Hacker Highschool

SECURITY AWARENESS FOR TEENS



Урок 1
Бути хакером

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

УВАГА

Проект Hacker Highschool є засобом навчання і, як в будь-якому навчальному засобі, існує небезпека. Деякі уроки, якщо ними зловживати, можуть призвести до фізичної травми. Також додаткові небезпеки можуть бути там, де ще недостатньо досліджень про можливі наслідки випромінювань від специфічної техніки. Студенти, які використовують ці уроки, повинні перебувати під контролем, і, в той же час, заохочуватися на вивчення, практику і заняття. ISECOM не несе відповідальності за застосування інформації, отриманої з даних матеріалів, і за подальші наслідки.

Наступні уроки та книги є відкритими і загальнодоступними на наступних умовах ISECOM:

Всі роботи проекту Hacker Highschool призначені для некомерційного використання з учнями початкової школи, слухачами юнацьких курсів Highschool, і студентами вищих навчальних закладів, приватних організацій або частково для домашнього навчання. Ці матеріали в будь-якій формі не можуть бути використані для продажу. Надання цих матеріалів будь-якому класу, навчальній організації або табору, в яких стягується плата, категорично заборонено без ліцензії, в тому числі на уроки в коледжі, університеті, професійно-технічних заняттях, літніх або комп'ютерних таборах тощо. Для придбання ліцензії відвідайте розділ сайту призначений для Ліцензування http://www.hackerhighschool.org/licensing.html.

Проект HHS є результатом праці відкритого співтовариства і, якщо ви знаходите наші труди цінними і корисними, ми просимо Вас підтримати нас шляхом придбання ліцензії, пожертвувань, або спонсорства.

Зміст

Співробітники журналу

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

Переклад

Vadim Chakryan, Kharkiv National University of Radio Electronics

ISECOM

Любов до злому

Передмова від **Pete Herzog**

Щоб Ви не чули про хакерів, правда в тому, що вони по-справжньому гарно роблять, так це — відкриття. Хакери — мотивовані, кмітливі та креативні люди. Вони проникають в суть роботи предмета до такої міри, що вони знають, як взяти його під свій контроль і переробити в щось інше. Це дозволяє їм переосмислити навіть великі ідеї, тому що вони можуть дійсно докопатися до суті того, як все функціонує. До того ж вони не бояться зробити одну й ту ж помилку двічі тільки з наукової цікавості, щоб подивитися чи має ця помилка завжди однакові результати. Ось чому хакери не сприймають провали як помилки або витрату часу, тому що кожен провал означає щось нове, що може бути вивчене. І всі ці риси необхідні кожному, хто хоче домогтися прогресу.

> Багато людей, яких називали хакерами, особливо з боку засобів масової інформації, або які мали проблеми зі "зломом", насправді не були хакерами.

Хакери - тип практичного вченого, що експериментує, хоча можливо іноді термін "божевільний учений" підходить більше, так як на відміну від професійних вчених, вони йдуть з головою в почуття, а не в формальні гіпотези. Це не обов'язково погано. Багато цікавих речей були розроблені або придумані людьми, які не слідують стандартним угодами про те, що було відомо або передбачалося правдою в той час.

Математик Георг Кантор запропонував нові ідеї про нескінченність і теорії множин, що викликало обурення серед багатьох колег-математиків настільки, що один назвав його ідеї "важкою хворобою", що заражає математику.

Нікола Тесла - якого вважали "божевільним вченим" в свій час, знав більше за всіх про те, як веде себе електрика. Він придумав, можливо, перший безколекторних двигун, в якому проходила електроенергія змінного струму, який в основному відомий як ефект Тесла або котушка Тесла.

Також був Ігнац Філіп Земмельвайс, який з'ясував, що доктора повинні мити свої руки між лікуванням пацієнтів, щоб захворювання не поширилося. Він зацікавився, чи є поширення захворювання між пацієнтами його провиною, тому він вирішив мити руки між візитами до пацієнтів, і, звичайно ж, випадки зараження зникли. Його ідеї пішли проти наукової конвенції про те, що було відомо в той час про мікроби (нічого), а також зручності лікарів, які відчували, що буде дуже клопітно зберігати руки в чистоті.

Те, що Ви думаєте, що Ви знаєте про хакерів, це те, що вони можуть прорватися в чужі комп'ютери і заволодіти рахунками чужих людей. Вони можуть читати вашу електронну пошту без вашого відома. Вони можуть дивитися через вашу веб-камеру без вашого дозволу і можуть бачити і чути Вас у власного будинку. Це не відповідає дійсності.

Деякі хакери бачать мережеву безпеку лише як ще один виклик, тому вони намагаються різними способами обдурити систему, але насправді те, що вони намагаються зробити - це перехитрити людей, що проектують та інтегрують мережі. Вони дізнаються так багато про мережі, як тільки можуть, де вона бере інструкції, правила використання і як вона взаємодіє

з операційними системами й іншими системами користувачів, які мають доступ до неї, і адміністраторами, які нею управляють. Потім хакери застосовують всі ці знання, щоб випробувати різні способи для отримання того, чого вони хочуть. Цей вид злому може бути дуже корисний у світі для розуміння того, що потрібно робити для того, щоб бути в більшій безпеці та створити більш досконалі технології.

На жаль, іноді злом здійснюється злочинцями і те, що вони хочуть, є незаконним і шкідливим. І про них, як правило, Ви читаєте в новинах.

Хакер **-** це не той, хто розміщує інформацію під чужим акаунтом, коли хтось залишає відкритою свою сторінку в соціальній мережі, або підглядає через плече за тим, як хтось вводить пароль, а потім заходить під його акаунтом в систему. Це не хакерство. Хакер також не той, хто завантажує скрипт кідді (англ. «script kiddie») програми для злому чужих електронних поштових адрес (англ. «e-mail»). Це не хакери; це просто злодії та вандали.

Злом - це дослідження. Ви ніколи не намагалися робити щось знову і знову різними способами, щоб змусити щось робити те, що Вам треба? Ви коли-небудь відкривали машину або пристрій, щоб подивитися, як вони працюють, досліджувати всі компоненти, а потім внести необхідні зміни, щоб побачити наскільки інакше вони стали працювати? Це злом. Ви зламуєте всякий раз, коли ретельно вивчаєте як щось дійсно працює, для того, щоб творчо використовувати це так, як Ви хочете.

Просто так вийшло, що спосіб, яким розроблений інтернет, а також величезне число різних додатків, систем, пристроїв і процесів робить його найбільш поширеним місцем, де можна знайти хакерів. Ви можете сказати, що він був створений хакерами, тому це найкращий майданчик для них. Але це не єдине місце. Ви можете знайти величезну кількість хакерів практично в кожній області і індустрії, і всі вони мають одну спільну рису: вони витрачають час на вивчення роботи речей, так що вони можуть змусити працювати їх по-новому. Вони не дивляться на речі як звичайні проектувальники, але, на відміну від них, хакери бачать більший або кращий потенціал, і зламують предмет для отримання чогось нового.

Не думайте, що Ви можете просто бути великим хакером. Тільки здійснюючи приголомшливі зломи з величезною смиренністю Ви може стати великим.

Злом сам по собі не є незаконним**.** Принаймні не більше незаконним, ніж кидати камінь. Все це зводиться до наміру. Якщо Ви кинули камінь і ваші наміри - поранити когось, то це злочин. Якщо Ви не мали наміру нікого образити, але хтось постраждав, то це не може бути злочином, але Ви понесете відповідальність за свої вчинки, і відшкодуєте збиток. У проекті ISECOM з підготовки хакерів (**Hacker Profiling Project**) було виявлено, що найбільший збиток від злому виходить від молодих, недосвідчених хакерів, які випадково ушкоджують чуже майно. Це як кидати каміння на вулиці просто для забави, але в процесі з'являться вм'ятини на машині і розбиті вікна. Може бути, збиток ненавмисний, але Ви знаєте, що Ви понесете відповідальність і заплатите за це. Так що будьте обережні, коли відбувається злом чужого майна. Краще зламувати власне майно.

Злом того**,** що Ви придбали і чим володієте може бути незаконним**.** Є хакери, які були покарані за злом власних пристроїв і комп'ютерів. Є хакери, які зламали програми, музику та

фільми, які вони купили, і вони були притягнуті до відповідальності за це. Зокрема, Вам може бути не дозволено легально зламувати програмне забезпечення, яке Ви придбали, навіть якщо це тільки заради перевірки, що воно досить безпечно, щоб запускати на своєму комп'ютері. Це відбувається тому, що до багатьох речей, що Ви купуєте, додається Ліцензійна угода кінцевого користувача (англ. «EULA — End User License Agreement»), яка говорить про те, чого Ви не повинні робити. І Ви погоджуєтесь з цим, коли відкриваєте або встановлюєте продукт, навіть якщо Ви не можете прочитати її, або навіть не знаєте про нею, до тих пір поки не відкриєте або становите програму. Майте це на увазі, коли Ви практикуєте хакерські навички на тому, що Ви придбали для власного користування.

Навіщо бути хакером?

Розглянемо, як вчені склали карту людського геному: вони використовували метод, розроблений для декодування паролів. Паролі зазвичай зберігаються в зашифрованому вигляді, тому їх важко вкрасти. Метод брутфорс (англ «brute-forcing») - це метод розшифровки паролів шляхом злому (англ «crack») їх зашифрованою форми перебором всіх можливих комбінацій. Він компрометує зашифрований хеш (англ «hash») пароля, перетворюючи кілька символів за раз, потім зшиває їх назад. Дослідники генома адаптували цю техніку, щоб скласти карту цілих 3,3 мільярда базових пар генома людини.

Хакерство проявляється на кухні, коли кухарі використовують рідкий азот в якості охолоджувального агента, щоб зробити ідеальне морозиво, або коли вони рубають помідори, щоб зробити картоплю фрі з томатним соусом замість кетчупу або їм просто потрібно зробити щось, для чого у них немає потрібного обладнання...

Хіміки зламують елементи та з'єднання протягом століть. Від природи молекули вибагливі, коли мова заходить про те, як вони ведуть себе в різних умовах (на жарі, холоді, в горах, або глибоко в океані), так що хіміки повинні добре розбиратися у властивостях хімічних речовин, тому вони можуть намагатися зламати одне потрібну речовину всі разом. Ніде це не проявляється більш очевидно, ніж у винаході нових лікарських засобів, коли сотні рослин вивчаються на предмет їх хімічних властивостей від коренів до плодів, видобуваються та поєднують з іншими для отримання нових препаратів. Потім хіміки намагаються знову і знову, іноді роками, отримати правильні комбінації і добитися потрібних результатів.

Хакерство використовується в бізнесі для розуміння ринку або купівельної поведінки деяких типів споживачів. Бізнесмени ретельно досліджують сили, які керують областю бізнесу, що їх цікавить, а потім намагаються змінити або вплинути на них так, що б змусити робити те, що їм потрібно. Іноді вони зламують продукт, а іноді зламують Вас (за допомогою реклами та праймінгу (англ «priming»), над якими ви будете працювати на уроках соціальної інженерії).

Хакерство також стає все більш важливою частиною війни. Висококваліфіковані солдати кмітливі та винахідливі в досягненні своїх цілей так само, як хакери. Зломщики кодів, розвідники-аналітики та польові офіцери використовують те, що є базовими хакерськими навичками, що б зрозуміти, що має противник, що він робить і як отримати користь з недоліків його обладнання. Так як все більше країн покладається на комп'ютери і мережі, використання злому в кібер-атаках і обороні стало важливою частиною національних збройних сил і розвідувальних операцій. Національні та міжнародні органи безпеки навіть приходять на хакер-конвенції, що б найняти хакерів!

Справжня причина бути хакером - це реальна влада. Ви можете робити дійсно класні речі, коли маєте потужні хакерські навички. Глибинні знання дають Вам велику силу. Якщо Ви знаєте, як щось працює від «а» до «я», Ви можете взяти це під контроль, значить у ваших руках справжня влада. Більше того, у Вас є сили захистити себе і тих, про кого Ви дбаєте.

Все більше і більше людей живуть в онлайні, як у формі відносин, люди знаходять роботу та заробляють гроші в Інтернеті. Інформація може бути корисною — або може нести загрозу — а хакери можуть захистити себе краще, ніж будь-хто інший. Вони можуть досліджувати те, що відбувається з їхніми даними. Вони можуть бути впевнені, що загальнодоступно тільки те, що вони хочуть, та й просто відчувають себе в безпеці. Це величезна конкурентна перевага в школі, на роботі і в житті, так як найменший негативну думку в кінцевому підсумку буде використано проти вас. Можете на це розраховувати.

Зламувати все, але не шкодите нікому.

Як зламувати

Розповідати Вам, як зламувати — теж саме, що пояснювати, як зробити сальто назад на колоді: яким би докладним не було пояснення Ви не зможете зробити це з першого разу. Необхідно розвивати навички, почуття та інтуїцію через практику чи інакше Ви будете падати навзнаки на обличчя. Але є деякі речі, які ми можемо сказати Вам, щоб допомогти в цьому і закликати Вас продовжувати практикуватися.

По-перше, Ви повинні знати деякі маленькі секрети про те, як хакери насправді працюють. Ми збираємося взяти їх з Методик тестування керівництва, або **OSSTMM** (www.osstmm.org). Хакери нагадують його, і воно вимовляється, як "оу-стем". OSSTMM (Open Source Security Testing Methodology Manual) - це Загальнодоступне Керівництво по Методиці Перевірки Безпеки, і, хоча можна його читати як інструкцію налаштувань DVD-плеєра, він є основним документом, який багато хакерів-професіонали використовують, щоб планувати і здійснювати свою атаку і захист. Глибина цього керівництва порівнянна з реальними скарбами, що відкриють Ваші очі.

Два способи отримати бажане

Наприклад, Вам слід знати, що, насправді, є тільки два шляхи отримати що завгодно: Ви самі берете його або є хтось, хто візьме його і віддасть Вам. Це означає, що всі захоплення в світі вимагає взаємодії (англ «interactions») між людиною і річчю. Очевидно, вірно? Але задумайтеся про це. Виходить, що всі захисні механізми повинні намагатися зупинити когось від взаємодії з річчю, яку вони захищають. Якщо Ви закриєте всі у величезному сейфі, Ви не зможете присікти всі взаємодії. Магазини повинні розставити речі на полиці, щоб покупці могли помацати їх. Компаніям необхідно відправляти інформацію клієнтам через електронну пошту, яка кріпиться до поштових серверів і передає повідомлення на інші поштові сервери.

Все це - взаємодії. Деякі з них відбуваються між речами і людьми, знайомими один з одним. Ми називаємо ці взаємодії довірчі відносини, чи просто довірою (англ «Trusts»). Коли взаємодії

відбуваються між незнайомими людьми або системами, ми називаємо їх взаємодії доступу (англ «Access»). Ви можете скористатися доступом, і взяти те що хочете, або Ви можете обдурити тих, кому довіряє жертва (мішень, ціль), щоб вони взяли те, що потрібно і віддали вам. Якщо Ви задумаєтеся про це на мить, то це означає, що безпека має на увазі захист чого-небудь, як від тих, хто цей об'єкт не знає, так і від тих, хто його знає і кому довіряє.

Вправи

1.1. Який тип взаємодії використовується в пошукових системах? Ретельно обдумайте: чи використовують деякі з них взаємодію Доступу? Чи є такі, що використовують взаємодію Довіри?

1.2. Наведіть простий приклад використання взаємодії Доступу та Довіри для отримання велосипеда, прикутого до стійки.

1.3. Наведіть приклад, як ви можете використовувати взаємодії Доступу або Довіри, що б проникнути в чужу електронну пошту.

Пожива для розуму: Шпигунство

Використання злому проти іноземної держави, вчинення злочинних актів злому і проникнення, порушення кордонів, крадіжки, знищення з метою отримання політичного або військової інформаційної переваги називається шпигунством. А коли злом відбувається закордонним бізнесом проти бізнесу іншої країни, щоб отримати перевагу - це економічне шпигунство.

Злом для отримання приватної та особистої інформації про окремих людей, з метою осоромити їх публічно називається DoXing. Якщо публічна інформація здобута про цільову особу або компанію для атаки, але не було скоєно кримінальних діянь, це називається аналізом документації (англ «document gridding») або OSInt (аналіз відкритих ресурсів, англ «Open Source Intelligence»).

Злом заради розуміння дії корпоративних мереж, систем, застосунків і пристроїв без реального порушення кордонів або вторгнення в систему, відомий як мережеве спостереження (англ «network survey»).

Злом з метою ретельного вивчення конкурента без порушення будь-яких законів (хоча те, що вони роблять можна назвати підлим або грубим) називається конкурентної розвідкою.

Ви, напевно, вмираєте від бажання почути, які жорсткі і грубі речі витворяє в рамках закону. Візьмемо приклад заподіяння незручності кому-небудь для отримання від нього інформації. Брехати йому - до тих пір, поки ви його не вбили - легально (хоча є закони, що забороняють викликати паніку в громадських місцях, наприклад, кричати «Пожежа!" У переповненому кінотеатрі, коли його немає).

Припустимо, хакер хоче знати, де компанія планує звести новий завод. Він аналізує документацію підприємства, щоб дізнатися, які люди уповноважені приймати це рішення. Потім хакер дзвонить в їх офіс, щоб дізнатися в яких містах вони бували, і, можливо, які заводи відвідували. Але, безумовно, це приватна корпоративна інформація, і ніхто її не розповість просто так, не піднімаючи тривогу. Тому хакеру потрібно добути інформацію хитрістю. Це не так складно, якщо підійти до процесу з уявою.

Хакер: Здрастуйте, я доктор Джонс, і я дзвоню Вам зі школи з приводу вашої дочки Ненсі.

Жертва: Серйозно? І що вона накоїла на цей раз?

Хакер: Ну, в неї було сильна носова кровотеча, яку ми не могли зупинити. Я б хотів запитати, чи не піддавалася вона впливу будь-яких хімічних препаратів, хімічного виробництва або щось на подобі цього? Ці симптоми зустрічаються рідко, за винятком людей, що піддаються впливу цих хімічних речовин. Ви можете мені що-небудь розповісти?

Жертва: (зливає інформацію)

У більшості своїй це не є незаконним, але заподіює непотрібне занепокоєння. Не кажучи вже про те, що змушує батька хвилюватися.

Злом заради захоплення всього світу

Злом це не просто взаємодії. Знаєте що. Багато людей кажуть, що політика це взаємодії. Може бути. Ви, мабуть, думаєте, що злом це порушення безпеки. Іноді це так. А насправді це захоплення контролю над чим-небудь і його зміна. Розуміння взаємодій, їх значення в реальному світі, використання понять, які обговорювалися раніше корисно, коли Ви намагаєтеся проникати, відкривати або навіть винаходити. Навіщо Вам це робити? Що б змусити те, чим Ви володієте робити те, що Вам треба. І утримувати інших від зміни вашої власності, що в інших людей може називатися безпекою (але ми не ці люди).

Іноді, коли ви купуєте що-небудь, компанія, яка Вам це продала, намагається силою або хитрістю переконати вас, що правила забороняють змінювати або модифікувати цей предмет. І ви погоджуєтеся з ними, до тих пір, доки приймаєте факт того, що порушення правил відбере можливість заміни або ремонту товару. Так що злом предмета не просто робить його вашим, а робить його вашим остаточно і незаперечно. Для деяких звучить страшнувато, але в цьому є свої переваги. Особливо якщо ви хочете утримати інших від посягань на ваше майно.

Для багатьох і багатьох людей безпека - значить помістити продукт у місце під замок, сигналізацію, ,брандмауером або щось, що теоретично збереже його в цілості. Але іноді все це працює не так добре, як має, або додає своїх проблем, які збільшують поверхню атаки (англ «Attack Surface»), тоді як продукти безпеки повинні її зменшувати. (Поверхня атаки це всі шляхи та взаємодії застосовувані для атаки кого-або чого-небудь.) Удачі Вам при отриманні поліпшеного продукту в світі масового маркетингу, передоплати, краудсорсингу та принципу «ви купили це« як є », і з цим Вам доведеться жити». Ось чому ви зламуєте свою безпеку. Вам необхідно проаналізувати товар і з'ясувати, як змінити його так, що б він працював краще. А потім Вам може знадобитися зламати ще раз, щоб компанія-продавець не привела його до первісного стану!

Тому пам'ятайте, що порушення безпеки, це лише одна з областей застосування хакерства, тому що, інакше Вам доведеться відмовитися від своєї свободи чи конфіденційності, які Вам не хотілося б втрачати. (Зрозуміло, що зараз Вас можуть не турбувати окремі речі які ви робите, кажете чи розміщуєте в мережі, але в Інтернету пам'ять довга, і йому усе простіше й простіше стає нагадати іншим про ваші справи та вчинки. Те, що відбувається в мережі - залишається в мережі. Запам'ятаєте це на майбутнє, навіть якщо сьогодні для Вас це не має значення).

Тепер, коли ви одержали уявлення про взаємодії, давайте розглянемо їх більш детально. Ви знаєте основні взаємодії, такі як Доступ і Довіра, але що ви чули про Видимість (англ «Visibility»)? Це третій тип взаємодії. Він такий же могутній, як інші два. Мовою поліцейських він спрощено звучить як можливість, але в хакерстві це повноцінне знання про те, чи існує щось, що взаємодіє із предметом, чи ні. За допомогою цієї взаємодії реалізується багато нових технік безпеки, таких як: обман, ілюзія та камуфляж. Також виникають зовсім нові хакерські методи обходу таких заходів безпеки!

Коли відомого грабіжника банків Джесси Джеймса запитали, навіщо він грабує банки, він відповів: «Тому, що там є гроші». Він мав на увазі, що через Видимість він довідався, що в банків є гроші, тоді як про інші речі він цього точно сказати не міг. Видимість: люди знають, які активи вони тримають. Але не все має Видимість. По суті Приватність це протилежність Видимості, і це потужний спосіб не стати мішенню. Де б Ви не перебували – на небезпечних вулицях, у джунглях або в Інтернеті, у першу чергу зберігайте низький рівень Відкритості та Видимості, щоб не бути атакованим.

Вправи

1.1 Інтернет - популярний засіб для створення міфів й увічнення помилкових історій, саме тому важко відрізнити правду від вигадки. Тому якщо ви хочете навчитися бути гарним хакером, заведіть звичку перевіряти факти й дізнаватися правду. От чому зараз ви підете й дізнаєтеся, чи дійсно Джессі Джеймс так сказав. І не задовольняйтеся відповіддю, знайденою на першій же веб-сторінці, а пошукайте трохи.

Тепер, коли ви звикли шукати інформацію, відшукайте правду про наступні прості речі:

1.2 Що значить слово «голка» на інуїтській мові, з якої воно походить? Які типи взаємодій ви зараз використали, що б відшукати відповідь?

1.3 Багато батьків, не замислюючись, указують на те, що цукор робить маленьких дітей гіперактивними. Чи не так це? Яка взаємодія в дійсності відбувається в маленьких животах, коли діти їдять багато цукерок або іншої солодкої їжі, що змушує їх рухатися надто активно?

1.4 Ви могли чути що цукор - причина карієсу, але яка насправді взаємодія в цьому випадку має місце, і що є реальна причина? Цукор це чи ні? Отримаєте бонусні бали, якщо зможете сказати яким типом взаємодії є чищення зубів у боротьбі з реальною причиною карієсу й знайдете назву хоча б однієї хімічної речовини спрямованого на корінь проблеми (*підказка: флюорит невірно*).

Чотирьох етапний процес

Взявши три типи взаємодії разом, Ви одержите Пористість, засновану на поверхні атаки. Це пори або "діри" у будь-якому захисті, які повинні бути, щоб вийшли будь-які необхідні взаємодії (а також будь-які невідомі або непотрібні). Наприклад, магазину усе ще необхідно розкласти товари на полиці, щоб люди могли доторкнутися до них, покласти в кошик і купити їх. Ці взаємодії повинні продати товари. Але власник магазина може бути не в курсі співробітників, які тайкома забирають речі з навантажувальної платформи - це і є небажану взаємодію.

Пористість — це те, що Вам потрібно знати про захист себе або атаки цілі. Але цього недостатньо, щоб проаналізувати, як їх зламати. Щоб зробити це, Ви повинні знати про три типи взаємодії більше, ніж Ви тільки що довідалися. Є ще один маленький секрет від OSSTMM і його називають Чотирьох етапний процес (англ. "FPP — Four Point Process"). У ньому надані чотири способи використання взаємодій для максимально глибокого аналізу, за якими ми можемо зрозуміти що потрібно зробити, щоб можна було спостерігати за предметом і бачити, що відбувається.

Процес відлунювання

Ми ростемо, відкриваємо й вивчаємо речі, взаємодіючи прямо з ними. Маленькі діти тикають висохлу білку ціпком, щоб переконатися, що вона мертва. Це називається процес відлунювання **(**англ**. «echo process»).** Він є самою основною й незрілою формою аналізу. Це як кричати в печеру й слухати відповідь. Процес відлунювання вимагає направляти в ціль різні типи взаємодії Доступу, а потім відслідковувати її реакцію, щоб з'ясувати, яким чином Ви можете взаємодіяти з нею. Цей процес є причинно-наслідковим типом перевірки.

Це незвичайний спосіб перевірки чогось, тому що, хоча це дуже швидка перевірка, але вона також не дуже точна. Наприклад, при використанні процесу відлунювання в тестуванні безпеки, ціль, яка не відповідає на запити, вважається безпечною. Те ж відбувається, коли вона не має Видимості. Але ми також знаємо, що якщо щось не реагує на певний тип взаємодії, то це не значить, що воно "безпечне". Якби це було так, то інші тварини не вбивали б опосумів, коли ті перетворювали мертвими, і кожен міг би урятуватися від ведмедя, просто

зомлівши від страху. Але це не правда. Уникнення Видимості може допомогти Вам пережити деякі типи взаємодій, але, звичайно, не всі.

На жаль, здебільшого люди в повсякденному житті використають для дослідження речі тільки процес відлунювання. Існує так багато інформації, втраченої через ці види одномірного аналізу, що ми повинні бути вдячні галузі охорони здоров'я, що пішла далі методу діагностики "Якщо я зроблю це, буде боляче?". Якби лікарні використали тільки процеси відлунювання для визначення стану здоров'я людини, то вони рідко по-справжньому допомагали б людям. Радує тільки те, що час у кімнаті очікування буде дуже коротким. От чому деякі лікарі, більшість учених й особлива хакери використають чотирьох етапний процес, щоб переконатися, що вони нічого не пропустили.

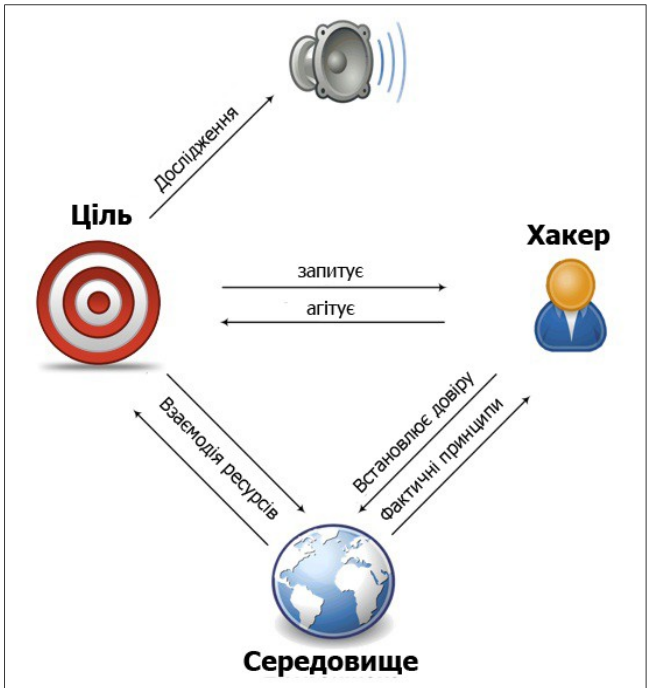

Рисунок **1.1** – Чотирьох етапний процес

Чотирьох етапний процес надає змогу подивитись на взаємодії наступними способами:

1. Індукція: що можна сказати про ціль по її оточенню? Як вона поводиться в цьому середовищі? Якщо ціль не перебуває під впливом навколишнього середовища, це також цікаво.

2. Наслідок: які сигнали (випромінювання) ціль посилає? Дослідіть будь-які відбитки або показники цих випромінювань. Система або процес, як правило, залишає характерну рису взаємодії з навколишнім середовищем.

3. Взаємодія: що відбувається, коли Ви заважаєте цілі? Цей пункт включає тести відлунювання, у тому числі очікувані та несподівані взаємодії з ціллю, щоб викликати в неї відповідні відгуки.

4. Втручання: наскільки довго ціль протримається до того, як зламається?Заберіть в цілі потрібні для функціонування ресурси, наприклад електрику, або, наприклад, Ви можете втрутитися в процес взаємодії цілі з іншими системами, щоб подивитися при яких екстремальних подіях ціль ще може функціонувати.

Повернемося до нашого прикладу про лікарню... чотири етапи FPP будуть виглядати наступним чином:

1. Функції взаємодії — це процеси відлунювання, у яких лікарі оглядають пацієнтів, говорять із ними, перевіряють їхні рефлекси на ліктях і колінах і використають інші інструменти діагностики.

2. Наслідок зчитує «випромінювання» від пацієнтів, такі як пульс, артеріальний тиск і мозкові хвилі.

3. Втручання це зміна або стресове порушення гомеостазу пацієнта, його поведінки, або рівня комфорту, щоб подивитися, що відбувається.

4. І, нарешті, індукція, що вивчає середовище, місця, які пацієнт відвідав перед тим, як він занедужав, і як вони можуть вплинути на пацієнта, якщо він, можливо, чогось торкнувся, прийняв усередину або вдихнув.

Вправи

1.1 Як Ви могли побачити, Чотирьох етапний процес дозволяє більш глибоко досліджувати взаємодії. Тепер Ви можете спробувати самі. Поясніть, як Ви могли б використати Чотирьох етапний прогрес, щоб довідатися чи працює годинник, і якщо він працює коректно, то чи показує він вірний час.

Що зламати

Коли ви щось зламуєте, необхідно встановити базові правила. Вам знадобляться мова та поняття, щоб знати, що ви насправді зламуєте. Сфера (англ «Scope») - слово, що ми використаємо для опису всіляких операційних середовищ, кожна з яких взаємодіє з річчю, що ви хочете зламати.

Пожива для розуму: Класи та Канали.

У професійній термінології (якою користуються й хакери), Сфера складається із трьох Класів, які підрозділяються на п'ять Каналів:

Клас	Канал
Фізична безпека (PHYSSEC)	Людський
	Фізичний
Безпека спектру (SPECSEC)	Безпроводовий
Безпека комунікацій (COMSEC)	Телекомунікації
	Дані мереж

Класи це не те, про що б Вам коштувало занадто турбуватися, але вони є офіційними ярликами, що використаються зараз в охоронній, урядовій і військовій індустрії. Класи визначають область вивчення, дослідження або операції. Тому якщо ви шукаєте більше інформації на будь-яку тему, дійсно корисно знати, як це називають професіонали.

Канали це звичайне позначення способів взаємодії з активами. Нерідко для злому гаджета використається, "Чотирьох Етапний Процес" для кожного каналу. Так, виглядає досить трудомістко, але подумайте, як це захоплююче, коли ви можете змусити щось працювати в такий спосіб, що не значиться в жодному керівництві, або, ще краще, навіть невідомий виробникові!

Активом (англ. «asset») може бути будь-що, що має цінність для власника. Це можуть бути фізичні об'єкти, такі як золото, люди, креслення, ноутбуки, телефон із частотою сигналу 900

МГц і гроші; або інтелектуальна власність, наприклад: особисті дані, відносини, бренди, бізнес процеси, паролі і слова, сказані по мобільному телефону.

Залежності (англ. «dependencies») - це речі поза активами власника, не здатні забезпечити свою самостійність. Не так багато комп'ютерів генерують для себе електрику, наприклад. Навіть якщо ситуація в якій Вам відключать електрику, малоймовірно, це все ще ваша сфера.

Мета безпеки — розподіл (англ. «separation») між активами і їхніми залежностями та усунення загрози.

Ми сказали, що безпека це функція поділу. Існує чотири способи забезпечити поділ:

- Перемістити актив, що б створити бар'єр між ним і загрозою.
- Перевести загрозу в безпечний стан.
- Знищити загрозу.
- Знищити актив. (Не рекомендується!)

Коли ми зламуємо, ми шукаємо точки, де можливо взаємодіяти з ціллю, і де не можна. Подумайте про двері усередині будинку. Деякі з них необхідні працівникам; інші - споживачам. Деякі - для порятунку від пожежі. А деякі взагалі не потрібні.

Проте, кожні двері — це точки взаємодії, що допомагає як при виконанні необхідних операцій, так і небажаних, таких як злодійство. Коли ми виходимо на сцену в ролі хакерів, ми не знаємо наперед причини (мотиви) всіх цих точок взаємодії, тому ми аналізуємо їх за допомогою Чотирьох Етапного Процесу.

Рисунок **1.2:** Пористість

Розглянемо, наприклад, хлопця, що хоче бути абсолютно захищеним від блискавки. Єдиний спосіб (будучи на планеті Земля) — забратися усередину гори, тому що блискавка зовсім точно не зможе проникнути через весь цей бруд і камені. Якщо припустити, що йому ніколи не буде потрібно вийти назовні, то його безпека 100%. Але якщо почати свердлити діри в скелі, блискавка буде мати на одну точку Доступу більше з кожною дірою, і Пористість збільшиться. OSSTMM розділяє поняття убезпечити себе від блискавки, і бути захищеним від неї. Простий факт – чим більше Пористість, тим більше ймовірність, що хакер зможе змінити й взяти під контроль те, що захоче.

Пожива для розуму: Пористість

Деякі приклади, які описують, як пори можуть бути розташовані, класифіковані та визначені в процесі злому.

Поняття	Значення
Видимість	Коли поліція розслідує злочин, шукають засіб, мотив і можливість. Якщо актив видимий, він може піддатися атаці, а якщо невидимий, то він не може стати метою атаки, хоча його й можна виявити. Деякі фахівці з безпеки люблять говорити що затемнення (англ. «obfuscation») — поганий захист, тому що воно не захищає, а лише приховує що-небудь. Але це непогана річ, особливо тоді, коли Вам не потрібний постійний контроль безпеки. До цього ефекту **OSSTMM** пропонує невеликий дорогоцінний секрет: "Безпека не повинна зберігатися вічно, а просто ледве довше чим те, що могло б помітити, що її немає."
Доступ	Доступ — число різних місць, де відбувається взаємодія із зовнішнім середовищем. Для будинку це можуть бути двері на вулицю або вікна, а для інтернет-сервера — число відкритих мережних портів або сервісів, доступних на цьому комп'ютері.
Довіра	Довіра - коли один об'єкт вільно взаємодіє з іншим об'єктом у межах заданої сфери. Довіра — причина того, що Ви не прохаєте у своєї матері посвідчення особи, коли вона приходить обійняти Вас. Це також те, чому Ви не підозрюєте, що вона отруїла Вашу їжу. Ви вчитеся довіряти речам у своїй сфері. Тоді, одного разу, якщо ваша мати буде захоплена інопланетною расою і дійсно отруїть Вашу їжу, Ви з'їсте її, нічого не підозрюючи. Таким чином довіра – це і діра в безпеці і проста заміна аутентифікації, спосіб, яким можна підтвердити, чи є хто-небудь тим, про кого ми думаємо. Довіра - дивна річ, тому що вона властива тільки людям і високо цінується в суспільстві. Без довіри ми ніколи не були б у змозі вільно взаємодіяти. Але через довіру нас легко обдурити, пограбувати й оббрехати. Дослідження OSSTMM в області довіри показує, що існує 10 причин довіряти кому-небудь. Вони називаються Критеріями довіри(англ. «Trust Properties») і якщо всі десять причин задовольняються, тоді ми можемо довіряти без ризику та занепокоєння. Але те ж саме дослідження показує, що більшості людей потрібен лише один виконаний критерій довіри для відчуття безпеки, а от дійсні параноїки або цинічні люди задовольняються всього трьома чинниками.

Ресурси

Ефективне дослідження вивчення й критичного мислення — ключові навички для хакерів. Злом є творчим процесом, заснованим більше на способі життя, чим на уроках. Ми не можемо навчити Вас усьому, що Вам необхідно знати, але ми можемо допомогти Вам зрозуміти, що Вам потрібно знати. Тому що наука рухається швидко, і те, що ми вивчаємо сьогодні, може

бути не актуально завтра. Набагато краще для Вас охопити традиції навчання хакерів, які є найважливішою частиною злому і які будуть відрізняти Вас від скрипт кідді (англ. «script kiddie»)(хакерське слово, що означає людину, що використає інструменти, не знаючи як або чому вони працюють).

Якщо Ви зіштовхнетеся в цьому уроці зі словом або поняттям, яке Ви не розумієте, дуже важливо, щоб Ви подивилися його значення. Ігнорування нових слів зробить важким для Вас розуміння концепції найближчих уроків. Вам буде запропоновано вивчити тему, а потім передбачається використання інформації, щоб виконати вправи цього уроку - але ці уроки не пояснять Вам, як виконати дослідження. Тому обов'язково витратьте стільки часу, скільки Вам необхідно, щоб навчитися використати різні доступні ресурси.

Книги

Ви можете бути здивовані, що ми не загострюємо Вашу увагу тільки на Інтернеті, але книги є відмінним способом довідатися про фундаментальну й фактичну науку все, що Ви хочете знати. Хочете довідатися щось із області інформатики, наприклад, про апаратні деталі Вашого комп'ютера? Ніщо не допоможе Вам більше, ніж читання книг по цій тематиці. Основною проблемою книг про комп'ютери є те, що вони дуже швидко застарівають. Секрет у тому, що потрібно навчитися бачити фундаментальну структуру під тонкою оболонкою деталей. MS-DOS і Windows дуже різні, але обоє засновані на принципі Булевої логіки, що привела до комп'ютерів починаючи із графині Ади Лавлейс, що написала перші комп'ютерні програми в дев'ятнадцятому столітті. Безпека й конфіденційність приватного життя може й змінилися в останні 2500 років, але «Мистецтво війни» Сунь-Цзи охоплює основні принципи, які усе ще застосовуються й сьогодні. (До речі, не існує більше швидкого способу уславитися нубом (англ. «n00b»), чим процитувати Сунь-Цзи. Ви повинні знати, як застосовувати деякі речі, але не говорити про них. І цитування «Мистецтва війни» доводить, що Ви насправді не читали його, тому що Сунь-Цзи говорить, що потрібно тримати Ваші реальні знання в таємниці).

Навіть при тому, що інформація, знайдена в книгах, може не бути настільки ж сучасної як інформація, що надходить із інших джерел, але відомості, отримані з книг, швидше за все будуть краще написані, чим в більшості інших джерел. Також іноді вона є більш точною. Письменник, що витрачає рік на написання книги, швидше за все витратить час, щоб перевірити факт, чим хтось, хто пише оголошення в блогах шість разів на день. (Подивіться Розділи Журнали та Блоги для одержання додаткової інформації.)

Але пам'ятайте, точність не означає об'єктивність. Джерела автора інформації можуть бути упереджені. "Книги з історії написані переможцями" (це цитата), і теж саме вірно, коли справа стосується політики й соціальних норм, які можуть забрати деяку інформацію з публікацій. Таке відбувається зі шкільними підручниками, які обрані в рамках політичного процесу й містять тільки ту інформацію, що вважається соціально прийнятної для вивчення. Так що не думайте, що Ви знайшли золоту істину тільки тому, що Ви прочитали це в книзі. Істина лише в тому, що будь-яка людина може написати книгу, і будь-яка книга може містити різні версії істини.

Не дивіться на книгу й не відмовляйтеся від неї через її розміри, перш ніж почнете її читати. Ніхто не читає більшість масивних книг, які Ви бачите, від кірки до кірки. Думайте про них, як про доісторичні веб-сторінки. Відкрийте одну на випадковій сторінці й почніть читати. Якщо Ви чогось не розумієте, ідіть назад і подивіться тлумачення (або перейдіть до того, що зрозуміло для Вас). Переходьте по книзі взад і вперед, начебто Ви переходите від однієї веб-сторінки до іншої. Цей тип нелінійних досліджень набагато більше цікавий і повноцінний для хакерів, тому що задовольняє Вашу цікавість більше, ніж читання.

І нарешті, коштовна навичка, що приходить із читанням книг, - це здатність добре писати. Це величезна перевага, коли Ви намагаєтеся розібратися в новій області знань. Це також допомагає заслужити більшу довіру інших читачів, особливо тих, хто володіє авторитетом.

Журнали та газети

Журнали і газети дуже корисні для надання короткої й своєчасної інформації. Хоча ці типи публікацій можуть бути скупі на деталі. Також пам'ятайте, що кожна газета або журнал мають свою власну аудиторію й свій порядок денний або тему, незалежно від будь-яких заяв бути "справедливими й незалежними". Знайте тему видання: журнал «Linux» не обов'язково гарне джерело інформації про Microsoft Windows, тому що Windows суперечить заявленим темам (конкуруючі операційні системи), і, чесно говорячи, читачі журналу «Linux» хочуть читати про перевагу Linux. Багато спеціалізованих журналів використають придушення доказів (англ. «cherry picking»), коли технічними прийомами виділяють тільки позитивні аспекти чого-небудь, що відповідає темі журналу, або негативні аспекти того, що не відповідає.

Будьте в курсі можливих погрішностей публікацій. Саме тут Вам дають думку замість фактів, або виняткові факти з історії під власною думкою, і тому Ви не зможете скласти особистої думки. Розгляньте джерело! Навіть "нейтральне" періодичне видання може бути сповнене упереджень і спекуляції, адже це гарний спосіб сказати "основне припущення", але насправді це часто тільки "здогади" з боку журналіста.

Існує величезні рух в області медицини за те, що всі медичні й фармацевтичні дослідження (або, принаймні, всі фінансовані державою) повинні бути опубліковані, навіть якщо вони провалилися, так лікарі зможуть зробити більш усвідомлений вибір про застосування ліків або процедур. У той час, як поточні медичні журнали публікують "факти" з дослідницьких випробувань, деталі й обставини як і раніше покриті туманом. Це дійсно важливо, коли Ви маєте справу із предметами, які ґрунтуються на наявних причинах. Причинно-наслідковий зв'язок вимагає, щоб причина передувала ефекту і породжувала його, а не навпаки.

Інші прийоми, що використовуються періодичними виданнями (як випадково, так і навмисно) — неофіційні дані, такі як думки людей, опубліковані як докази, незалежно від того чи є вони експертами чи ні; авторитетне свідчення, у якому працівники галузі, представлені як експерти, висловлюють своя думка, або люди, які є органами влади в одній області пропонують свою думку в іншій, у якій вони не мають досвіду; і, нарешті, спекуляція - видання чогось справжнім, лише тому що "всі" вважають, що це правда, хоча немає ніяких фактичних доказів.

Найкращий спосіб упоратися із проблемами точності й схованого плану - це добре й багато читати. Якщо Ви читали про цікаве питання в журналі, вивчите його далі. Візьміть одну сторону питання й шукайте підтвердження; а потім візьміть іншу й шукайте вже спростування. Це типова поведінка для деяких культур. Шукати інші сторони історії - частина їхніх соціальних звичок. Це дійсно потужна культурна риса, особливо якщо Ви намагаєтеся забезпечити успішну демократію.

Вправи

1.1 Пошукайте в Інтернеті три онлайн журнали про злом. Як Ви знайшли ці журнали?

1.2 Всі три журнали конкретно про комп'ютерний злом? Що ще вони пропонують, що може бути корисно в інших сферах або в іншому бізнесі?

Пожива для розуму: Спекуляція

Абзац з газетної статті про грабіж. Можете знайти тут Спекуляцію? Відзначте підозрілі області:

Банк іпотечного кредитування Лэйк Мідоу був пограбований у вівторок удень. Збройні бандити в масках прийшли за кілька хвилин до закриття, і втримували співробітників банку в заручниках впродовж години, поки щось не змусило їх зникнути на поза шляховику останньої моделі. Як повідомлялося, ніхто із заручників не постраждав.

Ніхто не міг ідентифікувати бандитів, і по наступних моментах після пограбування поліція змушена була припустити, що робота виконана професіоналами. Автомобіль був знайдений за банком у південній частині густого лісу у підніжжя гір Блюгрин. Поліція, імовірно, буде тепер шукати досвідчених, раніше суджених грабіжників, що мають відносинах з людьми, що проживають у цьому районі.

Із середньою кількістю в 57 повідомлень про пограбування щодня по всій країні, і населенням графства Блугрін, що обіцяє збільшитися до 50000 до наступного року, може обернутися лавиною банківських крадіжок у цьому регіоні. «Здається, це стає модним» - сказав комісар поліції Сміт.

Оскільки ми стаємо більше байдужними до спекуляції й залишаємося не інформовані про упередженість статистичних даних і результатів, у майбутньому всі наші новини могли б походити від єдиного журналіста, що спекулює ними в міру надходження. З вищеописаного приклада можна зробити тільки один реальний висновок: пограбування відбулося ввечері вівторка. Тепер для наочності, от як би виглядала замітка, якби ми змінили всю спекуляцію, щоб зробити її більш безглуздої:

Справедливий банк іпотечного кредитування був пограбований у вівторок увечері, коли раптово, перед самим закриттям, з'явилися грабіжники під виглядом курок, які попередили, що вони могли б утримувати співробітників банку в заручниках у полоні десяти років, але прибула повітряна куля, і вони втекли на ній. Як повідомлялося, ніхто із заручників не був покритий пір'ям.

Ніхто не міг ідентифікувати бандитів, таким чином після пограбування поліція змушена була припустити, що робота виконана професіоналами, і серед них був художник по костюмах та досвідчений повітроплавець. Повітряна куля була помічена над банком, та летіла на південь до антарктичної тундри. Поліція, імовірно, буде тепер шукати досвідчених візажистів, у яких також є зв'язки з людьми, що захоплюються повітряними кулями.

Із середньою кількістю в 57 повідомлень про пограбування щодня по всій країні й повідомленнями повітроплавальної індустрії про збільшення продажів до 47 газиліонів доларів до невизначеної дати в майбутньому, це могло стати початком лавини банківських крадіжок з використанням повітряних куль. «Здається, це стає модним» - сказав комісар поліції Гордон.

При такому нездоланному використанні спекуляції й статистики у всіх галузях, не дивно, що вона й в індустрію безпеки ввійшли з такою міццю. У цій галузі часто використається термін **FUD**, що є абревіатурою від слів Страх, Непевність й Сумнів (англ. «Fear, Uncertainty, and Doubt»). От як спекуляція й суб'єктивний аналіз ступеня ризику використається для залучення уваги й продажу ідей безпеки. На жаль, вони успішно грають на примітивних людських страхах і зростаючій нечутливості до спекуляції. Це привело до невідповідних рішень підтримки безпеки, застосовуваним неналежним чином і помилкової впевненості у владі. Очевидний провал навичок критичного мислення в населення, що експлуатується й комерційним сектором і злочинцями.

Пошукові системи

Google - добре відома, але не єдина пошукова система. Bing гарний у пошуку простих запитів, а Yahoo - при виконанні повного дослідження. Але знайте, що всі ці веб-сервіси хочуть знати про Вас усе, що можуть, а можливо навіть більше, ніж їм варто знати. Вони запам'ятовують всі ваші пошукові запити й веб-сайти, на які ви переходите.

Існують системи, такі як AltaVista й DuckDuckGo.com, які можуть надати Вам хоч якусь анонімність. Це може бути корисно коли ви ходити по темних кутах.

Веб-сайти доступні для пошуку, поки вони онлайн, і, звичайно, довгий час після. Звичайно вони зберігаються у вигляді кешованих сторінок (англ. «cached pages»). В Інтернеті кеш — це онлайн запис останньої версії веб-сайту, навіть якщо сам сайт канув у небуття. Пошукові системи й архіви сайтів зберігають цю інформацію невиразно довго, у поняттях Інтернету — «нескінченно». Перед тим як щось розмістити в Інтернеті, корисно згадати, що воно потім нікуди не дінеться. Ніколи. Можливо, Вам доведеться шукати посилання на збережену копію сторінки. Google, наприклад, зазвичай ставить позначку "кеш" поруч зі звичайним посиланням на результат.

Крім пошукових систем, існують також корисні суспільні кеші в таких місцях, як Інтернет-архів http://www.archive.org. Ви можете знайти версії цілих веб-сайтів, кешованих кілька років тому, які можуть бути дуже корисними для пошуку інформації, що "зникла".

Остання замітка про веб-сайти: не думайте, що Ви можете довіряти сайту просто тому, що він виявляється пошуковою системою. Багато хакерів поширюють атаки й віруси через сайти. Заразитися можна шляхом відвідування сайту, завантаження безневинних на вигляд програми, скринсейва або будь-якого іншого файлу. Ви можете підвищити свою безпеку, не завантажуючи програми з невідомих сайтів, і переконавшись у тому, що ваш браузер працює в пісочниці (англ. «sandbox»). Але цього може бути недостатньо. Браузер - це вікно в Інтернет, і, як через будь-яке вікно, погані речі можуть проникнути просто тому, що воно відкрито. Ви можете навіть не довідатися про це, поки не стане занадто пізно.

Вправи

1.1 Існує багато пошукових систем. Деякі з них добре справляються із проникненням у Невидиму мережу (англ. «Invisible Web»), область Інтернету, у яку важко проникнути більшості пошукових систем, наприклад деякі закриті бази даних. Гарний розвідувач знає, як всі їх використати. Деякі сайти спеціалізуються на відстеженні пошукових систем. Знайдіть п'ять пошукових систем, якими ви раніше не користувалися, і про які можливо навіть і не чули.

1.2 Є також пошукові системи, які шукають інші пошукові системи. Їх називають метасистемами. Знайдіть одну з таких метасистем.

1.3 Введіть запит «безпека й злом» (включаючи лапки) і запишіть три перших результати. Чим відрізняються результати, коли ви НЕ використаєте лапки?

1.4 Пошук теми дуже відрізняється від пошуку слова або фрази. У попередньому завданні ви шукали фразу. Тепер ви будете шукати ідею.

Зробіть так: подумайте про фразу, що може перебувати на тій сторінці, що ви шукаєте. Якщо ви хочете, щоб пошукова система видала Вам список журналів про

хакерство, ви не повинні вводити запит «список журналів про хакерство». Не так вже багато сторінок будуть містити цю фразу! У Вас буде кілька влучень, але не так багато.

Замість цього Вам треба подумати: «Якби я був на місці журналу, які типові пропозиції я б розмістив?» уведіть наступні слова й фрази в пошуковий рядок і визначите, які з них забезпечують кращий результат:

1. мій список улюблених журналів про хакерство

2. список професійних хакерських журналів

3. ресурси для хакерів

4. хакерські журнали

5. хакерські журнали список ресурсів

1.5 Знайдіть самий старий веб сайт Mozilla в Інтернет архіві. Для цього Вам буде потрібно знайти сайт "www.mozilla.org" на сайті архіву http://www.archive.org.

1.6 Тепер сполучимо все разом. Наприклад, ви хочете завантажити першу версію веб браузера Netscape. Використовуючи пошукові системи та Інтернет архіви, подивіться, чи зможете Ви визначити місцезнаходження й завантажити першу версію цього браузера.

Веб-сайти та веб-застосунки

Стандартом де-факто для обміну інформацією в цей час є веб-браузер. У той час, як ми класифікуємо все, що бачимо, як "веб", усе більше й більше, що ми дійсно використаємо - це "веб-застосунки", тому що не все в Інтернеті - це сайти. Якщо Ви перевіряєте електронну пошту, використовуючи веб-браузер, або одержуєте музику через служби веб-з'єднання, то Ви використаєте веб-застосунок.

Іноді веб-застосунки вимагають право доступу. Це означає, що Вам необхідне ім'я користувача й пароль, щоб одержати доступ. Наявність доступу, якщо у Вас є законне право на доступ, називається правом доступу (англ. «privileges»). Злом веб-сайта заради зміни сторінки може означати, що у Вас є доступ, але оскільки у Вас немає юридичного права, Ви не маєте привілейованого доступу. Коли продовжите використати Інтернет, Ви побачите, що в багатьох місцях доступ до привілейованих ділянок надають випадково.

Якщо знайдете щось подібне, добре б сповістити про це адміністраторові сайту. Однак, остерігайтеся можливих правових наслідків. На жаль, багато адміністраторів незадоволені небажаними звітами про вразливість.

Щоб внести свій внесок і зробити Інтернет більше безпечним, а також захистити себе, Ви повинні розглянути використання анонімного проксі-серверу (наприклад, Tor або anonymous remailers, і т.п.) для розсилання звітів про вразливість адміністраторам. Але пам'ятайте: всі ці анонімні технології мають свої слабкі місця, і Ви можете бути не таким анонімним, як Ви думаєте! (Не один хакер уже пізнав цей важкий шлях).

Вправи

1.3 Використайте розвідувач, щоб знайти сайти, які зробили помилку, надавши право доступу всім. Щоб зробити це, будемо шукати папки, які дозволяють нам побачити її зміст («перелік файлів у каталогів»), це, як правило, не повинне бути дозволене. Для цього ми будемо використати деякі виверти Google на http://www.google.com. Уведіть це в поле розвідувача:

allintitle:"index of" .js

Перегляньте результати і Ви зможете знайти той, котрий виглядає як список каталогів. Цей вид пошуку відомий, як Google злом.

1.4 Чи зможете Ви знайти інші типи документів цим методом? Знайдіть ще три каталоги, які містять .xls файли, .doc файли та .avi файли.

1.5 Є інші варіанти пошуку, схожі з "allintitle:"? Як Ви можете знайти їх?

Електронний журнал

Журнал, також відомий, як e-zine, є нащадком фензінов: невеликі, як правило, безкоштовні журнали з дуже маленькою аудиторією (менш 10,000 чоловік), які часто видаються аматорами й аматорськими журналістами. Фензін друкувався на папері. Журнали в Інтернеті, такі як знаменитий 2600 або веб-журнал Phrack, пишуться волонтерами; часто це означає, що виробники не редагують зміст на предмет не технічних помилок. Іноді різкі формулювання можуть бути дивні для тих, хто не знаком із цим жанром.

Такі журнали обговорюють дуже різкі теми або програми, і, як правило, дуже самовпевнені. Разом з тим вони найчастіше показують й обговорюють дві сторони питання, тому що, звичайно, не піклуються про те, що їм потрібно сподобатися рекламодавцями й абонентам.

Вправи

1.1 Пошукайте в Інтернеті три журнали на предмет злому. Як Ви знайшли ці журнали?

1.2 Чому Ви класифікуєте їх, як журнали? Пам'ятайте, тільки тому що вони продають його, як журнал або написали в назві "журнал" - не можна сказати, що він ним являється.

Блоги

Блог можна розглядати, як еволюцію журналу, як правило, у писемній формі однієї людини. Блоги оновлюються частіше, ніж більшість друкованих видань або журналів, а також створюють групи, зв'язані дуже сильними темами. Також важливо читати коментарі, як і розміщувати їх. Більше, ніж у журналах, у блогах відповіддю часто служить негайний і самовпевнений пост, з коментарями від всіх учасників. Це одна із цінностей блога.

Є мільйони блогів в Інтернеті, але лише невеликий відсоток з них є активними. Інформація більшості, однак, є усе ще доступною.

Вправи

1.3 Знайдіть в Інтернеті три блога про злом.

1.4 Які групи або співтовариства зв'язані з ним?

1.5 Чи блог належить до теми безпеки, правоохоронних органів або академічної теми?

Форуми та Списки розсилань

Форуми та списки розсилання розроблені засобами масової інформації, і вони дуже схожі на записі розмов на вечірці. Ставитеся небагато скептично до того, що Ви там читаєте. Розмови часто відволікають увага, багато чого зі сказаного — слухи, деякі люди тролять (знущаються), може спалахнути великий базар, і коли вечірка закінчилася, ніхто не впевнений, хто що сказав. Форуми й списки розсилань схожі, тому що існує багато способів допомогти поширенню неточної інформації — іноді навмисно — і існують шляхи сприяти анонімам. Оскільки питання й теми швидко міняються, щоб одержати всю інформацію важливо прочитати весь потік коментарів, а не тільки трохи перших.

Ви можете знайти форуми практично на будь-яку тему, а також онлайн-журнали та газети пропонують форуми для читачів, щоб вони написали відгук на статті, які вони видають. Тому форуми мають безцінне значення для одержання думок про статтю; незалежно від того, скільком людям сподобалося, обов'язково найдуться незадоволені.

Існує безліч розсилань по спеціальних темах, але їх важко знайти. Іноді найкращий спосіб полягає в пошуку інформації з певної теми, щоб знайти співтовариство розсилань, що займається цією темою.

Як хакеру, Вам важливо знати, що багато форумів і розсилання не знайти за допомогою основних пошукових систем. Хоча Ви й можете знайти форум або розсилання за допомогою пошукової системи, Ви не зможете знайти інформацію в окремих повідомленнях. Ця інформація є частиною невидимої мережі, оскільки містить дані тільки для пошуку безпосередньо на веб-сайті або форумі.

Вправи

1.6 Знайдіть два хакерських форуми. Як Ви знайшли ці форуми?

Чи можете Ви визначити теми або спеціалізації цих веб-сайтів?

Теми на форумах відбивають тему хостинга веб-сайту?

1.7 Знайдіть два списки розсилань про злом або про безпеку.

Хто є "власником" цих розсилань? Ви можете побачити список учасників? (Вам може знадобитися з'ясувати застосування розробленого списку, а потім шукати в Інтернеті сховані команди, щоб побачити всіх членів даного розсилання).

У яких списках можна чекати, що інформація більше фактична й менш самовпевнена? Чому?

Групи новин

Групи новин існують здавна. Вони були задовго до того, як з'явилася Всесвітня павутина. Google купив весь архів груп новин і помістив їх на сайті http://groups.google.com. Групи новин - це як архіви списків розсилань, але без пошти. Ви знайдете там записи з початку дев'яностих років. Люди розміщають там свої коментарі безпосередньо, як на звичайних сайтах.

> Як і веб архіви, архіви груп можуть бути важливі при пошуку того, хто подає дійсно оригінальні ідеї або створює продукт. Вони так само корисні при пошуку таємної інформації, що ніколи не розміщалася на веб сторінках.

Групи новин використаються зараз не менше, ніж раніше, до того, як всесвітня мережа стала основним засобом обміну інформацією. Однак, вони так само не придбали більшої популярності, оскільки були замінені на нові сервіси накшталт блогів та форумів.

Вправи

1.7 Використовуючи групи Google, знайдіть найстаршу групу новин, що оповідає про хакерство.

1.8 Знайдіть інші способи використання груп новин. Чи є спеціальна застосунок за допомогою якої Ви можете читати групи новин?

1.9 Як багато груп новин, що розповідають по хакерство, ви можете знайти?

1.10 Ви можете знайти поточний список всіх різних існуючих у цей час груп новин?

Вікі

Вікі — новітній інтернет-феномен. Вікіпедія (www.wikipedia.org) — ймовірно найвідоміша з них, але існує безліч інших. Як і багато чого іншого, вікі підтримується співтовариствами. Звіти часто затверджують, що вікі не точні, тому що редагуються аматорами й фанатиками. Але це ж відноситься й до книг, розсилань, журналів і всього іншого. Що важливо знати, так це те, що експерти – не єдине джерело великих ідей або фактичної інформації. Як вказує OSSTMM, факти з'являються з маленьких кроків підтвердження ідей і невеликих стрибків відкриттів. Саме тому вікі – більші джерела і професійних, і аматорських ідей, повільно й поступово підтверджуючих одне одного.

Вікі часто обговорює яку-небудь тему з усіх боків, і дозволяє простежити як інформація підтверджувалася, спростовувалася, уточнювалася й змінювалася за допомогою списку змін. Таким чином, це прекрасне місце для збору інформації, але часто для досліджень Вам доведеться переходити на сайт вікі.

Вправи

1.11 Пошукайте "Ада Лавлейс". Бачите результати з вікі?

1.12 Перейдіть на Вікіпедію й повторіть запит. Подивіться статтю про неї. Вона входила в результати вашого пошуку?

1.13 Перевірте зміни цієї сторінки Вікіпедії та подивіться на типи виправлень або змін. Які типи змін були внесені? Чи було щось змінене, а потім виправлене назад? А тепер виберіть популярну кінозірку або співака, що Вам подобається, подивіться сторінку у Вікіпедії про нього, і перевірте зміни. Зауважуєте розходження?

1.14 Знайдіть інший вікі-сайт і повторіть пошук. Який-небудь із результатів пошуку відображається в оригінальному запиті вашої пошукової системи?

Соціальні мережі

Ви користуєтесь сайтом соціальної мережі? Або навіть більше, ніж одним? Як хакер, ви добре інформовані, які мережі популярні на даний момент. А що на рахунок тих, які не так популярні, як раніше? Вони дотепер існують, і всі їхні дані в більшості випадків доступні.

Це означає, що існує величезний склад інформації про нас, що ми склали туди добровільно. І здебільшого вона залишиться там назавжди.

Соціальні мережі часто мають суб-групи або співтовариства по інтересах. Сайти із професійними темами мають групи з кібербезпеки, а сайти з "підпільною" темою часто мають хакерські групи. На професійних сайтах Ви (і всі інші) повинні використати своє дійсне ім'я. А на хакерських сайтах це не прийнято.

Саме головне, у соціальних мережах Ви використаєте Ваше дійсне ім'я або "прізвисько"? Ваше прізвисько можна співвіднести з Вашим дійсним ім'ям? Більшість людей не усвідомлюють, що вони використають прізвиська, але не рідкість, що випадково або навмисно вони розміщають свої дійсні імена, адреси, міста, школи, робочі місця й т.п. Якщо інші хакери зламають Ваше прізвисько, то з таких дрібних помилок вони можуть, як правило, досить швидко з'ясувати хто Ви насправді. Якщо Ви використаєте прізвисько, щоб бути анонімним для тих, хто Вас не знає, переконайтеся, що Ви вживаєте заходів, щоб усе зберігалося в такий же спосіб. І НІКОЛИ не переплутуйте Ваші прізвиська, якщо у Вас їх декілька.

Вправи

1.1 Пошукайте себе. Знайшли що-небудь? Чи є результати із соціальних мереж?

1.2 Перейдіть на сайт соціальної мережі, який ви користуєтеся. Не заходьте в свій акаунт, і повторіть пошук так, начебто ви стороння людина. Як багато інформації ви можете про себе знайти?
1.3 Перейдіть на сайт соціальної мережі, якою користується ваш друг. І знову не заходьте в свій акаунт, якщо маєте його. Пошукайте вашого друга. Як багато інформації змогли знайти?

Чат

Такі чати як: Internet Relay Chat (IRC) і Instant Messaging (IM), дуже популярний спосіб спілкування.

Як наукове джерело – чат – украй суперечливе, тому що Ви маєте справу з людьми в реальному часі. Деякі з них будуть дружелюбними, а деякі можуть бути й грубими. Деякі будуть необразливими жертвами, але деяких - шкідливими брехунами. Хтось буде розумний і готовий поділитися інформацією, а інший - зовсім не інформований, але не менш готовий ділитися. І може бути важко зрозуміти, хто є хто.

Однак, як тільки Ви освоїтеся в деяких групах і каналах, Ви можете бути прийняті в співтовариство. Ви будете задавати усе більше й більше питань, і Ви довідаєтеся кому можна довіряти. Зрештою, Ви зможете одержати доступ до самим новітніх хакерських експлойтів (також відомих, як zero day або 0day — невідома вразливість яку щойно відкрили і про неї знає лише маленька група людей) і поліпшити власні знання.

Вправи

1.1 Знайдіть три програми обміну миттєвими повідомленнями. У чому їхньої відмінності? Чи можуть вони використатися для обміну один з одним?

1.2 З'ясуєте, що таке IRC та як Ви можете підключитися до неї. Ви можете виявити, що мережа має канал автора ISECOM? Після того, як Ви підключилися до мережі, як Ви приєднаєтеся до обговорень каналу ISECOM?

1.3 Як Ви довідалися, які канали існують у IRC мережі? Знайдіть три канали про безпеку й три хакерських канали. Ви можете ввійти на ці канали? Там спілкуються люди або боти?

P2P (Peer to Peer)

P2P — це мережа в Інтернеті. У відмінності від традиційних клієнтів/серверів мережі, де кожен комп'ютер з'єднується через центральний сервер, комп'ютери в P2P мережі взаємодіють безпосередньо один з одним. Більшість людей асоціюють із P2P завантаження MP3 і піратських фільмів на відомому оригінальному Napster, але є багато інших P2P-мереж як для обміну інформацією, так і для проведення наукових досліджень в галузі розподіленого обміну інформацією.

Проблема з P2P-мережами — це те, що Ви можете знайти майже все, що на них є, але деякі речі в мережі нелегальні. А інші — легальні, але компанії, які створили їх, як і раніше вважають, що вони не повинні перебувати там, і раді вимагати гроші з власника будь-якого Інтернет-шлюзу, де їх завантажили.

На даний момент існує не так багато угод де розглядаються ситуації того, хто винен, власник комп'ютера, який був використаний для завантаження інформації, чи той хто інформацію завантажив насправді, чи той хто її розповсюджує. Це така ж ситуація, якби автомобіль був використаний для здійснення злочину, то власник автомобіля сів би у в'язницю, а не той, хто був за кермом. Закони Інтернету в цей час не справедливі, так що будьте обережні!

Будь те Ви або не Ви та людина, що ризикує завантаженням інтелектуальної власності, немає ніяких сумнівів, що P2P-мережа може бути життєво важливим ресурсом для пошуку інформації. Пам'ятайте: немає нічого нелегального в мережі P2P - існує багато файлів, які доступні для вільного поширення при всіляких ліцензіях - але також існує багато файлів у цих мережах, які не повинні там перебувати. Не бійтеся використати P2P-мережі, але будьте інформовані про можливі небезпеки, і про те, що Ви завантажуєте.

Вправи

1.4 Які три самі популярні та найбільше часто використовувані P2P - мережі? Як кожна працює? Яку програму Вам необхідно використати?

1.5 Досліджуйте протокол однієї з мережі P2P. Що він робить і як зробити завантаження швидше?

1.6 Пошукайте слова "download Linux". Ви можете завантажити дистрибутив з Linux за допомогою P2P?

Сертифікати

Існують сертифікати Тестера й Аналітика з питань безпеки OSSTMM, посвідчення «хакера» різних кольорів, сертифікати засновані на тій або іншій «найефективнішій практиці» (англ. «best practice») і посвідчень із усіма можливими божевільними ініціалами та пунктуацією.

Чому Вам важливі сертифікати? Тому що ви можете одержати деяких з них у будь-якому віці, і не обов'язково для цього мати вище посвідчення, і тому, що вони можуть поставити Вас у положення популярної людини, а не того, хто приганяє для нього кабріолет.

Проблема сертифікатів, заснованих на найкращій методиці в тому, що ці методики постійно змінюються, тому що краща методика це просто інший спосіб сказати «так, як усе зараз роблять». Часто так, як усі роблять, неправильно на цьому тижні й залишиться неправильним, коли вони оновлять методику на наступному тижні.

Тому існують науково-дослідні сертифікати, засновані на достовірних і повторюваних дослідженнях поводження людини й системи. Зрозуміло, наша головна організація, ISECOM, прямо попадає в сферу дослідницьких органів сертифікації. Від ISECOM або від іншої організації, шукайте засновані на навичках, аналітичних або прикладних знаннях (англ. «applied knowledge») посвідчення, які доведуть, що Ви вмієте зробити те, чому ви вчилися.

Семінари

Відвідування семінарів це відмінний спосіб почути докладну теорію й подивитися на свої навички в дії. Навіть семінари, присвячені певному продукту корисно відвідати, щоб побачити, як вони проводяться, доти, поки ви усвідомлюєте, що ця подія є маркетинговим кроком, і його реальне завдання полягає в продажі.

Ми були б недбалі, якби не згадали, що ми можемо доставити Hacker Highschool Seminars у майже будь-яке місце, і ми можемо розповісти кожний з доступних уроків. Семінари проводяться професійними хакерами, що розповідають студентам про злом і про те, як бути хакером, як погане, так і гарне. Ці семінари зосереджують погляд на тому, хто ж такі дійсні хакери, з досліджень в Hacker Profiling Project, спільного проекту з Організацією Об'єднаних Націй по вивченню хакерів і чому вони зламують. Після них ви зможете рухатися далі, відкриваючи для себе світлі сторони злому.

Одна з головних речей: ми можемо допомогти Вам знайти спосіб стати таким же допитливим і винахідливим як хакер. Хакери процвітають у тому, що вони роблять, тому що вони знають як само навчитися, виходять за рамки доступних уроків й опановують потрібними ним навичками, щоб йти далі.

Ви також можете попрохати, щоб ваші батьки й педагоги довідалися, як пристосувати й почати курс Hacker Highschool у вашій школі. Зв'яжіться з ISECOM для одержання додаткової інформації.

Подальше навчання

Тепер ви повинні практикуватися поки не освоїте дослідження. Чим краще ви зрозумієте це, тим більше й швидше ви будете знаходити інформацію, і швидше навчитеся. Але будьте обережні, і розвивайте критичний погляд. Не вся інформація правдива.

Не забувайте запитувати себе, навіщо комусь брехати? У те, щоб увічнити нечесний слух або в історії залучені гроші? І саме головне, що таке сфера (англ. "scope")?

Подібно всякому злому, дослідження містить у собі сферу. Це дійсно важливо, коли ви бачите статистику, подібно математиці, що використає відсотки, дроби й нерівності. Завжди перевіряйте, де має місце сфера і визнайте, що сфера повинна застосовуватися. Традиційне місце, де її можна розглянути – це злочинна або медична статистика, що охоплює невелику вибірку тільки в одній частині країни. Те, що зачіпає 10% з 200 учнів в одному місті, не означає, що в 10% усього населення країни та ж проблема. Так що читайте і знаходите інформацію з розумом. Виділення сфери інформації завжди приводить до більших розходжень!

Щоб допомогти Вам стати кращим дослідником, от деякі додаткові теми й терміни для вивчення:

Метапошук

Невидима мережа

Google злом

Як працюють пошукові системи

Загальнодоступна пошукова система

Словник хакерського сленгу (The Jargon File)

OSSTMM

Сертифікати 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