Hacker Highschool

SECURITY AWARENESS FOR TEENS



LEZIONE 1
ESSERE UN HACKER

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

ATTENZIONE

Il progetto Hacker Highschool è uno strumento di apprendimento e come tutti gli strumenti di apprendimento non è esente da pericoli. Alcune lezioni, se usate in modo improprio, possono causare danni fisici. Eventuali pericoli possono emergere anche in caso non si sia svolta una sufficiente ricerca in merito agli effetti di particolari tecnologie. Gli studenti che usano queste lezioni dovrebbero essere incoraggiati ad imparare, provare e testare. Ad ogni buon conto ISECOM non potrà essere ritenuta responsabile per un uso improprio di quanto esposto.

Le seguenti lezioni ed esercizi sono "open" e disponibili pubblicamente alle seguenti condizioni e termini stabiliti da ISECOM:

Tutti i contenuti del progetto Hacker Highschool vengono forniti per uso non commerciale agli studenti delle scuole elementari, scuole medie inferiori e scuole medie superiori, sia per le istituzioni pubbliche che per quelle private, ammettendone l'uso per le esercitazioni a casa. Non è ammessa la riproduzione del materiale per la vendita. L'utilizzo del materiale presente in queste lezioni è consentito per i corsi di ogni tipo che prevedono il pagamento di una tassa/quota d'iscrizione o frequenza, previa acquisizione di regolare licenza d'uso. Sono soggetti a tale norma anche i corsi presso le università, campi estivi e tutto quanto sia inteso come formazione. Per acquistare una licenza è possibile visitare la sezione LICENSE della pagina web della HHS all'indirizzo:

http://www.hackerhighschool.org/licensing.html.

Il progetto Hacker Highschool rappresenta lo sforzo di una comunità "open". Pertanto se troverete utile questo materiale vi invitiamo a supportarci tramite l'acquisto di una licenza, attraverso una donazione o una sponsorizzazione.

Sommario

Hanno contribuito

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

Per la versione in lingua italiana:

Raoul Chiesa, ISECOM (Coordinatore Team di lavoro edizione italiana)
Matteo Benedetti, Security Brokers ScPA
Ing. Selene Giupponi, Security Brokers ScPA
Francesco Mininni, Ing. PhD., Uff. E.I.
Riccardo Trifonio, Arma dei Carabinieri

ISECOM

Per amore dell'Hacking

Introduzione di Pete Herzog

Qualsiasi cosa possiate aver sentito sugli hacker, la verità è che sono veramente bravi in una cosa: scoprire. Gli Hacker sono motivati, pieni di risorse e creativi. Esaminano con attenzione come funzionano gli oggetti, a punto che sono in grado di prenderne il controllo e trasformarli in altro. Questo consente loro di rielaborare anche le grandi idee perché riescono ad andare in profondità, fino al cuore del meccanismo di funzionamento dell'oggetto. Inoltre non hanno paura di commettere due volte lo stesso errore per soddisfare la loro curiosità scientifica e capire se lo stesso errore ha sempre lo stesso risultato. Per questo gli Hacker non vedono un fallimento come un errore o come una perdita di tempo perché ogni fallimento significa qualcosa; qualcosa di nuovo da imparare. Queste sono le caratteristiche di cui ogni società ha bisogno per progredire.

> Molte persone che sono state chiamate hacker, soprattutto dai media, o che hanno avuto problemi per azioni di "hacking" non erano affatto hacker, in realtà.

Le sue idee erano in disaccordo sia con le convenzioni scientifiche del tempo, che si basavo su quanto noto ai tempi sui germi (nulla), sia con la comodità dei dottori che pensavano ci volesse troppa fatica a lavarsi continuamente le mani.

Quello che pensate di sapere degli hacker è che possono intrufolarsi nei computer degli altri e prendere possesso dei loro account. Possono leggere le vostre e-mail senza che lo sappiate. Possono usare la vostra web-cam senza permesso e possono guardarvi ed ascoltarvi violando la presunta privacy di casa vostra. Questo non è falso.

Alcuni hacker vedono la sicurezza delle reti come una ulteriore sfida da superare e quindi pensano ai metodi per poter aggirare o fregare il sistema. Il loro obiettivo, però, è quello di superare l'ingegno di chi ha progettato od installato la rete. Scoprono più informazioni possibili sulle caratteristiche della rete, sulle regole, sulle interazioni con i sistemi operativi e con gli altri sistemi coinvolti, sugli utenti che hanno accesso alla rete e sugli amministratori che la gestiscono. Fatto questo usano le informazioni raccolte per provare differenti metodi per obiettivo ottenere quello che vogliono. Questo tipo di hacking può avere effetti benefici sulla tecnologia perché consente di capire come incrementare la sicurezza e come migliorare la tecnologia in tal senso.

Sfortunatamente a volte l'attività di hacking è fatto da criminali ed i loro obiettivi sono illegali, invasivi e distruttivi. Tipicamente questi sono i soli hacker che fanno notizia.

Un hacker non è qualcuno che scrive un post da un account di un altro che lascia il proprio social network aperto ed incustodito. Nemmeno qualcuno che **da dietro le vostre spalle mentre navigate** guarda le password ed accede in seguito ai vostri account . Questo non è hacking. Un hacker non è nemmeno chi scarica dalla rete un tool da **script kiddie** per violare l'e-mail di altri utenti. Questi non sono hacker; questi sono solo ladri e vandali.

Hacking è ricerca. Avete mai provato a fare qualcosa tante volte, in modi differenti, fino a raggiungere il risultato che cercavate? Avete mai smontato un apparato od uno strumento per guardare come funziona, studiare i componenti ed effettuare delle modifiche per osservare le differenze nel funzionamento? Questo è hacking. Fate hacking tutte le volte che esaminate qualcosa in profondità per capire come funziona, al fine di manipolare l'oggetto ed adattarne il funzionamento alle vostre esigenze.

Per il modo in cui Internet è progettata e l'immenso numero di applicazioni, sistemi, apparati e processi di cui si compone, è il posto più comune in cui trovare hacker. Si potrebbe dire che essendo stata costruita da hacker è il loro campo giochi preferito. Ma non è l'unico posto. È possibile trovare ottimi hacker in ogni settore di ricerca ed in ogni campo dell'industria e tutti hanno una caratteristica in comune: spendono il proprio tempo per capire come funzionano le cose, per farle lavorare in un modo innovativo. Gli hacker non guardano alle cose con gli stessi occhi del progettista iniziale, ma vedono potenziali migliori e più grandi nell'oggetto e lo modificano affinché sia qualcosa di nuovo.

Non pensate di poter diventare facilmente grandi hacker. Solo compiendo dei grandi "hack" con grande umiltà, potrete essere grandi.

L'hacking di per sé non è illegale. Lo è quanto lo è lanciare un sasso. Tutto dipende dalle intenzioni. Se si lancia un sasso con l'intenzione di ferire qualcuno, questo costituisce reato. Se l'intenzione non è quella di ferire qualcuno, ma l'azione porta comunque al ferimento di qualcuno, probabilmente questo non costituisce reato, ma sarete comunque tenuti a pagare per risarcire i danni. Un progetto ISECOM chiamato **Hacker's Profiling Project** ha fatto emergere che i danni maggiori dovuti ad azioni di hacking sono causati da hacker giovani ed inesperti che danneggiano i sistemi altrui per sbaglio. Questo equivale a gettare una pietra per strada solo per gioco e colpire una macchina di passaggio sfondandone il parabrezza. Il danno, seppur non intenzionale, dovrà essere risarcito. Quindi fate attenzione a quando compite azioni di hacking sui sistemi che non vi appartengono. Limitatevi ad hackerare quello che è di vostra proprietà.

Potrebbe essere considerato illegale fare hacking su qualcosa che avete regolarmente acquistato e chi vi appartiene. Ci sono hacker che sono stati puniti perché hanno hackerato i propri dispositivi e computer. Ci sono hacker che hanno fatto hacking su software, musica e film che hanno acquistato e che sono stati citati in giudizio per questo. Nello specifico potreste non essere autorizzati a compiere azioni di hacking su ciò che acquistate, anche se lo fate semplicemente per testare la sicurezza del prodotto. Questo avviene perché molte delle cose che acquistate sono protette da un contratto detto **End User License Agreement (EULA).** Tali contratti esplicitano chiaramente che non è possibile farlo. Quando installate od aprite il programma accettate il contratto anche se non potete leggerlo fino ad avvenuta installazione. Tenete questo in mente quando farete pratica di hacking a casa vostra su oggetti e programmi che vi appartengono.

Un hacker è uno "smanettone", uno scienziato sperimentatore, sebbene il termine "scienziato pazzo" appaia più adeguato in quanto differentemente dagli scienziati tradizionali, gli hacker seguono l'istinto piuttosto che un'ipotesi formale. Questa non è un

caratteristica necessariamente negativa. Molti oggetti interessanti sono state realizzati o inventati da persone che non hanno seguito le convenzioni standard di quanto era noto e certo ai tempi.

Il matematico *Georg Cantor* suggerì nuove teorie riguardo l'infinito e gli insiemi che crearono scompiglio tale nel mondo della matematica che altri matematici si riferivano alle sue idee come ad una "grave malattia" che infettava la matematica.

Nikola Tesla è un altro esempio di persona considerata "scienziato matto" ai suoi tempi, ma era il massimo esperto di elettromagnetismo. Egli progettò il primo motore "brushless" alimentato a corrente alternata, anche se è più noto per l'effetto Tesla e per la bobina Tesla.

C'è stato inoltre *Ignaz Philipp Semmelweis* che comprese che i dottori devono lavarsi le mani tra la visita di due pazienti diversi per evitare il diffondersi delle malattie. Si chiese se fosse colpa sua che le malattie lo seguissero passando da paziente a un altro, decise quindi di lavarsi le mani tra una visita e l'altra e infatti la trasmissione delle malattie scomparve.

Perché essere un hacker?

Pensate a come gli scienziati hanno mappato il genoma umano: hanno usato un metodo sviluppato per decodificare le password. Le password sono tipicamente memorizzate in forma cifrata, di modo che sia difficile rubarle. Il **brute-forcing** è un metodo per decifrare le password effettuando il **cracking** della loro forma cifrata. Questo metodo rompe l' **hash** delle password, decifrando pochi caratteri alla volta, mettendo tutto insieme alla fine del processo. Gli studiosi del genoma hanno utilizzato lo stesso metodo per mappare tutte le 3,3 miliardi di coppie di basi del genoma umano.

L'hacking ha fatto la sua comparsa nelle cucine degli chef che hanno utilizzato l'azoto liquido come refrigerante per ottenere il gelato perfetto o quando hanno modificato le patitine fritte per inserire al loro interno il ketchup o semplicemente quando hanno fatto qualcosa per cui non avevano la giusta attrezzatura….

I chimici hanno fatto hacking su elementi e composti per secoli. Per natura le molecole si comportano con modalità ben precise a seconda dei diversi ambienti dove si trovano (caldo, freddo, elevate altitudini, profondità degli oceani), quindi i chimici hanno bisogno di comprendere profondamente le diverse proprietà dei composti chimici per provare a combinarli insieme per raggiungere i loro scopi. Questo è particolarmente evidente nello studio di nuovi farmaci, per cui centinaia di piante in una zona vengono studiate dalla radice ai frutti per comprenderne le proprietà chimiche e estratte e combinate per ottenere nuovi medicinali. Si prova e si riprova, spesso per diversi anni, prima di arrivare alla combinazione giusta che porta ad ottenere i risultati voluti.

L'hacking è usato anche in economia per comprendere il mercato o le abitudini di alcune categorie di acquirenti. I ricercatori approfondiscono con attenzione de diverse forze che influenzano lo specifico mercato analizzato e dopo cercano la maniera per cambiarlo o influenzarlo secondo le proprie intenzioni. A volte l'hacking avviene sul prodotto, a volte avviene su di voi (con la pubblicità ed il "**priming**" , un qualcosa con cui avrete a che fare nella lezione sul Social Engineering).

L'hacking è diventato anche parte cruciale del warfare. Soldati altamente specializzati e preparati si dimostrano pieni di risorse e creativi quando devono raggiungere l'obiettivo della loro attività: questo è esattamente l'atteggiamento hacker. "Code breakers" ("decifratori" o crittoanalisti), analisti di intelligence ed ufficiali sul campo usano quelle che sono le proprie conoscenze basilari di un hacker per capire le capacità del nemico, attività cosa sta facendo e come sfruttare a proprio vantaggio i punti deboli delle sue dotazioni. connesse Poiché sempre di più le nazioni si affidano ai computer e alle, l'uso dell'hacking per gli attacchi e per le difese informatiche è diventato una parte significativa delle attività delle forze armate e delle operazioni di intelligence. Le agenzie di sicurezza nazionali ed internazionali si recano presso le convegni hacker per reclutare hacker!

> Il vero motivo per voler essere un hacker è perché è una cosa molto forte. Si possono fare cose davvero interessanti quando si possiedono le capacità di un hacker di alto livello. Ogni profonda conoscenza conferisce un grande potere. Se si conosce il funzionamento di un qualcosa così profondamente da sapere come controllarlo, allora si ha un potere notevole tra le mani. Soprattutto si ha il potere di difendere se stessi e le persone care.

Sempre di più la vita delle persone è on-line e on-line sono le relazioni interpersonali, con Internet si trova lavoro e si fanno soldi. Le informazioni hanno un elevato valore – o sono una minaccia – e gli hacker possono proteggere se stessi meglio di chiunque altro. Possono capire quello che succede ai loro dati. Possono fare in modo di rivelare solo ciò che vogliono e tenere gli altri dati protetti e privati. Questo rappresenta un grosso vantaggio a scuola, a lavoro e nella vita, in quanto qualsiasi dato, anche insignificante, potrebbe essere usato contro di te. Contateci.

> Fai hacking contro tutto ma non far male a nessuno.

Come fare hacking

Dire come si fa hacking è come spiegare come fare un salto mortale all'indietro su una trave d'equilibrio: indipendentemente dal dettaglio della spiegazione, non si riuscirà a farlo da soli la prima volta. Bisogna prima sviluppare le competenze, la sensibilità e l'intuizione attraverso la pratica altrimenti si fallirà miseramente. Però ci sono comunque alcuni consigli che possiamo darvi per agevolare il vostro percorso ed incoraggiarvi a continuare sempre a far pratica.

Prima di tutto, dovreste conoscere alcuni piccoli segreti sull'hacking. Per questo faremo riferimento all'**OSSTMM** (www.osstmm.org). La maniera hacker di pronunciare questa sigla è "aw-stem". L'OSSTMM è l'**Open Source Security Testing Methodology Manual** e ,nonostante possa essere letto come le istruzioni di un lettore DVD, è il documento principale che molti professionisti dell'hacking utilizzano per pianificare ed eseguire gli attacchi e le difese. Nel manuale vi sono delle perle che vi apriranno gli occhi.

Due modi per ottenere quello che volete

Ad esempio, dovreste sapere che esistono sono solo due modi per ottenere ogni cosa: o lo prendete da soli o qualcuno lo prende per voi. Questo implica che tutto quello che fate per ottenere qualcosa in questo mondo richiede **interazioni** tra le persone e le cose. Ovvio, giusto? Ma pensateci. Questo significa che tutti i meccanismi di protezione devono provare a bloccare le interazioni di qualcuno con quello che i meccanismi stessi stanno proteggendo. A meno di non chiudere tutto in una enorme cassaforte, le interazioni non possono essere inibite completamente. La roba nei negozi deve essere sistemata sugli scaffali, perché la gente possa toccarla. Le relazioni commerciali richiedono l'invio di informazioni attraverso programmi e-mail che si connettono con server mail e che spediscono i messaggi verso altri server mail.

Queste sono tutte interazioni. Alcune di queste interazioni avvengono tra persone ed oggetti con cui si ha familiarità: per questo queste interazioni vengono definite "**Trusts**". Quando le interazioni avvengono tra persone o sistemi sconosciuti, vengono invece definite "**Accesses**". È possibile utilizzare un accesso per prendere possesso di qualcosa, oppure convincere qualcuno che possiede un "trust" con il nostro obiettivo a prenderlo per noi. Se pensate a questa situazione per un attimo capirete che sicurezza significa proteggere qualcosa sia da possiede quello che non si conosce sia da quello che si conosce e di cui ci si fida.

Esercizi

1.25 Che tipo di interazioni usa un motore di ricerca? Pensateci bene: qualcuno fornisce un Access? Qualcuno fornisce un Trust?

1.26 Fate un piccolo esempio di Access e Trust da utilizzare per prendere una bicicletta protetta da lucchetto ad una rastrelliera per bici.

1.27 Fate un piccolo esempio di come potete utilizzare un Access e un Trust per accedere all'account web-mail di un'altra persona.

Nutri La Mente: spionaggio

Quando l'hacking viene utilizzato contro un governo straniero per compiere azioni criminali di effrazione, intrusione, furto e distruzione per ottenere informazioni politiche o militari, si parla di **spionaggio**. Invece, quando queste azioni sono realizzati da entità commerciali di governi diversi per impossessarsi di informazioni economiche, si parla di **spionaggio economico.**

Quando l'hacking è utilizzato per impossessarsi di informazioni private e personali di singoli individui al fine di metterli alla gogna mediatica, allora si parla di **DoXing**. Invece, quando le informazioni pubblicamente accessibili sono sviscerate allo scopo di attaccare una persona o una società, ma nessun crimine è stato compiuto per ottenere le informazioni stesse, allora si parla di **document grinding** o di **OSInt (Open Source Intelligence)**.

Quando si utilizza l'hacking per comprendere il funzionamento della rete di un'azienda, dei suoi sistemi, applicazioni e apparati al fine di renderli oggetto di un attacco, ma senza introdursi nei sistemi stessi, allora si parla di **network surveying**.

Quando l'hacking è utilizzato per studiare a fondo un concorrente, senza violare nessuna legge (anche se potrebbe essere considerato comunque meschino e scortese), allora si parla di **competitive intelligence**.

Adesso starete probabilmente morendo dalla voglia di sapere quali sono questi metodi scortesi e meschini che vengono utilizzati, pur non sfociando nell'illegalità. Ade esempio pensate alla possibilità di stressare una persona o di farla preoccupare per ottenere informazioni. A meno di non uccidere il soggetto, raccontare bugie è ancora legale (sebbene ci siano leggi che sanzionano il procurato panico in luoghi pubblici, ad esempio gridare "Al fuoco!" in un cinema affollato quando non c'è nessun incendio).

Ammettiamo che un hacker voglia sapere dove un'azienda sta per costruire una nuova fabbrica. Userà il document grinding per capire quali sono le persone responsabili di questa decisione. In seguito l'hacker chiamerà i loro uffici per scoprire quali città e fabbriche hanno visitato di recente. Ovviamente queste informazioni sono riservate e nessuno le comunicherà senza allarmarsi. Pertanto l'hacker ha bisogno di trovare un modo per ottenerle in modo "ingannevole". Non è difficile immaginare l'ipotetica sequenza degli eventi.

Hacker: Salve, sono il Dottor Jones. Chiamo dalla scuola per parlarle di sua figlia Nancy.

Target: Davvero? Cosa ha combinato questa volta?

Hacker: Guardi, le sanguina il naso e non riusciamo a bloccare l'emorragia. Vorrei chiederle se è stata di recente esposta a qualche agente chimico, sostanze chimiche o così via. Questi sintomi sono rari tranne che in persone che sono state esposte a tali sostanze. Può dirmi qualcosa in merito?

Target: ("vuota il sacco")

Fare questo non è illegale in molti posti. Sicuramente è causa di stress aggiuntivo. Senza parlare del fatto che è davvero meschino far preoccupare in questo modo un genitore.

L'hacking per prendere possesso del vostro mondo

L'hacking non riguarda solo le interazioni. Lo sapete. Alcune persone dicono che la politica è fatta di interazioni. Forse. Probabilmente pensavate che l'hacking riguardi il violare la sicurezza. A volte lo è. Ma è soprattutto prendere il controllo di qualcosa o anche modificarlo. Comprendere le interazioni ed il loro significato nel mondo reale utilizzando le tecniche che abbiamo esposto, può risultare utile quando provate ad infiltrarvi, a scoprire o ad inventare. Perché dovreste farlo? Per avere la libertà di fare di quello che avete quello che volete. Ma anche per evitare che gli altri cambino qualcosa che avete in nome di quella che alcuni chiamano sicurezza (ma noi non siamo queste persone).

> Quando acquistate qualcosa capita che l'azienda da cui acquistate faccia di tutto per impedirvi di personalizzare o di modificare i suoi prodotti se non secondo le sue regole. Potete accettarlo, a patto che accettiate anche che se si rompe non si può pretendere che siano loro a risolvere il problema o a sostituirvelo.. Quindi l'hacking fa di qualcosa che possedete qualcosa di vostro, in modo inequivocabile. Potrebbe apparire inquietante per qualcuno, ma ha i suoi vantaggi. Specialmente se volete tenere gli altri lontani dalle vostre cose.

Per tante, tante persone (ma dovremmo dire troppe volte "tante", per enfatizzare la realtà), la sicurezza è impiegare un prodotto, sia esso un lucchetto, un allarme o un firewall o una qualsiasi altra cosa che in teoria tiene al sicuro. Ma questi prodotti a volte non funzionano come dovrebbero oppure hanno dei problemi intrinseci che aumentano la cosiddetta **Attack Surface**, quando un prodotto di sicurezza dovrebbe ridurla. (La superficie d'attacco comprende tutti i modi e le interazioni che permettono a qualcuno o qualcosa di essere attaccato). Sperare che i prodotti possano essere migliorati in un mondo dove la fanno da padrone cose come il mass-marketing, il pagamento a consumo, il crowdsourcing, il comprare prodotti "as-is" è assolutamente inverosimile. Per queste ragioni è necessario che voi facciate hacking sulla vostra sicurezza. Dovete analizzare il prodotto e capire dove sono le sue debolezze e come cambiarlo per migliorarne le prestazioni. E potrebbe essere necessario apportare modifiche più profonde affinché il produttore non possa ripristinare l'oggetto alle sue condizioni originarie!

Quindi, quando pensate all'hacking in termini di violazioni di sicurezza, ricordate che questa rappresenta solo un'area di utilizzo. Se non siete in grado di fare hacking, dovrete rinunciare ad un po' della libertà e della privacy a cui non vorreste rinunciare. (E sì, abbiamo ben presente che adesso non potrebbe interessarvi affatto che alcune cose che dite o pubblicate on-line siano di dominio pubblico. Ma Internet ha una memoria lunga e migliora sempre nel rendere disponibili i dati in caso di ricerche. Quello che va in rete rimane in rete. Quindi tenetelo presente per il futuro, anche se oggi non vi interessa affatto).

Adesso che vi siete fatti un'idea delle interazioni, andiamo più nel dettaglio. Conoscete le interazioni basiche Access e Trust, ma avete mai sentito parlare di **Visibility**? Questo è il terzo tipo di interazione. Ed è potente esattamente come gli altri due. Nel linguaggio della polizia può essere semplificato con il termine *opportunità* ma nell'hacking ci si riferisce piuttosto alla presenza di qualcosa con cui interagire o meno. Questo tipo di interazione porta con se tutta una serie di nuove tecniche di sicurezza come l'inganno,

l'illusione ed il camuffamento, ma porta con se anche tutte le nuove attività di hacking per evitare ed aggirare queste nuove misure di sicurezza!

Quando chiesero al famoso rapinatore di banche Jesse James perché rapinasse le banche, lui disse che il motivo è perché lì ci sono i soldi. Quello che intendeva è che attraverso la Visibility lui sapeva che c'erano dei soldi all'interno della banca, mentre per altri posti che avrebbe potuto rapinare non poteva esserne certo. Le banche hanno la Visibility: le persone conoscono quali beni custodiscono. Ma non tutto ha visibilità. È un dato di fatto che la Privacy sia l'opposto della Visibilità ed è un ottimo modo per evitare di diventare un obiettivo. Che siate in una strada pericolosa, in una giungla o in Internet, tenere una bassa **Esposure** ed evitare la Visibility è il primo metodo per evitare di essere attaccati.

Esercizi

1.28 Internet è così popolare nel creare miti e tramandare false storie che è difficile distinguere le informazioni reali dalle bufale. Quindi se volete imparare ad essere dei buoni hacker, prendete l'abitudine di verificare i fatti e imparare la verità sulle cose. Per questo avete il task di verificare se Jesse James fece veramente l'affermazione che abbiamo citato prima. E non fate le cose facili fermandovi alle informazioni delle prime pagine web, ma approfondite la ricerca.

Adesso che vi state abituando a cercare le cose, verificate la veridicità di questi luoghi comuni:

1.29 Nel linguaggio Inuit, lingua da cui deriva, cosa significa veramente la parola igloo? Che tipo di interazioni avete utilizzato per scoprirlo?

1.30 Molti genitori affermano che lo zucchero rende i bambini piccoli iper-attivi. Ma è vero? Che interazioni avvengono nella pancia dei bimbi per ottenere l'effetto di renderli iper-attivi e fare in modo che si comportino in modo stupido quando mangiano molte caramelle o cibi ricchi di zuccheri?

1.31 Potreste aver sentito che lo zucchero provoca le carie dentali, ma qual è la reale interazioni che avviene e che realmente causa questo effetto? Lo zucchero ne è realmente la causa o no? Vi sono dei punti extra se riuscite a dimostrare che spazzolare i denti è una interazione che può combattere la reale vera causa della carie e se trovate il nome di almeno un agente chimico che affronta alla radice il problema (*suggerimento: fluoruro è sbagliato*).

Il Four Point Process

Quando considerate i tre tipi di interazione insieme, vi trovate in una situazione di **Porosity**, il fondamento di una Attack Surface. Come la parola stessa suggerisce, i pori o "buchi" nelle difese esistenti sono essenziali perchè abbiano luogo le necessarie interazioni (e anche quelle ignote o inutili). Ad esempio un negozio ha la necessità di mettere i prodotti sugli scaffali di modo che i clienti possano toccarli, metterli nel carrello e comprarli. Queste sono interazioni necessarie per il processo di vendita. Ma potrebbe accadere che non si abbia conoscenza del fatto che gli impiegati portino via di nascosto i prodotti dalle rampe di carico e questa è sicuramente un'interazione non voluta.

La Porosity è qualcosa che dovete conoscere per proteggervi o per attaccare un obiettivo. Ma non è sufficiente analizzare qualcosa per hackerarla. Per farlo avete bisogno di approfondire la conoscenza dei tre tipi di interazione che abbiamo illustrato poco fa. Questo è un altro segreto dell'OSSTMM ed è chiamato **Four Point Process (FPP – Processo a quattro punti).** Questo processo delinea quattro modi in cui queste interazioni

sono utilizzate per analizzare qualcosa nel modo più approfondito possibile e con analizzare intendiamo manomettere in modo da osservare e capire cosa accade.

Il processo di Eco

Siamo cresciuti scoprendo e imparando cose, interagendo direttamente con esse. I bambini toccano lo scoiattolo rinsecchito con un bastone per vedere se è veramente morto.. Questo è noto come il **echo process**. È la forma di analisi più semplice ed immatura. È come gridare in una caverna ed aspettare la risposta. Il processo di eco presuppone l'utilizzo di differenti tipi di interazioni di Access ed la successiva osservazione della reazione, per comprendere in quali modi è possibile interagire con l'obiettivo. Il processo di eco rientra nelle verifiche di tipo causa ed effetto.

Questa è una maniera strampalata di testare qualcosa, perché sebbene un test di questo tipo sia molto rapido, è allo stesso tempo molto inaccurato. Per esempio quando utilizziamo il processo di eco per testare la sicurezza, definiamo un target sicuro quello che non risponde. Questo equivale a dire che l'obiettivo non ha Visibility. Ma sappiamo anche che solo perché qualcosa non risponde a un particolare tipo di interazione questo non significa che sia "sicuro". Se ciò fosse vero l'opossum non verrebbe mai ucciso da altri animali quando finge di essere morto e tutti sarebbero al sicuro dall'attacco di un orso solo svenendo per la paura. Ma sappiamo che questo non è vero. Ridurre la Visibility può aiutare a scampare a certi tipi di interazione, ma non a tutti.

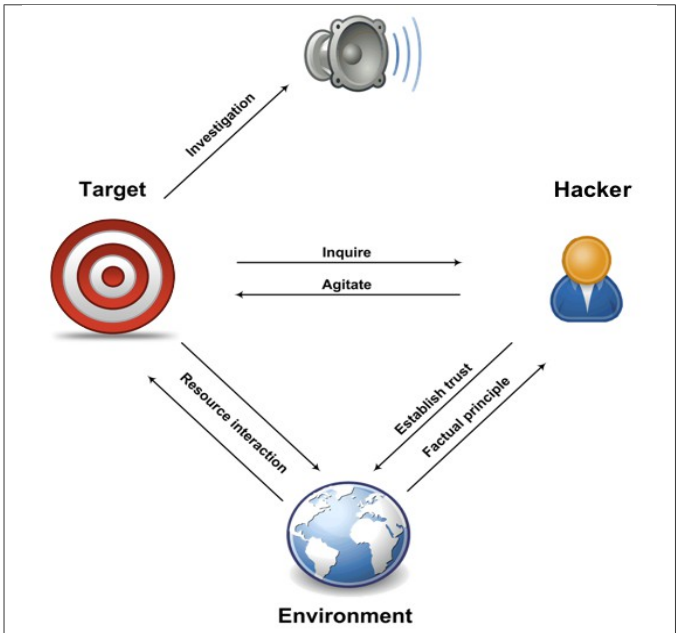

Figura 1.1: The Four Point Process

Sfortunatamente gran parte delle persone usano esclusivamente il processo di echo quando analizzano le cose nella vita di tutti i giorni. Ci sono così tante informazioni che vanno perse in questo tipo di analisi che dovremmo essere grati alla scienza medica di essersi evoluta superando il metodo mono-dimensionale di diagnosi "Fa male quando tocco qui?". Se negli ospedali si usasse questo metodo per determinare la salute di una persona, difficilmente sarebbe di vero aiuto per la collettività. Questo è il motivo principale per cui i dottori, gli scienziati e soprattutto gli hacker usano il Processo in Quattro Punti per essere sicuri di non perdere informazioni.

Il Processo a Quattro Punti esamina le interazioni nei seguenti modi:

- **Induction**: Cosa possiamo dire dell'obiettivo osservando il suo ambiente? Come si comporta nel suo ambiente? Se l'obiettivo non è influenzato dal suo ambiente, è comunque una informazione interessante.
- **Inquest**: Che segnali (emanazioni) emette l'obiettivo? Analizzate ogni traccia o segnale di tali emissioni. Un sistema od un processo tipicamente lasciano segni tracce caratteristiche delle loro interazioni con l'ambiente.

- **Interaction**: Cosa succede quando interagisci con l'obiettivo? Questo punto include il test dell'eco, con le interazioni attese ed inattese con l'obiettivo, per innescare le risposte.
- **Intervention**: Quanto posso sollecitare il sistema prima che si rompa? Interferite con le risorse necessarie all'obiettivo, come l'elettricità, oppure interferire con altri sistemi per capire gli estremi entro i quali può continuare ad funzionare.

Tornando all'esempio dell'ospedale.....il processo in quattro stadi dell'FPP procederebbe in questo modo:

1. L'interaction è il processo di eco in cui i dottori esaminano il paziente, gli parlano e gli controllano i riflessi ai gomiti ed alle ginocchia ed usano tutti gli strumenti del metodo "Ti fa male se faccio questo?".
2. L'Inquest implica leggere le emanazioni dal paziente come le pulsazioni, la pressione sanguigna e le onde celebrali.
3. L'intervention consiste nel cambiare o stressare l'omeostasi del paziente, il comportamento, la routine o il livello di comfort per vedere ciò che avviene.
4. Per concludere l'induction che consiste nell'esaminare l'ambiente, i luoghi visitati dai pazienti prima che si ammalassero e come questi possano aver influenzato il paziente, così come le cose che sono state toccate, ingerite o inalate dal paziente.

Esercizi

1.22 Come potete vedere, il processo in quattro punti consente di investigare in modo più sulle approfondito le interazioni. Adesso potete provarlo. Spiegate come potete utilizzare il Four Point Process per sapere se un orologio funziona - e se funziona correttamente indicando l'ora esatta.

Cosa "hackerare"

Quando fate hacking su un qualsiasi oggetto dovete fissare delle regole. conoscere Avete bisogno del linguaggio e dei concetti per conoscere quello su cui state facendo hacking. Lo **Scope** è la parola che utilizziamo per descrivere nella sua interezza l'ambiente in cui operiamo, che comprende ogni interazione possibile con l'oggetto dell'hacking.

Nutri la mente: Classes e Channels

Nella terminologia professionale (utile anche per gli hacker), lo Scopo è composto di tre **Classes** che si suddividono in cinque **Channels**:

Class	Channel
Sicurezza Fisica (PHYSSEC)	Umano
	Fisico
Sicurezza dello spettro (SPECSEC)	Wireless
Sicurezza delle Comunicazioni (COMSEC)	Telecomunicazioni
	Reti di Dati

Le Classes non sono qualcosa di cui dovete preoccuparvi troppo, ma sono le etichette ufficiali usate attualmente nel campo della sicurezza industriale, governativo e militare. Le Classes definiscono un'area di studio, di investigazione o di operazione. Quindi se state cercando informazioni su qualunque materia è sempre opportuno conoscere i termini che i professionisti usano.

I Channels sono i termini comuni per i modi in cui interagite con gli asset. È comune fare hacking su un gadget utilizzando il processo in quattro punti su ogni canale. Sembra un sacco di lavoro, ma immaginate la soddisfazione di trovare un metodo di hacking nuovo che non è descritto in nessun manuale o meglio ancora che non è conosciuto nemmeno dal produttore!

Un **Asset** può essere qualsiasi cosa che ha un valore per il proprietario. Può essere un bene fisico come l'oro, le persone, progetti, computer portatili, il segnale telefonico a 900MHz ed i soldi; ma anche tutte le proprietà intellettuali come dati personali, una relazione, un marchio un processo economico, password e qualcosa detto sfruttando il segnale a 900MHz del telefono.

Le Dependencies sono le cose connesse all'asset che il proprietario non può fornire in modo indipendente. Chi utilizza un computer tipicamente non produce l'energia elettrica necessaria al suo funzionamento. Anche se non è verosimile che qualcuno interrompa la vostra fornitura elettrica, questo rientra ancora nel nostro Scope.

L'obiettivo della sicurezza è la **Separation** tra un asset, le sue dependencies ed ogni minaccia possibile attuabile nei suoi confronti.

Diciamo che la **sicurezza è una funzione della separazione**. Ci sono quattro modi in cui possiamo creare questa separazione:

1. Muovere gli asset per creare una barriera tra essi e le minacce.
2. Modificare la minaccia in uno stato in cui non può fare danno.
3. Distruggere la minaccia.
4. Distruggere l'asset. (Non consigliato!)

Quando facciamo hacking cerchiamo posti in cui le interazioni con l'obiettivo sono possibili e dove non sono possibili. Pensate alle porte in un palazzo. Alcune sono necessarie per i dipendenti; altre servono per i clienti. Alcune possono essere delle uscite di sicurezza. Altre possono essere perfettamente inutili.

Ogni porta, comunque, è un punto di interazione, che consente le operazioni necessarie e quelle non volute, come il furto. Quando arriviamo sulla scena come hacker, non possediamo ancora la conoscenza su questi punti di interazione, quindi li analizziamo con il Four Point Process.

Considerate l'esempio di un ragazzo che vuole essere completamente al sicuro da un fulmine. L'unico modo per raggiungere questo obiettivo (se si trova sulla terra) è vivere dentro una montagna al cui interno è assolutamente impossibile che arrivi un fulmine a causa della terra e della roccia.. che Supponendo che il ragazzo non abbia più montagna bisogno di uscire, si può dire che è sicuro al 100%. Ma se iniziasse a scavare buchi nella roccia allora il fulmine potrebbe trovare nuovi punti di accesso e la Porosity aumenterebbe. L'OSSTMM fa differenza tra essere **Safe** dai fulmini e di essere **Secure** dai fulmini. Semplicemente più Porosity è presente e più semplice è per un hacker modificare e prendere il controllo di quello che vuole.

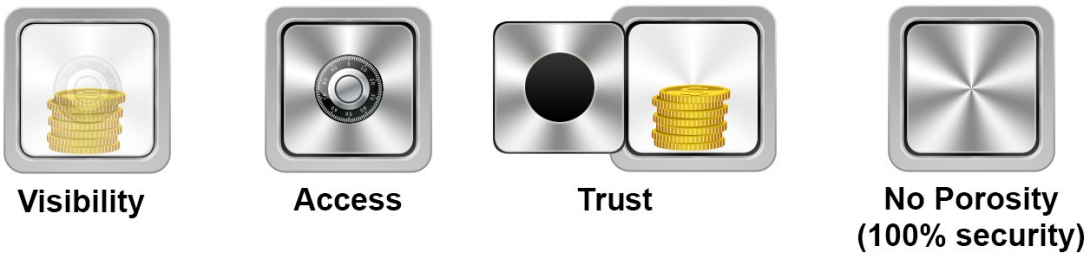

Figure 1.2: Porosity

Nutri la mente: Porosity

Ecco alcuni esempi che descrivono come pori possono essere individuati, classificati e definiti nel corso del processo di hacking.

Termine	Definizione
Visibility	Quando la polizia indaga su un crimine, vengono esaminati i mezzi, il movente e l'opportunità. Se un asset è visibile, può essere attaccato, ma se non è visibile non può essere preso di mira - sebbene possa essere scoperto. Alcuni professionisti della sicurezza dicono che l'**obfuscation** rappresenta una pessima misura di sicurezza poiché non protegge nulla, lo nasconde soltanto. Ma non è una cosa negativa soprattutto perché non sempre si ha bisogno di una risposta di sicurezza costante. Su di questo l'**OSSTMM** fornisce una perla di pensiero: *"La sicurezza non deve durare per sempre, ma abbastanza fino a che tutto il resto che può essere notato non sia sparito."*
Access	L'Access rappresenta il numero di posti differenti dove le interazioni possono avvenire dall'esterno dello Scope. Per un palazzo potrebbero essere le porte sulla strada oppure le finestre e per un server con accesso Internet potrebbero essere il numero di porte di rete aperte o i servizi disponibili su quel computer.
Trust	Il Trust si ottiene quando un'entità accetta liberamente interazioni da un'altra entità all'interno dello Scope. È per questo non chiedete a vostra madre un documento di identità quando viene ad abbracciarvi. Per la stessa ragione non sospettate che vi abbia avvelenato il cibo. Imparate a fidarvi delle cose nel vostro Scope. Se poi un giorno fosse rapita dagli alieni e sostituita (*come ne **L'invasione degli Ultracorpi***) e dovesse avvelenarvi il cibo, voi mangereste tutto senza alcun sospetto. Pertanto il trust è sia una falla di sicurezza sia un sostituto dell'autenticazione, la maniera in cui verifichiamo che qualcuno è chi ci aspettiamo che sia. Il Trust è un argomento strano perché è una cosa tipica dell'essere umano ed ha un valore notevole nella società. Senza trust non saremmo mai liberi di agire liberamente. Ma per lo stesso trust siamo facilmente presi in giro, ingannati, rapinati e crediamo alle menzogne. La ricerca sul trust dell'OSSTMM mostra che ci sono 10 ragioni per credere a qualcuno chiamate **Trust Properties** e se tutte e dieci le ragioni sono soddisfatte, allora possiamo fidarci senza alcuna preoccupazione. Ma la stessa ricerca mostra che la maggior parte delle persone ha bisogno di una sola condizione per concedere il trust ed ai veri paranoici e ai cinici ne bastano tre.

Risorse

La capacità di ricercare, imparare e pensare in modo critico sono le competenze chiave per un hacker. L'hacking, in realtà, è un processo creativo basato più sulla stile di vita che sugli insegnamenti. Non possiamo insegnarvi tutto quello che avete bisogno di sapere, ma possiamo aiutarvi a riconoscere cosa avete bisogno di imparare. Dal momento che la scienza avanza rapidamente, quello che insegniamo oggi potrebbe non essere rilevante

domani. È meglio per voi iniziare ad imparare come fa tipicamente un hacker, il che costituisce la parte principale dell'hacking e che vi distingue dagli **script kiddie** (un termine hacker che indica una persona che usa i tool senza sapere realmente come o perché funzionano).

Se, nel corso di questa lezione, leggi un termine od un concetto che non comprendi, è essenziale verificarlo, cercarlo nel vocabolario o in rete. Ignorare le parole nuove renderà più difficili le prossime lezioni. Vi è richiesto di indagare su un argomento e poi utilizzare le informazioni ricevute per completare gli esercizi nella lezione – ma le lezioni non vi spiegheranno come effettuare le ricerche. Quindi assicuratevi di spendere tutto il tempo che vi serve per imparare ad usare le risorse a vostra disposizione.

Libri

Potreste essere sorpresi dal fatto che non vi diciamo di ricercare tutto su Internet I libri rappresentano tuttora un valido strumento per imparare i fondamenti e la scienza fattuale di tutto quello che volete imparare. Volete saper qualcosa di informatica, tipo i dettagli hardware del vostro PC? Nulla vi aiuta di più che leggere un libro recente su questo argomento. Il problema principale dei libri di informatica è che possono diventare obsoleti molto rapidamente. Il segreto è comprendere le strutture fondamentali che sono al disotto dei dettagli. L'MS-DOS e Windows sono ovviamente differenti, ma sono entrambi basati sulla logica booleana su cui si sono basati i computer fin dai tempi in cui Ada, Contessa di Lovelace, scrisse il primo programma nel diciannovesimo secolo. I concetti di sicurezza e privacy possono essere cambiati negli ultimi 2500 anni, ma l'**Arte della Guerra** di Sun Tzu descrive principi fondamentali che sono validi ancora oggi. (A proposito, non vi è modo più rapido per mostrarsi **n00b** che citare Sun Tzu. Inoltre citare l'Arte della Guerra dimostra che non l'avete letto veramente poichè Sun Tzu dice di tenere la propria conoscenza un segreto).

Sebbene le informazioni dei libri potrebbero non essere aggiornate come le informazioni provenienti dagli altri mezzi di comunicazione, le informazioni dei libri sono tipicamente scritte meglio di quelle ricevute delle altre fonti. A volte sono anche molto più accurate. Uno scrittore che trascorre un anno a scrivere un libro controlla i fatti meglio di chi aggiorna un blog sei volte al giorno. (Guardate la sezione su Zine e Blog per maggiori informazioni).

Ma ricordate che accurato non significa imparziale. La fonte stessa di un autore potrebbe essere parziale. "I libri di storia sono scritti dai vincitori" (controllate questa citazione) e i politici e le norme sociali del tempo potrebbero impedire la diffusione di determinate informazioni. Questo accade tipicamente con i libri di testo scolastici che sono scelti con un processo politico e contengono solo le informazioni la cui conoscenza sia ritenuta "socialmente accettabile". Non pensate di avere trovato la verità assoluta perché l'avete letta in un libro. La verità è che chiunque può scrivere un libro e che ogni libro può contenere la versione della verità di chiunque.

Non prendete un libro ed abbandonate la sua lettura prima ancora di iniziare a leggerlo rendervi perché vi rendete conto di quanto è grande. Nessuno legge questi grandi libri affrontandoli dall'inizio alla fine. **Pensate a questi libri come se fossero delle pagine web preistoriche.** Apriteli ad una pagina qualsiasi ed iniziate a leggere. Se non capite qualcosa tornate indietro e cercate la spiegazione (oppure andate avanti per cercare qualcosa che abbia senso). Saltate da una pagina all'altra, in avanti ed indietro, così come fareste con i link di una pagina web. Questo tipo di ricerca non-lineare è spesso molto più interessante e soddisfacente per un hacker, poiché si tratta di soddisfare la vostra curiosità piuttosto che una lettura.

Infine chi legge libri sviluppa un'importante caratteristica, che è quella di scrivere bene. Questo è un grande vantaggio quando si sta cercando di capire e di partecipare a un nuovo argomento. E vi permette anche di acquisire credibilità con gli altri lettori, soprattutto per quelli in posizioni di autorità.

Riviste e Giornali

Riviste e giornali sono molto utili per fornire informazioni precise e puntuali. Anche se entrambi i tipi di pubblicazione possono essere molto avidi di dettagli. Dovete anche essere consapevoli che ogni rivista e giornale ha il proprio pubblico ed il proprio argomento, nonostante ogni dichiarazione che affermi l'essere "corretti e non di parte". Informatevi sull'argomento della pubblicazione: una rivista su Linux non è necessariamente una buona fonte di informazione su Microsoft Windows, perché Windows è una materia in conflitto con Linux (un sistema operativo concorrente) e i lettori delle riviste Linux vogliono francamente leggere della superiorità di Linux. Molte delle riviste specialistiche usano il **cherry picking,** la tecnica di evidenziare solo gli aspetti positivi di quanto descritto nella tematica della rivista oppure evidenziano solo gli aspetti negativi di quello di cui non si occupano.

Siate consapevoli delle possibili faziosità di una pubblicazione. Accade quando vi forniscono opinioni piuttosto che fatti oppure quando eludono i fatti per fare in modo di sostenere la loro visione o quando fanno in modo che non vi formiate una vostra opinione. Vagliate le fonti! Anche periodici che appaiono non di parte possono essere pieni di pareri e speculazioni, speculazioni è un modo elegante per dire "ipotesi plausibili", ma è più spesso solo semplici "supposizioni" da parte del giornalista.

C'è è una grande corrente di pensiero in ambito medico che vorrebbe che siano pubblicate tutte le sperimentazioni mediche e farmaceutiche (o almeno tutte le sperimentazioni finanziate con fondi pubblici), anche se queste sperimentazioni non hanno ottenuto i risultati sperati, questo per fare in modo che i medici possano fare scelte sempre più consapevoli su quale medicina e procedure utilizzare. Anche se attualmente le riviste mediche possono pubblicare i "fatti" che derivano dalle ricerche, i dettagli e le circostanze dietro quei fatti sono ancora oscuri. Questo è davvero importante quando voi trattate argomenti che si basano su specifiche cause. Il rapporto causa-effetto richiede che la causa preceda e sia la ragione dell'effetto.

Tra gli altri trucchi usati dai periodici (sia in modo involontario che di proposito) ci sono le cosiddette **prove aneddotiche**, ovvero opinioni pubblicate dalle persone come prove indipendentemente dal loro essere esperti della materia; ci sono anche le **prove autorevoli**, in cui gli addetti del settore sono presentati come esperti e forniscono il proprio parere, o esperti in un settore offrono la propria opinione in un altro settore in cui non hanno esperienza; ed infine ci sono le **speculazioni**, cioè ammantare di verità un qualcosa solo perché "tutti" credono che sia vero, anche se non c'è effettiva attribuzione a qualcuno di specifico.

Il modo migliore di trattare con l'accuratezza è di leggere tutto accuratamente. Se leggete qualcosa di interessante in una rivista, esaminate la questione in profondità. Esaminatene un aspetto e cercate conferme; dopo esaminatene un altro aspetto e cercate eventuali obiezioni. Alcune culture fanno questo usualmente. È parte della loro cultura verificare l'altra faccia della storia. Questo è un tratto culturale molto forte, specialmente se state cercando di garantire una democrazia di successo.

Esercizi

1.23 Cercate in Internet tre riviste online che trattano di hacking. Come le avete trovate?

1.24 Tutte è tre le riviste trattano specificatamente di hacking? Cosa altro offrono che possa essere utile in altri campi o per altre tematiche?

Nutri la mente: Speculazione

Il paragrafo che segue è preso da un articolo di giornale su una rapina. Potete trovare la speculazione? Annotate le aree su cui avete dubbi:

La Lake Meadow Bank and Mortgage Lender è stata rapinata martedì pomeriggio quando un uomo mascherato e armato di pistola è entrato pochi istanti prima della chiusura ed ha tenuto gli impiegati in ostaggio per un ora prima di fuggire su di un nuovo modello di SUV. Nessuno degli ostaggi è rimasto ferito.

Nessuno è riuscito a identificare l'uomo armato, cosa che porta la polizia a ritenere che si tratti di un professionista anche perché subito dopo la rapina, la macchina è stata vista dietro la banca dirigersi a sud verso la fitta foresta di Bluegreen Mountains. La polizia sta investigando su rapinatori esperti con precedenti penali e che abbiano rapporti con persone che vivono in zona.

Con una media di 57 furti alle banche riportati ogni giorno nel paese e la popolazione della Contea di Bluegreen che supererà le 50,000 unità entro il prossimo anno, questo potrebbe essere l'inizio di un'ondata di rapine nella zona. "Sembra l'inizio di una serie." ha riferito il commissario Smith.

Diventando più insensibili alla speculazione ed rimanendo funzionalmente ignoranti della distorsione dei dati statistici e dei risultati, tutte le nostre notizie future potrebbero venire da un singolo giornalista che specula su notizie in tempo reale. Nell'esempio sopra, c'è solo un fatto reale - una banca che è stata derubata nel pomeriggio di martedì. Ora, questo è quello che potrebbe apparire se cambiaste tutte le speculazioni per rendere tutto più ridicolo:

La Lake Meadow Bank and Mortgage Lender è stata rapinata martedì pomeriggio quando quello che sembra qualcuno mascherato da pollo è entrato pochi istanti prima della chiusura ed ha tenuto gli impiegati in ostaggio per oltre un decennio prima di fuggire su di in un mongolfiera a forma di pollaio. Nessuno degli ostaggi è rimasto ricoperto di piume.

Nessuno è riuscito a identificare il pollo, cosa che porta la polizia a ritenere che si tratti di un professionista del trasformismo oltre che un esperto aerostiere anche perché subito dopo la rapina, una mongolfiera è stata vista volare sopra la banca e dirigersi a sud verso la tundra dell'Antartide. La polizia sta ricercando esperti di travestimenti con l'hobby della mongolfiera,

Con una media di 57 furti alle banche riportati ogni giorno nel paese e l'industria degli aerostati che si aspetta vendite per oltre 47 fantastiliardi di dollari per il futuro, questo potrebbe essere l'inizio di un'ondata di rapine con mongolfiera. "Sembra l'inizio di una serie." ha riferito il commissario Gordon.

Visto l'uso spropositato di speculazioni e statistica in tutti i settori, è ovvio che questo modo di fare sia entrato con forza nel settore della sicurezza. Il termine comunemente utilizzato in queto settore è **FUD** che è l'acronimo per **Fear, Uncertainty, and Doubt**. La speculazione e l'analisi di rischi soggettiva sono usati nel settore della sicurezza per attirare l'attenzione di qualcuno a proprio vantaggio e vendere soluzioni di sicurezza. Sfortunatamente questo concetto si sposa molto molto bene con la grossolana paranoia della psiche umana e consente di sviluppare un torpore alla speculazione. Questo ha portato a soluzioni di sicurezza inappropriate, a sicurezza male applicata, a controlli di sicurezza reattivi e falsa fiducia nelle autorità. C'è un'evidente carenza di pensiero critico nella popolazione e questa carenza viene sfruttato sia dal settore commerciale che da quello criminale.

Motori di ricerca

Google è un motore di ricerca molto conosciuto, ma non è l'unico motore di ricerca esistente. Bing va molto bene con le ricerche formulate con semplici domande e Yahoo è affidabile per fare ricerche approfondite. Siate consapevoli che tutti questi servizi web vogliono sapere tutto quello che possono su di voi e probabilmente sanno molto più di quello che dovrebbero. Memorizzeranno le ricerche che effettuate ed i siti che visiterete dopo di queste.

> Ci sono motori di ricerca come Altavista e DuckDuckGo.com che potrebbero darvi un po' – oppure molto – anonimato il che potrebbe essere una cosa molto utile quando state cercando nei lati oscuri.

I siti web possono essere consultati mentre sono online e in genere anche molto tempo dopo che non lo sono più. tipicamente Tipicamente sono conservati sotto forma di **pagine cache**. Una cache Internet è una raccolta online di versioni passate di siti web o anche di siti web che sono stati oscurati. I motori di ricerca ed i siti di archiviazione mantengono queste informazioni in modo indefinito, il che nel linguaggio di Internet significa "per sempre". Questa è una cosa importante da ricordare prima di mettere qualsiasi cosa in Internet: questa non sarà cancellata. Mai. Dovreste cercare un link per una pagina cache. Google, per esempio, utilizzava un semplice link con l'etichetta "cache" accanto al classico link del risultato. Questo stile è stato modificato in un menù a tendina a destra del risultato in cui compare l'etichetta "cache" e potrebbe anche essere stato cambiato un'altra volta quando leggerete questa pagina.

Oltre ai motori di ricerca, ci sono anche cache pubbliche molto utili come l'**Internet Archive** che trovate all'indirizzo **http://www.archive.org**. Potete trovare le versioni cached nel corso degli anni di interi siti web, cosa molto utile per cercare informazioni che potrebbero essere "svanite".

Un nota finale sui siti web: non fidatevi di un sito web solo perché è proposto da un motore di ricerca. Molti attacchi hacker e virus si propagano visitando un sito web o scaricando programmi che appaiono innocui, salva schermo o altri file condivisi. Vi potete tutelare evitando di scaricare programmi da siti non affidabili e facendo in modo che il vostro browser sia eseguito in una **sandbox**. E achwe questo potrebbe non essere sufficiente. Un browser è una finestra su Internet e come ogni finestra, le schifezze potrebbero finire all'interno per il solo fatto che la finestra è aperta. Ed a volte non ve ne accorgerete fino a quando non sarà ormai troppo tardi.

Esercizi

1.26 Ci sono molti motori di ricerca. Alcuni vanno bene per raggiungere l'**Invisible Web**, aree di Internet in cui per molti motori di ricerca è difficile trovare informazioni, come alcuni database riservati. Un buon ricercatore sa come usarli tutti. Alcuni siti web sono specializzati nel tracciare i motori di ricerca. Quindi, cercate cinque motori di ricerca che non avete mai usato o di cui non avete nemmeno sentito parlare prima.

1.27 Ci sono anche motori di ricerca che ricercano negli altri motori di ricerca. Sono chiamati **meta search engines**. Travatene uno.

1.28 Ricercate "security and hacking" (virgolette comprese) ed annotate le prime tre risposte. Come variano i risultati quando NON inserite le virgolette?

1.29 C'è molta differenza nel cercare per argomento e nel cercare una parola od una frase. Nell'esercizio precedente avete cercato una frase. Adesso cercate un'idea.

Per fare questo **pensate ad una frase che potrebbe essere nella pagina che state cercando**. Se volete che un motore di ricerca fornisca una lista deklle riviste che parlano di hacking, non andreste lontano cercando "una lista di riviste online che parlano di hacking." Non sono molte le pagine web che contengono questa frase! Otterrete qualche risultato, ma non molti.

Invece, quello che dovete pensare è "se io realizzassi una rivista di hacking, quale potrebbe essere una frase tipica contenuta in questa rivista?". Inserite le parole e le frasi seguenti in un motore di ricerca e scoprite chi fornisce I migliori risultati per la vostra ricerca:

1. la mia lista di riviste preferiti sull'hacking
2. lista di riviste di hacking professionale
3. risorse per hacker
4. riviste di hacking
5. lista risorse riviste sicurezza hacking

1.32 Trovate la versione più vecchia del sito web di Mozilla sull'Internet Archive. Per farlo dovete cercare "www.mozilla.org" sul sito http://www.archive.org.

1.33 Adesso per mettere tutto insieme, diciamo che vogliate scaricare la versione 1 del browser Netscape. Usando i motori di ricerca e l'Internet Archive, vedete se riuscite a localizzare trovare e scaricare la versione 1.

Siti web ed Applicazioni web

Lo standard de facto per la condivisione delle informazioni attualmente passa attraverso un browser web. Sebbene classifichiamo tutto ciò che vediamo come "il web," sempre più spesso quello che usiamo realmente sono "applicazioni web", in quanto non tutto quello che c'è sul web è un sito. Se controllate la vostra mail usando un browser, oppure ascoltate musica utilizzando un servizio web, allora state usando un'applicazione web.

A volte le applicazioni web richiedono privilegi. Questo significa che avete bisogno di una login e di una password per avere accesso. Avere accesso quando si ha il diritto legale di accedere è detto avere i **privilegi**. Fare hacking di un sito web per cambiare una pagina può significare che avete avuto accesso, ma poiché non avete diritto di essere lì, non avete un accesso privilegiato. Continuando ad usare il web, capirete che molti posti vi lasciano accedere ad aree privilegiate per errore.

Quando vi capita qualcosa del genere è una buona abitudine riferire il tutto all'amministratore del sito. Tuttavia, attenzione ai possibili risvolti legali. Purtroppo, molti amministratori non gradiscono rapporti vulnerabilità non richiesti.

Per contribuire a rendere Internet un posto più sicuro e nello stesso tempo proteggere voi stessi, dovreste valutare l'utilizzo di un servizio di **anonymizer** (ad esempio, Tor o remailer anonimi, ecc.) per inviare le segnalazioni sulle vulnerabilità a questi amministratori. Ma siate consapevoli che tutte le tecnologie di anonimizzazione hanno i loro punti deboli e potreste non essere così anonimi come credete di essere! (Più di un hacker ha imparato questa lezione nel peggiore dei modi.)

Esercizi

1.34 Usate un motore di ricerca per cercare siti che hanno fatto l'errore di fornire privilegi di accesso a tutti. Per fare questo, cercheremo le cartelle che ci permettono di elencare il loro contenuto (un "directory listing"), qualcosa che tipicamente non dovrebbe essere consentito. Per far questo useremo dei trucchi nei comandi di Google all'indirizzo http://www.google.com. Inserite questo nel campo di ricerca:

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

Scorrete rapidamente i risultati e trovate quelli che appaiono come directory listing. Questo modo di fare ricerche è noto come Google Hacking.

1.35 Potete trovare altri tipi di documenti in questo modo? Trovate altri tre directory listing che contengono file .xls, .doc ed .avi.

1.36 Ci sono altre opzioni di ricerca come "allintitle:"? Potete trovarle?

Zines

Le zines, note anche come **e-zines**, sono le discendenti delle **fanzines**: piccole riviste, tipicamente gratuite, con limitata distribuzione (meno di 10,000 lettori) e spesso prodotti da giornalisti non professionisti. Le fanzines sono stampati su carta. Le zines su Internet, come il famoso **2600** o la web zine **Phrack**, sono scritte da volontari; questo significa che spesso i produttori non editano il contenuto per gli errori non-tecnici. A volte il loro linguaggio forte può essere una sorpresa per chi non è familiare con questo genere.

Le zines hanno argomenti forti e secondi fini e tendono ad essere molto supponenti. Tuttavia, sono anche più propensi a mostrare e discutere di tutte le sfaccettature dei problemi, dal momento che di solito non si preoccupano o non devono compiacere gli inserzionisti e abbonati.

Esercizi

1.37 Cercate nel web tre zine che trattano di hacking. Come avete trovato queste zine?

1.38 Perché avete classificato questi contenuti come zine? Ricordate, non basta che siano vendute come tali o che abbiano "zine" scritto nel titolo per essere effettivamente delle zine.

Blog

Un **blog** può essere considerato l'evoluzione delle zine, tipicamente con uno staff composto da una sola persona. I blog vengono aggiornati più spesso di quanto lo siano zine e pubblicazioni scritte e creano delle comunità legate a tematiche molto serie. È importante leggere sia i commenti che i post. Nei blog la risposta è immediata e ricca di opinioni ancor più che nelle zine, con commenti da ogni posizione. Questo è uno dei loro punti di forza.

Ci sono milioni di blog in Internet, ma solo una piccola percentuale è attiva. Le informazioni sono comunque ancora disponibili per quasi tutti.

Esercizi

1.39 Cercate in Internet tre blog sull'hacking.

1.40 A quali gruppi o comunità sono associati?

1.41 Ci sono nei blog tematiche su sicurezza, forze dell'ordine o accademiche?

Forum e Mailing List

I **Forums** e le **mailing list** sono media sviluppati collettivamente, sono una cosa tipo registrare conversazioni ad una festa. Dovete essere sempre scettici su quello che ci leggete. Le conversazioni spesso possono cambiare focus molto rapidamente, molto di quello che viene detto sono pettegolezzo , alcune persone si mettono a fare **trolling**, potrebbe scoppiare una **flame war** e quando la festa è finità nessuno è certo di chi ha detto cosa. I forum e le mailing list sono simili, perché consentono in molti modi alle persone di fornire informazioni inesatte – a volte anche in modo intenzionale – e ci sono sistemi per fornire contributi anonimi oppure fingendosi qualcun altro. Siccome gli argomenti cambiano spesso, per avere tutte le informazioni è importante leggere tutto il thread dei commenti e non solo i primi.

Potete trovare forum praticamente su ogni argomento e molti riviste online e quotidiani offrono forum ai propri lettori in cui poter fornire commenti agli articoli pubblicati. Per questo i forum i forum hanno un valore inestimabile se si vuole ottenere più di un parere su un articolo; non importa quanto una persona abbia gradito l'articolo, ci sarà sempre qualcuno a cui non piacerà.

Ci sono molte mailing list su specifici argomenti, ma possono essere difficili da trovare. A volte la miglior tecnica per trovarli essere può esser quella cercare le informazioni su un argomento in particolare per poi cercare una mailing list di una comunità che se ne occupa.

Come hacker, la cosa più importante per voi è che molti forum e mailing list non possono essere ricercate tramite i motori di ricerca. Mentre è possibile trovare informazioni su liste e forum attraverso un motore di ricerca, potrebbe non essere possibile trovare informazioni sul contenuto di uno specifico post. Questa informazione fa parte del web invisibile perché contiene dati che possono essere cercati solo direttamente sul sito web o sul forum.

Esercizi

1.42 Trovate due forum hacker. Come li avete trovati?

Potreste determina la tematica o gli argomenti di specialità di questi siti web?

I argomenti del forum riflettono le tematiche del sito web che lo ospita?

1.43 Trovate due mailing list su hacking o sicurezza.

Chi è "l'owner" di queste liste? Potete vedere I membri della lista? (Potreste esser necessario capire quale è l'applicazione con cui la lista è stata sviluppata e poi cercarne su Internet i comandi nascosti che consentono di visualizzare la lista degli iscritti.)

Su quali liste vi aspettate informazioni più corrette e meno influenzate dalle opinioni? Perché?

Newsgroups

I **Newsgroups** esistono da molto tempo. C'erano newsgroup da molto tempo prima che esistesse il World Wide Web. Google ha acquistato tutto l'archivio dei newsgroups ed ha messo tutto online all'indirizzo http://groups.google.com. I newsgroups sono come gli archivi mailing list, ma senza mail. Le persone postavano direttamente lì come fanno oggi con i commenti su un sito web. Troverete post dai primi anni 90 in poi.

> Come gli archivi web gli archivi dei gruppi possono essere importanti per trovare chi ha realmente dato vita a un'idea o ha creato un prodotto. Sono anche utili per trovare informazioni oscure che non potreste mai trovare in un sito web.

I newsgroup non sono usati meno oggi di quanto non lo fossero anni fa, prima che il web diventasse il canale principale per condividere informazioni. Tuttavia, non sono cresciuti ulteriormente poiché la loro popolarità è stata sostituito da uovi servizi web come blog e forum.

Esercizi

1.44 Usando Google's groups, cercate il più vecchio post sull'hacking.

1.45 Trovate altri modi per utilizzare i newsgroup. Ci sono applicazioni che potete utilizzare per leggere i newsgroup?

1.46 Quanti newsgroup potete trovare che parlano di hacking?

1.47 Potete trovare una lista attuale di tutti i vari newsgroup attualmente esistenti?

Wiki

I **Wiki** sono un fenomeno recente su Internet. Wikipedia (www.wikipedia.org) è probabilmente il più famoso, ma ve ne sono molti altri. Come molti altri siti, i wiki sono realizzati da comunità. Alcune fonti affermano che i wiki non sono affidabili perché sono aggiornati da amatori o appassionati. Ma questo vale per i libri, le mailing list, le riviste e tutto il resto. Quello che è importante sapere è che gli esperti non sono l'unica fonte di grandi idee o di informazioni valide. Come afferma l'OSSTMM, i fatti derivano da piccoli passi che verificano idee e non da grandi salti di scoperta. Ecco perché i wiki sono grandi fonti di idee sia professionali che amatoriali che pian piano si verificano reciprocamente.

I wiki spesso discutono molti aspetti di un argomento e permettono di seguire come l'informazione è argomentata, confutata, raffinata e cambiata attraverso la cronologia delle modifiche. Quindi ci sono grandi posti per scavare nell'informazione, ma spesso è necessario andare nel sito wiki per fare le ricerche.

Esercizi

1.48 Cercate "Ada Lovelace". Vedete risultati da wiki?

1.49 Andate su Wikipedia e ripetete la ricerca. Guardate l'articolo su di lei. Era incluso nella vostra ricerca precedente?

1.50 Verificate la cronologia delle modifiche della pagina wiki e guardate le informazioni che sono state corrette e variate. Che tipo di informazioni sono state cambiate? C'è qualcosa che è stato cambiato e poi riportato alla versione precedente? Adesso scegliete un attore o un cantante famoso ed andate sulla sua pagina Wikipedia e verificate le modifiche. Notate differenze?

1.51 Trovate un altro sito wiki e cercate nuovamente. Ci sono risultati che appaiono anche nella prima ricerca fatta?

Social Media

Usate un sito di social media? Oppure più di uno? Come hacker dovete conoscere i siti social popolari al momento. Cosa dire di quelli che non sono più popolari come erano in passato? Esistono ancora e nella maggior parte dei casi tutti i loro dati sono ancora disponibili.

Questo significa che esiste un enorme deposito di informazioni su di noi, molte delle quali abbiamo disseminato liberamente. E sarà lì praticamente per sempre.

I siti di social media hanno spesso sotto gruppi o comunità di interesse. I siti con tematiche di professionisti hanno gruppi di cybersecurity ed i siti con tematiche underground tipicamente hanno gruppi hacker. Sui siti di professionisti si è portati (come tutti gli altri) ad utilizzare il nome reale. Nei siti hacker, non tanto.

Cosa più importante di tutte: usate il nome reale sui siti di social media oppure usate uno "pseudonimo?" Ci sono modi con cui il vostro pseudonimo può essere ricondotto al vostro vero nome? Molte persone non si rendono conto che stanno usando il loro pseudonimo e quindi capita che per errore o di proposito postino il loro vero nome, l'indirizzo, la città, la scuola, il lavoro e così via, proprio mentre usano lo pseudonimo. Se un altro hacker fa DoXing sul vostro pseudonimo a causa di questi piccoli errori potrebbe scoprire facilmente chi siete. Se utilizzate uno pseudonimo per essere anonimi conosce con quelli che non vi conoscono, allora cercate di prendere ogni precauzione e fate di tutto perchè restiate tali. Se ne avete più di uno non confondete MAI i vostri pseudonimi .

Esercizi

1.52 Cercatevi. Ottenete qualche risultato (che riguardi effettivamente voi)? Tra i risultati ve ne sono di provenienti da social network?

1.53 Andate su un social media che utilizzate. Non effettuate il login, ma ripetete la ricerca come se foste un altro utente. Quanto riuscite a trovare di voi stessi?

1.54 Andate su un social media che usa un vostro amico. Ancora, non effettuate il login se avete un account. Cercate il vostro amico. Quanto potete leggere su di lui?

Chat

La **Chat**, che può apparire sotto forma di **Internet Relay Chat (IRC)** e **Instant Messaging (IM)**, è un modo davvero diffuso di comunicare.

> Come fonte di ricerca, la chat è estremamente fluida in quanto si interagisce in tempo reale. Alcuni potrebbero essere amichevoli ed altri scortesi. Alcuni potrebbero essere degli innocui giocherelloni, ma altri potrebbero essere dei pericolosi bugiardi. Alcuni saranno intelligenti e vorranno condividere informazioni, altri saranno totalmente disinformati, ma non meno volenterosi nella condivisione dei primi. Potrebbe essere difficile capire chi è chi.

Comunque, una volta che sarete a vostro agio con certi gruppi e canali, potreste essere accettati nella comunità. Vi sarà concesso di chiedere sempre di più e imparerete di chi vi potete fidare. Alla fine potrete avere accesso agli ultimissimi exploit (noti come **zero day**, significa nel senso che sono stati scoperti proprio in quel momento) ed amplierete le vostre conoscenze.

Esercizi

1.55 Trovate tre programmi di instant messaging. Cosa li rende differenti? Possono essere usati per scambiare messaggi tra loro?

1.56 Scoprite cos è IRC e come vi ci potete connettere. Potete scoprire la rete del canale ISECOM? Una volta collegati alla rete, come vi unirete al canale isecom-discuss?

1.57 Come sapete quali canali esistono in un rete IRC? Trovate tre canali di sicurezza e tre canali hacker. Potete entrare in questi canali? Chi parla sono persone o bot?

P2P

Il **Peer to Peer**, anche noto come **P2P**, è una rete all'interno di Internet. A differenza delle classiche reti client/server, dove ogni computer comunica attraverso un server centrale, i computer in una rete P2P comunicano direttamente tra di loro. Molte persone associano il P2P con lo scaricare mp3 e film pirata sul famigerato vecchio Napster. Ma ci sono molte altre reti P2P – sia per scambio di informazioni, che come mezzo per condurre ricerche sulla condivisione delle informazione distribuite.

Il problema con le reti P2P è che, mentre si può trovare praticamente di tutto in esse, alcuni contenuti sono presenti nella rete illegalmente. Altre cose sono disponibili in maniera legale ma le società che le producono credono che non dovrebbero esserci e sono felici di chiedere i danni ai proprietari di ogni **Internet gateway** da cui avvengono i download.

Al momento non vi è chiarezza se la responsabilità sia di chi possiede l'accesso ad Internet da cui viene fatto il download o se la polizia debba perseguire chi effettivamente effettua il download. Sarebbe come dire che se la vostra auto quando viene usata per commettere un crimine siete voi che finite in galera e non chi guidava la macchina. Le regole di Internet in questo momento non sono equilibrate né giuste, quindi fate parecchia attenzione!

Sia che siate o meno il genere di persona che rischia a scaricare proprietà intellettuale, non vi sono dubbi che le reti P2P possono essere una risorsa essenziale per cercare informazioni. Ricordate: non vi è nulla di illegale nelle reti P2P in quanto tali – ci sono una marea di file che sono disponibili per essere distribuiti liberamente sotto diverse licenze – ma ci sono anche un sacco di file che sono in queste reti e non dovrebbero essere lì. Non abbiate paura di usare le reti P2P, ma siate consapevoli dei pericoli e di cosa state scaricando.

Esercizi

1.58 Quali sono le tre reti P2P più popolari e più utilizzate? Come lavora ognuna di esse? Di che programma avete bisogno per utilizzarle?

1.59 Ricercate il protocollo di una di queste reti P2P. Come funziona e come rende il download più veloce?

1.60 Cercate le parole "download Linux." Potete scaricare una distribuzione (o distro) di Linux usando il P2P?

Certificazioni

Esiostono le certificazioni OSSTMM Security Tester e Security Analyst, vari tipi di certificazioni "hacker", certificazioni basate su una versione di "best practices" od altre e certificazioni con tutti i tipi di abbreviazioni e sigle.

Perché vi delle dovreste interessare alle certificazioni? Perché possono essere conseguite a qualsiasi età, perché non avete bisogno della laurea per conseguirle e perché vi possono mettere nella posizione della persona a cui si chiede consiglio piuttosto di quella che lo chiede.

Il problema con le certificazioni basate su best-practices è che esse cambiano spesso, in quanto *best practices* è solo un altro modo di dire "quello che tutti stanno facendo adesso". Spesso quello che tutti fanno è sbagliato questa settimana e sarà ancora sbagliato nella versione aggiornata della settimana successiva.

Poi ci sono le certificazioni basate sulla ricerca, basate su indagini valide e ripetibili fatte nei confronti del comportamento umano e dei sistemi. Non c'è bisogno di dire che la nostra organizzazione di riferimento, ISECOM, ricade esattamente nella sfera delle authority per le certificazioni basate sulla ricerca. Sia da ISECOM o da qualunque altro ente, controllate sempre che le certificazioni siano basate sulle competenze, sulle analisi o che siano certificazioni di **applied knowledge** che vi permettono di provare che potete fare quello che avete imparato. Sarà utile quando dovrete farlo realmente.

Seminari

Seguire seminari è un ottimo modo di ascoltare la teoria spiegata nel dettaglio e guardare le competenze in azione. Anche i seminari su specifici prodotti sono utili da seguire per capire come un prodotto dovrà essere utilizzato, tenendo ben presente che l'evento è comunque parte del piano di marketing e che il vero obiettivo di chi presenta è vendere.

Saremmo negligenti se non dicessimo che possiamo portare Hacker Highschool Seminars in varie località per presentare qualsiasi lezione disponibile. I seminari sono fatti da hacker professionisti che parlano agli studenti di hacking e di diventare hacker, sia degli aspetti positivi che di quelli negativi. Questi seminari trattano chi sono gli hacker partendo dal lavoro contenuto nella ricerca **Hacker Profiling Project**, un progetto di collaborazione con le Nazioni Unite che indaga su chi sono gli hacker e perché colpiscono. Inoltre scoprirete il lato luminoso dell'hacking e comprenderete che l'hacking non è sempre qualcosa di oscuro.

Una delle cose più importanti che possiamo insegnarvi a trovare il metodo per essere intellettualmente curiosi e intraprendenti come un hacker. Gli hacker hanno successo in quello che fanno perché sanno come insegnare a se stessi, andando oltre le lezioni disponibili ed imparando le competenze di cui hanno bisogno per andare oltre.

Vi invitiamo a chiedere ai vostri genitori ed insegnanti per sapere come dare una mano ed iniziare un capitolo Hacker High School presso la vostra scuola. Contattate ISECOM per maggiori informazioni.

Ulteriore Studio

Adesso dovreste far pratica fino a diventare dei veri maestri della ricerca. Più bravi diventerete e più informazioni troverete velocemente, più imparerete velocemente. Ma fate attenzione a sviluppare un occhio critico. Non tutte le informazioni sono vere.

> Ricordate sempre di chiedervi perché qualcuno dovrebbe mentire? C'è denaro in gioco nell'essere disonesto o mettendo in giro una voce o una storia. Da dove arrivano i fatti? E, cosa più importante di tutte, qual è l'obiettivo?

Come tutto l'hacking, la ricerca include un ambito. Questo è molto importante quando leggete le statistiche, come la matematica che usa percentuali, frazioni e probabilità. Va valutato sempre quale era il campo di applicazione e quale ambito deve essere applicato. Un esempio classico di questo sono le statistiche su crimine o sanità prese su solo un campione di popolazione e solo in una piccola parte della nazione. Se il 10% di 200 persone di una città ha un problema, questo non implica che il 10% dell'intera popolazione abbia lo stesso problema. Quindi siate furbi quando leggete un'informazione, così come dovete esserlo quando la cercate. Comprendere l'ambito dell'informazione fa sempre una grande differenza!

Per aiutarvi ad essere ricercatori migliori per il programma Hacker Highschool, qui ci sono altri argomenti e termini che dovrete approfondire:

Meta Search

The Invisible Web

Google Hacking

How Search Engines Work

The Open Source Search Engine

The Jargon File

OSSTMM

Le certificazioni 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)

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.