Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEKTION 1
DAS LEBEN ALS HACKER

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"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.

Informationen zur Nutzungslizenz

Die folgenden Lektionen und Arbeitsmaterialien sind öffentlich verfügbar unter den folgenden Bedingungen seitens ISECOM:

Alle Materialien der Hacker Highschool werden für den nicht-kommerziellen Einsatz in Grund-, Haupt-, Realschulen und Gymnasien zur Verfügung gestellt, sowohl für öffentliche und private Bildungseinrichtungen, als auch für Privatunterricht zu Hause. Die Materialien dürfen in keiner Form für den Wiederverkauf reproduziert werden. Der kommerzielle Einsatz der Materialien, welche käuflich erworben werden können, in jeglicher Form von Schulstunde, Unterricht, Training, Meeting, Kongress, Vorlesung, Fortbildung, Sommer- oder Abendschulen ist ohne vorigen Erwerb einer Lizenz explizit untersagt. Um eine Lizenz zu erwerben, besuchen Sie bitte http://www.hackerhighschool.org/license.

Das Hacker Highschool (HHS) Projekt ist ein Unterrichtswerkzeug. Der Einfluss auf die Lernenden liegt beim Lehrer, nicht jedoch beim Werkzeug. Aus diesem Grund erkärt sich ISECOM nicht für Schäden verantwortlich, welche aus einem eventuellen Missbrauch der hier publizierten Informationen hervorgehen.

Das HHS Projekt ist die Arbeit einer offenen Gemeinschaft. Wir hoffen, dass die Lesenden Nutzen in unsem Projekt finden werden und bitten um Unterstützung unserer Arbeit, sei es durch den Erwerb einer Lizenz, durch eine Spende, Sponsoring oder in anderer Form.

Für das gesamte Material: © ISECOM 2004

Inhalt

"License for Use" Information 2
Informationen zur Nutzungslizenz 2
Mitwirkende 4
1.0 Einleitung 5
1.1 Deine Quellen – Wie lernt ein Hacker 6
1.1.1 Bücher 6
1.1.2 Zeitungen und Magazine 7
1.1.2.1. Übungen 8
1.1.3 Zines und Blogs 8
1.1.3.1. Übungen 8
1.1.4 Foren und Mailinglisten 8
1.1.4.1. Übungen 9
1.1.5 Newsgroups 9
1.1.5.1. Übungen 10
1.1.6 Webseiten 10
1.1.6.1. Übungen 10
1.1.7 Chat 11
1.1.7.1. Übungen 11
1.1.8 P2P (Peer-to-peer Netzwerke) 12
1.2 Weitere Lektionen 12

Mitwirkende

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

ÜBERSETZUNG

Georg Berky

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

1.0 Einleitung

Willkommen zur Hacker Highschool. Wir wollen dich auf deinem Weg durch die Ausbildung zum Hacker begleiten. Das wichtigste, was wir in dir wecken wollen, ist deine Neugier, die die Grundlage für jedes weitere Lernen darstellt. Wir wollen dir helfen, in die Rolle eines verantwortungsvollen Hackers hineinzuwachsen, der fähig ist, Sicherheitsprobleme und Verletzung der Privatsphäre zu erkennen, und selbständig Entscheidungen zur Bewältigung dieser Probleme zu treffen.

Für viele Leute stellt "Hacken" wegen seiner kriminellen Natur einen Reiz dar. Wir wollen dir zeigen, dass ein noch viel größerer Reiz darin besteht, andere Leute auf Sicherheitslücken hinzuweisen und Sicheheitsprobleme öffentlich zu machen, ohne befürchten zu müssen, dafür ins Gefängnis zu kommen. Als sicherheitsbewusster Hacker ist es nicht nur dein Recht, sondern auch deine Verantwortung, die zuständigen Leute auf Sicherheitslücken und Verletzung der Privatsphäre hinzuweisen. Was wir tun, tun wir nicht nur, weil wir es können, sondern weil zu viele andere es nicht können. Weil es unsere Verantwortung als Hacker ist, helfen wir denjenigen, die diese Probleme nicht selbst lösen können. Dies ist die Arbeit vieler Watchdog ("Wachhund") Gruppen. Wir wollen dir helfen, diese Fähigkeiten und dieses Verantwortungsbewusstsein zu lernen.

1.1 Deine Quellen – Wie lernt ein Hacker

In dieser Lektion geht es darum, wie man lernt, was vielleicht die wichtigste Fähighkeit eines Hackers darstellt. Hacken ist mehr ein kreativer Prozess, als Auswendiglernen von Fakten, die einem von anderen erzählt werden. Wir können dir nicht alles, was du wissen willst und solltest beibringen, aber wir können dir beibringen, zu erkennen, was wichtig ist. Würdest du nur Fakten auswendiglernen, wärest du vielleicht schon morgen wieder vollkommen falsch informiert, allein deshalb, weil der technische und wissenschaftliche Fortschritt so schnell ist, wie in wenigen anderen Fachgebieten. Was wir dir beibringen wollen, ist das, was einen Hacker von einem Skript-Kiddie unterscheidet, das nur "Hackerprogramme" ausführt, ohne zu verstehen, was diese eigentlich tun und warum sie funktionieren. Zu lernen und Freude am lernen zu haben, den Drang zu verspüren, verstehen zu wollen, wie die Dinge funktionieren, ist der wichtigste Teil deiner Ausbildung.

Es kann und wird vorkommen, dass du Aussagen oder Wörter in diesem Buch nicht verstehst. Dabei ist es wichtig, dass du die Bedeutung dieser Wörter im Web nachschlägst, um sie dann in späteren Lektionen und Aufgaben zu verstehen. Andere Arbeitsbücher können von dir verlangen, im Web Informationen zu einem bestimmten Thema zu suchen, um dann damit die Übungsaufgaben in diesem Arbeitsbuch zu lösen. Wir werden dir später nicht mehr erklären, wie man im Web recherchieren kann. Dieses Buch ist das einzige, das dir eine gründliche und ausführliche Erklärung zu diesem Thema geben wird. Deswegen solltest du so viel Zeit darauf verwenden wie du brauchst, um zu lernen, wie du in den dir zur Verfügung stehenden Quellen nach Informationen suchst.

Beschränke dich dabei nicht auf Computer, Hacken und das Internet. Die besten Hacker ihres Faches sind vielseitig und vor allem kreativ. Viele von ihnen sind Maler, Schreiber und Designer. Deine Fähigkeiten als Hacker kannst du auch in anderen Gebieten einsetzen,

etwa in den Politikwissenschaften, wie es beispielsweise Machhiavelli in "Der Fürst" beschreibt.

Du solltest dich nicht nur für andere Gebiete interessieren, sondern auch Bücher lesen, die erklären, wie diese Gebiete funktionieren. Durch das Lesen von Büchern über verschiedenste Themen, von Psychologie bis Science Fiction, wirst du weitaus gewandter und vielseitiger als dich die Beschränkung auf ein einziges Gebiet jemals machen könnte. Beim Hacken geht es darum, herauszufinden, wie die Dinge funktionieren. Es ist egal, **wozu** sie entworfen worden sind, wichtig ist, **wie** sie funktioieren und wie man sie kreativ oder anders als es eigentlich geplant war einsetzen kann. Auf diese Weise findet und veröffentlicht man Sicherheitslücken und Schwachstellen.

1.1.1 Bücher

Bücher sind das ideale Hilfsmittel, um Fakten und Grundlagen eines Wissensgebietes, zu lernen. Du willst etwas über die Grundlagen einer Wissenschaft erfahren, etwa etwas über die Hardware in deinem Computer? Nichts wird dir mehr helfen, als ein aktuelles Buch zu diesem Thema zu lesen. Das Hauptproblem an Büchern ist, dass sie schnell veralten. Das Geheimnis des richtigen Bücherlesens liegt darin, die Struktur hinter der dünnen Hüllle bestehend aus Fakten in deinem Buch zu erkennen. MS-DOS, der Vorgänger von Windows, und Windows selbst unterscheiden sich offensichtlich um einiges, dennoch bauen beide auf den selben

Prinzipien der boole'schen Logik auf, denen Computer folgen, seit Prinzessin Ada von Lovelance im 19. Jahrhundert das erste Programm geschrieben hat. Die Problematik hinsichtlich Sicherheit und Privatsphäre mag sich in den letzen 2500 Jahren um einiges geändert haben, aber Bücher wie Sun Tzus "Die Kunst des Krieges" behandeln die selben grundlegenden Prinzipien, die heute noch immer gelten.

Die Informationen in einem Buch mögen nicht auf dem selben neuesten Stand sein wie die, die du aus anderen Quellen bekommen kannst, aber du wirst erkennen, dass das, was in einem Buch steht, eher den Kern und das Prinzip der Sache trifft, als das, was du vielleicht anderweitig findest. Jemand der ein Jahr darauf verwendet, ein Buch zu schreiben, wird sich eher an die Fakten halten, als jemand, der sechsmal am Tag sein Webblog auf den neuesten Stand bringt (siehe Abschnitt 1.1.3 Zines und Blogs). Sei dir auch im klaren darüber, dass exakte Informationen nicht immer frei von der Meinung des Informanten sind.

Du musst dir keine eigene Bibliothek anschaffen, aber vielleicht hältst du es ja für sinnvoll, beispielsweise Notizen an den Rand einer Seite zu schreiben, oder das, was du für wichtig hältst zu markieren. So etwas funktioniert natürlich nur mit eigenen Büchern.

Schlussendlich ist es wichtig, dass du nicht gleich nachdem du ein Buch angesehen oder bevor du mit dem Lesen angefangen hast aufgibst, weil es dir zu dick oder zu komplex erscheint. Der Großteil der dicken Bücher muss nicht von vorne bis hinten durchgelesen werden. Denke dir solche Wälzer einfach als prähistorische Webseiten: öffne das Buch an einer zufälligen Stelle und fange an zu lesen. Wenn du etwas nicht verstehst, blättere zurück und suche nach der Erklärung. Natürlich kannst du auch zum nächsten Abschnitt, der dir leichter verständlich erscheint, springen. Springe vor und zurück im Buch, so, als würdest du eine Webpage ansehen. Diese Art des "nicht-linearen Lesens" ist für Hacker oft viel interesanter, weil sie eher eine Befriedigung der Neugier darstellt, als konventionelles Lesen.

1.1.2 Zeitungen und Magazine

Zeitungen und Magazine sind die ideale Quelle, wenn man nach präzisen, aktuellen Informationen sucht, jedoch tendieren Magazine eher dazu, sich auf den Zeitgeist der Schreiber und Leser zu konzentrieren, als auf Fakten. Diese Tatsache ist sehr wichtig für einen Hacker. Social Engineering und das Knacken von Passwörtern sind meistens leichter, wenn man sich in der Popkultur auskennt. Man sollte allerdings auch wissen, dass Pop-Journalismus nicht immer das gleiche ist wie sorgfältiger Journalismus.

Was du noch beachten solltest ist das Leitmotiv deiner Quelle. Ein Linux-Magazin wird natürlich versuchen, Windows herunterzuspielen, weil der Konflikt zwischen den beiden Betriebssystemen genau das Leitmotiv ist, worüber die Abonnenten etwas lesen wollen.

Der beste Weg, diese beiden Fehlerquellen zu umgehen ist, dass du sorgfältig und breitgefächert Informationen sammelst. Wenn du in einem Magazin auf etwas Interessantes stößt, nimm an, dass du der Aussage glaubst und suche nach bestätigenden Informationen. Anschließend, solltest du annehmen, die Information sei falsch und nach Bestätigungen für diese neue Annahme suchen.

1.1.2.1. Übungen

A) Suche im Netz nach drei Online-Magazinen über Computersicherheit
B) Wie hast du diese Magazine gefunden?
C) Geht es in allen diesen Magazinen wirklich um Computersicherheit?

1.1.3 Zines und Blogs

Zines sind kleine Magazine, die man oft kostenlos bekommt und welche meistens weniger als 10'000 Leser haben. Sie werden oft von Hobbyschreibern und Amateurjournalisten verfasst. Zines wie etwa "2600" oder "Phrack Hacking" werden oft von Freiwilligen geschrieben und auch nächträglich meistens nicht wegen nicht-technischer Fehler korrigiert. Das bedeutet, dass die verwendete Sprache für die, die Leute, die sie nicht erwarten etwas rauh erscheinen mag. In Zines herrscht meistens ein bestimmtes Leitmotiv vor, von dem die Schreiber voreingenommen sein können, dennoch findet man in dieser Art von Informationsquelle eher Argumente für beide Seiten einer Diskussion, weil die Autoren nicht daran interessiert sind, Inserenten und Abonnenten nach dem Mund zu reden.

Blogs sind die moderne Version der Zines. Sie werden oft aktualisiert und drehen sich meist um mehrere sehr dominierende Leitmotive aus der Gemeinschaft der Schreibenden. Wie in Zines kann jeder einen Artikel kritisieren und eine gegenteilige Meinung vertreten. Bei Blogs ist es wichtig, die Kommentare ebenso wie den Artikel selbst zu lesen.

1.1.3.1. Übungen

A) Suche im Web nach drei Zines über Computersicherheit

B) Wie hast du diese Zines gefunden?

C) Warum hast du das, was du gefunden hast als "Zine" klassifiziert? Nur weil "Zine" im Titel steht, oder es als solches verkauft wird, muss es sich nicht unbedingt um eines handeln.

D) Suche im Web nach drei Blogs zum Thema Computersicherheit

E) Welche Gruppierung ist mit diesen Blogs in Verbindung?

1.1.4 Foren und Mailinglisten

Foren und Mailinglisten sind Medien, die aus einer bestimmten Gemeinschaft heraus entstanden sind, etwa so, wie wenn man auf Gespräche auf einer Party mitschneidet. Thema und Leitmotiv der Unterhaltung, wechseln häufig, und oft handelt es sich bei dem, was gesagt wird, um Gerüchte. Am Ende der Party erinnert sich oft niemand mehr, wer was gesagt hat.

Foren und Mailinglisten ähneln sich, weil es bei beiden für die Teilnehmer und Mitglieder viele Wege gibt, falsche Informationen zu einem Thema beizutragen – manchmal sogar willentlich. Ebenso gibt es Mittel und Wege, diese Informationen anonym zu verbreiten. Weil sich die Themen oft ändern, ist es wichtig, den ganzen Informationsstrang zu lesen, und nicht nur die ersten paar Beiträge, wenn man die besten Informationen erhalten will.

Es gibt fast zu jedem Thema ein Forum und viele Online-Magazine und Zeitungen bieten ihren

Lesern ein Forum an, wo diese ihre Meinung über die Artikel im Magazin oder der Zeitung schreiben können. Aus diesem Grund sind Foren von unschätzbarem Wert, wenn man nach mehr als einer Meinung zu einem bestimmten Thema sucht, denn egal wie sehr dir dieser Artikel gefallen hat, es wird immer jemanden geben, bei dem das nicht so war.

Die meisten Mailinglisten drehen sich um spezielle Themen, sind aber schwer zu finden. Oft musst du zu einer Frage zuerst eine bestimmte Idee haben, bevor du eine Mailingliste findest, die diese behandelt und unterstützt.

Das wichtigste, was es für einen Hacker über Mailinglisten und Foren zu wissen gibt, ist, dass sie nicht mit den grossen Suchenmaschinen durchsuchbar sind. Man kann zwar ein Forum oder eine Liste durch die Suche nach einem bestimmten Thema in einer Suchmaschinen finden, jedoch keine Informationen über einzelne Beiträge. Die letztgenannte Art der Information nennt sich "The invisible web" ("Das unsichtbare Netz"), weil es Informationen enthält, die für viele unsichtbar sind und nur durch eine sehr spezifische Suche, durch Metasuchmaschinen oder eine Suche direkt auf der Webseite des Forums gefunden werden können.

1.1.4.1. Übungen

A) Finde drei Foren zum Thema Computersicherheit

B) Wie hast du diese Foren gefunden?

C) Was ist das Leitmotiv der ganzen Webseite?

D) Spiegeln die Themen des Forums das Leitmotiv der Seite wider?

E) Finde drei Mailinglisten zum Thema Computersicherheit

F) Wer ist der "Eigentümer" dieser Listen?

G) Auf welcher dieser Listen würdest du eher exakte als voreingenommene Informationen erwarten? Warum?

1.1.5 Newsgroups

Newsgroups gibt es schon sehr lange, schon länger als das World Wide Web. Sie entstanden kurz nach der Erfindung von E-Mail durch Raymond Tomlinson aus den sogenannten MessageBoards, welche von Stephen Walker, der für die DARPA arbeitete, erfunden worden waren. Google kaufte ein Newsgroup-Archiv und machte dieses online verfügbar unter http://groups.google.com, worin man Beträge, die bis in die frühen 1990er zurückreichen finden kann. Dieses Archiv ist wichtig, wenn man herausfinden will, wer der eigentliche Eigentümer einer Idee oder Erfindung ist. Ebenso finden sich dort leicht obskure Informationen, die es normalerweise nicht bis auf eine Webseite schaffen.

Heutzutage werden Newsgroups nicht, wie vielleicht annehmbar, weniger verwendet als noch vor einigen Jahren, bis das Web zum Hauptmedium des Informationsaustausches geworden ist, jedoch sind sie auch nicht mehr viel gewachsen, da Blogs und Foren ihnen die Popularität streitig gemacht haben.

1.1.5.1. Übungen

A) Verwende Google Groups, um den ältesten Newsgroup-Beitrag über Computersicherheit zu finden.

B) Finde andere Wege, um Newsgroups lesen zu können. Gibt es andere Programme, die du dafür verwenden kannst?

C) Wieviele Newsgroups kannst du zum Thema "computer hacking" finden

1.1.6 Webseiten

Im Augenblick ist ein Webbrowser der de-facto Standard zur Weitergabe von Informationen. Wir nennen zwar alles, was wir mit einem Webbrowser erreichen können "Web", aber der richtige Ausdruck dafür ist "web-services". Wenn du mit deinem Browser E-Mails abholst, dann verwendest du einen Web-Service. Meistens erfordert die Verwendung von Web-Services bestimmte Privilegien, beispielsweise einen Benutzernamen und ein Passwort, um Zugriff auf den Service zu erhalten. Man hat die erforderlichen Privilegien, wenn man sowohl Zugriff, als auch das (legale) Recht für diesen Zugriff hat. Sich unberechtigt Zugriff auf eine Webseite zu verschaffen, um dann ihr Erscheinungsbild zu verändern (defacing), bedeutet zwar "Zugriff" zu haben, jedoch nicht, die entsprechenden Privilegien, da man natürlich nicht das (legale) Recht dazu hat, dies zu tun. Die meisten Leute sind daran interessiert, dass ein Zugriff auf eine Webseite nur mit den entsprechenden Privilegien stattfinden kann, dennoch wirst du viele Seiten finden, die ungewollt priviligierten Zugriff auf geschützte Bereiche erteilen. Du solltest dir angewöhnen solche Fehler dem Betreiber der Seite zu melden.

1.1.6.1. Übungen

A) Verwende eine Suchmaschine, um Seiten zu finden, die ungwollt privilierten Zugriff auf geschützte Bereiche erteilen. Um solche Seiten zu finden, suchen wir nach "directory listings" (einer Liste mit allen Dateien in einem Verzeichnis), auf die man zugreiffen, kann, wenn man nicht direkt im Browser die Seite aufruft. Rufe http://www.google.com auf und gib folgendes in das Suchfeld ein:

allintitle: "index of" .pdf

Klicke auf einige Links in den Suchergebnissen und du solltest einige Seiten finden, die wie ein directory listing aussehen. Diese Art der Informationssuche nennt sich "google hacking"

B) Suche auf diese Weise nach anderen Dokumenten mit Google und finde drei directory listings, die .avi und .xls Dateien enthalten.

C) Es gibt ausser Google noch viele andere Suchmaschinen, und ein neugieriger Sucher kann mit allen umgehen. Einige Webseiten spezialisieren sich auf "tracking search engines" (finde heraus, was genau das ist), etwa http://www.searchengine.com. Es gibt jedoch noch mehr dieser Suchmaschinen, und du kannst sie mit anderen Suchmaschinen finden. Es gibt sogar eine Suchmaschine für das "invisible web".
Suche nach 10 Suchmaschinen, die keine Meta-Suchmaschinen sind.

D) Suche nach "security testing and ethical hacking" und notiere die obersten drei Antworten

E) Such nach den selben Begriffen wie in E), jedoch ohne die Anführungszeichen

F) Die Suche nach einem Thema und die nach einem Satz oder einem einzelnen Wort unterscheiden sich erheblich. In Übung D hast du nach einem Satz gesucht, jetzt suchen wir nach etwas abstrakterem, einem Konzept oder einer Idee. Um die richtigen Ergebnisse zu erhalten, musst du darüber nachdenken, **was** genau du finden willst und **wie** du es finden willst. Willst du beispielsweise nach einer Webseite für Magazine über "ethical hacking" suchen, und gibst du "online source of magazines for ethical hacking" in deine Suchmaschine ein, wirst du zwar ein paar Meinungen zu dem Thema finden, jedoch ist das nicht so praktisch, wie wenn du gleich zu der Liste finden würdest. Frage dich stattdessen "Wenn ich eine solche Webseite erstellen würde, welche Informationen könnte man auf dieser Seite finden. Welche Schlüsselwörter, könnte ich aus diesen Informationen auswählen?" Gib die folgenden Worte in eine Suchmaschine ein und finde heraus, welche die besten Ergebnisse für deine Suche findet.

1) my favourite list of magazines on ethical hacking
2) list of ethical hacking magazines
3) ressources for ethical hackers
4) ethical hacking magazine
5) magazines ethical hacking security list ressource

G) Suche nach der ältesten Mozilla Webseite im Internet Archiv. Durchsuche "www.mozilla.org" auf der Webseite http://www.archive.org.

H) Um jetzt alles, was wir bis jetzt gelernt auf einmal anzuwenden, suche nach einer Downloadmöglichkeit für Version 1 des Netscape Browsers. Verwende Suchmaschinen und das Internet Archiv um diese Version zu finden und herunterzuladen. (Installiere sie jedoch nicht)

1.1.7 Chat

Chats, bekannt unter den Namen IRC ("internet relay chat") und IM ("instant messaging") sind sehr beliebte Möglichkeiten, um schnell mit anderen Leuten zu kommunizieren.

Chats liefern oft widerspüchliche und inkonstitente Informationen, weil man mit anderen Leuten in Echtzeit kommuniziert. Manche Leute werden unfreundlich sein, andere sehr hilfsbereit. Manche sind harmlose Witzbolde, andere bösartige Lügner. Einige sind intelligent und bereit, Informationen zu teilen, andere sind uninformiert, teilen aber trotzdem ihr (Un-) Wissen. Es kann sich als schwer herausstellen, zwischen den verschiedenen Typen zu unterscheiden.

Sobald du mit den Regeln einiger Gruppen und Channels vertraut bist, wirst du schnell ein Mitglied dieser Gemeinschaft und kannst mehr Fragen stellen. Ebenso lernst du, wem du vertrauen kannst und wem nicht. Vielleicht kommst du so sogar an die neuesten Informationen über Computersicherheit, bekannt als "zero-day" (Null Tage), also gerade erst entdeckt, wodurch du wiederum dazulernst.

1.1.7.1. Übungen

A) Finde drei Chatprogramme für IM (instant messaging). Worin unterscheiden sie sich? Können sich die einzelnen Programme auch untereinander "unterhalten"?

B) Finde alles über IRC heraus, was du erfahren kannst, und vor allem, wie du dich mit einem IRC Netzwerk verbindest. Sobald du das geschafft hast, komm in den ISECOM Chatroom, den wir auf unserer Homepage http://www.isecom.org angegeben haben.

C) Woher weißt du, welche Channels es in einem IRC Netzwerk gibt? Finde drei über Computersicherheit und drei für Hacker. Sprechen die Leute dort wirklich, oder sind sie Bots?

1.1.8 P2P (Peer-to-peer Netzwerke)

P2P, auch bekannt als peer-to-peer ist ein Netzwerk im Internet. Normalerweise kommunizieren Computer im Internet über einen zentralen Server. Im Fall von P2P findet die Kommunikation jedoch direkt zwischen den Teilnehmern (peers) statt. Die meisten Leute denken bei P2P sofort an das illegale Herunterladen von Musik oder Filmen, es gibt jedoch viele P2P Netzwerke, die dazu entwickelt worden sind, eine große Fülle von Informationen verteilt auszutauschen. Eine Webseite, die über diese Art von Netzwerken informiert ist http://infoanarchy.org, deren Philosophie es ist, dass Informationsaustausch frei sein sollte. Auf der infoanarchy Webseite findest du eine Liste von aktuellen P2P Netzwerken und Clients für diese.

Das Problem an P2P ist, dass man zwar so ziemlich alles mit ihnen finden kann, aber es befinden sich viele Daten illegalerweise in diesen Netzwerken. Wir behandeln hier die Verwendung von P2P Netzwerken zum illegalen Downloaden von geistigem Eigentum nicht, aber es steht ausser Frage, dass P2P eine Quelle von unschätzbarem Wert zum Sammeln von Informationen darstellt. P2P Netzwerke sind nicht illegal, es gibt eine große Zahl von Dateien, die man unter verschiedensten Lizenzen legal und kostenlos herunterladen kann, aber es gibt genausoviele Dateien, die dort besser nicht herumliegen sollten. Es gibt keinen Grund, Angst vor dem Verwenden von P2P Netzwerken zu haben, solange du dir über die Gefahren im klaren bist.

1.2 Weitere Lektionen

An dieser Stelle solltest du üben und dein Können beim Suchen und Forschen nach Informationen verbessern. Um dir etwas dabei zu helfen, haben wir einige interessante Themen zum Nachforschen aufgelistet.

Meta Search (Metasuche)
The invisible Web
Google hacking
How search engines work
The open source search engine