найти информацию в отдельных сообщениях. Эта информация является частью невидимой сети, поскольку содержит данные только для поиска непосредственно на веб-сайте или форуме.

Упражнения

1.19 Найдите два хакерских форума. Как Вы нашли эти форумы?

Можете ли Вы определить темы или специализации этих веб-сайтов?

Темы на форумах отражают тему хостинга веб-сайта?

1.20 Найдите два списка рассылок о взломе или о безопасности.

Кто является "владельцем" этих рассылок? Вы можете увидеть список участников? (Вам может понадобиться выяснить применение разработанного списка, а затем искать в Интернете скрытые команды, чтобы увидеть всех членов данной рассылки).

В каких списках можно ожидать, что информация более фактическая и менее самоуверенная? Почему?

Новостные группы

Новостные группы существуют с давних пор. Они были задолго до того, как появилась Всемирная паутина. Google купил весь архив новостных групп и поместил их на сайте http://groups.google.com. Новостные группы — это как архивы списков рассылок, но без почты. Вы найдете там записи с начала девяностых годов. Люди размещают там свои комментарии непосредственно, как на обычных сайтах.

Как и веб архивы, архивы групп могут быть важны при поиске того, кто подает действительно оригинальные идеи или создает продукт. Они так же полезны при поиске тайной информации, которая никогда не размещалась на веб страницах.

Новостные группы используются сейчас не меньше, чем раньше, до того, как всемирная сеть стала основным средством обмена информацией. Однако, они так же не приобрели большей популярности, поскольку были заменены на новые сервисы вроде блогов и форумов.

Упражнения

1.7 Используя группы Google, найдите старейшую новостную группу, повествующую о хакерстве.

1.8 Найдите иные способы использования новостных групп. Есть ли приложения для чтения новостных групп?

1.9 Как много новостных групп говорящих о хакерстве вы можете найти?

1.10 Вы можете найти текущий список всех различных существующих в настоящее время новостных групп?

Вики

Вики — новейший интернет-феномен. Википедия (www.wikipedia.org) — вероятно самая известная из них, но существует множество других. Как и многое другое, вики размещаются сообществами. Отчеты часто утверждают, что вики не точны, так как редактируются любителями и фанатиками. Но это же относится и к книгам, рассылкам, журналам и всему прочему. Что важно знать, так это то, что эксперты — не единственный источник великих идей или фактической информации. Как указывает OSSTMM, факты появляются из маленьких шагов подтверждения идей и небольших прыжков открытий. Именно поэтому вики - большие источники и профессиональных, и любительских идей, медленно и постепенно подтверждающих друг друга.

Вики часто обсуждает какую-либо тему со всех сторон, и позволяет проследить как информация подтверждалась, опровергалась, уточнялась и изменялась с помощью списка изменений. Таким образом, это прекрасное место для сбора информации, но часто для исследований вам придется переходить на сайт вики.

Упражнения

1.11 Поищите “Ада Лавлейс". Видите результаты из вики?

1.12 Пойдите на Википедию и повторите запрос. Посмотрите статью о ней. Она входила в результаты вашего поиска?

1.13 Проверьте изменения этой страницы Википедии и посмотрите на типы исправлений или изменений. Какие типы изменений были внесены? Было ли что-то изменено, а потом исправлено на исходное? А теперь выберите популярную кинозвезду или певца, который вам нравится, посмотрите страничку в Википедии о нем, и проверьте изменения. Замечаете различия?

1.14 Найдите другой вики-сайт и повторите поиск. Какой-нибудь из результатов поиска отображается в оригинальном запросе вашей поисковой системы?

Социальные сети

Вы пользуетесь сайтом социальной сети? Или даже больше, чем одним? Как хакер, вы хорошо осведомлены, какие сети популярны на данный момент. А что на счет тех, которые не так популярны, как раньше? Они до сих пор существуют, и все их данные в большинстве случаев доступны.

Это означает, что существует огромный склад информации о нас, которую мы сложили туда добровольно. И в большинстве своем она останется там навсегда.

Социальные сети часто имеют суб-группы или сообщества по интересам. Сайты с профессиональными темами имеют группы по кибербезопасности, а сайты с "подпольной" темой часто имеют хакерские группы. На профессиональных сайтах Вы (и все остальные) должны использовать свое настоящее имя. А хакерских сайтов не так много.

Самое главное, в социальных сетях Вы используете Ваше настоящее имя или "прозвище"? Ваше прозвище можно соотнести с Вашим настоящим именем? Большинство людей не осознают, что они используют прозвища, но не редкость, что случайно или нарочно они размещают свои настоящие имена, адреса, города, школы, рабочие места и т. п. Если другие хакеры взломают Ваше прозвище, то из таких мелких ошибок они могут, как правило, довольно быстро выяснить кто Вы на самом деле. Если Вы используете прозвище, чтобы быть анонимным для тех, кто Вас не знает, убедитесь, что Вы принимаете меры, чтобы все сохранялось таким же образом. И НИКОГДА не путайте Ваши прозвища, если у Вас их несколько.

Упражнения

1.15 Поищите себя. Нашли что-нибудь? Есть ли результаты из социальных сетей?

1.16 Перейдите на сайт социальной сети, которой вы пользуетесь. Не логиньтесь, и повторите поиск так, как будто вы сторонний человек. Как много информации вы можете про себя найти?

1.17 Перейдите на сайт социальной сети, которой пользуется ваш друг. И снова не логиньтесь, если имеете там аккаунт. Поищите вашего друга. Как много информации смогли найти?

Чат

Чат, который находится на форумах **Internet Relay Chat (IRC)** и **Instant Messaging (IM)**, очень популярный способ общения.

Как научный источник, чат крайне противоречив, потому что Вы имеете дело с людьми в реальном времени. Некоторые из них будут дружелюбными, а некоторые могут быть и грубыми. Некоторые будут безобидными шутниками, но некоторые — вредоносными лжецами. Кто-то будет умен и готов поделиться информацией, а другой — совершенно неинформирован, но не менее готов делиться. И может быть трудно понять, кто есть кто.

Однако, как только Вы освоитесь в некоторых группах и каналах, Вы можете быть приняты в сообщество. Вы будете задавать все больше и больше вопросов, и Вы узнаете кому можно доверять. В конце концов, Вы можете получить доступ к самым новейшим хакерским подвигам (также известным, как **zero day** или **0day**, что обозначает, что он был обнаружен прямо сейчас) и улучшить собственные знания.

Упражнения

1.21 Найдите три программы обмена мгновенными сообщениями. В чем их отличия? Могут ли они использоваться для обмена друг с другом?

1.22 Выясните, что такое IRC и как Вы можете подключиться к ней. Вы можете обнаружить, что сеть имеет канал автора ISECOM? После того, как Вы подключились к сети, как Вы присоединитесь к обсуждениям канала isecom?

1.23 Как Вы узнали, какие каналы существуют в IRC-сети? Найдите три канала о безопасности и три хакерских канала. Вы можете войти на эти каналы? Там общаются люди или боты?

P2P

Равный равному также известен, как **P2P —** это сеть в Интернете. В отличии от традиционных клиентов/серверов сети, где каждый компьютер соединяется через центральный сервер, компьютеры в P2P сети взаимодействуют непосредственно друг с другом. Большинство людей ассоциируют с P2P скачивание MP3 и пиратских фильмов на известном оригинальном Napster, но есть много других P2P-сетей для обмена информацией, а также в качестве средства проведения научных исследований по распределению обмена информацией.

Проблема с P2P-сетям — это то, что Вы можете найти почти все, что на них есть, но некоторые вещи в сети нелегальны. А другие — легальны, но компании, которые создали их, по-прежнему считают, что они не должны находиться там, и рады потребовать денег с владельца любого **Интернет-шлюза,** где его загрузили.

На данный момент существует не так много соглашений о том, что человек, чей доступ в Интернет использовался для загрузки контента, несет ответственность, если полиции на самом деле нужно поймать человека, который этот сделал. Это, как говорится, если машина использовалась для совершения преступления, владелец автомобиля, а не водитель, идет в тюрьму. Законы Интернета в настоящее время не справедливы, так что будьте осторожны!

Будь то Вы или не Вы тот человек, который рискует загрузкой интеллектуальной собственности, нет никаких сомнений, что P2P-сеть может быть жизненно важным ресурсом для поиска информации. Помните: нет ничего нелегального в сети P2P — существует много файлов, которые доступны для свободного распространения при самых различных лицензиях — но также существует много файлов в этих сетях, которые не должны там находиться. Не бойтесь использовать P2P-сети, но будьте осведомлены о возможных опасностях, и о том, что Вы скачиваете.

Упражнения

1.24 Какие три самые популярные и наиболее часто используемые P2P - сети? Как каждая работает? Какую программу Вам необходимо использовать?

1.25 Исследуйте протокол одной из сети P2P. Что он делает и как сделать загрузку быстрее?

1.26 Поищите слова “download Linux” . Вы можете скачать дистрибутив из Linux с помощью P2P?

Сертификаты

Существуют сертификаты Тестера и Аналитика по вопросам безопасности OSSTMM, удостоверения «хакера» различных цветов, сертификаты основанные на той или другой «самой эффективной практике» и удостоверений со всеми возможными сумасшедшими инициалами и пунктуацией.

Почему вам важны сертификаты? Потому что вы можете получить некоторые из них в любом возрасте, и не обязательно для этого иметь высшее образование, и потому, что они могут поставить вас в положение популярного человека, а не того, кто пригоняет для него кабриолет.

Проблема сертификатов, основанных на самой лучшей методике в том, что эти методики постоянно меняются, так как лучшая методика это просто другой способ сказать «так, как все сейчас делают». Часто так, как все делают, неправильно на этой неделе и останется неправильным, когда они обновят методику на следующей неделе.

Поэтому существуют научно-исследовательские сертификаты, основанные на достоверных и повторяющихся исследованиях поведения человека и системы. Разумеется, наша головная организация, ISECOM, прямо попадает в сферу исследовательских органов сертификации. От ISECOM или от другой организации, ищите основанные на навыках, аналитических или прикладных знаниях(англ «applied knowledge») удостоверения, которые докажут, что Вы умеете сделать то, чему вы учились.

Семнары

Посещение семинаров это отличный способ услышать подробную теорию и посмотреть на свои навыки в действии. Даже семинары, посвященные определенному продукту полезно посетить, чтобы увидеть, как они проводятся, до тех пор, пока вы осознаете, что это событие является маркентинговым шагом, и его реальная задача заключается в продаже.

Мы были бы небрежны, если бы не упомянули, что мы можем доставить Hacker Highschool Seminars в любое место, и мы можем распространить любой из доступных уроков. Семинары проводятся профессиональными хакерами, рассказывающими студентам о взломе и о том, как быть хакером, как плохое, так и хорошее. Эти семинары сосредотачивают взгляд на том, что же такое настоящие хакеры, из исследований в Hacker Profiling Project, совместного проекта с Организацией Объединенных Наций по изучению хакеров и почему они взламывают. После них вы сможете двигаться дальше, открывая для себя светлые стороны взлома.

Одна из главных вещей: мы можем помочь вам найти способ стать таким же любознательным и изобретательным как хакер. Хакеры преуспевают в том, что они делают, потому что они знают как самообучиться, выходят за рамки доступных уроков и овладевают нужными им навыками, чтобы идти дальше.

Вы также можете попросить, чтобы ваши родители и педагоги узнали, как приспособить и начать курс Hacker Highschool в вашей школе. Свяжитесь с ISECOM для получения дополнительной информации.

Дальнейшее изучение

Теперь вы должны практиковаться пока не освоите исследование. Чем лучше вы поймете это, тем больше и быстрее вы будете находить информацию, и быстрее обучитесь. Но будьте осторожны, и развайте критический взгляд. Не вся информация правдива.

> Не забывайте спрашивать себя, зачем кому-то врать? В то, чтобы увековечить нечестный слух или историю вовлечены деньги? И самое главное, что такое область?

Подобно всякому взлому, исследование включает в себя область. Это действительно важно, когда вы видите статистику, подобно математике, которая использует проценты, дроби и неравенства. Всегда проверяйте, где имеет место область и признайте, что область должна применяться. Традиционное место, где ее можно разглядеть – это преступная или медицинская статистика, охватывающая небольшую выборку только в одной части страны. То, что затрагивает 10% из 200 учащихся в одном городе, не означает, что у 10% всего населения страны та же проблема. Так что читайте и находите информацию с умом. Выделение области информации всегда приводит к большим различиям!

Чтобы помочь вам стать лучшим исследователем, вот некоторые дополнительные темы и термины для изучения:

Метапоиск

Невидимая сеть

Гугл-взлом

Как работают поисковые системы

Общедоступная поисковая система

Словарь хакерского сленга (The Jargon File)

OSSTMM

Сертификаты ISECOM:

- OPST (OSSTMM Professional Security Tester)
  - OPSA (OSSTMM Professional Security Analyst)
  - OPSE (OSSTMM Professional Security Expert)
  - OWSE (OSSTMM Wireless Security Expert)
  - CTA (Certified Trust Analyst)
  - SAI (Security Awareness Instructor)

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM