Hacker Highschool
SECURITY AWARENESS FOR TEENS

LES 1
BEVEILIGINGSBEWUSTZIJN VOOR TIENERS

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Informatie over de Gebruiksvoorwaarden

De lessen en werkboeken van het Hacker Highschool (HHS) project zijn beschikbaar onder de volgende door ISECOM gestelde voorwaarden:

Alle informatie uit het HHS-project mag, niet-commercieel, gebruikt worden voor en door basisschool-leerlingen en studenten van middelbaar en hoger onderwijs. Dit materiaal mag niet worden gereproduceerd voor (door-)verkoop in welke vorm dan ook. Gebruik van dit materiaal in een klas, cursus, training, kamp of andere georganiseerde vorm van kennisoverdracht waarvoor geld wordt gevraagd is expliciet verboden zonder een licentie. Om een licentie te regelen kunt u het onderdeel LICENSE bezoeken op de website van de Hacker Highschool, www.hackerhighschool.org/license.

Het HHS-project is een leermiddel en, zoals met elk leermiddel, de docent/trainer bepaalt in grote mate het effect van het leermiddel. ISECOM kan geen aansprakelijkheid aanvaarden voor de positieve of negatieve gevolgen van het gebruik van dit materiaal en de daarin opgenomen informatie.

Het HHS-project is een initiatief van de open community, en wanneer u de resultaten van onze inspanning waardevol genoeg vindt om het te gebruiken, vragen we u uw steun te betuigen door:

- de aankoop van een licentie;
- een donatie
- ons te sponsoren.

Op al het werk berust copyright van ISECOM, 2004.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Inhoudsopgave

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Auteurs

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Vertaald door:

Raoul Teeuwen

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

1.0 Introductie

Welkom bij het Hacker Highschool programma! Dit programma is zo opgezet dat het je veelzijdigheid en vindingrijkheid aanmoedigt. De rode draad van het lesmateriaal speelt in op je nieuwsgierigheid naar het hacker-zijn, en zal je hacker-vaardigheden stapsgewijs verbeteren op een manier dat je ze op een verantwoorde manier kunt gebruiken om problemen op gebied van beveiliging en privacy te doorzien en om je eigen omgeving goed te beveiligen.

Hacken is opwindend omdat het illegaal kan worden toegepast om op andere computers in te breken. Wij willen je laten zien dat het echter zeker zo opwindend kan zijn als je je hack-vaardigheden gebruikt om anderen te wijzen op gaten in de beveiliging en om die te publiceren zonder met justitie in aanraking te komen. Als burger van de meeste landen is het niet alleen je recht, maar zelfs je plicht, problemen op gebied van beveiliging en privacy te melden bij de juiste organisatie(s). Dat doe je dan niet omdat je dat kunt, maar omdat vele anderen het niet kunnen. Je helpt zo hen die zichzelf niet kunnen helpen. Dit is wat zogenaamde 'watchdog groepen' doen. Dit is wat jij gaat leren te doen.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

1.1 Bronnen

Deze les leert je leren een zeer belangrijke vaardigheid voor een hacker. Hacken, het echte werk, is een creatief proces dat meer neerkomt op een manier van leven dan het volgen van wat lessen. We kunnen je niet alles leren wat je moet weten, maar we kunnen je wel helpen te herkennen wat je moet leren. Dit komt ondermeer door de continue ontwikkelingen in de wereld van computers. Wat we je vandaag leren, kan morgen al niet meer relevant zijn. Dus is het beter als je in gaat zien hoe een hacker denkt en leert, omdat dat je zal onderscheiden van de script kiddies (personen die hack-tools gebruiken zonder te weten hoe en waarom ze werken).

In het lesmateriaal zul je woorden en begrippen tegenkomen die je nog niet snapt; je zult het internet of een bibliotheek moeten gebruiken om uit te zoeken wat ze betekenen. Als je een woord of onderwerp niet snapt zul je echt even uit moeten zoeken wat het betekent. Door eroverheen te stappen is de kans groot dat je later lesmateriaal ook niet snapt. In andere werkboeken kan je de vraag krijgen om over een onderwerp informatie op te zoeken op het internet; die informatie heb je dan nodig om de oefeningen in het werkboek te maken maar in de werkboeken zal niet worden uitgelegd hoe je de informatie op internet moet opzoeken. Het werkboek dat je nu leest is het enige uit de serie waarin wordt uitgelegd hoe je goed onderzoek doet. Het is daarom verstandig om zoveel tijd te nemen als je nodig hebt om goed te begrijpen hoe je goed onderzoek doet en waar je je informatie vandaan kunt halen.

Beperk jezelf niet tot computers, hacken of het internet. Goede hackers zijn veelzijdig en creatief. Veel van hen zijn schilders, schrijvers en ontwerpers. Hack-vaardigheden kunnen ook worden toegepast op andere gebieden, zoals Politieke Wetenschap (bekijk The Prince van Machiavelli als voorbeeld).

Naast je interesse voor andere gebieden, helpt het ook als je weet of leert hoe (andere) bedrijven werken. Door boeken te lezen op gebieden uiteenlopend van psychologie tot science fiction wordt je een veel betere en veelzijdige hacker. Bedenk dat het er bij hacken om gaat uit te vinden hoe iets werkt, los van hoe iets is ontworpen. Door die manier van werken ben je in staat gaten in de beveiliging, kwetsbaarheden en lekken te vinden.

1.1.1 Boeken

Boeken zijn een geweldige bron als je de basis en feiten wil leren van/over een voor jou nieuw onderwerp waarin je je wil inlezen. Wil je meer weten over de basis van een wetenschap, bijvoorbeeld over de details van je PC? Niets zal je beter helpen dan er een aktueel boek over te lezen.

Het grootste probleem met boeken over computers, is dat ze zo snel verouderen. Het geheim zit hem erin dat je moet leren de (stabielere) structuren te zien die aan de basis liggen, en die verstopt zitten onder het dunne laagje details. MS-DOS en Windows verschillen duidelijk van elkaar, maar beiden zijn gebaseerd op Booleaanse logica waarmee alle computers werken sinds Ada, gravin van Lovelace, het eerste computer-programma schreef in de negentiende eeuw. Bezorgdheid op gebied van beveiliging en privacy zijn wellicht anders dan 2.500 jaar geleden, maar de basisprincipes zoals die in The Art of War van Sun Tzu zijn beschreven, zijn nog steeds toepasbaar.

Ook al is niet alle informatie in een boek zo aktueel als informatie van andere bronnen, je zult merken dat informatie uit boeken vaker juist is dan informatie uit andere bronnen. Een

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

schrijver die een jaar aan een boek werkt zal zijn feiten beter controleren op juistheid, dan iemand die zes keer per dag zijn weblog bijwerkt. (Zie paragraaf 1.1.3 Zines en Blogs voor meer informatie.) Maar bedenk ook dat 'juist' niet hetzelfde is als objectief/onbevooroordeeld.

Het is niet nodig zelf een bibliotheek aan te leggen, maar mogelijk wil je aantekeningen in de kantlijnen zetten of op een andere manier aandacht vestigen op interessante dingen die je leest, en dit kan alleen in je eigen boeken.

Tot slot: kijk niet naar een boek en geef het dan al op, alleen omdat het een dik of moeilijk boek lijkt. De meeste van die dikke papierbundels die je om je heen ziet zijn niet van voor naar achteren gelezen. Bekijk ze als prehistorische webpagina's. Sla er één open op een willekeurige pagina en begin te lezen. Als je iets niet snapt, blader dan terug en ga op zoek naar de uitleg die je nodig hebt (of blader vooruit naar informatie die je wel snapt). Spring zo door het boek, voorwaarts en achterwaarts, net zoals je op het internet van link naar link zou klikken. Deze manier van lezen is voor hackers vaak veel leuker, omdat het meer uitgaat van ontdekken en nieuwsgierigheid, dan van lezen.

1.1.2 Tijdschriften en kranten

Het gebruik van tijdschriften en kranten raden we je van harte aan om aan duidelijke, actuele informatie te komen. Echter, tijdschriften gaan vaak niet erg diep in op details en beperken zich tot aspecten waarvan ze denken dat de lezers ze interessant vinden. Dit is voor een hacker belangrijk om te beseffen social
engineering en met name het kraken van wachtwoorden, is makkelijker als je veel weet van pop-cultuur maar je moet wel weten dat pop-journalistiek niet altijd staat voor 'grondige journalistiek'.

Waar je ook op moet letten is het thema van een tijdschrift. Een Linux-tijdschrift zal vooral kritisch zijn richting Microsoft Windows, omdat dat een strijdig thema is en omdat het merendeel van hun lezers dat willen lezen.

De beste manier om deze beperking van tijdschriften te overkomen is door veel verschilende tijdschriften te lezen. Als je iets interessants leest in een tijdschrift, zoek dan naar meer informatie over dat punt. Stel je voor dat je het gelooft, en ga op zoek naar informatie die bevestigt wat je hebt gelezen. Doe vervolgens alsof je het niet gelooft, en ga op zoek naar informatie met argumenten dat het niet klopt.

Oefening:
A. Ga op het internet op zoek naar 3 tijdschriften op gebied van beveiliging.

B. Hoe heb je deze tijdschriften gevonden?

CGaan alle 3 de tijdschriften over computer-beveiliging?

1.1.3 Zines en Blogs

Zines zijn kleine, vaak gratis tijdschriften met een kleine oplage (minder dan 10.000 lezers) en worden vaak gemaakt door hobbyisten en amateur-journalisten. Zines, zoals het beroemde 2600 zine of Phrack Hacking web zine, zijn geschreven door vrijwilligers en ze worden vaak

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

niet door redacteuren gecorrigeerd op taalgebruik. Sommige zines zijn daarom taai om doorheen te komen als je nog niet gewend bent aan het taalgebruik. Zines beperken zich vaak tot een heel specifiek thema en de informatie is sterk gekleurd door de mening van de schrijver.
Echter, je zult in zines vaker een verhaal van beide kanten horen, omdat de schrijver en uitgever van de Zine zich niet druk hoeft te maken over de mening van adverteerders of abonnees.

Blogs/weblogs zijn een moderne vorm van het zine. Blogs worden vaker bijgewerkt en maken gebruik van communities om zich te beperken tot een beperkt thema. Net als zines, echter, kan iedereen kritiek uiten op een verhaal en een andere mening uiten. Bij blogs is het net zo belangrijk om de *reacties* op een bericht te lezen, als dat het belangrijk is om het bericht *zelf* te lezen.

Oefeningen:

A. Zoek op het internet naar 3 zines met betrekking tot computer beveiliging.

B. Hoe vond je deze zines?

C. Waarom vind je dat elk van hen een zine is? Bedenk dat het feit dat ze het een zine noemen of omdat zine in de naam staat, nog niet wil zeggen dat het een zine is.

D. Zoek op het internet naar 3 blogs over computer-beveiliging.

E. Welke communities zijn er mee gerelateerd?

1.1.4 Forums en Mailing Lists

Forums en mailing lists zijn gemeenschappelijk ontwikkelde media, vergelijkbaar met de opnames van een serie gesprekken tijdens een feest. Op een feest verandert het onderwerp van het gesprek vaak, veel van wat gezegd wordt betreft geruchten en, als het feest over is, weet niemand meer zeker wie nu wat gezegd heeft. Forums en mailing lists zijn vergelijkbaar omdat er veel manieren zijn voor mensen om onjuiste of onvolledige informatie te delen soms met opzet en er zijn manieren om anoniem bij te dragen. En het is, omdat het onderwerp en thema snel kan veranderen, van belang om alle bijdrages te lezen en niet alleen de eerste, om de beste informatie te verkrijgen.

Je kunt forums vinden over bijna elk onderwerp, en veel online tijdschriften en kranten bieden forums zodat lezers kunnen reageren op gepubliceerde artikelen. Vanuit dat oogpunt zijn forums zeer waardevol, omdat ze je laten kennismaken met andere meningen. Want hoe erg een artikel jou wellicht aansprak, er is vast iemand die het artikel maar niets vond.

Er zijn ook rond veel onderwerpen mailing lists, maar die zijn soms moeilijk te vinden. Vaak moet je eerst op zoek naar een idee, voordat je erachter komt dat en waar er een gerelateerde mailing list bestaat.

Voor een hacker is het van belang te weten dat veel forums en mailing-lists niet worden doorzocht door de grote zoekmachines. Soms vind je wel onderwerpen via een zoekmachine, maar zijn de individuele bijdrages binnen dat onderwerp niet door de zoekmachine in kaart gebracht. Deze informatie wordt het onzichtbare web genoemd,

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

omdat het informatie en gegevens bevat die voor veel mensen onzichtbaar is omdat je er op een speciale manier voor moet zoeken, bijvoorbeeld via meta-zoekmachines of met de zoekmachine van het forum of de mailinglist zelf.

Oefening:
A. Vind 3 computer beveilgings forums.
B. Hoe vond je deze forums?
C. Weet je het hele thema van de website?
D. Passen de onderwerpen in de forums bij het thema van de website waar het forum bij hoort/op wordt gehost?
E. Vind 3 computer beveiligings mailing lists.
F. Wie is de eigenaar van de lists?
G. Op welke list denk je dat je de meest feitelijke en objectieve informatie aantreft, en waarom?

1.1.5 Nieuwsgroepen

Nieuwsgroepen bestaan al heel lang. Er bestonden al nieuwsgroepen lang voordat het WWW bestond. Google heeft het hele nieuwsgroepen-archief opgekocht en online gemaakt via http://groups.google.com . Je zult er bijdrages tegenkomen van vroeg in de 90-er jaren. Het archief is van belang om te achterhalen wie de originele eigenaar van een idee of produkt is. Ook zul je er informatie vinden over onderwerpen die te klein of specialisitisch zijn om er een webpagina voor op te zetten.

Nieuwsgroepen worden nog steeds zo intensief gebruikt als jaren geleden, voor de tijd dat het web de belangrijkste manier werd om informatie te delen. Aan de andere kant groeit het gebruik ook niet meer, omdat ze in populariteit plaats hebben moeten maken voor nieuwe web-services als blogs en forums.

Oefeningen:
A. Gebruikmaken van Google's groepen, zoek de oudste posting in een nieuwsgroep die je kunt vinden over beveiliging.

B. Zoek naar een andere manier om de informatie in nieuwsgroepen te gebruiken zijn er wellicht applicaties waarmee nieuwsgroepen te lezen zijn?

CHoeveel nieuwsgroepen kun je vinden waarin wordt gesproken over computers hacken?

1.1.6 Websites

De de facto standaard om informatie te delen is momenteel via een webbrowser. Alhoewel we dat allemaal als het web aanduiden, is de juiste naam webservices, omdat niet alles op het web in de vorm van een website is. Als je je e-mail gebruikt via een webbrowser, dan gebruik je een webservice. Vaak is voor het gebruik van webservices autorisatie nodig. Dat betekent dat je een inlognaam en wachtwoord nodig hebt om toegang te krijgen. Als je legaal toegang hebt, zegt men dat je geautoriseerd bent. Als je al hackend op een website binnendringt om de pagina aan te passen, dan heb je wel toegang, maar omdat het niet gaat om legale toegnag, is geen sprake van geautorisatiseerde toegang. Wij richten ons alleen op geautoriseerde toegang, maar als je ervaring met gebruik van het web toeneemt zul je op veel plaatsen komen waar je per abuis toegang hebt tot gebieden waar eigenlijk

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

autorisatie voor nodig is. Als je dit merkt, is het goed gebruik om dit te melden aan de eigenaar van de website.

Websites zijn doorzoekbaar via een groot aantal zoekmachines. Het is zelfs mogelijk is eigen zoekmachine te maken, als je genoeg tijd en harde-schijf-ruimte hebt. Vaak krijgt een zoekmachine autorisatie voor het doorzoeken van een website, en die speelt het eigenlijk door naar jou. Soms gaat dat in de vorm van cache. Een cache is een geheugengebied op de server van de zoekmachine, waar de zoekmachine pagina's opslaat die voldoen aan je zoekopdracht. Als je klikt op de link cached, dan krijg je in plaats van de echte pagina, de pagina te zien zoals de zoekmachine die aantrof toen hij de website bezocht. De zoekmachine gebruikt de cache om aan te tonen dat zijn zoekresultaten goed zijn; als de website bijvoorbeeld down gaat of wordt aangepast in de periode nadat de zoekmachine de pagina voor het laatst bezocht. Maar je kunt de cache ook voor andere doeleinden gebruiken, bijvoorbeeld om een trage server te omzeilen.

Een van de meest publieke caches vind je op http://www.archive.org . Daar tref je caches van hele websites van jaren terug.

Een laatste opmerking over websites: ga er niet van uit dat je de inhoud van een website kunt vertrouwen omdat je hem vond via een zoekmachine. Veel hack-aanvallen en virus-aanvallen verspreiden zich door slechts een bezoek aan een (bewust voor verspreiding gemanipuleerde) webpagina of door het downloaden van een uitvoerbaar programma. Je beschermt jezelf door geen programma's te downloaden van websites die je niet kent en door een browser te gebruiken waarop alle bescchikbare updates zijn aangebracht.

Oefeningen:
A. Vind, gebruikmakend van een zoekmachine, sites die per abuis iedereen toegang hebben gegeven tot gebieden die eigenlijk alleen bereikbaar zijn als je de juiste autorisatie hebt. Om dit te doen zoeken we naar directory listings die toegankelijk zijn als je niet direct naar de betreffende webpagina gaat. Ga hiervoor naar http://www.google.com en vul in het zoekveld het volgende in:

allintitle: "index of" .pdf

Klik op een link in de resultaatlijst en daar zit er vast 1 tussen die eruit ziet als een directory listing.
Dit soort zoekslagen staat bekend als Google Hacking.

B. Kun je op deze manier andere type documenten vinden, gebruikmakend van Google? Vind nog 3 directory listings waarin .xls bestanden en .avi bestanden te zien zijn.

C. Er zijn nog meer zoekmachines naast Google. Een goede onderzoeker weet ze allemaal te gebruiken. Sommige websites zijn gespecialiseerd in het volgen van zoekmachines, zoals http://www.searchengine.com. Daarnaast zijn er nog meer van zulke sites, en je vindt ze via zoekmachines. Er is zelfs een zoekmachine voor het onzichtbare web. Vind 10 zoekmachines die GEEN meta zoekmachines zijn.

D. Zoek op security testing and ethical hacking en noteer de 3 eerste resultaten.

E. Zoek nu hetzelfde, maar zet de woorden niet tussen quotes (). Noteer de 3 eerste resultaten. Zijn het andere?

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

F. Als je op zoek bent naar een onderwerp, moet je anders zoeken dan wanneer je zoekt naar een woord of zin. In oefening D zocht je op een zin. Nu ga je op zoek naar een idee. Om dit te doen moet je even nadenken over wat je wil, en hoe je het wil vinden. Bijvoorbeeld, je wil een online bron vinden over tijdschriften die gaan over ethical hacking. Als je online resource of magazines for ethical hacking intikt op een zoekmachine, dan vind je een aantal meningen over het onderwerp. Best waardevol, maar niet zo waardevol als de echte webpagina die over zulke tijdschriften gaat. Om dat te doen moet je je afvragen, Als ik een webpagina over zulke tijdschriften zou maken, welke informatie zou er dan op staan, en op welke woorden moet ik dan zoeken om die pagina te vinden? Vul de volgende woorden en zinsdelen als zoekopdrachten op zoekmachines in en kijk wat de beste resultaten oplevert:

1. my favorite list of magazines on ethical hacking
2. list of ethical hacking magazines
3. resources for ethical hackers
4. ethical hacking magazine
5. magazines ethical hacking security list resource

G. Zoek de oudste pagina van Mozilla in het Internet Archive. Om dit te doen surf je naar de http://www.archive.org website en zoek je daar op www.mozilla.org.

H. Om alle losse lesjes nu bijeen te brengen: stel dat je versie 1 van de Netscape webbrowser wil downloaden. Gebruik zoekmachines en de Internet Archives-website en probeer versie 1 te vinden en download deze (maar installeer hem niet!).

1.1.7 Chat

Chats, ook bekend als Internet Relay Chat (IRC) en als Instant Messaging (IM), zijn populaire manieren om snel met anderen te communiceren.

Als een bron voor onderzoek zijn chats erg inconsistent , omdat je te maken hebt met personen in real time. Sommigen zullen vriendelijk zijn, en sommige zullen onaardig zijn. Er zullen onschldige grappenmakers tussen zitten, maar ook gevaarlijke leugenaars. Sommige zijn intelligent en zijn bereid kennis te delen, anderen weten eigenlijk niet waar ze over praten, maar zullen je toch tips en informatie geven. Het kan moeilijk zijn om te weten met welk type je te maken hebt.

Maar zodra je een beetje bekend bent geraakt met bepaalde groepen van mensen en chat-kanalen dan kun je opgenomen worden in zo'n community, zul je meer vragen kunnen stellen en je zult leren wie je kunt vertrouwen. Uiteindelijk zul je het nieuwste van het nieuwste kunnen leren op gebied van computerbeveiliging (ook bekend als zero day, wat inhoudt dat het nog maar net ontdekt is) en je kennis kunnen uitbreiden.

Oefeningen:
A. Zoek 3 chat-programma's voor instant messaging. Waar zitten de verschillen? Kun je met allemaal communiceren met de anderen?

B. Zoek uit wat IRC is en hoe je er een verbinding mee maakt. Zodra het je gelukt is verbinding te maken, zoek dan de ISECOM chatroom op zoals aangekondigd op de voorpagina van http://www.isecom.org.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

C. Hoe weet je welke kanalen er zijn om in te praten op IRC? Vind 3 computer beviliging kanalen en 3 hacker kanalen. Kun je toegang krijgen tot deze kanalen? Zijn er op die kanalen mensen aan het praten, of gaat het om bots?

1.1.8 P2P

Peer to Peer, ook bekend als P2P, is een netwerk binnen het Internet. In plaats van dat veel lokale computers via een centrale computer met elkaar communiceren, communiceren de computers in een P2P-netwerk direct met elkaar. De meeste mensen denken bij P2P aan het downloaden van MP3's en illegale films, maar er zijn veel anderen P2P-netwerken zowel om een grote verscheidenheid aan informatie te delen en om onderzoek te doen naar gedistribueerd informatie delen. Een website die is opgezet om hier informatie over te geven is http://infoanarchy.org ; daar gaat men er van uit dat informatie gratis moet zijn.
Op de Infoanarchy website tref je een lijst van beschikbare P2P-netwerken en -programma's.

Het probleem met P2P netwerken is dat, alhoewel je over bijna alle onderwerpen informatie kunt vinden, delen van de informatie op het netwerk illegaal is. Het Hacker Highschool programma keurt het gebruik van P2P-netwerken voor illegale downloads af, maar het is zeker dat P2P-netwerken een belangrijke informatiebron kunnen zijn. Onthoud: er is niets illegaals aan P2P-netwerken je treft er veel bestanden die gratis gedeeld mogen worden onder een varieteit aan licentievormen maar je treft er ook veel bestanden die er eigenlijk niet horen. Wees niet bang om P2P-netwerken te gebruiken, maar wees je bewust van de gevaren.

1.2 Meer Lessen

Je zou je nu moeten bekwamen in de kunst van het onderzoeken. Hoe beter je daar in bent/wordt, hoe meer informatie je snel weet te vinden, en hoe sneller je zult leren. Om je te helpen een betere onderzoeker te worden voor het Hacker Highschool programma, tref je hier wat extra onderwerpen en begrippen om te onderzoeken:

Meta Search
The Invisible Web
Google Hacking
How Search Engines Work
The Open Source Search Engine

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM,ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.