Hacke, wenn du nicht gehackt werden willst

Letzte Überarbeitung: 14.04.04 Version: 2.6

Vorwort

Dieses Tutorial hab ich für die Zielgruppe Anfänger geschrieben. Ich habe es so einfach und verständlich wie möglich geschrieben, darum kann es vorkommen, dass einige Sachen zu allgemein behandelt werden.
Für Fortgeschrittene sollte sich daher nicht viel Neues finden.
Aber es ist, wie ich finde, durchaus lesenswert.
Man kennt vielleicht das Sprichwort: „Wer nicht mit den Wölfen heult, wird von ihnen gefressen“ oder so ähnlich.
In diesem Text beziehe ich mich auf dieses Sprichwort, aber im übertragenden Sinne auf den Computer und den „Mythos“ des Hackers.
Das soll jetzt nicht heißen, dass ich hier zeige, wie man in Server[1] einbrechen kann, das würde mindestens 100.000 Seiten brauchen um alle einzelnen Themengebiete umfassend und verständlich zu erläutern.
Hier geht es mehr um das Grundwissen, die Philosophie und wie man sich das Fachwissen aneignen kann.

Die jeweils Neuste Version dieses Tutorials kann man von www.egocrew.de herunterladen.

Erst mal zur Definition von hacken, bzw. Hacker

In den Medien wird ein Hacker als jemand beschrieben, der die Macht und das Wissen hat sämtliche Computer zum Absturz zu bringen, Daten zu stehlen und weltweiten Schaden anzurichten.
Okay, langsam merken die Medien auch, dass sie alles zu sehr aufbauschen und setzten ihre Ansprüche an die Hacker tiefer ;-)
Dieser Erklärung ist jedoch gänzlich falsch. Was in etwa auf diese Beschreibung passt sind nicht Hacker sondern Cracker.
Cracker sind so zu sagen die bösen Hacker. Obwohl diese sehr oft auch nicht die Möglichkeiten besitzen, um den Schilderungen der Medien gerecht zu werden.
Dann gibt es noch die Möchtegern-Hacker, auch Script-Kiddies genannt.
Diese benutzenTrojaner[2] und vorprogrammierte Programme um in Rechner einzudringen und Schaden anzurichten.
Daher das Wort „Script“, also Programm oder Programmcode. Das „Kiddie“ leitet sich von dem englischen „kid“ (Kind) ab, da oft Jugendliche hinter solchen Attacken stecken.
Script-Kiddies wissen oftmals durch ihr junges Alter und die fehlende Erfahrung gar nicht, was sie überhaupt tun.
Ich gebe mal ein Beispiel. Ich habe schon Script-Kiddies erlebt, die mit Methoden zum Eindringen in Windows NT-Rechner versucht haben in einen Linux Rechner einzubrechen.
Script-Kiddies sind häufig gelangweilte Teenager, die versuchen mit dem erstbesten Tool Spass zu haben.
Diese Tools sind meist so einfach gestrickt, dass eigentlich jeder normale, etwas gebildete User[3] sie bedienen kann.
So und dann gibt es noch eine 3. Gruppe, das sind die Leute, die ihre Programme usw. Selbst schreiben und wirklich etwas von der Materie, dem Aufbau eines Systems verstehen.
Nicht dass diese Leute immer ihre eigenen Programme schreiben, aber Erfahrung darin haben sie meistens.
Diese Menschen leben eine Philosophie aus, man könnte es durchaus als Lebensstil bezeichnen.
Für diese Gruppe wäre der Begriff Hacker zutreffend, aber die meisten dieser Leute lehnen es ab als Hacker bezeichnet zu werden, weil diese Bezeichnung durch die Medien in den Schmutz gezogen wurde.
Früher, als der Begriff Hacker entstand, bedeutete es „Jemand, der auf der Tastatur rumhackt“.

Da Computer damals nicht so weit verbreitet waren (so um 1960, als der Begriff entstand),
war ein Hacker zu sein schon etwas besonderes, aber nichts Außergewöhnliches.
Wenn man einen Computer besaß war man automatisch ein Hacker.
Später dann, gegen Ende der 70er Jahre und Anfang der 80er Jahre wurde der Begriff Hacker als Bezeichnung
für einen Programmierer geprägt. Erst Ende der 80er, Anfang der 90er kam es zu den bereits erwähnten Bedeutungen.
Wenn man einmal Berichte oder Texte von Programmierern aus der Zeit liest z.B. von Linus
Torvalds (*Erfinder von Linux*), bemerkt man, dass sie sich und andere Programmierer oft als Hacker bezeichnen.
Sie bleiben ihrer Bezeichnung treu. Und ich hoffe, dass sich diese Form der Wortbedeutung wieder durchsetzten wird.
Was vielleicht auch einige wissen, es gibt noch andere Begriffe für Hacker und Cracker.
Einige haben die Begriffe WhiteHat und BlackHat lieber (zugegeben, sie klingen mehr nach gut und böse ;-)).
WhiteHat's sind Leute, die in Rechner einbrechen um zu lernen, sie richten keinen Schaden an, aber
hinterlassen dem Admin[4] meist eine humorvolle Nachricht oder einen Hinweis auf die Sicherheitslücke durch die Sie
eindringen konnten.
Also sind WhiteHats nützlich; besser ein WhiteHat im Server als einen echten Schadensverursacher ;-).
BlackHat's hingegen dringen in Systeme ein um Daten zu stehlen und das System zu zerstören.
Sozusagen sind BlackHat's die Cracker. Wer vielleicht noch erwähnenswert ist, sind die GreyHat's.
Das sind „Hacker" (Ihr wisst, was ich meine), die vom Staat oder einer Firma beauftragt worden sind das Firmensystem auf
Mängel zu überprüfen oder Verbrechern auf die Spur zu kommen.
Die Begriffe kommen wahrscheinlich aus den Westernfilmen. Da gab es ja auch immer den guten mit dem weißen Hut und
den bösen mit dem schwarzen Hut. So, damit hätten wir das mal geklärt.

Noch ein paar Worte zur Philosophie und Lebensweise der echten Hacker.

Wer kennt sie nicht, die jungen, gut durchtrainierten Hacker aus den Filmen. Zugegeben, solche Hacker gibt es auch.
Aber eigentlich denkt man, wenn man den Begriff Hacker hört, immer an einen etwas korpulenteren Mann
mit Vollbart, Jeans und Sandalen. ;-)
Das war für mich immer die Idealvorstellung eines Hackers. Diese Hacker sind die ältere Generation - die Generation, die
mitgeholfen hat die Computer und die Systeme so zu gestalten, wie sie heute sind.
Diese Menschen wie z.B. Richard Stallman haben die Philosophie hinter der ganzen Technik geprägt.
Durch Stallmans Manifest der Offenheit (Freiheit) der Sourcecodes[5] entstand Ende der 80er, Anfang der 90er eine
Massenbewegung, die es bis dato noch nicht in der Welt der Technik gab.
Tausende von Hackern halfen mit Programme, die unter Stallman' s GPL[6] standen und noch immer stehen, zu verbessern
und zu erweitern. Dieses Netzwerk von Freiwilligen kontrollierte die Arbeit ihrer Mitstreiter indem sie Bugs[7] beseitigten oder
neue Funktionen implementierten[8].
Hacker leben nach einigen Grundprinzipien. Es gibt verschiedene Ausführungen der genauen Regelungen, aber ich will
hier einmal die elementarsten auflisten.

- Alle Informationen müssen frei sein
- Dringe nur in geschützte Systeme ein um auf Sicherheitslücken aufmerksam zu machen und um zu lernen
- Nutze deine Fähigkeiten nie zur Zerstörung und Diebstahl von Daten
- Beurteile einen Hacker oder andere User nachdem was sie tun und nicht nach Rasse, Hautfarbe, Geschlecht usw.

Zu der Philosophie der Hacker zählt auch das gewisse „Feeling". Ich finde es zum Beispiel sehr stimmungsvoll an meinem
Linux PC zu sitzen, eine Tasse heißen Cappuccino zu trinken, den melancholischen Song „Creep" von Radiohead zu hören
und dabei zuzusehen wie einige Pakete auf der Konsole[9] (bloß kein XTerm[10] ;-)) kompiliert[11] werden.
Das sollte jeder einmal ausprobiert haben ;-). Am besten ist es noch, wenn der Raum nur spärlich beleuchtet ist.

Dieses Gefühl, etwas endlich perfekt eingestellt zu haben und es dann ins System zu integrieren, ist wie eine Droge. Jeder, der dieses Gefühl kennt, wird mir zustimmen, dass es einfach grandios ist.
Hacker zu sein, heißt etwas erschaffen, manche nennen es Kunst, manche Sourcecodes und die Medien die sich nur oberflächlich mit dem ganzen Thema beschäftigen, nennen es Gefahr.
Doch ist es wirklich Gefahr, die von solchen Codezeilen ausgeht?
Wenn man es mal genauer betrachtet, nutzten solche Programme zwar Sicherheitslücken aus um das System zu „öffnen“ und vielleicht Schaden zu verursachen, aber damit haben die Schöpfer dieser Programme oft wenig am Hut.
Für sie zählt es auf das Problem aufmerksam zu machen. Was andere damit machen, ist vielleicht nicht in ihrem Sinne. Aber wenn es immer nur danach gehen würde, was potenzielle Angreifer mit speziellen Sachen anstellen könnten, wären die Medizin und Technik nicht auf dem heutigen Stand.
Die Philosophie, die dahinter steckt, ist lobenswert, aber sie kann nicht für das Handeln Anderer verantwortlich gemacht werden.
Ich hoffe dass ich einen kleinen Einblick in die Philosophie der Hacker geben konnte.

Kleiner Buch Tipp (1)

Das Buch „Netzpiraten“ von Armin Medosch & Janko Röttgers ist eine gut recherchierte Lektüre über die Internetkultur und die verschiedenen Gruppierungen im Internet, wie z.B. Virenprogrammierer, Freiheitskämpfer, und Professoren, die zuviel hacken ;-).
Auf jedenfall lesenswert um die Vorgänge innerhalb des Netzes besser verstehen zu können.

Emanzipation - die Haecksen erheben sich

Die Welt wird von Männern dominiert, das ist seit Jahrtausenden der Fall. Doch die Emanziption der Frau wächst stetig an. Auf dem Arbeitsmarkt, in der Politik, eigentlich überall. Doch was ist im Internet los? Wann hört man schon einmal von einer Frau, die eine Sicherheitslüche aufgedeckt oder eine Software geschrieben hat?
Die Emanzipation zieht weite Kreise, nun ist sie auch bei den “Hackern” angekommen.
Seit einigen Jahren gibt es eine Anlaufstelle für weibliche “Hacker”, sogenante “Haecksen”.
Auf www.haecksen.org sind die technisch interessierten Damen zu Hause.
Es ist eine Gruppierung innerhalb des CCC' s (Chaos Computer Clubs www.ccc.de), die es sich zur Aufgabe gemacht hat, Frauen zu helfen selbstverständlich und kreativ mit der Technik umzugehen und das Bild in den Köpfen der Menschen, nämlich dass “Hacker” männlich sind, zu verändern.

Aber warum hört man so selten von Frauen im Underground? Ich kann nur Vermutungen anstellen. Wahrscheinlich liegt es zum größten Teil an dem selbst aufgezwungenen Klischee, Männer: Sport und Technik; Frauen: Kinder und Haushalt. Es liegt einfach nicht in der weiblichen Natur sich mit hochtechnischen, kryptischen Hintergründen auseinander zu setzten. Frauen wollen sich attraktiv und sexy fühlen, und ein Computer trägt wenig dazu bei. ;-)
Aber was macht die “Haecksen” so besonders, dass sie sich eben doch damit ausseinander setzen?
Meiner Meinung nach sind es Frauen, die in ihrem Herzen Entdecker sind. Immer auf der Suche nach Neuem und Interessantem. Sie sind rebellisch und versuchen dies mit dem Ausbruch in die Welt der Underdogs auszudrücken. Sie wollen sich beweisen, Mut zeigen und Spaß haben.
Frauen sind eine starke Bereicherung, sie denken völlig anders und kommen somit auf andere Wege und Lösungen.
Eine der populärsten “Haecksen” ist Gigabyte aus Belgien, sie wird auch die Lara Croft des digitalen Undergrounds genant. Sie war über Jahre hinweg ein sehr bekannter Name unter den Virenautoren. Ihre Viren waren anders, als man gewöhnt war. Ihrem Virus “Yaha” folgte z.B. Kurz darauf “YahaSux”, der die von “Yaha” befallenen PC' s wieder säuberte. Sie nutze Viren als praktische Mahnungen für mehr IT-Sicherheit.

Eine andere Kreation, nämlich "Quizy", konfrontiere den User[3] mit einem Zehn-Fragen-Quiz zur Weihnacht. Gelang es dem User[3] alle Fragen zu beantworten, erhielt er eine Anleitung zur Säuberung seines Systems.
Im Februar 2004 wurde Gigabyte dann von den belgischen Behörden gefasst.
Ihre Webseite ist noch über ein Webarchiv aufzurufen http://web.archive.org/web/*/http://coderz.net/gigabyte

Ich hoffe, dass mehr Frauen den Einstieg in die Welt der “Hacker” schaffen werden. Sie werden sich zwar durchsetzten müssen, aber das werden sie schon irgendwie hinbekommen :-)

Die Pseudo-Hacker-Sprache

Wer kennt es nicht, die kryptischen, auf den ersten Blick unsinnig wirkenden Kombinationen, aus allem, was die Tasten hergeben. Diese Form der Schreibweise wurde eingeführt um bei den Suchmaschinen nicht so leicht gefunden zu werden. Hauptsächlich also eine Schutzfunktion vor Strafverfolgung. Bis dato wurde nach “Hacker” gesucht, wenn man bestimmte Tools oder Menschen suchte. Um wieder mehr unter sich zu sein, wurde diese spezielle Form der Schreibweise geboren.
Nehmen wir einmal das am häufigsten auftretende Wort.
“31337” oder “1337”. Was hat es damit auf sich? Nun, es bedeutet “elite” oder “leet”. Die Buchstaben werden durch Zahlen ersetzt, die den Buchstaben in gewisser Weise gleichkommen. Auch sehr bekannt ist “h4xx0r”, das für “Hacker” steht.
Neben dieser Verfremdung von Worten gibt es auch noch die “Z-Variante” - bekannt von so vielen Worten, wie z.B. “Toolz, Warez[12], Hackz, Cheatz[13], etc.”.
Heutzutage gelten diese Arten der Schreibweisen als 14/\/\3 (lame[14]) ;-).
Sie werden eigentlich nur noch von Script-Kiddies oder Gamern benutzt, um zu zeigen, dass sie dem “Underground” angehören. Dabei merken sie nicht, dass sie sich im Grunde nur lächerlich machen. Ab und zu sieht man in Foren ein paar Menschen dieser Sorte, über deren Wortwahl man nur schmunzeln kann.
Merkt euch, wer wirklich Kentnisse hat, würde nie solche - inziwschen kindische - Begriffe verwenden. Er hätte es gar nicht nötig. Klar, ab und zu macht es Spass in Chatrooms[15] eben solche Leute damit aufzuziehen. ;-)
Noch ein Tipp, wenn man in einer Suchmaschine Ergebnisse bekommt, die diese Pseudo-Hacker Begriffe beinhalten, sollte man die Finger davon lassen. Es handelt sich meistens um unseriöse Seiten, die mit Dialern und Bannern nur so gespickt sind.

Die Worte, die im Computerbereich und in noch größerem Ausmaß im Bereich der “Hacker” benutzt werden, stammen größtenteils aus dem Science-Fiction Szene, da zu der Zeit, als sich die Computerkultur entwickelt hat, auch die Blütezeit des Science-Fiction war. Gemeint sind die 60er. Es ist nicht verwunderlich, dass sich diese zwei Welten seht schnell überschnitten. Science-Fiction träumt von Zukunft, von hochtechnologischer Entwiclung und Weltraumschlachten. Der Computer gab dem neue Möglichkeiten, schneller an dieses Ziel zu kommen. Sei es durch simple Spiele, Austausch in Foren über Details von SF-Serien, Comics oder wissenschaftlicher Forschung. Und wer sich auf diese Weise damals mit dem Computer beschäftigte, der wollte bald mehr und wurde in den meisten Fällen zu einem “Hacker”.
Teilweise finden sich aber auch Fantasy-Einflüsse in der Sprache (und den Programmen) der “Hacker” wieder. Besonders J.R.R. Tolkiens Werk, der “Herr der Ringe” hat es ihnen angetan. :-)

Wie die sprachliche Entwicklung weitergehen wird, steht noch in den Sternen. Vielleicht geht es mehr ins japanische, wer weiss. Eins ist aber klar, diese Spachkultur entwickelt sich stetig weiter, und viele Worte finden ihren Weg in die Medien, wo sie einen völlig anderen Sinn bekommen. So wie es schon unserem bekanntesten Wort, “Hacker”, ergangen ist.

Was soll „Hacke, wenn du nicht gehackt werden willst“ bedeuten, wenn es gar keine richtigen Hacker gibt?

Hacken bedeutet in Computer Fachkreisen, dass jemand das OS[16] beherrscht, dass er Programme schreiben kann um damit seine Arbeit zu erleichtern bzw. sich so gut auskennt das er in andere Systeme eindringen könnte.
Hacken muss also nicht immer etwas schlechtes, gefährliches sein (gefährlich für den Betroffenen eines Angriffs).
Ich will damit sagen, dass "Hacke, wenn du nicht gehackt werden willst" bedeuten soll, sich mit seinem System auseinander zu setzen, zu verstehen wie alles genau funktioniert und daraus lernen, wie Angreifer es schaffen in das System einzudringen und wie man dies verhindern kann.
Um generell besser mit seinem OS arbeiten zu können und vielleicht auch eine höhere Effizienz des Computers und des Systems zu erreichen.
Am besten sollten man sich zuerst fragen, warum man z.B. Windows benutzt und nicht Linux.
Die meisten User wissen nicht einmal, dass es so etwas wie Linux oder andere Betriebsysteme gibt, ihnen wurde von Irgendjemandem Windows vorgesetzt weil es das marktführende Betriebsystem ist und das einzige ist was sie kennen.
Es ist gut, dass Linux endlich wieder mehr Akzeptanz in den Medien findet.
Das ist auch kein Wunder, wann hört man heutzutage schon mal die Schlagzeile „Revolution von ganz unten zerstört allmählich Weltmonopol Microsoft“.
Wie ich vor einiger Zeit gelesen habe, sagen Prognosen voraus, dass Linux im Jahre 2008 auf ca. 20% der Computer weltweit installiert sein wird.

Hier mal eine Liste von Betriebsystemen mit ihren Vor- und Nachteilen

- *BeOS*
  Pro: Frei von Betriebssystem-Altlasten, da es völlig neu konzipiert wurde; sehr hohe Performance bei Multimedia-Anwendungen; Netzwerkbereich mittlerweile sehr gut ausgestattet
  Contra: Wenig Software für Büroanwendungen; nur ein Benutzer kann mit Root-Rechten[17] arbeiten
  Webseiten: www.be-faq.de

- *BSD (FreeBSD, OpenBSD, NetBSD)*
  Pro: Sehr hohe Sicherheit; kompakt; kostenlos und OpenSource (Quellcodes sind frei verfügbar); 100%ig konfigurierbar; sehr stabil
  Contra: Einige Funktionen aus dem Unix/Linux Bereich werden nicht unterstützt; Viele kommerzielle Software wird nicht unterstützt; manche neuere Hardware wird noch nicht unterstützt; schwerer zu erlernen als z.B. Windows
  Webseiten: www.bsd.org ; www.freebsd.org ; www.netbsd.org : www.openbsd.org

- *Dos*
  Pro: Nicht teuer; relativ stabil; "wenige" Befehle; relativ schnelle Bootgeschwindigkeit
  Contra: Keine grafische Darstellung möglich; relativ unflexibel, daher kein vernünftiges Arbeiten möglich
  Webseiten: www.freedos.org
  (Es gibt noch mehr Seiten, aber diese ist die wohl interessanteste in Bezug auf Dos Systeme)

- *MacOS / MacOS X*
  Pro: Einfach und intuitiv zu bedienende Oberfläche; echtes Plug &Play[18]; manuelles Einstellen von Ressourcen wie IRQs[19] entfällt; gründlichere Deinstallation, da Programm und Dateien in einem Verzeichnis liegen; sehr stabil (stürzt so gut wie nie ab)
  Contra: Wenig Software und Spiele; kein echtes Multitasking[20]; geringe Treiberunterstützung für neuere Hardware; keine Unterstützung von x86er[21]Systemen.
  MacOS ist an die Computer der Firma Apple vollständig gebunden; sehr hoher Preis für benötigte Hardware und das Betriebsystem
  Webseiten: www.apple.com/de

- *Netware*
  Pro: Geringe Hardwareanforderungen; sehr stabil; zuverlässige Verwendung von Virtuellem Speicher; austauschbare Dateisysteme durch „Installable File Systems[22]“
  Contra: Bedienung per Befehlszeile; geringe Hardwareunterstützung
  Webseiten: www.novell.com

- *OS/2*
  Pro: Sehr stabil; austauschbare Dateisysteme durch „Installable File Systems[22]“
  Contra: Wenig Software für Privatanwender; geringe Hardwareunterstützung
  Webseiten: www.os2world.com

- *Unix / Linux*
  Pro: Oft kostenlos und OpenSource (Quellcodes sind frei verfügbar); 100%ig konfigurierbar; sehr stabil; servertauglich; viele verschiedene Unix/Linux Distributionen[23], sodass jeder eines findet was seinen Wünschen entspricht; viele verschiedene Grafische Oberflächen; geringe Hardwareanforderungen; eignet sich sehr gut als Datenbank oder Backup-Server, sowie Firewall[24] und Router[25]; sehr schnelle Weiterentwicklung
  Contra: Viele kommerzielle Software wird nicht unterstützt; manche neuere Hardware wird noch nicht unterstützt; schwerer zu erlernen als z.B. Windows; Noch nicht ganz NTFS[26] kompatibel
  Webseiten: www.suse.de ; www.redhat.org ; www.debian.org ; www.distrowatch.org
  (Es gibt noch viel mehr Distributionen[23], aber diese Links sollten für den Anfang reichen)

- *Windows*
  Pro: Einfach zu bedienen; sehr gute Unterstützung im Bezug auf Gerätetreiber; viel Software, die darauf läuft
  Contra: Sehr teuer; instabil; Viren- und Angriffs-anfällig; Keine integrierten Online-Schutzmechanismen, Lizenzgebunden[27]; man ist an eine vorgegebene grafische Oberfläche gebunden; wenig konfigurierbar; hohe Anforderungen an die Hardware(WinXP)
  Webseiten: www.microsoft.com

- *Zeta (Ausgegangen wird vom Release Candidate 2)*
  Pro: Aus BeOS entstanden, aber zu 80% neu geschrieben; sehr hohe Performance vor allem im Multimedia Bereich; läuft auch auf alter Hardware sehr schnell; intutiv bedienbar
  Contra: Wenig Software; noch schlechte Hardwareunterstützung; Netzwerkbereich lässt noch zu wünschen übrig
  Webseiten: www.yellowtab.com

Wenn man also herausgefunden hat, warum man ein bestimmtes Betriebsystem verwendet
(z.B. Windows wegen MS Office und dessen funktionaler Oberfläche), sollte man sich darüber schlau machen.
Auch jemand der nur mit seinem Office arbeitet, sollte über sein Betriebsystem bescheid wissen und was man alles damit machen kann. *(Zumindestens solange, bis die Systeme auch für Einsteiger sicher sind, das soll heißen, dass die Systeme alles verbieten, solange bis man es freischaltet).*
Wenn dieser User[3] wichtige Daten an seinem Privat PC bearbeitet und nicht weiß wie er sich schützen kann, könnte im schlimmsten Fall die Konkurrenz an diese Daten kommen.
Das ist vielleicht übertrieben, aber solche Beispiele helfen die Leute wachzurütteln und sie auf die Gefahren hinzuweisen.

Wie macht man sich schlau und lernt mehr über sein Betriebsystem und andere Anwendungen??

Am besten über Tuts (Tutorials) oder auch HowTo' s genannt. Das sind kleine (oder größere) Texte die ein spezielles Thema behandeln z.B. „Kernel[28] kompilieren unter Linux".
Am besten sucht man Tuts über www.google.de oder man probiert es mal auf www.tutorials.de.
Die beste Möglichkeit bei Google gute Ergebnisse zu erzielen, ist mehrere Suchwörter einzugeben, z.B. „Tutorial+Windows+Netzwerk+einrichten" (statt der „+" kann man auch einfach Leezeichen machen, das bleibt sich gleich). So ist die Chance größer das zu finden was man sucht. Eine andere Möglichkeit wären Fachbücher, man sollte sich aber vorher genaustens darüber erkundigen was für einen das bessere Buch ist.

Einige Verlage die immer sehr gute Bücher drucken sind z.B. „O'Reilly" und „Markt & Technik".
Ich will jetzt nicht sagen, dass die anderen Verlage nur Schrott drucken, aber ich (und jede Menge andere) habe die besten Erfahrungen mit diesen Verlagen gemacht. Was auch besonders für Anfänger zu empfehlen ist, sind die Bücher aus der „…für Dummies" Reihe. Man sollte sich da wirklich nicht vom Namen abschrecken lassen ;-)

Kleiner Buch Tipp (2)

Ein Buch das eigentlich perfekt für den Einstieg ist, ist „Der Hacker Guide" von Markt & Technik.
Es gibt ihn für verschiedene Anwendungsgebiete, z.B. Der Hacker Guide für Windows oder für Linux.
Die 2 Auflage heißt „Der *neue* Hacker Guide". Das Buch ist zwar dick, aber man sollte sich davon nicht abschrecken lassen. Es ist gut erklärt und auch zum Nachschlagen sehr gut geeignet. In den Büchern geht es nicht um das Hacken an sich sondern eher um das Schützen vor Angriffen. Dann gibt es noch die Möglichkeit sich in Foren, oder auch Boards genannt, weiterzubilden. Diese gibt es auf Webseiten und im Usenet[29]
Infos was das Usenet ist und wie man dorthin kommt gibt's auf: www.usenet-abc.de

Einige gute Boards sind:
- www.buhaboard.de (Rund um PC, Elektronik, Programmieren…)
- www.rootboard.de (Unix / Linux Board)
- www.linuxforen.de (Linux Board)
- www.programmierer-board.de (Rund ums Programmieren)
- www.root-shell-club.com/board (Alles mögliche)
- www.hackeinsteiger-board.de (Viel für Newbies[30])
- www.systemroot.org (Auch ein sehr umfangreiches Board)
- www.serverhelp.de (Für Server Admins etc. Interessant)
- www.macuser.de/forum (Ein sehr umfangreiches Board für Mac User)
- www.egocrew.de/board (Relativ junges Board, aber sehr umfangreich)

Man sollte jedoch, bevor man eine Frage stellt, die Suchfunktion des Boards benutzen. Die meisten Boardmitglieder sind ziemlich ungehalten, wenn eine Frage zum zigtausendsten Mal gestellt wird.

Dinge über die man sich auf jeden Fall informieren sollte

- Das Betriebsystem
- Anti-Viren Software / Viren allgemein
- Firewalls[24]
- DoS[31] und sein großer Bruder dDoS[32](Denial-of-Service & distributed Denial-of-Service)
- Intrusion Detection[33]
- Logging[34] (Besonders im Linux Bereich sehr nützlich)
- Backups[35] (Denn wenn alles nichts hilft braucht man das)

Das sind nur die Grundlegenden Themen, über die jeder Bescheid wissen sollte. Und denkt nicht, dass man alles innerhalb von 3 Wochen lernen kann (Bei Windows vielleicht schon ;-))
Es gibt immer etwas Neues, besonders im Unix / Linux Bereich. Aktualität ist sozusagen das Wichtigste.
Wer immer die aktuellen Versionen hat, läuft nicht so leicht Gefahr von Sicherheitslücken innerhalb der Programme betroffen zu sein.

Wenn man immer aktuell bleiben will im Bezug auf Sicherheitslücken, Exploits[37] usw. empfehle ich:
- www.golem.de
- www.heise.de
- www.packetstormsecurity.org
- www.security-gui.de
- www.securityfocus.com
- www.slashdot.org

Auf http://online.securityfocus.com/archive
kann man sich Newsletter[38] abonnieren um immer auf dem Laufenden zu sein.

Programmiersprachen, warum und welche?

Wie man vielleicht weiß, wachsen Programme und Betriebsysteme nicht auf Bäumen. Es ist den tatkräftigen Programmierern (Auch Hacker genannt *siehe oben*) zu verdanken, dass wir heute so eine Vielfalt an Programmen und Betriebsystemen für den Computer haben. Aber wie entstehensolche Programme eigentlich?
Nun ja zu allererst braucht man eine Programmiersprache. Man wählt diese nach dem aus, wofür man sie verwenden will. „HTML“ z.B. ist dazu da einfache Webseiten zu programmieren, wohin entgegen „C“ für komplexe Programme zu benutzen ist. Warum sollte man denn überhaupt eine Programmiersprache lernen, wo doch schon alles, was man braucht, da ist, werden manche jetzt fragen.
Es scheint zwar so, als ob es alles gäbe, was man braucht, aber durch die Entwicklung immer schnellerer und leistungsfähigerer Computer kann ein Betriebsystem auch immer mehr. Um diese Kapazität vollständig auszunutzen und die immer neueren Versionen von anderen Programmen, kann man seine Programme als Alternative benutzten oder Funktionen implemetieren[8], die man braucht, aber nicht vorhanden sind. Bei Linux ist es so, dass jeder die Einsicht in den Programmcode (oder Sourcecode) hat. Jeder kann mitmachen um das System zu verbessern und zu ergänzen.
Da wäre es schon von Vorteil eine Programmiersprache zu können.

Wie bereits erwähnt, würde es helfen mehr über sein Betriebsystem zu lernen. Aber nicht nur Linux ist ein Gemeinschaftsprojekt. Es gibt tausende davon. Besuchen Sie doch einmal www.sourceforge.net.
Dort gibt es solche Projekte für die verschiedensten Arten von Programmen.
Programmieren ist für die meisten keine Arbeit sondern Hobby. Es macht Spass, etwas aus dem Nichts zu erschaffen. Man kann sozusagen „Gott“ spielen. Es ist einfach ein gutes Gefühl zu wissen, dass man etwas geschaffen hat, mit dem andere Menschen arbeiten. Das ist auch ein Teil der Hacker Philosophie. Das alles sind Gründe um eine Programmiersprache zu erlernen. Da es sehr viele Programmiersprachen gibt, sollte man sich wirklich entscheiden, was man will. Ich habe die wichtigsten Sprachen mit ihren Anwendungsgebieten aufgelistet. Ich gehe hier nur auf Programmiersprachen für den Software Bereich ein, nicht auf Websprachen wie PHP und HTML (Jedoch ist HTML im Eigentlichen Sinne keine Programmiersprache sondern eine sogenannte Markup Language[36]).
Und in diesem Bereich, auch nur auf die am meist genutzten Sprachen. Die angegebenen Webseiten sind natürlich nicht alle zu dem Thema, aber es sind Webseiten, die ich für geeignet halte um genauer zu informieren.

- *C*
  - Für fast alle Betriebsysteme geeignet
  - Sehr leistungsfähig
  - Hardwarenahe programmieren (volle Kontrolle)
  - Nicht ganz einfach zu lernen und zu beherrschen
  - Das portieren auf andere Systeme ist möglich, aber teils sehr schwierig sehr verbreitet
  - Webseiten: www.c-programme.de
  - Anwendungsgebiete: Von kleinen Scripten bis zu umfangreicher Software, allerdings ist es schwieriger grafische Oberflächen zu erstellen

- *C++*
  - Für fast alle Betriebsysteme geeignet
  - Weiterentwicklung von C
  - Objektorientiert
  - Schwierig zu lernen (schwieriger als C, lohnt sich aber mehr)
  - Sehr verbreitet
  - Webseiten: www.c-plusplus.de ; www.gcc.gnu.org
  - Anwendungsgebiete: Genau wie C ist mit C++ alles möglich

- *Delphi/Kylix*
  - Delphi für Windows / Kylix für Linux
  - Einfach zu lernen
  - Objektorientiert
  - Webseiten: www.delphi-source.de ; www.kylix-forum.de ; www.borland.com
  - Anwendungsgebiete: Grafische Programme

- *Perl*
  - Für fast alle Betriebsysteme geeignet
  - Sehr leistungsfähig (Kann alles ;))
  - Man kann oft Sachen in einer Zeile realisieren, die mit anderen Sprachen viel länger wären
  - Manche finden es für Anfänger zu schwer als Einstieg in die Programmiersprachen (Zu unübersichtlich)
  - Webseiten: www.perl.org ; www.perl-archiv.de
  - Anwendungsgebiete: Von kleinen Scripts für Systemaufgaben bis zu komplexen Programmen, allerdings nur im Textformat

- *Visual Basic*
  - Nur für Windows geeignet
  - Ideal um Windows Anwendungen zu programmieren
  - Nicht sehr flexibel
  - Objektorientiert
  - Webseiten: www.activevb.de ; www.vbarchiv.de
  - Anwendungsgebiete: Grafische Programme

Ein wichtiger Aspekt, der für Fortgeschrittene interessant sein dürfte, ist die Exploitprogrammierung.
Exploit[37] Programmierer, bauen sehr oft Fehler in ihre Exploits ein, damit nicht jedes Script Kiddie eine „geladene Waffe" besitzt. Wenn man die passende Sprache beherrscht, kann man viel aus diesen Exploits[37] lernen.

Rechtliche Fragen zum „Hacking"

Ich könnte hier anfangen Paragraphen aufzuzählen um den Sachverhalt darzustellen, doch das würde so gut wie niemandem nützen. Stattdessen versuche ich kurz und klar zu sagen, was erlaubt ist und was nicht.
Das Ansehen von Daten, die durch Sicherheitsmechanismen gesichert sind (z.B. Firewall[24], Verschlüsselung etc.), ist strafbar, da man dabei die genanten Sicherheismechanismen zuvor umgehen muss. Also ist das bloße Umgehen oder Knacken von solchen Mechanismen strafbar. Man muss noch nicht einmal Schaden anrichten. Das Verbreiten dieser sensiblen Daten ist ebenfalls strafbar. Ganz klar, jegliches Kopieren (außer als eigene Sicherheitskopie) und verbreiten von kostenpflichtiger, lizensierter Software oder Daten (bspw. MP3´s, Filme etc.) ist verboten.
Das Portscannen hingegen ist nicht verboten. Es ist vergleichbar mit dem Klingeln an einer Haustür um zu sehen ob jemand da ist, der das Haus bewacht. Beim Portscannen ist es dasselbe. Man klingelt und anhand der Reaktion kann man sehen, ob jemand den Computer bewacht (Firewall[24]).
Das Verschicken von Spam E-Mails ist auch strafbar, da dabei zum einen eine Sicherheitsschwäche des Mail Servers ausgenutzt wird um die Spams zu verschicken, und zum anderen hat man einen Fall von persönlicher Belästigung, wobei letzteres sogut wie nie vorkommt, weil nicht die Empfänger von Spam-E-Mails, sondern die Betreiber der Mail-Server die Spammer verklagen.
Ein Fall, der auch noch erwähnenswert ist, ist das programmieren von schädlichem Code[5]. Viren, Trojaner, Exploits, etc. Es ist nicht verboten diese zu schreiben. Das veröffentlichen ist auch nicht strafbar. Allerdings ist es strafbar, damit Schaden anzurichten. Wenn der Code[5] (oder die ausführbare Datei) veröffentlicht wurden und jemand anderer damit Schaden anrichtet, kann euch nichts passieren. Es wäre allerdings sinnvoll einen Haftungsausschluss bei den entsprechenden Downloads anzubringen, sonst könnte der Angeklagte auf Unwissenheit plädieren. Es ist aber sehr unwahrscheinlich, dass er damit durchkommen würde.
Das sind die grundlegenden Sachverhalte. Wer es genauer wissen will, sollte nach Forendiskusiionen zu dem Thema suchen, da die Gesetze nicht ganz eindeutig sind, findet sich dort genügend Material zu spezielleren Fällen.

Abschließenden Worte

Man lernt nie aus. Deshalb ist es wichtig, egal ob man „Hacker“ (siehe Erklärungen oben) werden will oder einfach nur, um sein System sicher zu halten, immer auf dem neusten Stand zu sein.
Sicherheit ist das A & O im Computerzeitalter. Darauf sollte man wirklich achten, denn heutzutage kann jedes Script-Kiddie großen Schaden anrichten. Das liegt mit daran, dass ihnen die Gefahr des Geschnapptwerdens, mangels technischem Wissen, nicht bewusst ist. Ich rate Ihnen nicht den Weg eines Crackers einzuschlagen, es kann nämlich ziemlich verlockend sein, vor allem, wenn man das Wissen dazu hat.
Egal wie schierig es aussehen mag, geben sie nicht so leicht auf. Wäre es einfach, würde es doch keinen Spaß machen ;-)
Ich hoffe, Ihnen hat mein Tutorial gefallen, und sie ein wenig zum Nachdenken gebracht.

Erklärungen

1 : **Server** = Rechner, der Informationen und Dienste (z.B. E-Mail-Server) bereit stellt
2 : **Trojaner** = Programm, mit dem man Computer fernsteuern kann. Auch Rootkits genannt
3 : **User** = Benutzer auf einem Computer
4 : **Admin** = Kurzform von Administrator. Ein Benutzer mit allen Rechten auf dem Computer oder im Netzwerk
5 : **Sourcecode** = Quellcode, oder Programmiercode eines Programms.
6 : **GPL** = General Public License. Von Richard Stallman geschriebenes Dokument über den freien Zugang- und die Offenlegung von Daten.
www.gnu.org/copyleft/gpl.html (Original GPL Version)
www.gnu.de/gpl-de.html (Deutsche Übersetzung der GPL)
7 : **Bugs** = Fehler und Sicherheitslücken in Programmen
8 : **Implementieren** = Funktionen oder Verbesserungen in Programme einfügen
9 : **Konsole** = Auch Shell genannt. Vollbild Eingabemodus für Befehle, z.B. die „bash“ unter Linux
10 : **XTerm** = Konsole unter Linux, die in einem Fenster im grafischen Modus aufgerufen werden kann
11 : **Kompilieren** = Einen Sourcecode[5] in ein fertiges Programm umwandeln. Hierzu wird der "Compiler" benötigt
12 : **Warez** = Kostenpflichtige Software die auf zum illegalen Download angeboten wird
13 : **Cheatz** = Eigentlich "Cheats". Kleine Tricks mit denen man sich in Computerspielen Vorteile verschafft
14 : **lame** = Adjektiv von Lamer. Kommt vom englischen "lahm, schwach". Ein Lamer ist ein Nichtskönner, Looser
15 : **Chatrooms** = Bereiche in denen man fast anonym mit anderen Menschen reden (chatten) kann.
16 : **OS** = *Englisch:* Operating System = Betriebsystem
17 : **Root Rechte** = Rechte des Administrators. Der Administrator kann sämtliche Änderungen am System vornehmen
18 : **Plug & Play** = Hardware Erkennung und Einrichtung
19 : **IRQ** = Interrupt Request (Unterbrechungsanforderung). IRQ ist der Name für die Hardwareinterruptsignale, über die sich Hardware (z. B. serielle oder parallele Anschlüsse) an den Prozessor wenden.
Da Interrupts in der Regel nicht gemeinsam benutzt werden können, werden Geräten eindeutige IRQ-Adressen zugewiesen, über die sie mit dem Prozessor kommunizieren können
20 : **Multitasking** = Mehrbenutzerfähiges Arbeiten. Das heißt, gleichzeitiges arbeiten mit mehreren angemeldeten Benutzern oder mehrfaches, gleichzeitiges Arbeiten mit dem gleichen Nutzer.
Dies kann direkt passieren oder per Zugriff aus dem Netzwerk oder Internet
21 : **x86** = Computer wie 286er, 386er, 486er, Pentiums und AMD’ s, auch PC (Personal Computer) genannt
22 : **Installable File Systems** = Alle Dateisysteme wie z.B. Fat32 (Windows) oder ext2 (Linux/Unix). Abkürzung ist IFS
23 : **Distributionen** = Verschiedene Linuxe von verschiedenen Herstellern, z.B. SuSE, Debian oder RedHat
24 : **Firewall** = Eine bildlich gesprochene Schutzmauer; die Firewall schützt ein System vor unerlaubtem Zugriff
25 : **Router** = Computer, der den Netzwerkverkehr regelt und Computer in einem Netzwerk mit dem Internet verbindet

26: **NTFS** = Abkürzung für "New Technology File System“. Dieses File System (Dateisystem) wurde erstmals mit Windows NT verwendet. Es unterstützt lange Dateinamen, erweiterte Dateiattribute und sehr große Speicherkapazitäten bis ca. 17 Milliarden GB

27 : **Lizenzgebunden** = Bestimmte Auflagen müssen erfüllt werden, z.B. müssen Sie sich bei Microsoft registrieren und dürfen die Software nicht vervielfältigen

28 : **Kernel** = System Kern auf den alles aufbaut

29: **Usenet** = Computernetz, das vor dem Internet entstand. Es ist eine Art riesiges schwarzes Brett. Im Usenet gibt es nur öffentlich zugängliche Nachrichten. Das heißt, dass auf eine einmal gepostete Nachricht beliebig viele Teilnehmer antworten können, welche dann zu oft langen und komplizierten Ketten von Rede und Gegenrede führen, welche man Threads nennt

30 : **Newbies** = Einsteiger, Anfänger, Neuling. Kommt vom englischen „New“ (neu)

31: **DoS** = Denial-of-Service. Bombardieren eines Rechners mit Datenpaketen bis dieser zusammenbricht.

32: **dDoS** = distributed Denial-of-Service. Siehe DoS[31] nur, dass dieser Angriff von mehreren Rechnern gleichzeitig auf das Opfer abgefeurt wird

33 : **Intrusion Detection System** = Einbrecher Warnungs- oder Frühwarnsystem. Schlägt Alarm, wenn ein bestimmter Fall eintritt, z.B. Port Scanning oder ein bestimmter Angriff. Abkürzung ist IDS

34 : **Logging** = Mitschreiben von Aktivitäten im System und Angriffen

35 : **Backups** = Sicherheitskopien von Daten. Meist werden diese auf externen Medien wie CD’ s oder Magnetbändern gespeichert, um im Falle eines Datenverlustes das System möglichst schnell wieder zum laufen zu bekommen

36: **Markup Language** = Sprache, die nur eingegebene Daten anzeigt, also keine dynamischen Daten, die z.B. aus einer Datenbank gelesen werden

37 : **Exploits** = Um den Begriff Exploit zu beschreiben, braucht man etwas länger, aber grob gesagt ist ein Exploit ein Programm, das eine Sicherheitslücke ausnutzt um Zugriff auf einen Computer zu erlangen

38 : **Newsletter** = Neuste Nachrichten per E-Mail zugesandt

Für Fragen, Kritik oder Verbesserungsvorschläge schreibt mir eine Mail an: darkchill@gmx.de
<darkchill>

Danke an meine Beta Leser und Korrekturmenschen :-)
DarkStan, Christian Brozinski, H-o-S, AgentPhreak und ein ganz dickes Dankeschön an Amalthea