Achtung - teils illegal

Diese Tools nutzen Profi-Hacker

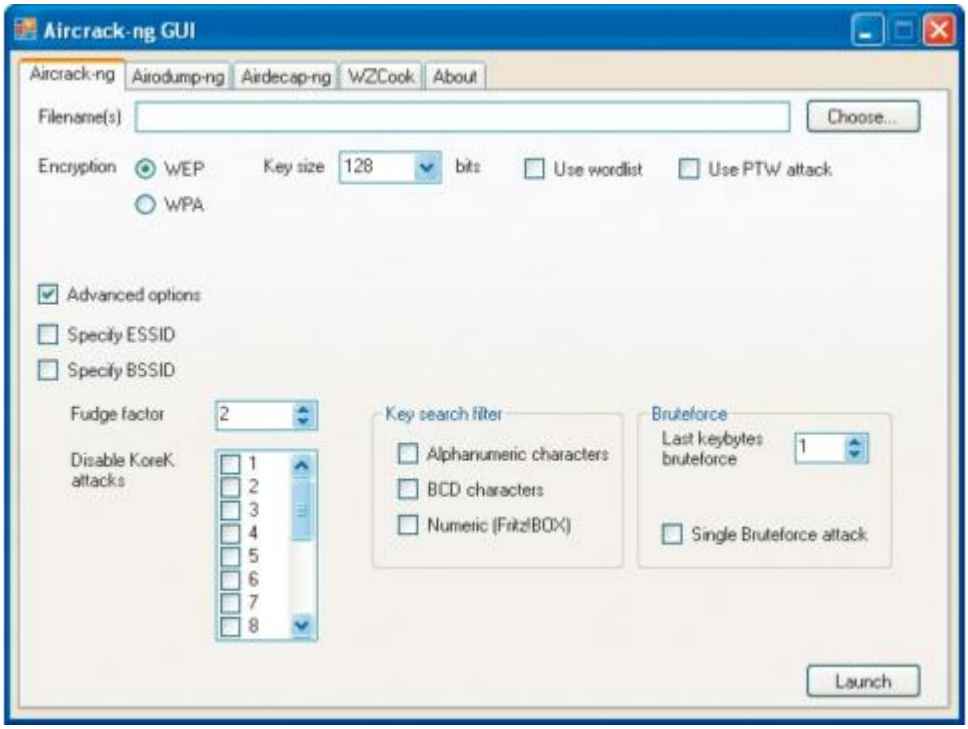
04. Januar 2016 | Von Panagiotis Kolokythas (Autor) | cio.de

Wir stellen Ihnen 20 Hacker-Tools vor, die von Profis genutzt werden. Darunter finden Sie auch Programme, die sich zu illegalen Zwecken missbrauchen lassen. Bei diesen Tools haben wir aus Sicherheitsgründen auf den Download-Link verzichtet.

20 - teils illegale - Hacker-Tools.
Foto: IBM

Nicht alles, was nützlich ist, ist auch erlaubt. Das gilt vor allem für die Hacker-Tools, die wir Ihnen heute vorstellen. Bei einigen Tools dürfen wir keinen Download-Link angeben, weil deren Nutzung und Verbreitung aufgrund des Strafgesetzbuches in bestimmten Fällen verboten sein kann (siehe weiter unten). Dies ist allerdings umstritten.

Die 20 besten Hacker-Tools

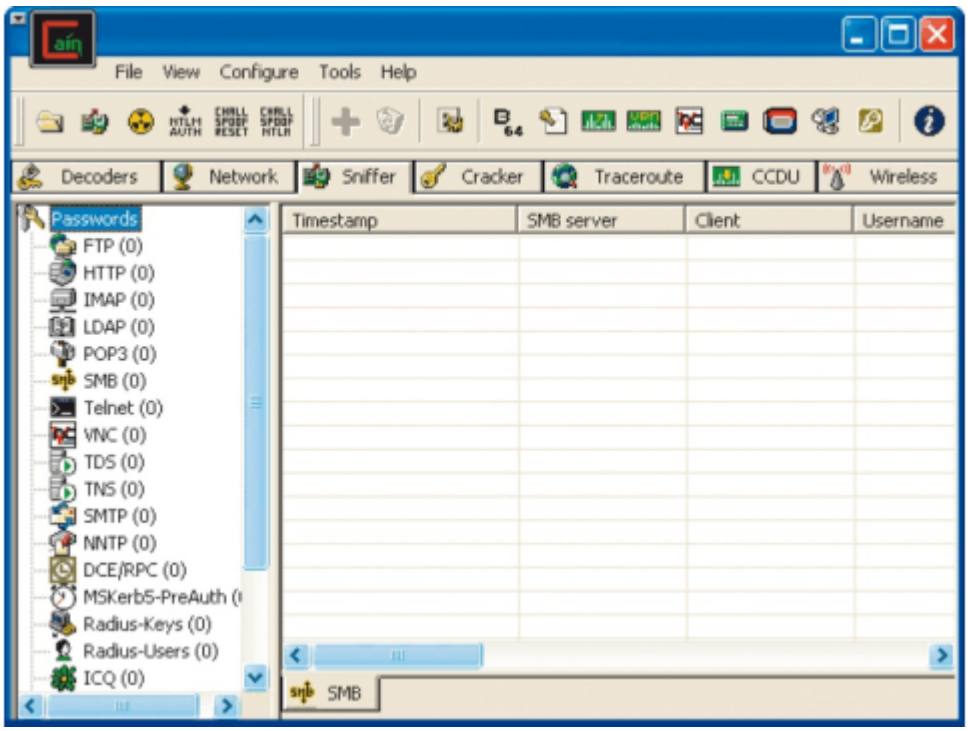


Aircrack-ng

WLANs sollte man tunlichst verschlüsseln, damit kein Fremder Schindluder treiben kann. Das alte WEP-Verfahren ist dafür allerdings ungeeignet: Die neue Version von Aircrack-ng ermittelt binnen Sekunden den Schlüssel eines WEP-geschützten Funknetzes. Schlüssel des sichereren WPA-Verfahrens kann Aircrack-ng nur durch Ausprobieren sämtlicher Buchstaben- und Zahlenkombinationen herausbekommen. Das dauert lange und ist bei komplexen Passwörtern sogar aussichtslos.

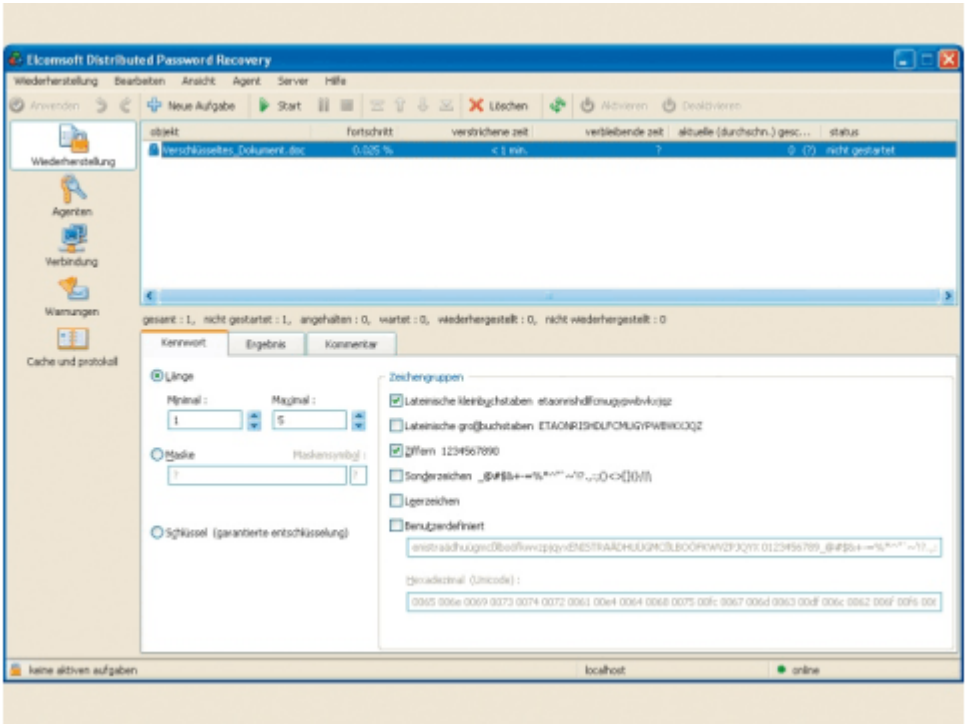
Blues Port Scanner

Blue's Port Scanner überwacht bei einer aktiven Internet-Verbindung alle Ports des Rechners, über die Daten ausgetauscht werden.



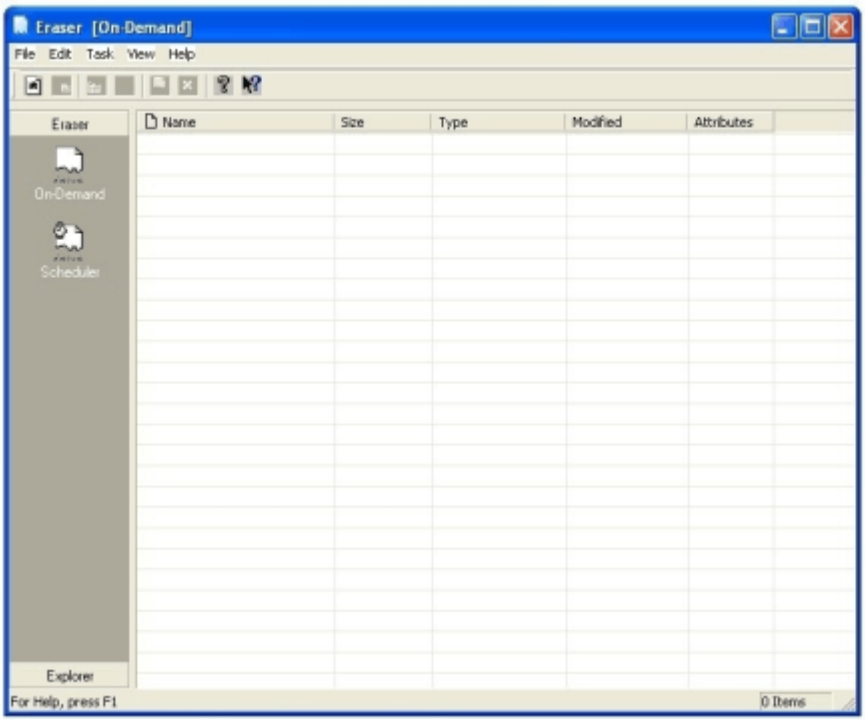
Cain & Abel

Mit Cain & Abel lässt sich Datenverkehr in einem lokalen Netz belauschen. Das Tool ist in der Lage, die Zuordnungstabelle im Router oder Switch so zu ändern, dass es die Datenpakete abfangen kann. Über einen Trick lassen sich auch verschlüsselte HTTPS-Verbindungen belauschen. Cain & Abel zeigt nicht den rohen Datenverkehr an, sondern pickt sich die für Hacker relevanten Informationen heraus, zum Beispiel Benutzernamen, Passwörter und VoIP-Gespräche.



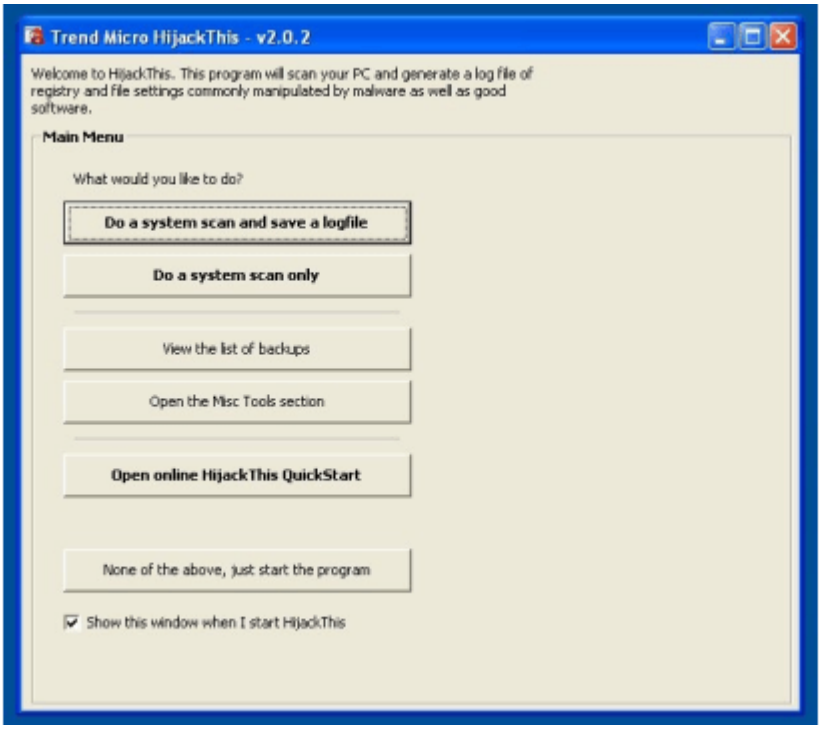
Distributed Password Recovery

Elcomsoft Distributed Password Recovery 2.60.176 ist ein Hochleistungs-Tool zum Entschlüsseln von Passwörtern. Das Besondere an der Software: Sie kann die Rechenleistung von Grafikkarten mit Nvidias GPU Geforce 8 und 9 einbeziehen. Diese Graphical Processing Units sind bei Kryptografie-Berechnungen aktuellen CPUs mehrfach überlegen. Zudem ist das Programm in der Lage, die Berechnung im Netzwerk zu verteilen. Das Tool kann unter anderem Office-Dokumente und Windows-Passwörter knacken.



Eraser

Wenn Sie Dateien von Ihrer Festplatte löschen, lassen sich diese wiederherstellen. Das ist gerade bei vertraulichen Dateien ärgerlich, vor allem, wenn sich mehrere Anwender einen PC teilen.



HijackThis

Einige Websites nutzen Sicherheitslücken im Internet Explorer aus, um Software zu installieren, die den Startseiten-Eintrag im IE ändert. Das Gratis Tool HijackThis ist auf solche Arten von Schädlingen spezialisiert.
Download: HijackThis

Hotspot Shield

Wollen Sie die Freiheit des Internets auch außerhalb Ihrer vier Wände oder dem Büro nutzen, werden Sie mit Ihrem Wireless-Lan sehr leicht Opfer von Hackern, die die Verbindung zum Hotspot für Angriffe nutzen können. Dagegen schützt Sie der kostenlose Hotspot-Shield.

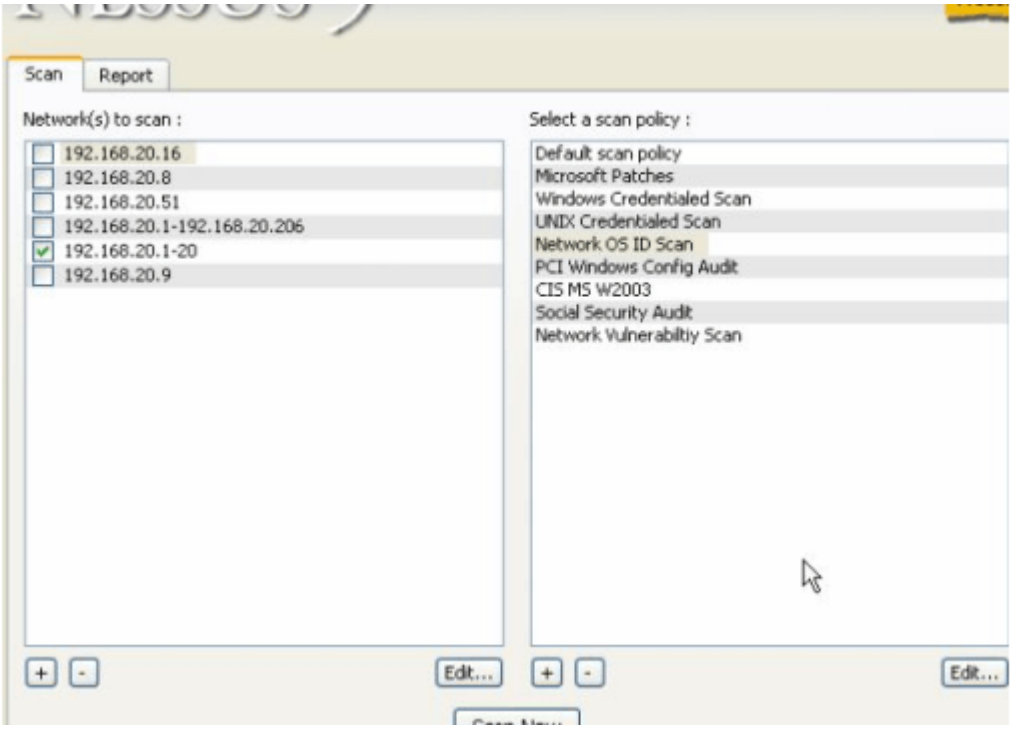
Download: Hotspot Shield

IceSword

An den versierten Benutzer wendet sich das Sicherheitstool Icesword, das nach eingeschleusten Rootkits im System fahndet und diese dann zum Löschen anbietet.
Download: IceSword

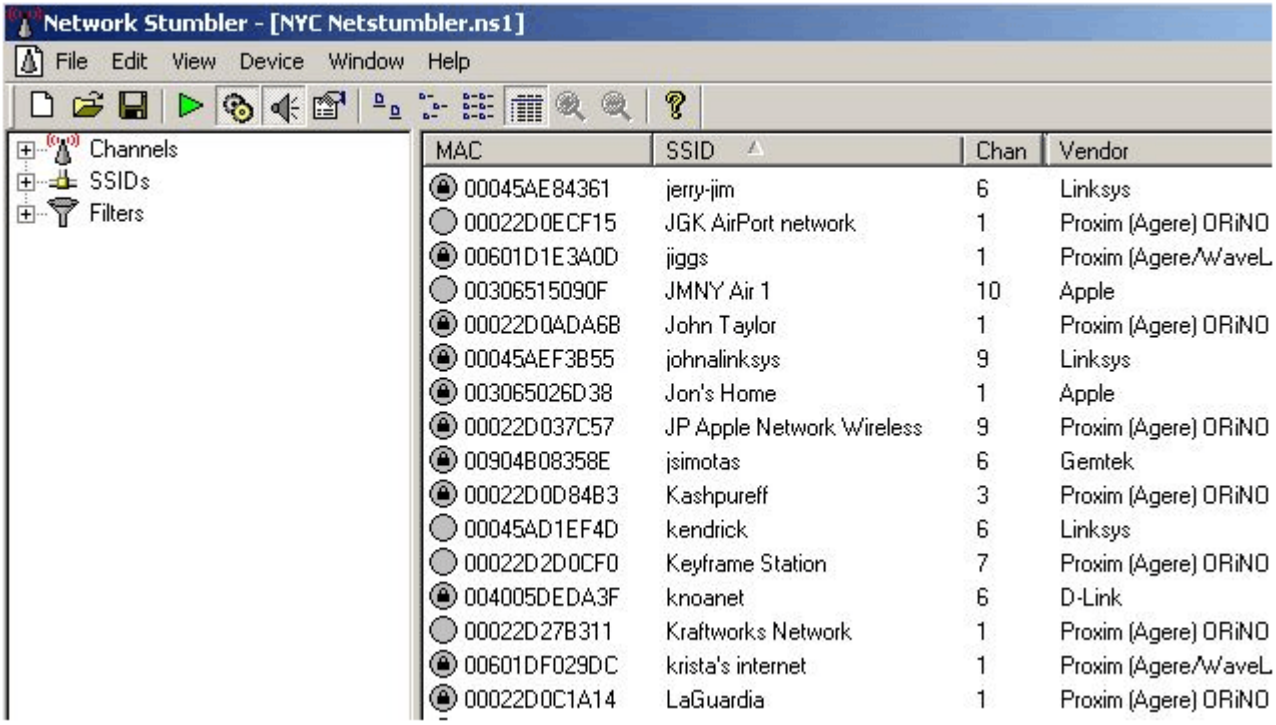
Kismet

Kismet erkennt, ob Unbefugte in Ihr Netzwerk eindringen wollen. Die Windows-Variante von Kismet benötigt den Airpcap-Adapter von Cace.



Nessus

Mit Nessus lassen sich einzelne PCs oder ganze Netzwerke komfortabel nach Sicherheitslücken untersuchen.

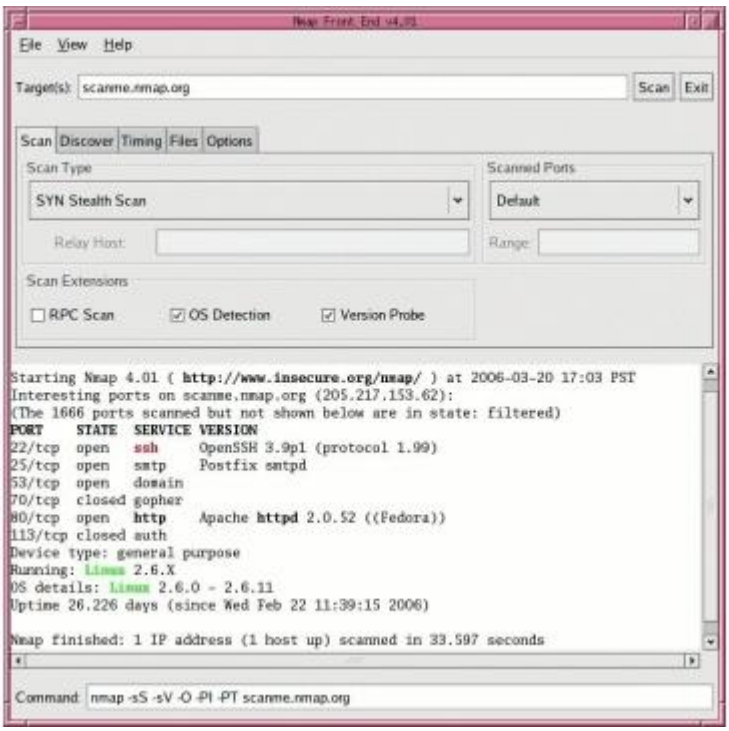


NetStumbler

Das Tool findet alle in der Nähe aktiven W-LANs und zeigt sie zusammen mit der SSID (Service Set Identifier) in Listenform an. Es führt alle wichtigen Infos wie Verschlüsselung und Funkkanal auf.
Download: NetStumbler

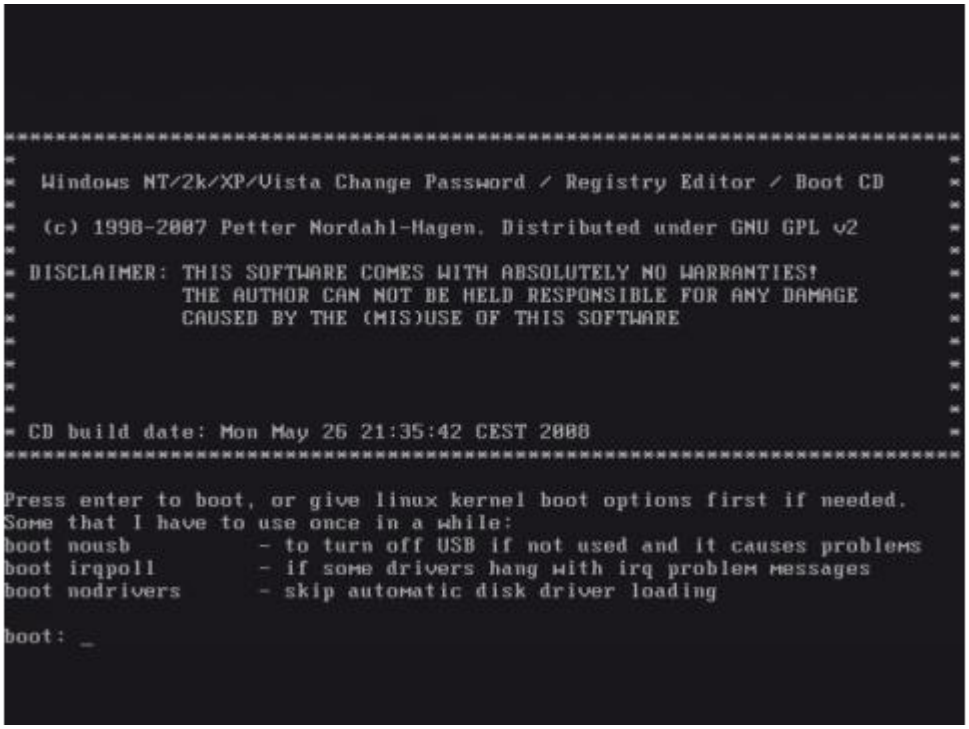
NetWorx

Möchten Sie wissen, was in Ihrem Netzwerk geschieht, dann gibt Ihnen Networx erschöpfende Auskunft. Als Icon im Tray verborgen, sammelt das Tool alle Informationen und zeigt diese auf Wunsch an.
Download: NetWorx



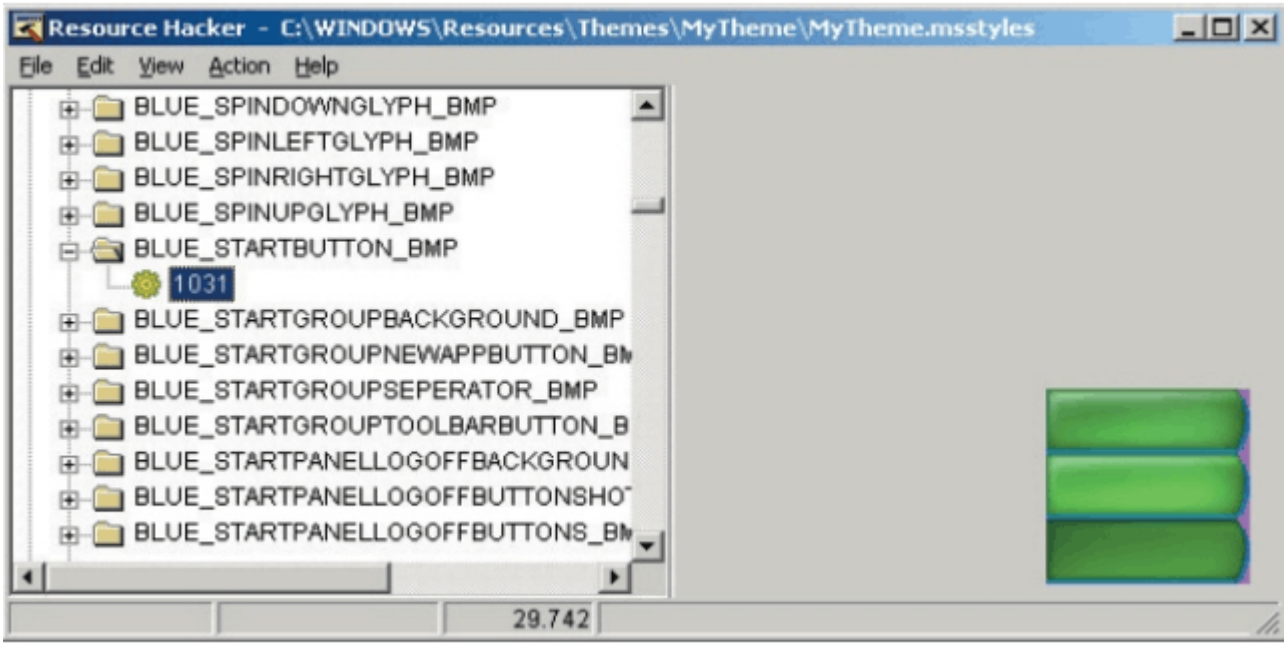
Nmap

Nmap prüft Rechner im Netzwerk oder im Internet auf offene Ports. So können Sie beispielsweise feststellen, welche Rechner im Internet oder LAN welche Dienste anbieten.



Offline NT PW & Registry Editor

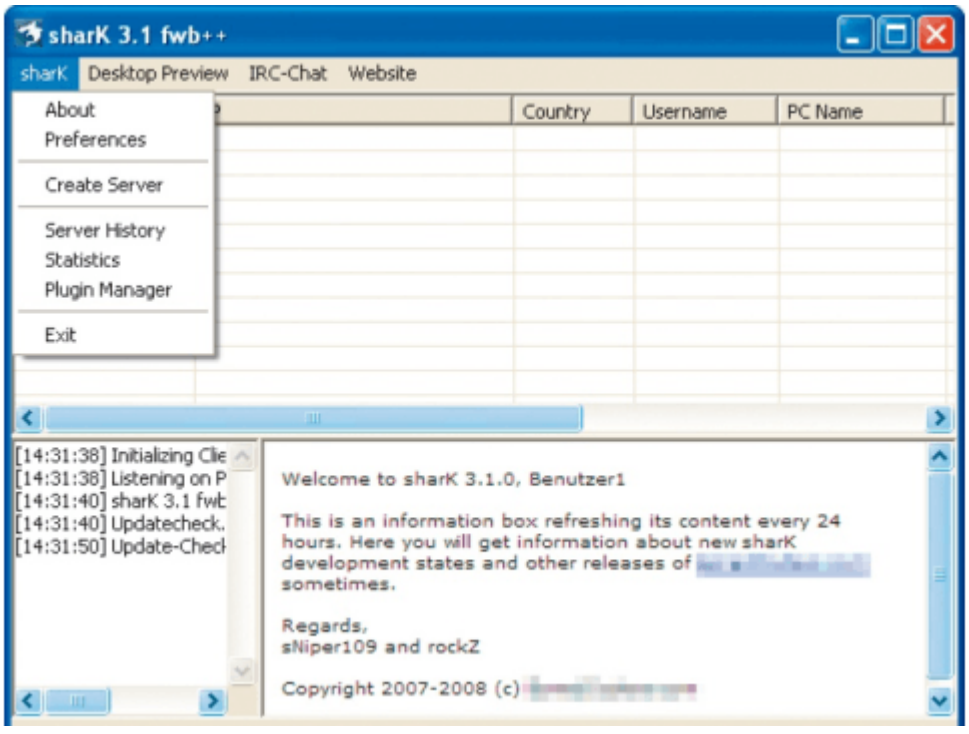
Offline NT Password & Registry Editor erfüllt nur einen simplen Zweck, den aber sehr effektiv: Es ermöglicht, das Anmelde-Passwort von Windows XP und Vista auszuhebeln.



Resource Hacker

Mit Resource Hacker lassen sich die Bedienerführungen vieler Windows-Programme verändern. Konkret sind Menüs, Beschriftungen, Tastaturkürzel, Steuerelemente und Dialogboxen manipulierbar.

[Download: Resource Hacker]



Shark

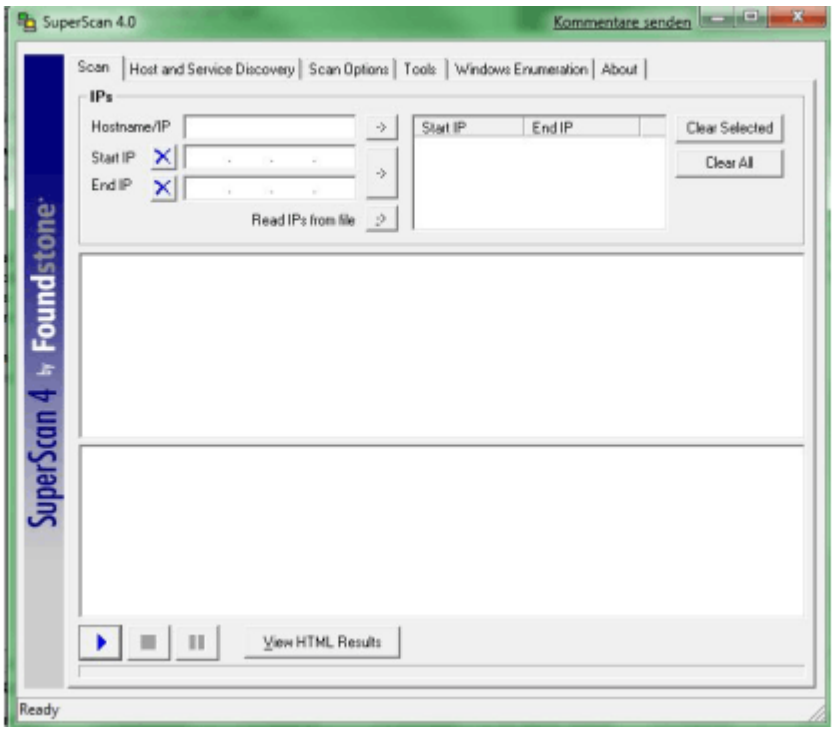
Rechner übers Internet fernsteuern – das ist der Einsatzweck von Shark. Anders als legale Remote-Desktop-Software wie Ultravnc ermöglicht Shark das aber auch ohne Kenntnis und Einwilligung des Nutzers, der vor dem entfernten PC sitzt. Die Server-Komponente von Shark tarnt sich auf vielerlei Arten, um unerkannt zu bleiben. Der Angreifer kann sie so seinen Opfern unbemerkt unterschieben, zum Beispiel per Mail oder als nützliches Programm getarnt über Web-Seiten. Die Server melden sich in regelmäßigen Abständen beim Angreifer und warten auf seine Befehle.

Snort

Snort ist ein sehr populäres Intrusion-Detection-System für Windows- und Linux-Systeme. Das Tool ist vielfältig und bietet nahezu alle Funktionen, die der Nutzer von einem aktuellen Intrusion-Detection-System erwartet.

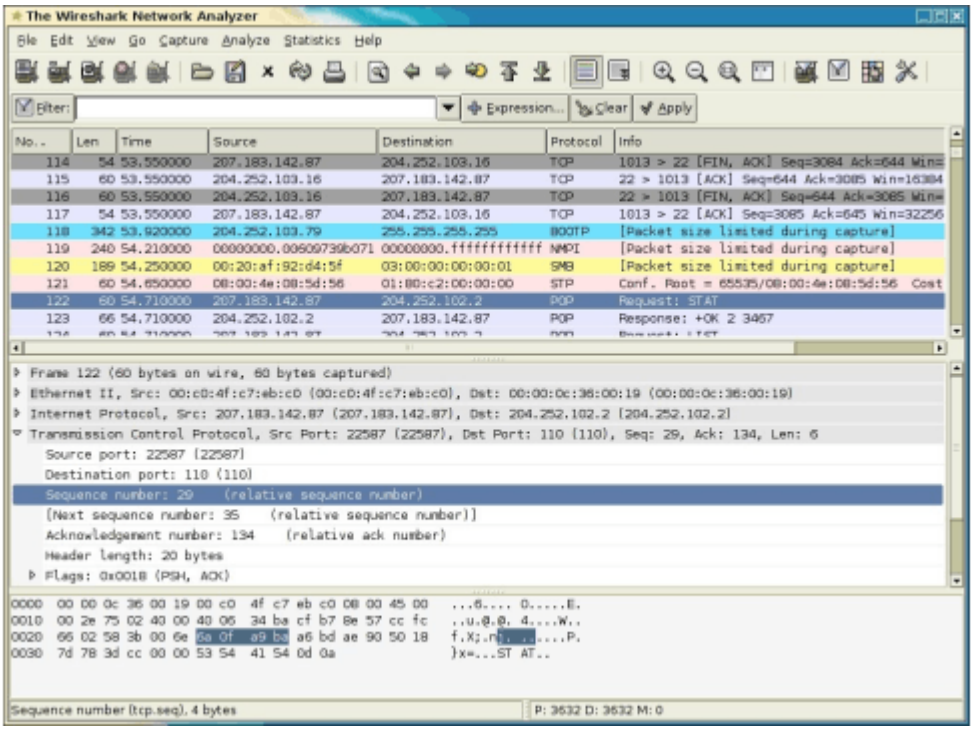
Stealther

Mit dem Gratis Firefox AddOn Stealther können Sie anonym im Internet surfen.
[Download: Stealther]



Superscan

Mit Superscan kommen Sie Hackern bei der Suche nach potenziellen Angriffszielen auf Ihrem PC zuvor. Die englischsprachige Freeware scannt Ihr System nach offenen Ports und zeigt alle möglichen Einstiegspunkte an. Dazu sendet das Suchprogramm eine Verbindungsanfrage an jede Portadresse. Anhand der Antworten erkennen Sie alle offenen Ports. Je weniger Ports geöffnet sind, desto besser.



Wireshark

Sie möchten sehen, welche Daten bei Ihnen durch die Leitung ins Internet fließen. Sie möchten so zum Beispiel feststellen, welcher Server ein bestimmtes Programm kontaktiert und was es sendet. Das Tool nutzt den universellen LAN-Treiber Winpcap, der sich vor den Treiber der Netzwerkkarte einklinkt. Dieser protokolliert alle Daten, die gesendet und empfangen werden und gibt diese an Wireshark weiter.

Mit einem Gratis-Tool könnten Sie ihren Rechner nach potenziellen Angriffszielen durchleuchten lassen. Ein böswilliger Hacker könnte aber auch genau dieses Tool nutzen, um einen fremden Rechner zu durchleuchten. Ein anderes Tool erweist sich ebenfalls als nützlich, wenn es darum geht zu überprüfen, welche Daten durch die Leitung ins Internet fließen. Aber auch dieses Tool ist hierzulande nicht erlaubt.

Hacker-Tools: Deutschland hat im August 2007 EU-Vorgaben zur Bekämpfung von Computerkriminalität umgesetzt. Der Paragraph 202c des Strafgesetzbuches hält unter "Vorbereiten des Ausspähens und Abfangens von Daten" fest: Wer eine Straftat nach § 202a (Ausspähen von Daten) oder § 202b (Abfangen von Daten) vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

15 Top-Hacker und -Spammer

Jeremy Jaynes

Er war für den ersten amerikanischen Strafprozess gegen das Versenden von unerlaubten Werbemails verantwortlich. Mit Hilfe einer gestohlenen AOL-Datenbank, welche die Kontaktadressen von mehr als 90 Million Anwendern enthielt, belästigte er die Mitbevölkerung mit Spam-Mails. Monatlich verdiente er mit dieser illegalen Tätigkeit zwischen 400.000 und 750.000 US-Dollern. Schlussendlich wurde er im November 2004 schuldig gesprochen und sollte für neun Jahre ins Gefängnis. 2008 wurde er frühzeitig entlassen. Vielleicht bekommen Sie heute noch eine Mail von Jeremy, alias Gaven Stubberfield.

Robert Alan Soloway, alias Badvertise500, Oregondude541 oder auch Worldmailer541

Er hat es geschafft, er kann sich als Top-Ten-Spammer bezeichnen. In seinen besten Zeiten hat er annähernd 500 Millionen bis zu einer Milliarde Mails pro Tag versendet. Robert verdiente sich seinen Unterhalt indem er Firmen Mail-Adressen zur Verfügung stellte und Spam-Mails verschickte. Bereits 2005 wurde er zu einer Zahlung von sieben Millionen US-Dollar an Microsoft verurteilt. Den Höhepunkt seiner dubiosen Karriere erreichte er im Mai 2007. Er wurde in Untersuchungshaft genommen und wegen 35 Anklagepunkten dem Richter vorgeführt. Eine Verurteilung steht noch aus.

Alan Ralsky

Er bezeichnete sich selbst als legalen, kommerziellen E-Mailer, obwohl er jahrelang Internetnutzer mit Spam belästigte. Beispielsweise bewarb er kleine, chinesische Firmen mit Spam-Mails. Zuvor hatte er sich aber kräftig mit Firmen-Aktien eingedeckt. Diese illegale Werbekampagne hatte einen kurzzeitigen Anstieg des Kurses zur Folge - genug Zeit, dass Alan seine Aktien gewinnbringend verkaufen konnte. Nur eines seiner wirtschaftlich lukrativen Tätigkeitsfelder. Januar 2008 wurde Ralsky wegen seiner dubiosen Machenschaften, wie etwa Aktienbetrug, Geldwäsche und Botnetz-Betrieb vom US-Bundesgericht angeklagt.

Kevin Mitnick

Der Inbegriff eines Hackers: Er ist wohl einer der bekanntesten Hacker der frühen Computergeschichte. Condor, wie sein Spitzname lautet, wird von der breiten Öffentlichkeit als der Hacker schlechthin angesehen. Ihm war es möglich, so ziemlich jeden Computer unter seine Gewalt zu bringen. Seinen umstrittenen Ruhm erreichte er durch diverse Hacks in das Netzwerk des Pentagons und in die NSA-Computer. Erstmals wurde Mitnick 1988 verhaftet. 1995 folgte der nächste längere Aufenthalt im Gefängnis. Nach fünfjähriger Haft wurde er mit einer Bewährungsauflage in die Freiheit entlassen. Er durfte für drei Jahre keine EDV-Systeme benutzen. 2003 war es Mitnick wieder erlaubt im Internet zu surfen. Sein erster Webseiten-Besuch wurde vom amerikanischen Fernsehen live übertragen. Heute fungiert Condor als Sicherheitsberater und Online-Journalist.

Karl Werner Lothar Koch

"Wissen muss für jeden Menschen gleich zugänglich sein!": Diese durchaus sinnvolle Aussage stammt von einem deutschen Hacker-Anarchisten namens Karl Werner Lothar Koch. Hagbard Celine, sein Pseudonym in Netzwerken, wurde berühmt, durch den so genannten KBG-Hack. Seine Hacker-Gruppe drang in westliche Computersysteme ein, stahl Informationen und verkaufte diese schlussendlich an den sowjetischen Geheimdienst. Wegen lächerlichen 75 US-Cent Differenz in der Buchhaltung, enttarnte der amerikanische Astrophysiker Clifford Stoll die Machenschaften dieser Hacker-Vereinigung. Unter anderem gründete Karl einen Ableger des Chaos Computer Clubs und war fortwährend davon überzeugt, dass Illuminaten existierten. Der dauerhaft Drogen konsumierende Hagbard versuchte diese durch seine Hacks in die Schranken zu weisen. 1989 wurde Karl Kochs verbrannte Leiche in einem Wald gefunden. Hacker-Freunde sind der festen Überzeugung, dass es sich um einen Mord handelte. Die offizielle Todesursache lautet Selbstverbrennung.

Sanford Wallace

Auch bekannt unter dem Pseudonym "Spamford", hat sich einen Namen als Massenversender von Spam-Mails gemacht. Spamford hatte anscheinend schon immer etwas übrig für die Belästigung von Personen durch ungewollte Mitteilungen. Seine Karriere startete er mit Werbefaxen, so genannten "Junk Fax". In den späten Neunzigern gründete Sanford die Firma Cyber Promotions. Die Selbstvermarktungskampagne, durch Mail-Spamming, verhalf Sanfords Firma Cyber Promotions zu einer Spitzenposition im Mail-Marketing. In den folgenden Jahren ging es bergauf und bergab mit seinen Spam-Vorhaben. Abermals erregte er Aufsehen mit der Beteiligung an dem Projekt SmartBotPro. Die Software SmartBot verbreitete eine Spyware, freundlicherweise bat die Firma gleichzeitig auch eine Software zur Entfernung für 30 US-Dollar an. Schlussendlich wurde SmartBot verklagt und musste eine Strafe von über vier Millionen US-Dollar akzeptieren.

Boris F., besser bekannt als Tron

Er galt als einer der talentiertesten Hacker seiner Zeit. Im Gegensatz zu Kim und Karl ging es ihm nie ums Geld. Er wollte mit seinen Hacks nur beweisen, dass fast jedes Computer-System der Welt Lücken vorweist. Ihm machte es einfach Spaß, sich mit der Elektronik und den damit verbundenen Sicherheitssystemen auseinanderzusetzen. Beispielsweise knackte er Bezahlsender und Telefonkarten-Unternehmen. Grundsätzlich ging es Tron aber immer darum, sich mit vermeintlich sicheren Standards auseinanderzusetzen und daran "rumzufummeln". So gelang es ihm beispielsweise, dramatische Sicherheitslücken in dem weltweit anerkannten Mobilfunkstandard GSM ausfindig zu machen. Nicht nur diese "Heldentat" verschaffte ihm einen Ehrenplatz im Chaos Computer Club. Im Oktober 1998 fand ein Spaziergänger an einem Baum die erhängte Leiche von Boris F. Der CCC zweifelt bis heute an dem angeblichen Selbstmord von Tron.

Richard Stallman

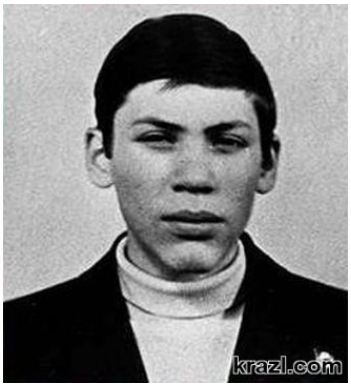
Er ist ein Guter der Szene. Im ursprünglichen Sinne ist er ein Hacker, aber großteils verantwortlich als Aktivist für freie Software und Programmentwicklung. Er gründete das GNU-Projekt und war der erste Präsident der Free Software Foundation. Stallman gilt als Vorkämpfer der "freien Software" und hält beständig an dem Gedanken fest, dass gute Software durchaus von End-Usern direkt entwickelt werden kann. Sein Credo: Freier Zugang auf die Programmiersprache und deren Code.

Robert Tappan Morris

Auch bekannt unter dem Kürzel rtm, ist verantwortlich für den ersten Internet-Wurm der Computergeschichte. Im Jahre 1988 programmierte er im Alter von 23 den mittlerweile legendären Morris-Wurm. Ironischerweise war zu dieser Zeit sein Vater der Chef der NSA-Sicherheitsabteilung. Robert wurde als Urheber des Wurms geschnappt, zu einer Bewährungsstrafe verklagt, bekam eine saftige Geldstrafe und musste sozialen Dienst ableisten. Heute unterrichtet Professor Robert Tappan Morris am weltberühmten Massachusetts Institute of Technology, kurz MIT.

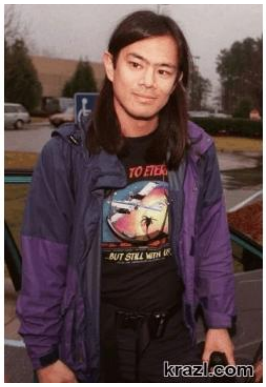
Kevin Lee Poulsen, alias Dark Dante

Er beschäftigte sich schon in jungen Jahren mit Phreaking, dem Manipulieren von Telefonanrufen mittels Pfeifsignalen. Eigentliche wollte Dark Dante Anfang der Neunziger nur ein paar Reisen gewinnen, etwas "Taschengeld" sein Eigen nennen und in einem sportlichen Porsche durch die Gegend heizen. Diese Wünsche erfüllte er sich durch konkrete Manipulation der Telefonanlagen von Radiostationen. Beispielsweise gewann jeder 102. Anrufer bei den KISS-FM-Wettbewerben nicht minder wertvolle Preise. Natürlich waren Kevin und seine Freunde Ronald Austin und Justin Peterson des Öfteren der 102. Anrufer. Spionage wurde Poulsen im Jahre 1992 unterstellt. Auch für so manch illegalen Hack in die Systeme von Telefongesellschaften ist er verantwortlich. Insgesamt verbrachte Dark Dante fünf Jahre hinter Gitter. Wie viele Ex-Hacker beschäftigt sich Poulsen heutzutage mit der Sicherheitsproblematik und ist als freier Journalist tätig.



Vladimir Leonidovich Levin

Er erleichterte in einem seiner Hacker-Coups die Citibank um die stolze Summe von zehn Millionen US-Dollar. Auch er kam nicht ungestraft davon. Bereits 1995 wurde er von Interpol geschnappt. Erst 1998 erging der Schuldspruch und er musste für drei Jahre ins Gefängnis. Eine Strafe von über 240.000 US-Dollar hatte er ebenfalls zu begleichen.

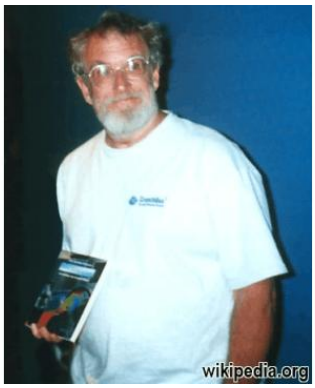


Tsutomu Shimomura

In Hacker-Kreisen wird unterschieden zwischen guten und schlechten Taten. Diejenigen, die schlimmes im Sinn haben, werden als "Black Hats" bezeichnet. Die "guten" Hacker, wie es beispielsweise Tsutomu Shimomura ist, werden "White Hat" genannt. Geschichtlich betrachtet, erreichte er seine Berühmtheit durch die Verfolgung von Kevin Mitnick. Eines schönen Tages drang Kevin in das Netzwerk-System des Supercomputing Centers in San Diego ein. Sein Pech, dass Tsutomu Shimomura dort arbeitete, den Hack und Datenklau bemerkte und die digitale Verfolgung aufnahm. Tsutomus Hacker-Einsatz führte schlussendlich zur Verhaftung von Condor.

Gary McKinnon

Der Mann ist besser bekannt unter seinem Alias Solo. Er hat anscheinend eine Schwäche für UFOs und außerirdische Lebensformen. Eigenen Angaben zufolge, drang er nämlich nur in die Computer des amerikanischen Militärs, der NASA, des Pentagons und zahlreichen anderen wichtigen Organisationen ein, um Information über UFOs zu erhalten. Sie können es glauben oder nicht - er behauptet jedenfalls, dass er so manchen Hinweis entdeckt hätte. Trotzdem wartet der britische Systemadministrator noch immer auf seine Auslieferung und Verurteilung in den USA. Im schlimmsten Fall muss er eine siebzigjährige Haftstrafe absitzen, denn dieser Gray-Hat-Hacker wird beschuldigt "den größten Angriff auf militärische Computer" begangen zu haben.



John T. Draper

John T. Draper. Der Mann ist besser bekannt unter dem Pseudonym Captain Crunch, ist einer der bekanntesten Hacker und Phreaker der sechziger und siebziger Jahre des letzten Jahrtausends. Seine Popularität verdankt er einer Spielzeug-Pfeife, die als Werbeaktion den so genannten Cap'n Crunch Cornflakes beilag. Er fand heraus, dass er durch Abkleben einiger Pfeifenlöcher einen Frequenz-Ton von genau 2600 Hertz erreichen konnte. Pfiff er diesen Ton in den Telefonhörer, war er in der Lage, Telefonate zu manipulieren. Seine Methode des Telefon-Phreakings wurde weiterentwickelt und führte schlussendlich zu dem feststehenden Begriff des Blue-Boxings. Schnell verbreitete sich dieser Phreaking-Weg in der Szene, sogar das organisierte Verbrechen, wie etwa die Mafia, wurde auf Drapers Errungenschaft aufmerksam. 1971 wurde Captain Crunch erstmalig verhaftet, schloss aber gleichzeitig Freundschaft mit Steve Jobs und Steve Wozniak. Unter anderem programmierte er in seiner Haftzeit das erste Textverarbeitungs-Tool Easy Writer für den Apple II.

Kim Schmitz

Laut Kimble, wie sich Kim Schmitz in der Hacker-Szene nannte, hatten seine Hacker-Taten das "rühmliche" Motiv, die Firmen auf Sicherheitsmängel aufmerksam zu machen. Trotzdem war er unumstritten der Medienkönig der deutschen Hacker-Szene, verantwortlich für Computer-Manipulationen, Kreditkartenfälschungen, Einbrüche in Großrechner oder diverse Datenausspähungen. Sein kriminelles Computerunwesen trieb er weltweit. Beispielsweise hackte er auch amerikanische Calling-Cards, rief mit deren Hilfe seine gegründeten Talk-Lines an und kassierte schlussendlich enorme Geldsummen. Dies ist nur eines von vielen Vergehen. 1994 durfte Kim erstmalig dem Gefängnis einen Besuch abstatten. Mittlerweile widmet sich Kimble legaleren Angelegenheiten, wie etwa als Geschäftsführer einer Datensicherheits-Firma.