Hacker Highschool

SECURITY AWARENESS FOR TEENS



LECȚIA 1
A FI UN HACKER

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

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

ATENȚIE

Proiectul Hacker Highschool este un instrument de învățare și ca în folosirea oricărui instrument de învățare, există și pericole. Anumite lecții, dacă sunt folosite în mod abuziv, pot duce la vătămare corporală. Există de asemenea, pericole aditionale, acolo unde nu există suficientă cercetare referitoare la posibilele efecte ale emanațiilor din anumite tehnologii. Studenții care participă la aceste lecții, trebuie să fie supravegheați dar și încurajați să învețe, să încerce si să lucreze practic. Cu toate acestea, ISECOM nu își asumă responsabilitatea în cazul în care informația este întrebuințată în mod abuziv.

Următoarele lecții și registre de lucru sunt deschise și accesibile publicului, în următorii termeni si condiții ale ISECOM:

Toate lucrările folosite în Proiectul Hacker Highschool sunt prevăzute pentru a fi folosite în scopuri non-comerciale de către elevi de scoală primară, elevi de liceu primar si elevi de liceu dintr-o instituție publică, privată sau care fac parte dintr-o formă de învățământ de acasă. Aceste materiale nu pot fi copiate spre a fi puse la vânzare sub nici o formă. Furnizarea acestor materiale, a oricărei lecții, curs, training sau sesiune de tabără, pentru care se percep taxe, este strict interzisă fără o licență, inclusiv dacă este vorba de clase de colegiu, cursuri universitare, clase de scoli cu program de schimb de elevi, tabere de vară sau de calculatoare sau alte forme de învățământ asemănătoare. Pentru a cumpăra o licență, vă rugăm să vizitați secțiunea LICENȚĂ a paginii web HHS, pe care o puteți găsi aici: http://www.hackerhighschool.org/licensing.html.

Proiectul Hacker Highschool este un efort al unei comunități deschise, iar în cazul în care găsiți valoare în acest proiect, vă rugăm să ne oferiți suportul dumneavoastră prin achiziționarea unei licențe, oferirea unei donații sau a unei sponsorizări.

Table of Contents

Contribuitori

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

Traducere

Laurent Chrzanovski

ISECOM

Din Dragoste pentru Hacking / For the Love of Hacking

Introducere de Pete Herzog

Indiferent ce ați auzit referitor la hackeri, cel mai adevărat este că un lucru îl fac foarte, foarte bine: să caute. Hackerii sunt motivați, plini de resurse și creativi. Înțeleg foarte bine cum funcționează lucrurile, încât ajung la punctul în care știu cum să preia controlul lor și să le schimbe în altceva. Acest lucru le permite să regândească chiar si ideile mari, deoarece stiu cum să ajungă chiar la baza funcționalității lucrurilor. Mai mult decât atât, ei nu se tem să facă aceeasi greseală de două ori, deoarece sunt dirijați de un sentiment de curiozitate stiințifică, prin care vor să vadă dacă acea greseală are întotdeauna aceleasi rezultate. Acesta este motivul pentru care hackerii nu văd esecul ca o greseală sau o pierdere de timp, deoarece pentru ei, fiecare esec înseamnă ceva, iar acel ceva este un lucru nou care va fi învățat. Acestea toate sunt trăsături de care orice societate are nevoie pentru a putea progresa.

> *Mulți oameni care au fost numiți hackeri, în special de către mass-media, sau care au fost implicați în probleme de "hacking", nu erau de fapt hackeri.*

Un hacker este un fel de om de stiință care face experimente pe lucruri noi apărute, cu toate că i s-ar potrivi mai degrabă termenul de savant "nebun", deoarece spre deosebire de oamenii de stiință profesioniști, hackerii se aventurează direct, lăsându-se ghidați mai degrabă de un simțământ decât de o ipoteză oficială. Acest fapt nu este neapărat un lucru gresit. Multe lucruri interesante au fost proiectate sau inventate de către persoane care nu au urmat convențiile standard a ceea ce se stia sau se credea a fi adevărat la vremea aceea.

Matematicianul *Georg Cantor* a propus idei noi legate de infinit si teoria mulțimilor, idei care au cauzat indignare între mulți dintre colegii săi matematicieni, ajungând la punctul în care, unul din ei, a numit concepțiile sale o "boală gravă" care infectează matematica.

Nikola Tesla este alt om, care a fost considerat în zilele lui un "savant nebun", dar care avea mai multe cunostințe decât orice altă persoană, referitoare la modul în care se comporta electricitatea. El a fost cel care a proiectat primul motor care functiona pe baza de Curent Alternativ, dar a fost recunoscut mai ales pentru fenomenul numit efectul Tesla si bobina Tesla.

Mai apoi a fost *Ignaz Philipp Semmelweis*, care si-a dat seama ca doctorii trebuie sa se spele pe mâini între tratamentele efectuate pacienților pentru a împiedica răspândirea bolilor. Acesta se întreba dacă el purta vina faptului că bolile se transmiteau de la un pacient la altul, motiv pentru care a decis să încerce să se spele pe mâini între vizitele pe care le efectua la pacienții săi, lucru care bineînțeles a condus la dispariția transmisiei bolilor. Ideile sale luptau atât împotriva convențiilor stiințifice a ceea ce se cunostea atunci referitor la microbi (adică nimic), cât si a comodității doctorilor care simțeau că e prea mare bătaie de cap să se tot spele pe mâini.

Ceea ce credeți că știți referitor la hackeri este că acestia au posibilitatea de a intra în alte computere si de a prelua controlul asupra conturilor altor oameni. Pot să va citească email-urile fără ca voi să fiți constienți de acest lucru. Se pot uita prin webcam-

ul vostru fără permisiunea voastră si pot să vă observe si să vă asculte în presupusa intimitate a propriei voastre locuințe. Acest fapt nu este eronat.

Anumiți hackeri văd în securitatea unei rețele doar o altă provocare, drept urmare, se joacă cu modalități prin care încearcă să păcălească sistemul, însă în realitate ei încearcă să fie mai destepți decât cei care au instalat sau proiectat rețeaua. Acestia încearcă să descopere cât mai multe informații referitoare la rețea, cum ar fi locul de unde aceasta îsi primeste instrucțiunile, regulile pe care le foloseste, modul în care interacționează cu sistemele de operare, celelalte sisteme din jurul ei, utilizatorii care au acces la ea si administratorii care o administrează. Mai apoi se folosesc de acele informații pentru a încerca diverse metode de a obține ceea ce doresc. Acest tip de hacking poate fi de un foarte mare folos pentru întrega lume, în sensul în care putem să înțelegem cum să fim mai în siguranță si cum sa cosntruim o tehnologie si mai buna.

Din păcate însă, uneori hacking-ul este făcut de către criminali, iar ceea ce vor ei este ilegal, invaziv si distructiv. Tocmai acestia sunt hackerii despre care auziți de obicei la știri.

Un hacker nu este cineva care publică informații referitoare la contul cuiva atunci când acea persoană lasă deschisă din greseală o pagină de socializare sau care face **shoulder-surfing** la parole, urmând ca mai apoi să se logheze în contul lor. Acesta nu este hacking. De asemenea, un hacker nu este cineva care descarcă un instrument de tip **script kiddie** pentru a intra cu forța în contul de email al unei anumite persoane. Aceia nu sunt hackeri; aceia sunt doar niste hoți si vandali.

Hacking-ul este cercetare. Ai încercat vreodată ceva iar si iar în diferite moduri pentru a obține ceea ce doreai? Ai încercat vreodată să desfaci o masinărie sau un device, pentru a observa modul în care funcționează, pentru a cercetare care sunt componentele, urmând ca mai apoi să faci modificări pentru a vedea dacă funcționează diferit? Acesta este hacking-ul. Faci hacking de fiecare dată când examinezi cu atenție modul în care un lucru funcționează cu adevărat, pentru ca mai apoi să manipulezi acel lucru să facă ceea ce doresti tu.

Întâmplarea face ca datorită modului în care este proiectat internetul si datorită numărului imens de aplicații, sisteme, device-uri si procese diferite, tocmai acesta să fie cel mai probabil loc în care să găsim hackeri. Am putea să afirmăm că internetul a fost construit de către hackeri si tocmai datorită acestui fapt, să constituie cel mai bun loc de joacă pentru hackeri. Dar nu este singurul loc. Putem să găsim hackeri buni aproape în orice câmp de muncă si industrie si toți au un lucru in comun: faptul că își dedică timp învățând cum funcționează lucrurile, în asa fel încât să le facă să funcționeze în alte moduri noi. Acestia nu au privit în acelasi mod un lucru anume, asa cum au facut cei care l-au proiectat, ci au văzut în schimb, un potențial mai mare sau mai bun pentru acel lucru si drept urmare, au hackuit acel lucru în ceva nou.

Nu te gândi că poți fi un hacker excepțional. Deoarece doar prin a face hack-uri bune si cu multă modestie, poți să fii la rândul tău un hacker de excepție.

Hacking-ul în sinea lui nu este ilegal. Cel puțin nu mai mult decât aruncatul unei pietre. Totul se reduce la intenție. Dacă arunci o piatră si intenția ta este aceea de a vătăma

pe cineva, aceea este o crimă. Dacă nu intenționezi să rănești pe cineva, însă cineva totusi este rănit în final, chiar dacă nu este o crimă în sinea ei, totusi esti responsabil pentru acțiunile tale si va trebui să plătesti daunele. Un proiect ISECOM numit **Hacker Profiling Project**, a descoperit că cele mai multe prejudicii datorate hacking-ului, provin de la hackeri tineri si fără experiență, care provoacă din greseală daune proprietăților altora. Acest lucru este asemănător cu aruncatul pietrelor în stradă de dragul distracției, urmând ca în cadrul acestui proces să fie îndoite caroseriile masinilor sau să fie sparte geamurile ferestrelor. Poate că paguba nu este făcută în mod intenționat, dar trebuie să te astepți să fii făcut responsabil si să plătesti pentru ea. Astfel, trebuie să fiți cu luare-aminte atunci când faceți hacking cu proprietățile altora. Rămâneți la stadiul de a face hacking cu propriile voastre lucruri.

Poate fi ilegal să faci hacking la ceva ce ai cumpărat si deții. Sunt hackeri care au fost pedepsiți pentru că si-au hackuit propriile device-uri si computere. Există hackeri care au hackuit programe, muzică si filme pe care ei le-au cumpărat – si au fost judecați pentru acest lucru. Mai exact, nu ai voie în mod legal să hackuiesti un software pe care l-ai cumpărat, chiar dacă este doar pentru a verifica dacă este suficient de sigur pentru a fi rulat pe propriul computer. Acest lucru se poate datora faptului că ceea ce ați cumpărat poate avea un contract sau un **End User License Agreement (EULA)**, care precizează că nu aveți voie să faceți acest lucru. Mai apoi, sunteți de acord cu acest lucru atunci când deschideți sau instalați produsul respectiv, chiar dacă nu puteți să citiți sau să fiți constienți de acest fapt, decât după ce ați deschis sau instalat produsul. Țineți cont de acest fapt atunci când vă exersați abilitățile de hacking asupra lucrurilor pe care le-ați cumpărat, în intimitatea propriei voastre locuințe.

De ce să fii un Hacker? / Why Be a Hacker?

Gândiți-vă la modul în care oamenii de stiință au trasat harta genomului uman: au folosit o metodă dezvoltată pentru decodificarea parolelor. De obicei, parolele sunt stocate într-o formă criptată, pentru a fi mai greu de furat. Hierarchical shotgun **brute-forcing** este o metodă pentru decriptarea parolelor prin **spargerea** formelor lor criptate. Această metodă rupe **hasura** criptată a parolei, descoperă câteva caractere dintr-o dată, iar mai apoi le leagă la loc. Cercetătorii genomului au adaptat aceeasi tehnică pentru a trasa harta tuturor celor 3.3 miliarde de perechi de bază ale genomului uman.

Hackingul si-a făcut apariția în bucătării atunci când bucătarii au folosit nitrogenul lichid ca si agent de răcire pentru a crea inghețata perfectă sau atunci când au hackuit mâncarea pentru a face rosii prăjite cu sos de cartofi pe post de ketchup sau în momentul în care este nevoie să pregătească ceva pentru care nu au echipamentul necesar...

Chimistii hackuiesc elementele si compusii acestora de secole. Prin natura lor, moleculele sunt delicate atunci când vine vorba de modul în care se comportă în diferite medii (vreme caldă, vreme rece, pe munți sau în adâncul oceanelor) si astfel chimistii trebuie să înțeleagă în mod profund proprietățile chimicalelor cu care lucrează, în asa fel încât să aibă posibilitatea de a obține acel element de care au nevoie. Nicăieri nu este acest fapt mai evidențiat ca în invenția produselor farmaceutice noi, unde sute de plante dintr-o regiune sunt studiate pentru proprietățile chimice care se găsesc în rădăcini si în fructe si care sunt extrase si combinate cu altele pentru a crea medicamente noi. Mai apoi,

crecetătorii încearcă din nou si din nou, câteodată pe o perioadă de câțiva ani, pentru a realiza combinațiile perfecte si pentru a determina produsul să facă ceea ce doresc ei.

Hacking-ul este folosit în afaceri pentru a înțelege o piață sau comportamentul de cumpărător pentru diferite tipuri de consumatori. Ei fac cercetări aprofundate legate de forțele care dirijează domeniul de afaceri de care sunt interesați, iar mai apoi încearcă să-l schimbe sau să-l influențeze, ca să-l determine să facă ceea ce doresc ei. Câteodată hackuiesc produsul, iar câteodată vă hackuiesc pe voi (prin intermediul publicității si a **priming-ului**, un subiect cu care o să lucrați la lecția de Social Engineering).

Hackingul a început să devină de asemenea, o parte critică a războiului. Soldații foarte înzestrați sunt creativi si plini de resurse în atingerea scopurilor lor, asemenea lor sunt si hackerii. Spărgătorii de coduri, analistii de informații si ofițerii de teren se folosesc, de ceea ce sunt practic, abilități de hacking, pentru a-si da seama ce anume deține inamicul, ce anume face si cum să profite de orice slăbiciune din echipamentul lui. În timp ce din ce în ce mai multe țări se bazează pe computere si rețele, utilizarea hacking-ului în atacuri si protecții cibernetice, a devenit o parte valoroasă a forțelor armate si a operațiunilor de inteligență ale unei națiuni. Agențiile naționale si internaționale de securitate participă chiar si la convenții de hacking pentru a recruta hackeri!

Motivația reală de a fi hacker este cea a puterii. Poți să faci lucruri foarte interesante atunci când deții abilități foarte bune de hacking. Orice informație detaliată îți oferă o putere imensă. Dacă stii cum funcționează un anumit lucru în asa fel încât să-l poți controla, atunci să stii că deții o forță de temut. Mai mult decât atât, deții puterea de a te apăra atât pe tine cât si pe cei la care ții.

Pe măsură ce se formează relații, iar oamenii își găsesc de lucru si banii sunt obținuți pe seama internetului, din ce în ce mai multe vieți personale sunt online. Informația poate fi valoroasă – sau de temut – iar hackerii se pot apăra mai bine decât oricine. Acestia pot verifica ce se intâmplă cu datele lor. Se pot asigura că oferă doar ce informații doresc în acelasi timp rămânând mai în siguranță si mai ascunsi. Acesta este un avantaj competitiv enorm la scoală, la servici si în viață, deoarece până si cea mai mică percepție negativă va fi folosită împotriva voastră în cele din urmă. Puteți să fiți siguri de asta.

Hackuieste fiecare lucru dar să nu faci rău.

Cum să faci Hacking / How to Hack

Să vă spunem cum să faceți hacking este ca si cum v-am explica cum să faceți un flip pe spate pe o bârnă: indiferent cât de detaliată este explicația, nu o să resusiți singuri de prima dată. Trebuie să vă dezvoltați abilitățile, simțirea si intuiția prin practică dacă nu vreți să dați gres. Există totusi anumite lucruri pe care vi le putem împărtăsi pentru a vă ajuta pe parcurs si pentru a vă încuraja să exersați în continuare.

În primul rând, ar trebui să stiți câteva secrete mici referitoare la modul în care funcționează de fapt hacking-ul. Vom prelua aceste informații de la **OSSTMM** (www.osstmm.org). Hackerii pronunță fonetic această abreviere "aw-stem." OSSTMM-ul se referă la **Open Source Security Testing Methodology Manual** si chiar dacă conține instrucțiuni asemănătoare folosirii unui DVD palyer, acesta reprezintă principalul document folosit de către hackeri profesionisti pentru a planifica si executa atacurile si defensivele proprii. În profunzimea acelui manual se regăsesc niste comori adevărate care vă vor deschide ochii.

Două Metode prin care să Obțineți ceea ce Doriți / Two Ways to Get What You Want

Spre exemplu, ar trebui să stiți că există doar două metode prin care puteți să obțineți orice: obțineți acel lucru prin forțe proprii sau vă folosiți de altcineva să obțineți acel lucru, iar mai apoi îl primiți de la acea persoană. Aceasta înseamnă că tot ceea ce se obține în lume presupune **interacțiuni** între persoana si lucrul în cauză. Pare de la sine înțeles, nu? Totusi gândiți-vă la acest lucru. Asta ar însemna ca toate mecanismele de protecție să încerce să oprească pe cineva să interacționeze cu acel lucru pe care îl protejează. În cazul în care nu puteți să încuiați totul într-un seif imens, nu aveți cum să faceți acest lucru. Magazinele trebuie să pună pe rafturi marfă în asa fel încât cumpărătorii să o poată atinge. Afacerile trebuie să trimită informații prin aplicații de email, care se leagă de servere de email si care la rândul lor trimit mesajele altor servere de email.

Toate acestea sunt interacțiuni. O parte din aceste interacțiuni se fac între oameni si obiecte între care există deja o familiarizare. Numim aceste interacțiuni **Trusts**. Atunci când interacțiunile au loc între persoane sau sisteme necunoscute, le numim **Accesses**. Vă puteți folosi de un acces pentru a obține personal ceea ce doriți, sau puteți să păcăliți pe cineva care deține un trust cu ținta în cauză, pentru a obține ceea ce doriți, iar mai apoi să vi-l ofere. Dacă stați să vă gândiți un moment la acest lucru, asta ar însemna ca securitatea să protejeze ceva anume atât de cei pe care nu îi cunoaste, cât si de cei pe care îi cunoaste si în care are încredere.

Exerciții

1.1 Ce tip de interacțiune foloseste un motor de căutare? Gândiți-vă cu atenție: oferă cineva Access? Oferă cineva un Trust?

1.2 Dați un exemplu simplu referitor la utilizarea unui Access si a unui Trust pentru a duce o bicicletă blocată la un stand de biciclete.

1.3 Dați un exemplu simplu despre cum puteți să vă folosiți de un Access si de un Trust pentru a vă loga în contul de web-mail al altei persoane.

Hrană pentru Minte: Spionaj / Feed Your Head: Espionage

Atunci când se foloseste hacking-ul împotriva unui guvern străin pentru a comite acte criminale de intrare prin efracție, de violare a proprietății, de furt si de distrugere, pentru a obține avantajul în ceea ce priveste informații de natură politică sau militară, se numeste **spionaj**. Însă atunci când hacking-ul este înfăptuit de către o organizație străină împotriva altei organizații dintr-o altă țară, pentru a obține un avantaj în afaceri, acest lucru se numeste **spionaj economic.**

Atunci când se foloseste hacking-ul în vedrea obținerii de informații personale referitoare la anumiți indivizi, pentru a-i stânjeni în mod public, se numeste **DoXing**. Dacă se caută informații în vederea planificării unui atac asupra unei persoane sau a unei companii, însă fără a folosi metode de natură criminală, se numeste **document grinding** sau **OSInt (Open Source Intelligence)**.

Atunci când se foloseste hacking-ul pentru a înțelege modul în care funcționează rețeaua, sistemele, aplicațiile si dispozitivele unei companii, care este ținta unui atac, fără a intra prin efracție sau fără a viola spațiul sistemelor în cauză, se numeste **network surveying**.

Atunci când se foloseste hacking-ul pentru a înțelege mai bine un competitor, fără a încălca vreo lege (cu toate că ceea ce fac ei poate fi considerată o răutate sau o nerusinare), se numeste **competitive intelligence**.

Probabil că sunteți curiosi să știți care anume metode răutăcioase si deranjante sunt încă legale. Gândiți-vă cum ar fi să provocați stress si îngrijorare cuiva, pentru a obține informații de la acea persoană. Atâta timp cât nu omorâți acea persoană, a-i spune minciuni este complet legal (cu toate că există legi împotriva provocării de panică publică cum ar fi strigarea de "Foc!" într-un cinema aglomerat, când de fapt nu există asa ceva).

Să zicem că hacker-ul doreste să stie locația nouă în care o companie urmează să-si stabilească noua fabrică. Acestia se folosesc de document grinding pentru a afla care sunt persoanele care dețin acea putere de decizie. Apoi hacker-ul sună la biroul acelor persoane pentru a afla prin ce orase au umblat si poate chiar si ce fabrici au vizitat. Desigur toate acestea reprezintă informații private pentru companie si nimeni nu le va oferi benevol fără a ridica semnale de alarmă. Asadar, hacker-ul trebuie să-i păcălească pentru a primi acea informație de la ei. Nu este greu să ne imaginăm scenariul.

> Hacker: Bună ziua, sunt Dr. Jones, si vă sun de la scoală în legătură cu fiica dumneavoastră Nancy.
>
> Ținta: Serios? Ce a făcut?
>
> Hacker: Se pare că îi curge foarte tare sânge din nas si nu putem opri sângerarea. As vrea să vă întreb dacă a fost expusă la chimicale, cum ar fi cele folosite în fabricație sau ceva asemănător. Aceste simptome sunt rare dar se manifestă mai ales la persoane care au fost expuse la acest gen de chimicale. Puteți să-mi dați ceva detalii referitor la aceasta?
>
> Ținta: (spune tot)

Această metodă nu este ilegală dar în cele mai multe locuri cauzează stress nedorit. Ca să nu mai vorbim că este de-a dreptul răutăcios să provoci o asemenea grijă unui părinte.

A face Hacking pentru a Prelua Controlul asupra Propriei Lumi / Hacking to Take Over Your World

Hacking-ul nu se referă doar la interacțiuni. Cunoașteți acest lucru. Unii oameni spun că politica presupune interacțiuni. Poate. Dar probabil că si voi ați crezut că hacking-ul se referă la a sparge bariera de securitate. Câteodată asa este. Dar de fapt se referă la a prelua controlul asupra unui anumit lucru sau pur si simplu să-l schimbi. Înțelegerea interacțiunilor si a ceea ce însemnă ele în lumea reală, folosirea termenilor de bază despre care am discutat, toate acestea sunt folositoare atunci când încercați să vă infiltrați, să descoperiți sau chiar să inventați. De ce ați face acest lucru? Tocmai pentru a avea libertatea de a face ca ceva ce dețineți, să facă ceea ce doriți. Si pentru a-i împiedica pe alții să modifice ceva ce dețineți din cauza a ceea ce unii numesc securitate (însă noi nu suntem ca acei oameni).

Uneori s-ar putea să cumpărați ceva iar compania de la care ați cumpărat acel lucru s-ar putea să încerce în mod forțat sau ascuns să se asigure că nu puteți să modificați sau să schimbați acel produs în afara regulilor lor. Voi puteți să fiți de acord cu acest lucru, în măsura în care acceptați ca atunci când îl stricați, ei să nu îl poată repara sau înlocui. Asadar, a face hacking asupra unui lucru pe care îl deții, înseamnă mai mult decât posesia lui si îl face irevocabil si de netăgăduit al tău. Chiar dacă acest lucru pare înfricosător pentru unii, totusi are cu siguranță avantajele sale. Mai ales dacă vrei să-i ții pe alții departe de lucrurile tale.

Pentru foarte mulți oameni (putem să punem mai mulți de "foarte" pentru a sublinia că ne referim la "prea mulți"), securitatea constă în a pune un produs într-un loc securizat printr-un lacăt sau o alarmă sau un firewall sau orice altceva care teoretic păstrează acel lucru în siguranță. Însă câteodată acele produse nu funcționează asa de bine precum ar trebui, sau vin cu propriile probleme care nu fac decât să mărească **Suprafața de Atac (Attack Surface)**, pe când un produs făcut pentru securitate ar trebui să o diminueze. (Suprafața de Atac reprezintă toate căile, toate interacțiunile, care permit ca ceva sau cineva să fie atacat.) Mai departe mult noroc în îmbunătățirea acelui produs într-o lume bazată pe foarte mult marketing, pe plăți făcute pe loc, pe crowd-sourcing si pe ideologii de tip "ai cumpărat produsul asa cum este si te descurci singur mai departe". Tocmai din acest motiv faci hacking la securitatea ta. Trebuie să analizezi produsul si să-ți dai seama unde anume cedează si cum să-l modifici în asa fel încât să funcționeze mai bine. Mai apoi, s-ar putea să fie nevoie sa-l hackuiesti mai mult pentru a împiedica compania de la care l-ai cumpărat să-l schimbe înapoi cum era din fabrică!

Asadar, atunci când vă gândiți la hacking ca la o spargere a barierei de securitate, să vă aduceți aminte că aceasta reprezintă doar unul din multele domenii pentru care este folositor, deoarece dacă nu s-ar putea face acest lucru, atunci s-ar putea să trebuiască să renunțați la niste libertăți si intimitate, la care să nu vreți de fapt să renunțați. (Înțelegem că poate nu vă pasă în acest moment despre anumite lucruri pe care le faceți, spuneți sau postați, însă Internetul are o memorie foarte bună si devine din ce în ce mai bun în a-i ajuta pe alții să țină minte acele amintiri despre tine. Ceea ce se petrece pe internet, rămâne pe internet. Asadar, să aveți în vedere acest lucru pentru voi cei care veți fi în viitor, chiar dacă vouă celor de azi nu vă pasă.)

Acum că ați înțeles ideea referitoare la interacțiuni, haideți să le aprofundăm puțin. Cunoașteți interacțiunile de bază cum ar fi Acces si Trust, dar ați auzit de **Visibility (Vizibilitate)**? Aceasta este al treilea tip de interacțiune. Este la fel de puternic ca si

celelalte două. În limbajul de poliție, este cunoscut în mod simplu ca *oportunitate* dar în hacking se referă la a sti dacă există sau nu ceva cu care să interacționezi. Acest tip de interacțiune aduce cu sine mai multe tehnici de securitate cum ar fi decepția, iluzia si camuflajul, precum si metode cu totul noi de hacking folosite în evitarea si ocolirea măsurilor de securitate cum ar fi decepția, iluzia si camuflajul!

Atunci când faimosul jefuitor de bănci Jesse James a fost întrebat de ce a jefuit bănci, acesta a răspuns ca acolo sunt banii. Ceea ce a vrut de fapt să spună a fost că prin intermediul Vizibilității el stia că băncile aveau bani, în timp ce alte locuri pe care putea să le jefuiască, nu aveau. Băncile au Vizibilitate: oamenii stiu ce bunuri dețin ele. Însă nu totul are Vizibilitate. De fapt, Privacy (Intimitatea) este opusul Vizbilității si este o metodă puternică pentru a evita să devii o țintă. Indiferent dacă ne referim la străzi rău famate, în junglă sau pe internet, să păstrezi o **Expunere (Exposure)** scăzută si să eviți Vizibilitatea, este în sinea ei o metodă prin care te feresti să fii atacat în primul rând.

Exerciții

1.4 Internetul este atât de cunoscut pentru crearea de mituri si pentru perpetuarea povestilor false încât este greu să-ți dai seama care este o informație reală si care este doar o înselăciune. Asadar, dacă vrei să înveți să fii un hacker bun, obisnuieste-te să-ți verifici informațiile si să cauți adevărul. Tocmai din acest motiv va trebui să căutați dacă Jesse James chiar a spus acel lucru. Si să nu vă mulțumiți doar cu prima pagină web pe care o găsiți, trebuie să aprofundați un pic.

Acum că v-ați deprins cu căutatul informațiilor, găsiți adevărul legat de următoarele lucruri obisnuite:

1.5 În limba Inuită din care provine cuvântul igloo, ce înseamnă cu adevărat? Ce tip de interacțiuni ați folosit acum pentru a afla?

1.6 Foarte mulți părinți sunt rapizi în a trage cocluzia că zahărul face copiii mici să fie hiperactivi, dar oare este adevărat? Ce tip de interacțiuni se intâmplă cu adevărat în burțile lor mici atunci când copiii mănâncă foarte multe dulciuri si produse cu zahăr ca să-i facă să se prostească si să fie energici?

1.7 S-ar putea să fi auzit că zahărul cauzează cavități (carii) în dinții vostri dar care este acțiunea reală care are loc – ce anume le cauzează cu adevărat cariile? Este într-adevăr zahărul sau nu? Primiți puncte bonus dacă puteți spune ce este periajul ca interacțiune pentru combaterea adevăratei cauze si pentru aflarea a cel puțin un nume al uneia din chimicalele care sunt folosite pentru cauza problemei (*indiciu: nu este fluor-ul*).

Procesul în Patru Puncte / The Four Point Process

Atunci când combini cele trei tipuri de interacțiuni, obții **Porozitatea (Porosity)**, care reprezintă baza unei Suprafețe de Atac. Si asa cum sugerează cuvântul, se referă la porii sau la "găurile" din orice defensivă pe care o deții, pentru ca orice interacțiune să aibă loc (acelasi lucru fiind valabil pentru orice interacțiune necunoscută sau inutilă care are loc). Spre exemplu, un magazin tot are nevoie să pună produse pe rafturi, pentru ca oamenii să le poată atinge, să le pună într-un cos de cumpărături si să le cumpere. Acestea sunt interacțiunile de care au nevoie pentru a vinde lucruri. Însă s-ar putea să nu fie constienti de angajații care fură lucruri pe la rampa de încărcare, care este o interacțiune pe care nu o doresc.

Porozitatea este ceva despre care trebuie să vă informați pentru a vă proteja si pentru a ataca o țintă. Însă nu este suficient să analizezi ceva pentru a stii să-l hackuiesti. Pentru a face acest lucru, trebuie să cunoasteți ceva mai profund referitor la cele trei tipuri de interacțiuni pe care le-ați învățat. Acesta este încă un mic secret de la OSSTMM si se numeste **Four Point Process (FPP)**. Acesta subliniază patru metode prin care aceste metode sunt folosite pentru a analiza ceva cât mai profund posibil, iar atunci când zicem analiză, ne referim la a ne juca cu acel lucru în asa fel încât să-l observăm si să vedem ce se întâmplă.

Procesul Echo / The Echo Process

Crestem descoperind si învățând lucruri prin interacționarea cu acestea în mod direct. Copiii mici înghiontesc cu un băț o veveriță moartă pentru a vedea dacă într-adevăr este moartă. Acesta se numeste **procesul echo (echo process)**. Este cea mai bazică si cea mai simplă formă de analiză. Este ca si cum țipi într-o pesteră si asculti să vină răspunsul. Procesul echo presupune implementarea anumitor tipuri de Acces asupra unei ținte iar mai apoi monitorizarea reacțiilor sale pentru a ne putea da seama în ce moduri putem reacționa cu aceasta. Procesul echo este o verificare de tip cauză-si-efect.

Aceasta este o metodă ciudată de a verifica ceva, deoarece cu toate că presupune un test foarte rapid, totusi nu este foarte precisă. Spre exemplu, atunci când folosim procesul echo în testarea securității, o țintă care nu răspunde este considerată securizată. Aceasta este la fel ca atunci când nu avem Vizibilitate. Totusi stim că dacă un lucru nu răspunde unui tip anume de interacțiune, nu înseamnă că acel lucru este "securizat." Dacă acest lucru ar fi adevărat, atunci opossumii nu ar fi omorîți niciodată de către alte animale atunci când s-ar preface că sunt morți si toată lumea ar fi în siguranță față de atacurile ursilor doar prin lesinul provocat de frică. Totusi nu este deloc adevărat. Evitarea Vizibilității s-ar putea să vă ajute să supraviețuiți anumitor tipuri de interacțiuni dar cu siguranță nu la toate.

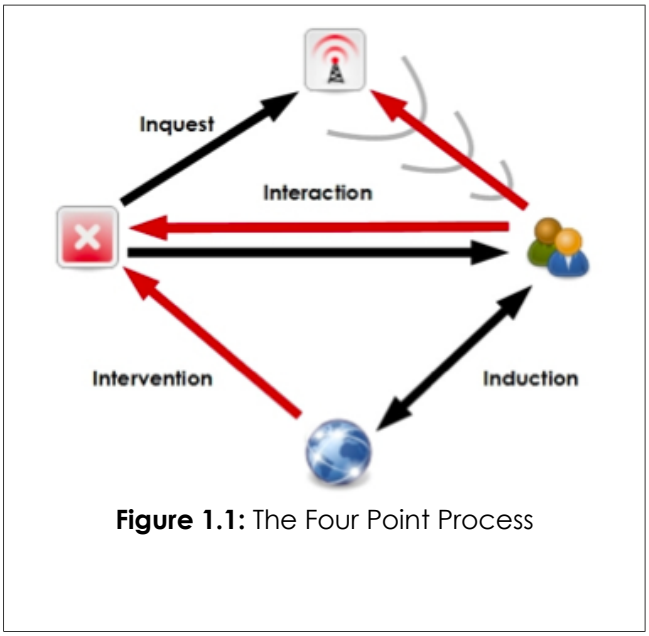

Figure 1.1: The Four Point Process

Din păcate însă, majoritatea modalităților prin care oamenii verifică lucrurile din viața lor de zi cu zi, se referă strict la procesul echo. Există foarte multă informație care se pierde în acest tip de analiză uni-dimensională încât ar trebui să fim mulțumiți de faptul că instituțiile de sănătate au evoluat dincolo de metoda de diagnoză "Doare dacă apăs aici?." Dacă spitalele ar folosi doar procesul echo pentru a determina starea de sănătate a unei persoane, atunci nu ar mai ajuta cu adevărat pe nimeni. Pe de altă parte însă, perioadele de asteptare din săli, ar scădea foarte mult. Tocmai din acest motiv, unii doctori, majoritatea oamenilor de stiință si în special hackerii folosesc Four Point Process pentru a se asigura că nu le scapă nimic.

Four Point Process te determină să privesti interacțiunile în modurile următoare:

1. **Induction**: Ce anume putem să spunem referitor la țintă din perspectiva mediului său înconjurător? Cum se comportă în acel mediu? Dacă ținta nu este influențată de propriul mediu, atunci si acest lucru este interesant.
2. **Inquest**: Ce semnale (emanații) emite ținta? Investigați orice urme sau indicatori ale acelor emanații. Un sistem sau un proces în general lasă în urmă o semnătură de interacțiuni cu mediul său.
3. **Interaction**: Ce se întâmplă când înghiontesti acel lucru? În acest punct este nevoie de teste echo, inclusiv interacțiuni asteptate si neasteptate cu ținta, pentru a provoca răspunsuri.
4. **Intervention**: Cât de mult se va îndoi înainte de a se rupe? Interferează cu resursele de care are nevoie ținta, cum ar fi curentul, sau joacă-te cu interacțiunile sale cu alte sisteme pentru a înțelege extremele până la care poate continua să opereze.

Să privim înapoi la exemplul nostru cu spitalul... cele patru stagii ale FPP ar arăta ceva de genul acesta:

1. Funcția **interaction** este procesul echo prin care doctorii înghiontesc pacienții, vorbesc cu ei si le testează reflexele de la coate si genunchi si folosesc alte instrumente ale metodei "Doare dacă apăs aici?."
2. **Inquest** reprezintă citirea **emanațiilor** pacientului, cum ar fi pulsul, presiunea arterială si undele creierului.
3. **Intervention** reprezintă schimbarea sau agitarea homeostaziei pacientului, a comportamentului, a rutinei, sau a nivelului de confort pentru a vedea ce se întâmplă.
4. Si în final **induction**, care reprezintă examinarea mediului, a locurilor pe care pacientul le-a vizitat înainte de a se îmbolnăvi si modul în care acestea au putut afecta pacientul, cum ar fi ceva ce acestia au atins, au ingerat sau inspirat.

Exercițiu

1.8 Asa cum puteți observa, Four Point Process vă permite să investigați interacțiunile mai în profunzime. Acum puteți să încercați si voi. Explicați cum ați folosi Four Point Process pentru a determina dacă un ceas funcționează – iar mai apoi dacă funcționează bine prin păstrarea orei corecte.

Ce anume să Hackuiesti / What to Hack

Atunci când hackuiesti orice, trebuie să stabilesti niste reguli de bază. Ai nevoie de limbajul si de conceptele respective ca să cunosti ce anume hackuiesti de fapt. **Scope** este un cuvânt pe care îl folosim pentru a descrie mediul total posibil de operare, care la rândul său reprezintă fiecare interacțiune pe care o are respectivul obiect pe care vrei să-l hackuiesti.

Hrană pentru Minte: Clase si Canale / Feed Your Head: Classes and Channels

În terminologia profesională (care este de asemenea folositoare pentru hackeri), Scope este format din până la trei Clase care se subdivid în cinci **Canale**:

Clasa	Canalul
Physical Security (PHYSSEC)	Uman
	Fizic
Spectrum Security (SPECSEC)	Wireless
Communications Security (COMSEC)	Telecomunicații
	Rețele de Date

Clasele nu sunt ceva de care ar trebui să vă fie frică. Ele sunt etichetele oficiale folosite actual în industria securității, în guvern si în armată. Calsele definesc un domeniu de studiu, investigație sau de operare. Deci dacă cumva căutați mai multă informație referitoare la orice subiect, este bine de stiut cum este numită de către profesionisti.

Canalele reprezintă termenii obisnuiți pentru metodele în care interacționați cu bunurile de interes. Nu este neobisnuit să hackuiesti un dispozitiv prin folosirea Four Point Process la fiecare Canal. Într-adevăr pare mult de lucru, însă gândiți-vă cât de interesant este atunci când descoperiți o metodă de a-l face să funcționeze într-un mod care nu este descris în nici un manual, sau chiar mai mult decât atât, să descoperiți un mod de funcționare care e necunoscut chiar si producătorilor!

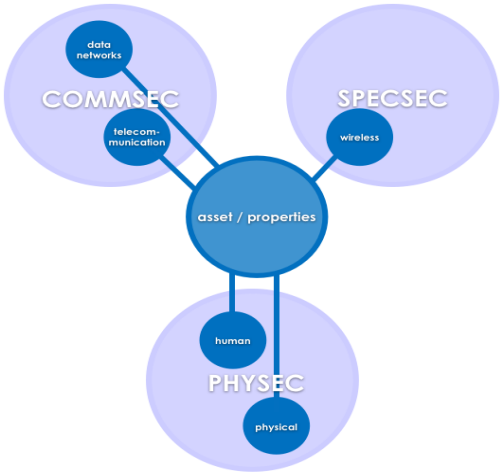

Figure 1.2: Scope

Un **Asset (Bun esențial)** poate fi orice lucru care reprezintă o valoare pentru proprietarul lui. Poate fi un bun fizic ca de exemplu aur, oameni, planuri de clădiri, laptop-uri, frecvența de 900 MHz folosită de telefonia mobilă si banii; sau o proprietate intelectuală ca de exemplu datele personale, o relație, un brand, datele unei afaceri, parolele si ceva comunicat prin intermediul semnalului de 900 MHz folosit de telefonia mobilă.

Dependencies sunt lucrurile care stau dincolo de bunurile proprietarului si independența acestuia. De exemplu, nu mulți dintre deținătorii de calculatoare personale își generează propria energie electrică necesară folosirii acestora. Chiar dacă sunt sanse mici ca cineva să-ți taie curentul electric, tot ține de scopul tău.

Scopul securității este Separarea dintre un bun si dependețele sale si orice amenințare care poate apărea asupra lor.

Spunem că **securitatea este o unealtă de** separare. Sunt patru căi prin care putem crea această separare:

- Mutarea bunului pentru a crea o barieră între el si posibila amenințare.
- Punerea amenințării într-o stare inofensivă.
- Distrugerea amenințării.
- Distrugerea bunului. (Nu este recomandat!)

Când spargem un cod ne uităm după locurile unde este posibilă si nu este posibilă interacțiunea cu ținta. Gândeste-te la usile dintr-o clădire. Unele sunt acolo pentru angajați; iar altele sunt pentru clienți. Pe unele dintre ele va fi nevoie să le folosesti ca să scapi în caz de incendiu. Altele nu vor fi folosite niciodată.

Cu toate acestea, fiecare ușă este un punct de trecere, unul care ajută la efectuarea operațiunilor necesare dar si pentru unele nedorite cum ar fi furtul. Când intrăm în peisaj ca si hackeri, la început nu cunoastem motivele pentru care există toate aceste puncte de trecere si deci le analizăm prin intermediul Four Point Process.

Luăm ca exemplu un om care vrea să fie protejat permanent de fulgere. Singurul mod în care se poate face acest lucru (cât timp ne aflăm pe pământ) este ca omul să intre într-un munte, unde va fi complet imposibil pentru fulger să ajungă la el prin toată acea suprafață formată din pământ si piatră. Presupunând că niciodată nu va avea nevoie să iasă afară, din nou putem spune că este în siguranță 100%. Dar dacă începem să facem găuri în munte, cu fiecare gaură făcută, fulgerul va mai avea o cale de acces în plus. OSSTMM face diferență dintre a fi **protejat** de fulger si a fi în **siguranță** față de el. Mai simplu spus cu cât sunt mai multe porozități, cu atât este mai usor pentru un hacker să modifice sau să controleze ce doreste.

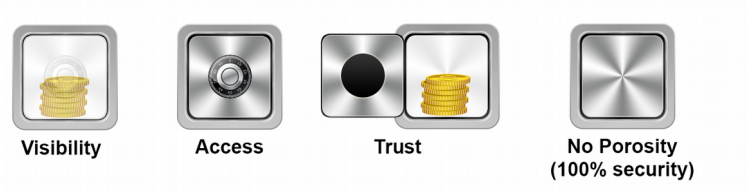

Figure 1.3: Porosity

Hrană pentru Minte: Porosity / Feed Your Head: Porosity

Mai jos sunt prezentate niste exemple în care se arată cum pot fi localizați, clasificați si determinați porii în timpul procesului de hacking.

Termen	Definiție
Visibility	La investigarea unei crime, poliția caută mijloacele, motivele si oportunitățile. Dacă un bun esențial este vizibil, atunci poate fi atacat, dar dacă nu este vizibil, nu poate fi luat ca țintă, dar ar putea fi descoperit. Unii profesionisti în domeniul securității ar vrea să spună că **obfuscation (mascarea)** reprezintă un nivel scăzut de securitate deoarece nu protejează nimic, ci doar ascunde. Dar acest lucru nu este neapărat negativ mai ales că nu întotdeauna ai nevoie de o securitate foarte strictă. În susținerea acestui fapt **OSSTMM** ne oferă acest mic secret: "Securitatea nu trebuie să fie permanentă, ci să țină mai mult decât orice altceva despre care să se creadă că nu mai există."
Access	Accesul reprezintă numărul de locuri diferite prin care se poate face comunicarea în afara scopului predefinit. Referindu-ne la o clădire, aceste lucruri pot fi reprezentate de usi si geamuri, iar referindu-ne la un server legat la internet, aceste lucruri pot fi reprezentate de numărul de porturi de rețea deschise sau de servicii disponibile pe acel calculator.
Trust	Încrederea se manifestă atunci când o entitate acceptă comunicarea fără interdicție cu o altă entitate într-un scop comun. De aceea când mama ta vrea să te îmbrățiseze, nu îi ceri numărul de înregistrare. De asemenea, nu o suspectezi că ți-a otrăvit mâncarea. Înveți să ai încredere în lucrurile din cercul tău. Si dacă într-o zi mama ta va fi răpită de o rasă extraterestră si înlocuită (ca în **Invasion of the Body Snatchers**) si îți va otrăvi mâncarea, o vei mânca fără să ai nici o suspiciune. De aceea încredrea e o gaură de securitate, dar totodată si element înlocuitor pentru autentificare sau modul în care putem valida că cineva este cine credem noi că este. Încrderea este un subiect ciudat pentru că este un lucru specific oamenilor si foarte valoros în societate. Fără încredere, nu am fi capabili să interacționăm liber. Dar datorită încrederii, suntem usor de păcălit, prostit, furat si chiar de mințit. Cercetările OSSTMM despre încredere arată că, pentru a putea avea încredere în cineva, există 10 motive numite **Proprietățile Încrederii (Trust Properties)** si dacă toate cele 10 motive sunt îndeplinite, atunci putem acorda încredere acelei persoane fără să ne facem vreo grijă. Însă aceeasi cercetare arată că majoritatea oamenilor au nevoie doar de un singur motiv din cele 10 ca să aibe încredere, iar oamenii care sunt cu adevărat paranoici sau cinici, acceptă doar trei motive ca să acorde încredere.

Resurse / Resources

Căutarea efectivă, învățatul si gândirea critică sunt abilități de bază pentru un hacker. În realitate, hacking-ul este un proces creativ care se bazează mai mult pe tipul de viață pe care îl duci decât pe învățături. Nu putem să vă predăm tot ceea ce trebuie să știți, dar putem să vă ajutăm să recunoasteți ceea ce trebuie să învățați. Din cauză că stiința avansează atât de rapid, ceea ce predăm astăzi, poate fi irelevant maine. E mult mai bine pentru voi să acceptați obiceiuri de învățare pentru hackeri, care reprezintă de fapt cea mai importantă parte din procesul de hacking si care vă va separa de **script kiddie** (un cuvânt de hacker care reprezintă o persoană care foloseste instrumente fără ca să stie cum sau de ce funcționează).

Dacă o să dați de un cuvânt sau de un concept în această lecție pe care nu îl înțelegeți, este foarte important să verificați ce înseamnă acel cuvânt. A nu băga în seamă cuvintele noi, nu va face altceva decât să vă îngreuieze înțelegerea conceptelor din lecțiile care vor urma. O să fiți pusi să cercetați un subiect iar mai apoi să folosiți informațiile pe care le veți găsi pentru a completa exercițiile din acea lecție – însă acele lecții nu vă vor explica cum să faceți cercetarea respectivă. Deci asigurați-vă că petreceți timpul de care aveți nevoie ca să învățați să folosiți diferitele resurse pe care le aveți la îndemână.

Cărți / Books

S-ar putea să vă mire că nu vă direcționăm direct către internet, însă cărțile sunt o metodă excelentă de a învăța bazele si stiința bazată pe fapte a tot ceea ce doriți să explorați. Vreți să învățați ceva despre calculatoare, cum ar fi detaliile de hardware din PC-ul vostru? Nimic nu vă va ajuta mai mult decât cititul unei cărți în domeniu. Principala problemă cu cărțile pentru computere este că se învechesc (nu mai sunt de actualitate) foarte repede. Secretul constă în învățarea structurii de bază care se găseste sub stratul fin al detaliilor. MS-DOS si Windows sunt de departe foarte diferite, însă ambele au la bază principiile logicii Booleane, care au condus computerele de la Ada, Contesa de Lovelace, care a scris primul program pentru computere în secolul nouăsprezece. Poate că îngrijorările legate de securitate si intimitate s-au schimbat în ultimii 2,500 de ani, însă **Arta Războiului (The Art of War)** scrisă de Sun Tzu, cuprinde principii fundamentale care încă se aplică astăzi. (Legat de aceasta, nu există un mod mai rapid de a arăta ca un **n00b – începător –** decât prin citarea lui Sun Tzu. Anumite lucruri ar trebui doar să le știți, dar să nu le ziceți. Iar citarea din Arta Războiului dovedeste că de fapt nu ai citit cartea, deoarece Sun Tzu chiar afirmă că ar trebui să ții secrete cunostințele de valoare.)

Chiar dacă informațiile pe care le găsiți în cărți s-ar putea să nu fie la fel de actuale ca cele provenite din alte surse, ceea ce găsiți în ele s-ar putea să fie mult mai bine scris decât în multe alte surse. Uneori sunt chiar si mai precise. Un scriitor care petrece un an ca să scrie o carte este mult mai înclinat să verifice faptele decât cineva care actualizează un blog de sase ori pe zi. (Vezi Secțiunile referitoare la Zines si Blog-uri pentru mai multe informații.)

Însă țineți minte – "precis" nu înseamnă "imparțial". Sursele informațiilor autorului s-ar putea să fie chiar ele părtinitoare. "History books are written by the winners" - "Cărțile de istorie sunt scrise de cei care învinge" (verificați acest citat), acelasi lucru este valabil si atunci când normativele sociale si politice ale vremii pot interveni împotriva publicării anumitor informații. Acest lucru se întâmplă atunci când manualele scolare sunt selecționate printr-un proces politic si care conțin doar informațiile considerate a fi acceptate de stiut din punct de vedere social. Să nu credeți că ați găsit un adevăr de netăgăduit doar pentru că l-ați citit dintr-o carte. Adevărul este că oricine poate scrie o carte si orice carte poate conține versiunea oricui a adevărului.

Să nu priviți la o carte si să vă dați bătuți înainte să începeți doar pentru că e foarte mare. Nimeni nu citeste majoritatea acestor cărți masive pe care le vedeți în jur. **Gândiți-vă la ele ca la niste pagini web din preistorie.** Deschide una din ele la o pagină oarecare si începe să citesti. Dacă nu înțelegi ceva, mergi înapoi si caută explicația (sau treci mai departe la ceva ce are sens). Treci prin carte înapoi si înainte, asa cum faci de obicei atunci când treci de la un link la altul într-o pagină web. Acest tip de cercetare non-lineară este de obicei mai interesant si mai satisfăcător pentru hackeri, din moment ce se face mai mult din considerentul satisfacerii propriei curiozități decât a cititului.

În final, un lucru pe care îl dobândesc ca abilitate neprețuită cei care citesc cărți, este capacitatea de a scrie bine. Acesta este un avantaj imens indiferent dacă încerci să înțelegi sau să aderi la un domeniu nou. De asemenea, ceea ce spui devine mult mai credibil pentru alți cititori, în special pentru cei care sunt în posturi de conducere.

Reviste si Ziare / Magazines and Newspapers

Revistele si ziarele sunt extrem de folositoare în aprovizionarea de informații concise si actuale. De asemenea să țineți minte că fiecare ziar sau revistă are propriul său auditoriu si propria planificare si temă, indiferent de orice afirmații cum că ar fi "corecte si imparțiale." Fiți la curent cu tema publicației: o revistă de Linux nu este neapărat o sursă bună de informații referitoare la Microsoft Windows, deoarece Windows este o temă de conflict (un sistem de operare competitiv), si în care mai degrabă ar găsi cititorii informații referitoare la superioritatea Linux-ului. Multe dintre revistele de specialitate se folosesc de **cherry picking,** o tehnică care scoate în evidență doar aspectele pozitive ale unui subiect care se potriveste cu tema revistei sau care scoate în evidență aspectele negative ale subiectelor care nu se potrivesc cu tema revistei.

Trebuie să fiți constienți de posibilele părtiniri ale publicației. Acolo vă oferă opinii si nu fapte sau se scot faptele dintr-o poveste pentru a se putea implementa propriile păreri sau ca să nu vă puteți forma propria opinie. Aveți în vedre sursa! Chiar si aparițiile periodice "neutre" pot fi pline de părtiniri si speculații , o formă drăguță de a spune că "își dau cu părerea într-un mod educat" dar care este mai degrabă doar "dat cu părerea" din partea jurnalistului.

Există o miscare puternică în domeniul medical care doreste publicarea tuturor proceselor medicale si farmaceutice (sau măcar cele care au fost plătite din banii publici) chiar si dacă au dat gres tocmai pentru ca doctorii să facă alegeri mult mai informate legate de ce fel de medicamente si ce tip de proceduri să folosească. În timp ce jurnalele medicale curente s-ar putea să publice "faptele reale" din cadrul proceselor de cercetare, detaliile si circumstanțele din spatele acelor fapte sunt totusi înceţosate. Acest fapt este foarte important atunci când ai de a face cu subiecte care se bazează pe cauze profunde. Cauzarea presupune ca acea cauză să aibe precedent si este tocmai motivul efectului.

Alte trucuri folosite de periodice (atât din greseală cât si în mod intenționat) sunt **probele de tip anecdotă (anecdotal evidence)**, care sunt opinii publicate ca si probă, ale unor oameni, indiferent dacă acestia sunt sau nu experți; **proba autoritară (authoritative evidence)**, în care anagajații unei industrii sunt reprezentați ca si experți, îsi dau cu părerea, sau persoane care dețin o autoritate într-un domeniu, care îsi oferă părerea într-un alt domeniu în care nu au nici o specialitate; si în final, **speculația**, a îmbrăca ceva în adevăr pentru că "toată lumea" crede că asa este, chiar dacă nu există vreo atribuire către cineva anume.

Cea mai bună metodă de a face față problemelor legate de precizie si planificări este să fii cât mai bine si mai vast informat. Dacă citesti despre un subiect interesant dintr-o revistă, cercetează mai în profunzime. Preia o parte a subiectului si caută confirmări; preia cealaltă parte si caută contradicții. Unele culturi fac acest lucru din start. Acest lucru face parte din obiceiurile lor sociale să caute alte variante ale povestii în cauză. Aceasta este o trăsătură culturală cu adevărat puternică, mai ales dacă încerci să asiguri o democrație de succes.

Exerciții

1.9 Căutați pe Internet informații referitoare la trei reviste online care vorbesc despre hacking. Cum ați găsit aceste reviste?

1.10 Toate cele trei reviste sunt strict despre hacking-ul computerelor? Care informații oferite ar putea fi de folos în alte domenii sau alte tipuri de afaceri?

Hrană pentru Minte: Speculația / Feed Your Head: Speculation

Următorul paragraf face parte dintr-un articol de ziar despre un jaf. Puteți identifica Speculațiile? Notați părțile pe care le suspectați:

Banca Lake Meadow si Mortgage Lender a fost jefuită Marți după-masă când oameni mascați si înarmați au intrat cu cîteva momente chiar înainte de inchidere si au ținut angajații ostatici timp de o oră după care au fugit într-un model nou de SUV. S-a anunțat că nici un ostatic nu a fost rănit.

Nimeni nu i-a putut identifica pe cei înarmați, fapt care a determinat poliția să creadă că acesta a fost un jaf profesionist deoarece imediat după jaf, a fost reperată masina în spatele băncii îndreptându-se spre sud, către partea deasă de pădure a Munților Bluegreen. Poliția caută în mod sigur hoți cu experiență care s-ar putea să aibă dosare penale si care să aibă de asemenea relații cu persoane care locuiesc în acea zonă.

Având în vedere media de 57 de jafuri de bănci raportate zilnic pe cuprinsul aceste țări si cu o presupunere ca populația districtului să atingă un număr de peste 50,000 până anul viitor, acesta ar putea fi startul unei crize de jafuri de bănci din acea zonă. Declarația comisarului de poliție Smith este următoarea "Se pare că e începutul unei tendințe."

Pe măsură ce devenim din ce în ce mai insensibili la speculații si pe măsură ce rămânem ignoranți la părtinirea acordată datelor si rezultatelor statistice, se poate ca viitorul tuturor stirilor noastre să fie rezultatul unui singur jurnalist care nu face altceva decât să speculeze asupra stirilor în timp ce acestea au loc. În exemplul scurt de mai sus, există un singur fapt real – acela că o bancă a fost jefuită Marți după-masa. Acum, de dragul a ceea ce este deja evident, stirea ar fi arătat ca în exemplul de mai jos dacă am fi schimbat toate speculațiile doar pentru a face lucrurile să pară si mai ridicole:

Banca Lake Meadow si Mortgage Lender a fost jefuită Marți după-masă când niste găini mascate au intrat cu cîteva momente chiar înainte de inchidere si au ținut angajații ostatici timp de un deceniu, după care au fugit într-un balon cu aer cald care avea forma unui cuib de găini. S-a anunțat că nici un ostatic nu a fost acoperit de pene.

Nimeni nu a putut identifica găinile, fapt care a determinat poliția să creadă că au avut în cadrul grupului lor un expert în domeniul deghizărilor precum si un aeronaut împlinit, deoarece chiar cu câteva momente după jaf, a fost reperat balonul deasupra băncii îndreptându-se spre sud, către tundra din Antarctica. Poliția caută în mod sigur artisti de make-up cu experiență si care s-ar putea să aibă legături cu pasionați de baloane.

Având în vedere media de 57 de jafuri de bănci raportate zilnic pe cuprinsul aceste țări si cu o presupunere ca vânzările din industria baloanelor să atingă un prag de 47 de catralioane de dolari în viitorul apropiat, acesta ar putea fi startul unei crize de jafuri de bănci în care se vor folosi baloane cu aer cald. Declarația comisarului de poliție Gordon este următoarea "Se pare că e începutul unei tendințe."

Odată cu utilizarea coplesitoare a speculațiilor si a statisticilor din toate industriile, nu este de mirare că acest fenomen si-a făcut intrarea cu forța si în domeniul securității. Termenul obisnuit folosit în acest domeniu este **FUD**, care este de fapt un acronim pentru **Fear, Uncertainty, and Doubt (Teamă, Incertitudine si Îndoială)**. Toate acestea se datorează modului în care speculația si analiza de risc subiectivă sunt folosite în securitate pentru a capta atenția intereselor cuiva si pentru a vinde soluții de securitate. Din păcate, acest lucru se potriveste de minune cu paranoia primitivă din psihicul uman si cu numărul crescând de speculații. Acest fapt a condus mai departe către soluții de securitate nepotrivite, securitate folosită în mod eronat, controale de securitate reactive si o falsă încredere în autorități. Există în mod clar o greseală în ceea ce priveste abilitățile critice de gândire din cadrul populației si este exploatată atât de către sectorul comercial, cât si de către criminali.

Motoarele de Căutare / Search Engines

Google este un motor de căutare foarte cunoscut dar nu este sigurul de acest fel. Bing este foarte bun cu căutări sub forma de întrebări iar Yahoo este foarte bun pentru a face cercetare amănunțită. Trebuie să fiți conștienți de faptul că toate aceste servicii web doresc să stie totul despre voi si că probabil cunosc mai multe lucruri decât ar trebui. Acestea vă vor înregistra căutările si site-urile pe care le veți vizita după căutări.

> Există motoare precum AltaVista si DuckDuckGo.com care s-ar putea să vă ofere un pic – sau chiar mai multă – anonimitate, fapt care s-ar putea să fie chiar un lucru bun atunci când faceți căutări prin colțuri ascunse.

Website-urile sunt supuse căutărilor atunci când sunt online si de obicei o lungă perioadă si după aceea. În mod normal sunt păstrate sub forma de **cached pages (pagini salvate în memoria cache)**. Memoria cache de Internet este un registru online a versiunilor mai vechi de website-uri care au dispărut. Motoarele de căutare si site-urile arhivate păstrează aceste informații pe o perioadă nedeterminată, care în termeni de Internet însemnă "pentru totdeauna." Acest fapt este o informație valoroasă de care trebuie să ne aducem aminte înainte să puneți orice pe Internet: nu o să dispară deloc. Niciodată. S-ar putea să trebuiască să căutați un link către copia salvată a unei pagini. Google spre exemplu, obisnuia să pună un link intitulat "Cache", pe lângă link-ul normal al unui rezultat. Acesta a fost mutat într-un meniu de tip fly-out din partea dreaptă si este posibil să fi fost mutat din nou la data la care citiți aceste informații.

Pe lângă motoarele de căutare, există de asemenea cache-uri publice în locuri precum **Internet Archive (Arhiva de Internet) la adresa http://www.archive.org**. Puteți să găsiți versiuni de website-uri întregi de pe parcursul anilor, care pot fi de folos în găsirea de informații care au "dispărut."

Un lucru final de reținut despre website-uri: să nu vă încredeți într-un website doar pentru că apare într-un motor de căutare. Multe din atacurile si virusii hackerilor sunt împrăstiate (declansate) prin simpla vizitare a unui website sau prin descărcarea unor programe, a unor screen-saver-e sau a unor fisiere partajate, aparent inofensive. Puteți să vă protejați prin a nu descărca programe de pe site-uri care nu sunt de încredere si prin a vă asigura că browser-ul vostru rulează într-un **sandbox**. Însă aceste metode s-ar putea să nu fie suficiente. Un browser este o fereastră către Internet si ca orice altă fereastră, multe lucruri rele se pot infiltra doar pentru că este deschisă. Uneori s-ar putea să nu fiți conștienți de acest fapt, decât atunci când este deja prea târziu.

Exerciții

1.11 Există multe motoare de căutare. Unele sunt bune pentru a ajunge la **Invisible Web (Web-ul Invizibil)**, porțiuni ale Internetului care sunt foarte greu de găsit pentru anumite motoare de căutare, cum ar fi anumite baze de date private. Un cercetător bun stie cum să le folosească pe toate. Unele website-uri sunt specializate în urmărirea motoarelor de căutare. Asadar, găsiți cinci motoare de căutare pe care nu le-ați folosit sau de care poate nici măcar nu ați auzit până acum.

1.12 Există de asemenea, motoare de căutare care caută alte motoare de căutare. Acestea se numesc **meta search engines (motoare de căutare meta)**. Găsiți unul din aceste motoare de căutare meta.

1.13 Căutați după "security and hacking" (incluzând si ghilimelele) si observați primele trei răspunsuri. În ce fel diferă căutările atunci când NU folosiți ghilimelele?

1.14 Este complet diferită căutarea după un subiect, față de căutarea după un cuvânt sau o frază. Acum o să căutați o idee.

Pentru a face aceasta, **gândiți-vă la fraze care s-ar putea să fie pe pagina pe care o căutați**. Dacă vreți ca motorul de căutare să vă ofere o listă de reviste online despre hacking, nu o să ajungeți prea departe cu rezultatele dacă o să căutați pur si simplu după "o listă de reviste online despre hacking." Nu vor fi multe pagini web care vor conține acea fraza! S-ar putea găsiți câteva dar nu multe.

În schimb, trebuie să vă gândiți la ceva de genul acesta, "Dacă as face o revistă de hacking, cum ar arăta o propoziție obisnuită din acea revistă?" Introduceți următoarele cuvinte si fraze într-un motor de căutare si descoperiți care din ele vă oferă cele mai bune rezultate pentru căutarea voastră:

1. my list of favorite magazines on hacking

2. list of professional hacking magazines

3. resources for hackers

4. hacking magazine

5. magazines hacking security list resources

1.15 Găsiți cel mai vechi website de la Mozilla în Internet Archive. Pentru a face acest lucru trebuie să căutați pe "www.mozilla.org" în website-ul http://www.archive.org.

1.16 Acum ca să asamblați toate informațiile, să zicem că vreți să descărcați versiunea 1 web browser-ului Netscape. Folosind motoarele de căutare si Internet Archives, vedeți dacă reusiți să localizați si să descărcați versiunea 1.

Website-uri si Aplicații Web / Websites and Web Applications

Standardul *de facto* pentru partajarea de informații, se face la ora actuală printr-un web browser. În timp ce noi numim tot ceea ce vedem că face parte din "web," din ce în ce mai multe lucruri pe care le utilizăm sunt de fapt "aplicații web," mai ales din moment ce nu tot ceea ce se găseste pe internet este un website. Dacă verificați email-ul prin intermediul unui browser web, sau dacă vă descărcați muzică folosind un serviciu conectat la web, de fapt folosiți o aplicație web.

Câteodată aplicațiile web au nevoie de privilegii. Aceasta înseamnă că pentru a avea acces, aveți nevoie de un nume de login si de o parolă. Să ai acces atunci când deții dreptul legal să primesti acces, presupune să deții **privileges (privilegii)**. Să intri cu forța într-un website prin hacking pentru a schimba o pagină, poate însemna să ai acces, dar din moment ce nu deții nici un drept legal pentru a fi acolo, nu ai acces privilegiat. În timp ce vei folosii web-ul, o să afli că multe locuri oferă acces către secțiuni privilegiate din greșeală.

Atunci când descoperi ceva de genul acesta, este bine să raportezi acest lucru la administratorul website-ului. Cu toate acestea, ai grijă la eventualele repercusiuni. Din păcate, mulți administratori se supără atunci când primesc rapoarte de vulnerabilitate nesolicitate.

Pentru a contribui la a face Internetul un loc mai sigur, protejându-vă în acelasi timp, ar trebui să luați în considerare folosirea unui serviciu de tip **anonymizer** (epre ex., Tor sau anonymous remailers, etc.) pentru a trimite rapoarte de vulnerabilitate către acesti administratori. Dar aveți grijă: toate aceste tehnologii anonime au punctele lor slabe si s-ar putea să nu fiți atât de anonimi precum credeți că sunteți! (Mai mult de un hacker au aflat acest lucru pe propria piele.)

Exerciții

1.17 Folosiți un motor de căutare pentru a găsi site-uri care au făcut greseala să ofere acces privilegiat la toată lumea. Pentru a face acest lucru, o să căutăm foldere care ne dau voie să listăm conținutul (se numeste "directory listing"), ceva ce în mod normal n-ar trebui să fie permis. Pentru aceasta vom folosi câteva trucuri de comandă Google de la adresa http://www.google.com. Introduceți următoarea frază în căsuța de căutare:

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

Verificați rezultatele si s-ar putea să găsiți unul care seamănă cu listarea unui director. Acest tip de căutare este cunoscut sub denumirea de Google Hacking.

1.18 Puteți să găsiți alte tipuri de documente în felul acesta? Găsiți încă trei listări de directoare care conțin fisiere .xls, .doc, si .avi.

1.19 Există si alte opțiuni de căutare asemănătoare cu "allintitle:"? Cum le puteți găsi?

Zines

Zines, cunoscute ca si **e-zine-uri**, sunt descendente din **fanzines**: mici, de regulă gratuite, publicatii cu o distributie mică, (mai putin de 10 000 de cititori) si adesea scrise de jurnalisti amatori sau pasionati. Fanzine-urile sunt tipărite pe hârtie. Zine-urile de pe internet, ca de exemplu faimosul **2600** sau **Phrack** sunt scrise de voluntari, acest lucru înseamnă că nimeni nu verifică continutul pentru erori non-tehnice. Câteodată, limbajul dur îi poate lua prin surprindere pe cei care nu sunt familiari cu acest gen.

Zine-urile au o puternică tematică sau agendă, si tin să fie foarte dogmatice. Cu toate acestea, tin să arate si să conteste ambele părti ale situatiei, pentru că de regulă, nu le pasă de cititori si abonații lor.

Exerciții

1.20 Caută pe internet trei zine-uri care au ca subiect hacking-ul. Cum le-ai găsit?

1.21 Cum le-ai clasificat ca zine-uri? Tine minte, doar pentru că au în titlul lor zine, nu înseamnă neapărat că chiar sunt.

Blog-urile / Blogs

Un **blog** poate fi considerat o evolutie de la zine-uri, adesea scris de o singură persoană. Blogurile sunt actualizate mai des decât majoritatea publicatiilor sau revistelor si creează comunități legate de teme foarte puternice. Este la fel de important să citesti comentariile cât si postările. Chiar mai mult decât pe zine-uri, răspunsul este adesea imediat si la obiect cu comentarii de ambele părti. Lucrul acesta este unul din marile lor atuuri.

Există milioane de bloguri pe internet, dar numai un mic procent din ele sunt active. Totusi, informația din ele este încă valabilă.

Exerciții

1.22 Caută pe internet trei bloguri care au ca subiect hackingul.

1.23 Cu ce grupuri sau comunități sunt acestea asociate?

1.24 Este o tematică pe blog despre securitate, forte de ordine ori academică?

Forum-urile si listele de e-mail / Forums and Mailing Lists

Forumurile si **listele de e-mail** sunt locuri de dezvoltare comune, asemănătoare cu a înregistra o conversatie la o petrecere. Păstrează-ti o doză de scepticism cu privire la ce citesti acolo. Focusul conversatiei se schimbă adesea, conversatii off-topic, umor, sarcasm, unii oameni fac **trolling**, **un flame war** poate porni oricând, dar când totul s-a terminat nimeni nu are certitudinea cine, ce a zis.

Forumurile si listele de e-mail sunt similare, pentru că sunt multi oameni care contribuie cu informatie mai putin precisă – câteodată intentionat – sunt căi ca cineva să posteze sub formă anonimă sau dându-se drept altcineva. Deoarece, topicurile si temele se schimbă rapid, pentru a obtine toata informatia este important să citesti tot topicul de comentarii, nu doar câteva.

Poti găsi forumuri despre aproape orice topic, si sunt multe reviste online si ziare care ofera forumuri pentru cititorii care vor să răspundă la articolele pe care ei le publică. Din acest motiv, forumurile sunt de nepretuit pentru a obtine mai multe opinii la articol, indiferent cât de mult i-a plăcut unei persoane, sigur există cineva căruia nu i-a plăcut.

Sunt multe liste de e-mail pentru topicuri speciale, dar pot fi greu de găsit. Câteodată, cea mai bună tehnică este să cauti informatia despre un anumit subiect pentru a găsi o comunitate care se ocupă de ea.

Ca hacker, ceea ce este cel mai important pentru tine este să stii că multe forumuri si liste de e-mail, nu pot fi căutate prin intermediul motoarelor majore de căutare si nu puteti găsi informatiile cu privire la postările individuale. Această informatie este parte a web-ului (internetului) nevăzut, ascuns, deoarece contine informatii care pot fi căutate doar direct pe website sau forum.

Exerciții

1.25 Găseste două forumuri pentru hacking. Cum ai găsit aceste forumuri? Poti determina temele sau subiectele de specialitate ale acestor website-uri?

Subiectele din forumuri reflectă tema de specialitate a acestor website-uri?

1.26 Găseste două liste de hacking sau de email de securitate.

Cine este "proprietarul" acestor liste? Poti vedea lista de membri? (s-ar putea să ai nevoie să-ti dai seama de aplicatia cu care a fost dezvoltată lista si să cauți pe web pentru comenzile ascunse pentru a vedea lista de membri).

Pe care listă te-ai astepta ca informatia să fie mai concretă si mai putin dogmatică? De ce?

Newsgroups

Newsgroups – Grupurile de stiri – există de mult timp. Au fost grupuri de stiri cu mult înainte de a exista world wide web. Google a cumpărat întreaga arhivă de grupuri de stiri, si le-a publicat online pe http://groups.google.com. Grupurile de stiri sunt ca listele de discutii dar fără e-mail. Oamenii sunt listati acolo direct, ca si cum ar face un comentariu la un website. Veti găsi posturi acolo de la începutul anilor 1990.

La fel ca si arhivele web, newsgroup-urile pot fi importante pentru a vedea cine a găsit initial o idee sau a creeat un produs. Ele mai sunt de folos când găsesti informatie obscură care nu ar fi putut ajunge pe o pagină web.

Newsgroup-urile nu mai sunt asa des folosite astăzi, cum au fost cu ani în urmă, înainte ca web-ul să devină centrul principal de distributie a informatiei. Cu toate acestea, nu au crescut iar popularitatea lor este înlocuită de noile servicii web precum forumuri si blog-uri.

Exerciții

1.27 Utilizând grupurile google, găseste cea mai veche postare având ca subiect hacking-ul.

1.28 Găseste alte căi pentru a folosi newsgrupurile. Există aplicatii care pot fi citite de pe grupurile de stiri?

1.29 Câte grupuri găsesti care au ca subiect de discutie hackingul?

1.30 Poti găsi o listă actualizată a tuturor diferitelor grupuri de stiri existente în prezent?

Wikis

Wikis sunt un fenomen mai nou de pe internet. Wikipedia (www.wikipedia.org) este probabil cel mai cunoscut, dar mai sunt multi altii. Ca multe alte site-uri wiki, sunt puse împreună de către comunități. Rapoartele adesea sustin că wiki-urile nu sunt precise pentru că sunt scrise de către amatori si fanatici. Dar acest lucru este valabil si pentru cărti, liste de discutii, reviste si orice altceva. Ce este important de stiut este că expertii nu sunt singura sursă de mari idei si informatii bazate pe fapte. OSSTMM subliniază că faptele provin din etapele mici de idei verificate si nu din mari salturi de descoperiri. De aceea, wiki-urile sunt mari surse de idei amatoare si profesionale care se verifică reciproc.

Wiki-urile vor pune în discutie mai multe părti ale topicului si îti vor permite să urmăresti cum informatia este argumentată, refuzată, filtrată si schimbată prin o listă de modificări. Deci, acestea sunt locuri ideale pentru a descoperi informatii, dar adesea trebuie să te duci direct pe site-ul wiki pentru a face căutări.

Exerciții

1.31 Caută "Ada Lovelace." Vezi rezultatele din wiki?

1.32 Intră pe Wikipedia si repetă căutarea. Uitati-vă la articolul despre ea. A fost el inclus în rezultatele căutării?

1.33 Verifică editările de pe pagina wikipedia si uită-te la lucrurile care au fost corectate si schimbate. Ce fel de lucruri s-au schimbat? A fost ceva care s-a modificat si apoi s-a revenit la forma initială? Acum alege un star de cinema popular sau cântăret si du-te pe pagina de wikipedia si verifică editările. Observi vreo diferentă?

1.34 Găseste un alt site wiki si fă o nouă căutare. Oricare din rezultate a fost arătat în căutarea originală de pe motorul de căutare?

Social Media

Folositi un site de social media? Sau mai mult decât unul? Ca hacker, esti constient de popularitatea site-urilor social media din acest moment? Dar si de acelea care nu mai sunt asa de populare cum au fost? Ele încă există, si toate informatiile sunt încă valabile, în cele mai multe cazuri.

Acest lucru înseamnă că există un depozit de informație despre noi, marea majoritate a ei e pusă acolo de noi si vizibilă pentru oricine. Si va exista acolo, pentru totdeauna.

Site-urile social media, adesea au subgrupuri si comunităti de interes. Site-urile cu o temă profesională au grupuri de cybersecurity, iar site-urile cu o tematică "underground" au frecvent si grupuri de hackeri. Pe site-urile profesionale este de asteptat ca toti să utilizeze numele lor real. Pe site-urile de hacking, nu.

Folositi numele real pe site-urile social media sau un „nickname" (poreclă)? Este vreo posibilitate ca nickname-ul pe care il folosesti să ducă către identitatea ta reală? Cei mai multi oameni nu realizează atunci când folosesc nickname-uri, dar nu este iesit din comun pentru ei sau accidental ori câteodată intentionat să iti publici numele real, adresa, orasul, scoala, job-ul, si asa mai departe atunci când folosesti nickname-uri Dacă un alt hacker îti compromite nickname-ul, atunci el poate cu usurintă să afle cine esti cu adevărat din cauza acestor mici greseli. Dacă folosesti un nickname pentru a fi anonim pentru cei care nu te cunosc, atunci ia măsuri pentru a păstra acest lucru. NICIODATĂ nu confunda nickname-urile, dacă ai mai multe decât unul.

Exerciții

1.35 Caută-te pe internet. Ai găsit vreun rezultat despre tine? Rezultatele sunt si de pe retelele sociale?

1.36 Du-te pe site-ul social pe care îl folosesti. Nu te loga, dar repetă căutarea ca si cum ai fi altcineva din afară. Cât de multe poti afla despre tine?

1.37 Du-te pe un site social, pe care un prieten îl foloseste. Din nou, nu te loga dacă ai un cont. Caută-ti prietenul. Cât de mult poti afla despre prietenul tău?

Chat

Chat-ul, care vine în formele de **Internet Relay Chat (IRC)** si **Instant Messaging (IM)**, este un mod foarte popular de a comunica.

> Ca o sursă de cercetare, chat-ul este extem de inconsistent, pentru că, ai de-a face cu persoane în timp real. Unii vor fi prietenosi, altii vor fi nepoliticosi. Unii vor fi pusi pe glume, altii vor fi mincinosi. Câțiva vor fi inteligenti si dispusi să distribuie informația, si câțiva vor fi complet dezinformati dar cu toate astea distribuie informația. Poate fi dificil să-i deosebesti pe fiecare în parte.

Cu toate acestea, odată ce te simti confortabil cu anumite grupuri sau canale, poți fi acceptat în comunitate. Vei primi permisiunea de a pune tot mai multe întrebări, si vei învăta în cine să te încrezi. În cele din urmă, vei avea acces la cele mai noi exploituri de hacking (cunoscute ca si **zero day**, adică care sunt descoperite chiar acum) si îti vei dezvolta propria cunoastere.

Exerciții

1.38 Găseste trei programe de mesagerie instantanee. Ce le face diferite? Pot fi toate utilizate în comunicare?

1.39 Găseste ce este IRC si cum te poti conecta la el. Poti descoperi ce retele suporta canalul ISECOM? Odată ce te alături retelei, cum te conectezi la canalul de discutii ISECOM?

1.40 Cum stii ce canale există pe o retea de IRC? Găseste trei canale de securitate si trei canale de hacking. Te poți alătura lor? Sunt oameni care discută între ei sau sunt roboti?

P2P

Retelele Peer to Peer, cunoscute si sub prescurtarea de **P2P**, sunt rețele de pe internet. Spre deosebire de reteaua obisnuita client-server, unde fiecare computer comunică printr-un server central, calculatoarele din reteaua P2P, comunică direct unele cu altele. Cei mai mulți asociază retelele P2P cu melodiile Mp3 si continutul piratat de pe infamul Napster, dar sunt multe alte retele P2P – care au ca scop schimbul de informatii, si mijlocul de a conduce o cercetare pe distribuirea de informatii.

Problema cu retelele P2P este că puteti găsi orice pe ele, chiar si lucruri care sunt ilegale. Dar si alte lucruri care sunt legale, dar care companiile care le-au creat vor ca ele să nu fie distribuite acolo si cer bani de la orice proprietar de **gateway**, în care sunt puse spre download.

La acest moment, nu este niciun acord cu privire la persoana a cărei acces la internet a fost folosit pentru a descărca continut ilegal, sau dacă politia trebuie să prindă chiar persoana care a făcut-o. Este ca si cum dacă masina ta este folosită pentru a comite o crimă, proprietarul si nu soferul ar trebui să meargă la închisoare. Legile internetului nu sunt corecte, deci trebui să fii foate atent!

Indiferent dacă sunteti sau nu genul de persoană care riscă descărcarea de proprietate intelectuală, nu există nicio îndoială despre retelele P2P – doar o multime de fisiere care sunt disponibile pentru a fi liber descărcate sub o mare varietate de licente – dar există, deasemenea, o multime de fisiere de pe aceste retele care nu ar trebui să fie acolo. Nu vă fie teamă de a utiliza retelele P2P, dar să fiti constienti de pericole inerente a ceea ce descarci.

Exerciții

1.41 Care sunt trei din cele mai populare si mai folosite retele P2P? Cum functionează fiecare? Ce programe trebuie să folositi?

1.42 Verifică protocolul unei retele P2P. Cum functionează si cum face descărcarea mai rapidă?

1.43 Caută cuvintele cheie „download linux". Poti descărca o distributie (distro) de linux utilizând P2P?

Certificări / Certifications

Există certificări OSSTMM Tester de securitate si analist de securitate, certificări variate de „hacker", certificări bazate pe o versiune a "celor mai bune practici" sau alte certificări cu tot felul de initiale si semne de punctuatie.

De ce îti pasă de certificări? Pentru că le poti obtine la orice vârstă, pentru că nu-ti trebuie diplomă pentru aceasta si pentru că te pui în pozitia de a fi căutat, nu de a căuta.

Problema cu certificatele de bună practică, este că ele se schimbă des, iar pentru cele mai bune practici există un mod de a spune "ceea ce fac ceilalți acum." Deseori, ceea ce toată lumea face gresit în această săptămână, va fi în continuare gresit atunci când se actualizează săptămâna viitoare.

Apoi, există certificări bazate pe cercetare, bazate pe cercetare validă si repetabilă în comportamentul uman si al sistemului. Este de prisos să vă spunem că organizatia noastră mamă, ISECOM, se încadrează perfect în domeniul autorităților care oferă certificări bazate pe cercetări. Fie din ISECOM sau din altă parte, uită-te după certificări bazate pe abilități si pe analize sau pe cretificări ale **stiințelor aplicate,** care te fac să dovedesti că poti să faci ceea ce spui că ai învătat. Îți vor fi de folos atunci când vei avea nevoie de ele.

Seminarii / Seminars

Participarea la seminarii este o modalitate foarte bună de a auzi teoria explicată în detaliu si pentru o vedea pusă în practică. Chiar seminariile focusate pe produs sunt bune pentru a participa si a vedea cum un produs este destinat spre utilizare, atata timp cât tu esti constient de faptul că evenimentul este o strategie de marketing si că scopul lor este să-ti vândă.

Am fi neglijenti dacă nu am mentiona că putem aduce Hacker Highschool Seminars în mai multe locatii, si putem acoperi toate lectiile disponibile. La aceste seminarii, hackeri vor vorbi cu elevii despre hacking si de viata unui hacker, atât de bine, cât si de rău. Aceste seminarii îti arată adevărata viată a hackerilor din **Hacker Profiling Project**, un proiect de colaborare cu Organizatia Natiunilor unite de a explora cum sunt hackeri si de ce s-au apucat de hacking. Vom merge să-ti arătăm partea bună a hackingului , pentru că hackingul nu este întotdeauna un lucru rău.

Unul din lucrurile cele mai puternice cu care te putem ajuta este să găsesti calea de mijloc între a fi la fel de curios ca un intelectual cât si plin de resurse ca un hacker. Hackerii au succes în ceea ce fac, pentru că ei stiu cum să se disciplineze singuri si să învete abilitătile de care au nevoie pentru a merge mai departe.

Esti de asemenea invitat să-ti întrebi părintii si profesorii dacă îti permit să începi un curs de hacking în scoala ta. Contactati ISECOM pentru mai multe informatii.

Studiu aprofundat / Further Study

Acum ar trebui să exersezi până esti un maestru în cercetare. Cu cât înveti mai mult, cu atât vei găsi mai multă informatie si mai rapid vei învăta. Dar să fii atent, deasemenea, să-ti dezvolti ochiul critic. Nu toate informatiile sunt adevărate.

> Întotdeauna întrebati-vă de ce ar minti cineva? Are cineva de câstigat bani dacă nu e onest si împrăstie un zvon sau o poveste? De unde provin faptele? Si, cel mai important, care este scopul?

Ca toate hackingurile, studiul necesită un domeniu de aplicare. Asta e foarte important atunci când veti vedea statistici, cum ar fi matematica, care utilizează procente, fractiuni si cote. Puteti vedea acest lucru la statisticile nationale privind criminalitatea sau sănătatea luate de la un esantion mic din doar o parte a tării. Doar pentru că ceva afectează 10% din oameni din 200 studiati într-un singur oras, nu înseamnă că întreaga natiune are aceeasi problemă. Astfel, fii inteligent în modul în care citesti aceste informatii, precum si modul în care le găsesti. Întotdeauna va exista o diferență mare mare atunci când îți vei dai seama care este scopul informației!

Pentru a vă ajuta să deveniti un cercetător mai bun în Hacker Hightschool Program, iată unele subiecte si termeni suplimentari, pentru aprofundare:

- Căutare Meta / Meta Search
- Internetul invizibil / The Invisible Web
- Google Hacking
- Cum functionează motoarele de căutare / How Search Engines Work
- Motorul de căutare Open Source / The Open Source Search Engine
- Dosarul cu jargoane / The Jargon File
- OSSTMM
- Certificări 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