

*Wszystkim, którzy troszczyli się o mnie,  
gdy byłem pędrakiem,  
zwłaszcza moim kochającym rodzicom  
i Kiarze*

## O autorze

Ankit Fadia urodził się 24 maja 1985 r. Wyrósł w atmosferze sprzyjającej rozwijaniu zainteresowań o charakterze naukowym. Wcześniej zafascynowała go informatyka.

Witryna Hacking Truths, którą początkowo stworzył dla małego kręgu przyjaciół, szybko się rozrosła i zdobyła tysiące użytkowników, zamawiających subskrypcję informacji i dokumentacji. Głównym celem witryny było promowanie etycznego hackingu. Hakerzy działający zgodnie z kodeksem etycznego hackingu zrewolucjonizowały sytuację na scenie bezpieczeństwa.

Ankit publikuje również artykuły w kilku magazynach komputerowych i witrynach internetowych. Można się z nim skontaktować pod adresem <http://hackingtruths.box.sk>.

Oprócz nauki i techniki interesuje się także obserwacjami nieba i samolotami. W wolnych chwilach słucha muzyki. Nie odmawia sobie pizzy i lodów. Jest fanem serialu „Z archiwum X”. Interesuje się zjawiskami paranormalnymi.

# Przedmowa

Siedemnastolatek Ankit Fadia napisał bardzo dobrą książkę. Wyjaśnia w niej bardzo szczegółowo m.in. niuanse znaczeń terminów „haker” i „cracker”. Doradza, jak rozpoznać tych, którzy mają złe intencje, i jak obronić się przed ich atakami.

Hacking jest nieustannym źródłem zmartwień wszystkich, którzy na co dzień korzystają z technologii komputerowej. Dzisiaj, kiedy żyjemy wśród zaawansowanych technologii, sieci szerokopasmowych, technologii multimedialnych, sztucznej inteligencji, wirtualnej rzeczywistości i systemów rozpoznawania głosu, tzw. nieetyczny haker może podglądać dane lub nawet je zniszczyć. Na podstawie własnych badań i literatury Ankit sformułował wskazówki, jak rozpoznawać hakerów, którzy mają złe zamiary i mogą uszkodzić oprogramowanie systemu i sprzęt.

To wspaniałe, że tak młody człowiek napisał książkę na tak ważny, a często pomijany temat. Poruszył w niej niemal wszystkie aspekty hackingu, wiele jego przemyśleń może zmienić nasze spojrzenie na technologie informatyczne. Autor przekazuje nam wiedzę niezbędną w dzisiejszym szybko zmieniającym się świecie.

Jestem przekonana, że książka ta zdobędzie szerokie grono czytelników.

Dr S. Chona  
Dyrektorka Delhi Public School  
R. K. Puram  
New Delhi

# Wstęp

Słowa „hacking” i „hakerzy” są na ogół odbierane negatywnie. Bardzo często kojarzone są z przestępcami komputerowymi, którzy uszkadzają systemy, wypuszczają wirusy i czynią inne szkody. Trudno kogoś winić, że tak postrzega hakerów. Opinia publiczna bardzo często akceptuje poglądy przekazywane w środkach masowego przekazu, a dzisiejsze media mylnie nazywają przestępców komputerowych „hakerami”. Tymczasem hakerzy nie mają nic wspólnego z działaniami przestępczymi. Negatywne nastawienie do hakerów nie ma uzasadnienia w rzeczywistości.

Obraz prezentowany w mediach jest mocno zniekształcony. Hakerzy są normalnymi, sympatycznymi i bardzo inteligentnymi ludźmi, którzy, wykorzystując swoje umiejętności w konstruktywny sposób, pomagają organizacjom chronić dokumenty i poufne dane. Dzięki nim rządy mogą się dowiedzieć, jak zabezpieczać dokumenty o znaczeniu strategicznym dla państwa. Czasem nawet hakerzy dostarczają dowodów w postaci elektronicznej. Dzięki temu znacznie łatwiej jest bronić się przed przestępcami komputerowymi.

Pan Malik jest programistą w firmie z listy Fortune 500. Kiedy podzieliłem się z nim pomysłem napisania książki na temat hakerstwa, w której poparłbym hakerów kierujących się etyką, zareagował niedowierzaniem i odrzucił pomysł. Stwierdził, że publikowanie instrukcji hackingu zwiększy jedynie liczbę przestępstw komputerowych. W jego opinii należało raczej zaostrzyć prawo, aby skuteczniej karać przypadki nieuczciwego hackingu (a właściwie crackingu). Pomyślał, że jestem niespełna rozum i sprzeciwił się idei powstania tej książki oraz witryny internetowej o podobnym charakterze. Tak zdecydowanie negatywne stanowisko w tej sprawie jest zrozumiałe, ponieważ pseudohakerzy wykradli mu kiedyś pulę godzin na połączenie z Internetem i od tamtego czasu jego opinia o hakerach była, delikatnie mówiąc, „zła”.

Od czasu, kiedy małpa straciła bujne owłosienie i przybrała pionową postawę, człowiek nauczył się wykorzystywać do obrony narzędzia, które równocześnie są narzędziami agresji. Typowymi przykładami są energia jądrowa lub zwykły nóż.

Pewnego wieczoru oglądałem w telewizji program o szczepionkach i ich znaczeniu dla ludzkości. Wynalezienie szczepionek to najlepsza rzecz, jaka mogła się zdarzyć w świecie medycyny. Szczepionki ocaliły i ocalają miliony istnień ludzkich. Uderzyło mnie to, że zwalczanie zła złem daje dobre wyniki.

Największym problemem misji kosmicznych NASA było usuwanie odpadów fizjologicznych oraz zaopatrzenie załogi w czystą wodę. Pewien młody biolog zaproponował, aby „odpady fizjologiczne poddać skomplikowanemu procesowi konwersji do

czystej wody zdanej do picia”. Początkowo inni naukowcy odrzucili ten niekonwencjonalny pomysł. Jednak po szczegółowych debatach doszli do wniosku, że uzdatnianie substancji z natury szkodliwych jest ciekawym wyzwaniem.

Historia udowodniła, że aby ochronić się przed niebezpieczeństwem lub je zlikwidować, trzeba umieć wykorzystać niektóre ze szkodliwych elementów tak, by przyniosły pozytywny efekt. Postaram się udowodnić, że historia lubi się powtarzać.

Żaden system prawny nie odstraszy przestępców komputerowych. Crackerzy są coraz sprytniejsi i z coraz większą łatwością włamują się do systemów, czynią wielkie szkody, po czym znikają bez śladu. Nawet najlepszy system prawny będzie całkowicie nieskuteczny, jeśli administratorzy systemu pozostaną ignorantami w dziedzinie bezpieczeństwa i poprzestaną na kojarzeniu hakerów z przestępcami. Najwyższy czas pokazać wszystkim, jakie metody wykorzystują crackerzy, jak przeprowadzają ataki i jak chronić przed nimi systemy komputerowe. Jeżeli tego nie zrobimy, crackerzy będą górą, a tego przecież nie chcemy, prawda?

Gdyby pan Malik wiedział więcej o metodach działania przestępców komputerowych, potrafiłby zabezpieczyć swoje konto internetowe (i miał lepsze zdanie o hakerach). Ten, kto dowie się, jak włamać się do systemu komputerowego, postara się o załatwienie luki bezpieczeństwa, zanim zdarzy się nieszczęście. Po prostu zamiast obawiać się ognia i uciekać przed nim, korzystajmy z jego ciepła.

Ankit Fadia

# Zastrzeżenie

Poglądy wyrażane w książce są wyłącznie opiniami Autora. Wszystkie rady i wskazówki zostały podane w dobrej wierze, ale nie ma całkowitej pewności, że zawsze będą skuteczne. Czytelnik korzysta z tej książki wyłącznie na własną odpowiedzialność. Wydawca nie ponosi żadnej odpowiedzialności za ewentualne szkody, powstałe w wyniku wykorzystania informacji zawartych w tej książce.

# Rozdział I

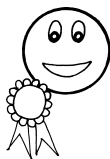
## Kim jest haker?

W tym rozdziale:

- Hakerzy: kim oni są
- 14-latek z tej samej ulicy nie jest przestępcą
- Hakerzy: zachęcające przykłady osiągnięcia sukcesu

Większość ludzi uważa hakerów za komputerowych wandalów. Spróbujcie jednak nazwać hakera przestępcą, a zdenerwuje się, a może nawet zareaguje jeszcze gorzej. Hakerzy nie są przestępcami. Dlaczego większość ludzi tak ich postrzega? Odpowiedzialność ponoszą media. Ogromna większość ludzi czerpie swoje opinie z mediów, nie zastanawiając się nad prawdziwością przekazywanych treści. To media namalowały obraz hakera, który jest wandalami uszkodzającym pliki systemowe na serwerach, uwalniającym wirusy, zmieniającym zawartość witryn internetowych i odpowiedzialnym za wiele innych rzeczy.

Prawdziwi hakerzy określają włamywaczy mianem crackerów. Autorzy wirusów komputerowych nie są hakerami, a jedynie programistami kodującymi wirusy.



Haker – w tradycyjnym znaczeniu tego słowa – to komputerowy hobbysta, wiedzący prawie wszystko o sprzęcie i oprogramowaniu, powszechnie szanowany za swoją głęboką wiedzę. Jednak z upływem lat reputacja hakerów systematycznie się obniżała. Dziś budzą obawę i są postrzegani jako subkultura o znamionach przestępczych.

Hakerzy wiedzą prawie wszystko o tym, jak działają programy komputerowe. Potrafią wykonać rzeczy pozornie niemożliwe.

Często udaje im się odkryć sposoby wykorzystania programów komputerowych odmienne od założeń producenta lub autora. Analizując kod programu metodą prób i błędów, wyszukują nowe funkcje i odkrywają jego tajniki. Owszem, włamują się do systemów komputerowych, ale nie powodują szkód ani nie kradną haseł. Informują administratora systemu o lukach i zagrożeniach bezpieczeństwa. Próbuje wykryć nieznane dotąd cechy programów. Można powiedzieć, że hakerstwo jest zdobywaniem wiedzy, a hakerzy są tymi, którzy mają o kilka bitów informacji więcej niż inni. Znają rzeczy, o których przeciętni użytkownicy komputerów mogliby tylko pomarzyć.



Trzy najważniejsze oznaki świadczące o tym, że dana osoba nie jest prawdziwym hakerem:

1. Posługiwanie się dziwacznymi nazwami w rodzaju: Avenger (Mściciel), Dark Cloud (Ciemna chmura), Skull (Czaszka), Kewl Dude itd. Oczywiście sam pseudonim daje niewiele informacji.
2. Przechwałki, co jest oczywistą oznaką, że komuś brakuje rzetelnej wiedzy.
3. Lekceważący i obraźliwy stosunek do osób początkujących, które zadają pytania.

Hakerzy są miłymi ludźmi, od których można się wiele nauczyć. Zwykle są bardzo uczynni i chętnie służą pomocą i dzielą się swoją wiedzą.

Trzeba jednak przyznać, że hakerów rozdziela od crackerów bardzo cienka linia i niewielu opiera się pokusie jej przekroczenia.

Przyczyną, dla której tak zwani hakerzy przekraczają tę granicę i stają się crackernami, jest chęć zdobycia rozgłosu. Jest to jednak popularność typu negatywnego. Proszę mi wierzyć, że włamać się do systemu komputerowego jest bardzo łatwo. W ten sposób można zdobyć rozgłos w hakerskim podziemiu, ale nie trwa on długo. Populacja hakerów rozrosła się i ludzie szybko zapominają o wcześniejszych osiągnięciach.

Zwykli ludzie nie darzą takiej osoby sympatią. Trudno się temu dziwić, jeśli ktoś niszczy witryny WWW, wykonuje ataki powodujące zablokowanie serwerów (denial of service), wypuszcza wirusy itd. Z tego względu społeczeństwo widzi w hakerach przestępców.

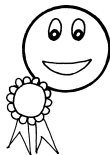
Cracker ma szansę stać się znanym jedynie w środowisku komputerowego podziemia. W przeciwieństwie do niego etyczny haker będzie popularny w szerszych kręgach, również w „normalnej” części społeczeństwa. Cracker może mu tylko pozazdrościć większego rozgłosu.

Cracker jest ścigany przez administratorów systemów i policję. Inaczej ma się rzecz, jeśli zawiadomisz administratora o dziurach w zabezpieczeniach systemu. Będzie wdzięczny. Może nawet zaproponuje, byś włamywał się do jego systemu w celu testowania zabezpieczeń. Czyż nie o tym właśnie marzą wszyscy hakerzy?



Przestępstwa komputerowe są ścigane z mocy prawa i są traktowane bardzo poważnie. Wśród kar, które czekają cyberkryminalistów, są więzienie, wysokie grzywny, a nawet dożywotni zakaz używania komputerów. Sądy na ogół niechętnie zwalniają ich za kaucją.

Nie jest to podręcznik dla prawników. Podam tylko konkretny przykład, który pomoże Wam dokonać właściwego wyboru.



W USA żył sobie kiedyś 13-letni haker. Miał kolegę. Obaj uwielbiali programowanie i hacking. Prześcigali się nawzajem we włamywaniu do swoich komputerów. Obaj byli bardzo inteligentni i chcieli zrobić karierę.

Obaj koledzy mogli stać się crackerami i robić różne głupie rzeczy, które w rezultacie zrujnowałyby im życie. Ale na swoje szczęście, a także na szczęście nas wszystkich, tego nie zrobili. Dziś znamy ich jako Billa Gatesa i Paula Allena. Obaj są bardzo, bardzo zamożni.

Gdyby przekroczyli granice etyki, mogliby tkwić całe życie w więzieniu. Ludzie nazwaliby ich przestępcami, a administratorzy systemów chcieliby ich #&^\*\*#. Nasi bohaterowie mają jednak głowy na karku i dziś zajmują pozycję, o jakiej marzy wielu z nas.

Nie mówię, że mielibyśmy zupełnie zrezygnować z hackingu. Popieram hacking i chciałbym, aby więcej ludzi się nim zajmowało i włamywało do komputerów, pod warunkiem, że będą to robić w słusznym celu. Nie czyńcie nikomu szkody. Prawdziwy haker wie, że podstawową zasadą etyki hakera jest nie czynić żadnego zła, nie usuwać żadnych plików i nie czynić żadnej szkody w systemie, do którego się włamał. Wykorzystajcie swoją wiedzę, aby zrobić coś legalnego, na przykład poprawić jakość usług świadczonych przez różne firmy. Skorzystają na tym wszyscy, branża komputerowa i cała gospodarka. Jeżeli zrobicie przynajmniej jedną z tych dobrych rzeczy, staniecie się sławni i bogaci.

## Rozdział II

# Znajdowanie informacji w sieci

W tym rozdziale:

- Internetowe zasoby dla hakerów
- Co musi znaleźć się w składnicy wiedzy hakera
- Najlepsze witryny hakerskie

Internet jest najbardziej wyczerpującą i wszechstronną składnicą informacji i wiedzy. Nietrudno się w nim zgubić. Trzeba umieć poruszać się w sieci. W tym rozdziale omówię metody wyszukiwania użytecznych informacji.

Zajmijmy się najpierw wyszukiwarkami. Z doświadczenia wynika, że metawyszukiwarki dają dokładniejsze wyniki niż zwykłe wyszukiwarki. Moim ulubionym narzędziem jest serwis Askjeeves pod adresem [www.askjeeves.com](http://www.askjeeves.com). Wśród zwykłych wyszukiwarek prym wiedzie Altavista ([www.altavista.com](http://www.altavista.com)). Nie tylko przeszukuje zasoby WWW, ale także ma opcję przeszukiwania grup dyskusyjnych (usenet newsgroups). Aby dokładnie sprawdzić zawartość grup newsowych, należy skorzystać z Dejanews ([www.dejanews.com](http://www.dejanews.com)).

Sama wiedza, które wyszukiwarki są najlepsze, to za mało. Trzeba jeszcze umieć efektywnie z nich korzystać. Po wpisaniu haseł w rodzaju „hacking”, „cracking”, „hacker” lub nawet „learn to hack” pojawiają się odsyłacze do bardzo wielu witryn i artykułów w grupach dyskusyjnych.

Znaczna liczba odsyłaczy wcale nie ułatwia zadania. Wśród nich będą dziwaczne witryny, w których na czarnym tle pojawia się czcionka o nietypowych kolorach i rozmiarach, witryny z czaszkami i czerwonymi obracającymi się oczyma, z plikami JPEG ogromnych rozmiarów, a także witryny z banerami w rodzaju „learn to hack Hotmail” (naucz się włamywać do serwisu Hotmail) i pretensjonalnymi hasłami w rodzaju „I am a 31337 haxor, doodz!!!” Tak się jakoś składa, że w takich witrynach próżno szukać przydatnych informacji. Należą one do osobników posługujących się gotowymi programami ściągniętymi z Internetu, którzy nie mają większego pojęcia o tym, co robią. Nic dziwnego, że są szybko wyłapywani, a media mają pożywkę do materiałów przedstawiających hakerów w negatywnym świetle.

Trzeba wiedzieć, w jaki sposób wykorzystywać wyszukiwarki w celu znalezienia użytecznych informacji. Za pomocą cudzysłowu można precyzyjnie formułować hasła i ograniczyć zakres poszukiwań. Na przykład wyszukiwanie za pomocą hasła *hacking Hotmail* (bez cudzysłowu) przyniesie w rezultacie bardzo różne hiperodsyłacze: i takie, które nie mają związku z włamywaniem się na serwery Hotmail, na przykład odsyłacze do informacji prawnych dotyczących firmy Hotmail, a także takie informacje, które są ściśle związane z włamywaniem się na serwery Hotmail. Za to poszukiwanie za pomocą tego samego zwrotu, ale w cudzysłowie („hacking Hotmail”) daje oczekiwane wyniki.

Parametry wyszukiwania można uściślić, używając operatorów logicznych (AND, +, OR, NOT, -). Na przykład wpisanie hasła „hacking – exploits” daje wyniki związane z włamywaniem się, ale nie związane z exploits. W podobny sposób można stosować operatory + oraz NOT.

Istnieją także wyszukiwarki wyspecjalizowane w dziedzinie bezpieczeństwa systemów i sieci komputerowych. Najbardziej popularną z nich jest Astalavista ([astalavista.box.sk](http://astalavista.box.sk)). Bardzo dobra jest także wyszukiwarka Antisearch ([www.antisearch.com](http://www.antisearch.com)). Z kolei Anticode ([www.anticode.com](http://www.anticode.com)) służy do wyszukiwania oprogramowania z dziedziny bezpieczeństwa. Serwisy Anticode i Antisearch są własnością firmy Antionline.

Grupy dyskusyjne służą do wymiany doświadczeń zarówno początkujących, jak i doświadczonych hakerów. Jednak w każdej grupie znajdzie się ktoś, kto zamiast podzielić się informacją, próbuje udowodnić swoją intelektualną wyższość, a na zadane pytanie reaguje zaciętrzewieniem.

Czy jest coś złego w zadawaniu pytań? Oczywiście, że nie. Nawet na najgłupsze pytanie można dać dobrą odpowiedź. Najlepszą metodą nauki jest zadawanie pytań. Dlatego odpowiadam najlepiej, jak umiem, na każde pytanie.

Nie jest łatwo zostać hakerem. Nie można nim się stać tak po prostu w ciągu jednego dnia. Trzeba być doświadczonym i inteligentnym programistą i znać od podszewki przynajmniej jeden system operacyjny. Trzeba także być za pan brat z sieciami, TCP/IP i różnymi innymi protokołami.

Większość ludzi idzie na skróty i zamiast dokładnie studiować różnego rodzaju dokumentację, uruchamia gotowe programy i z powodu braku doświadczenia i wiedzy przypadkowo czyni szkody w systemie zdalnym, a potem spędza resztę życia w więzieniu!

Aby stać się prawdziwym hakerem, trzeba ciężko pracować. Nie ma innej drogi! Najlepiej zaopatrzyć się we wszystkie możliwe dokumentacje i instrukcje. Jestem wyznawcą teorii „pobierania wszystkiego za darmo z Internetu”, ale niestety nie zawsze daje ona oczekiwany efekt. Pewne książki koniecznie trzeba kupić.

Najwięcej informacji tkwi w dokumentach RFC (Request For Comment). W czasach Arpanetu RFC były grupami dyskusyjnymi. Zawierają najpełniejszy opis działania Internetu. Idealnym rozwiązaniem byłoby nauczenie się na pamięć całej dokumentacji RFC. Ale co doradzić tym wszystkim, którzy muszą spać i jeść i nie mają aż tak wiele wolnego czasu? Można im dać pełną listę dokumentów RFC z numerami i tytułami. Najlepszą metodą odnalezienia konkretnego RFC jest użycie wyszukiwarki (polecam Google). Jeśli potrzebny jest dokument RFC 821, wystarczy w polu wyszukiwania wpisać „RFC 821”.

Istnieje też spis wszystkich RFC!! Jest to RFC 825. Zanim jednak ściągniesz z sieci 2 kB tych dokumentów, pamiętaj, że są adresowane do zaawansowanych użytkowników. Nowicjusze mogą mieć problemy z ich zrozumieniem.



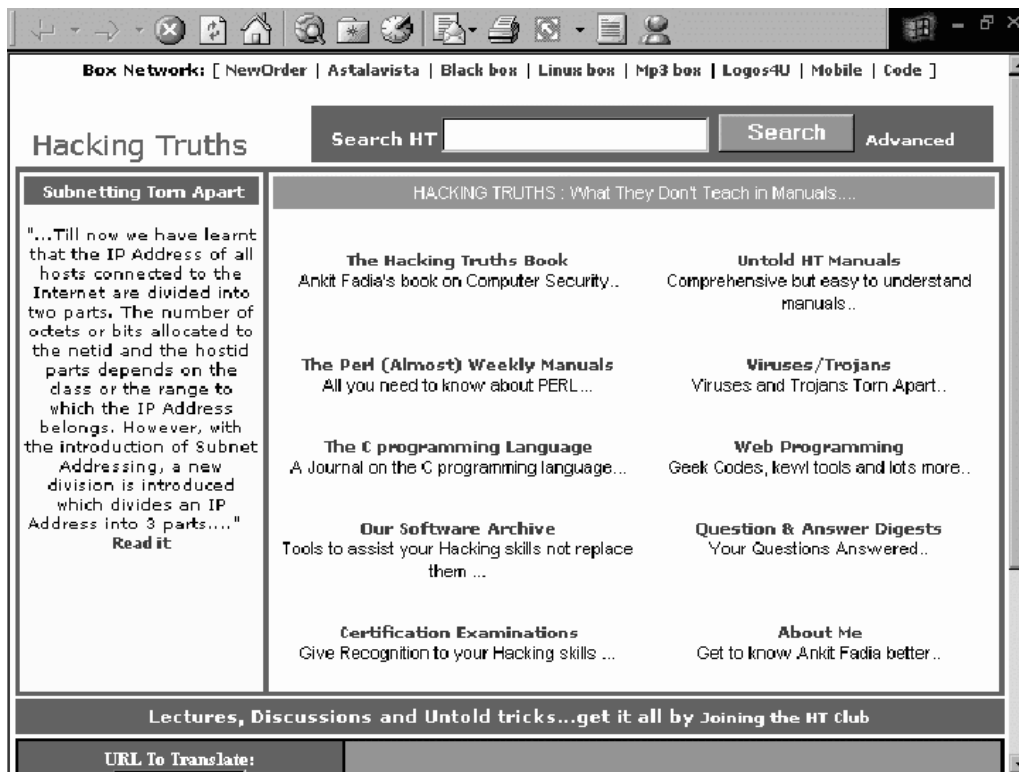
Pełna lista dokumentów RFC znajduje się w witrynie [antionline.com](http://antionline.com).

Są też lżej strawne wersje dokumentów RFC, oznaczane skrótem FYI (For Your Information). Aby dowiedzieć się więcej na temat FYI i gdzie ich szukać, sięgnij po RFC 1150. Jest jednak za wcześnie na zagłębianie się w szczegóły. Oto lista moich ulubionych witryn zawierających całość informacji, jakie mogą być przydatne nowicjuszowi, a nawet bardziej zaawansowanemu użytkownikowi.

1. Witryna Hacking Truths ([hackingtruths.box.sk](http://hackingtruths.box.sk))

W mojej opinii jest to jedna z najlepszych witryn hakerskich. Są w niej obszerne i wyczerpujące materiały na temat hackingu, crackingu, języka Perl, C, C++ i programowania witryn WWW. Jest to coś w rodzaju niezbędnika hakera. Można tam również zapisać się do grupy dyskusyjnej. Wszystkie materiały opublikowane w tej witrynie są wysyłane do wszystkich członków grupy. Aby się przyłączyć, należy wysłać e-mail na adres: [programmingforhackers-subscribe@egroups.com](mailto:programmingforhackers-subscribe@egroups.com).

Ten portal dla zainteresowanych zagadnieniami bezpieczeństwa został stworzony przez szczerze Wam oddanego:



2. PHRACK ([www.phrack.com](http://www.phrack.com))  
PHRACK jest e-magazynem zrozumiałym jedynie dla wtajemniczonych. Publikowane są w nim fantastyczne materiały dla zaawansowanych.
3. MSDN Online ([msdn.microsoft.com](http://msdn.microsoft.com))  
Witryna jest przeznaczona dla tych, którzy naprawdę chcą stać się hakerami. Jest to biblioteka tekstów praktycznie na temat każdego języka programowania obsługiwane przez Microsoft lub stworzonego w tej firmie, począwszy od programowania WWW do szczegółów języka C++.
4. The Packet Storm Archive ([packetstorm.security.com](http://packetstorm.security.com))  
Największe hakerskie archiwum w sieci. Jest tam lista biuletynów elektronicznych dla hakerów i wielkie zasoby oprogramowania. Ze względu ma materiał instruktażowy warto zajrzeć także do witryny neworder.box.sk, podobnej do Packet Storm.
5. Security Focus ([www.securityfocus.com](http://www.securityfocus.com)) jest miejscem, w którym ukazują się różnego rodzaju informacje techniczne na temat najnowszych programów, exploits, słabych punktów systemów i programów itp.

## Rozdział III

# Hacking w systemie MS Windows

W tym rozdziale:

- Jak poradzić sobie z zabezpieczeniami BIOS i Windows
- Różne triki w systemie Windows
- Zacieranie śladów

Bieżący rozdział jest poświęcony MS Windows jako obiektowi działań hakerskich. Czytając rozdział, zyskasz nie lada umiejętności, które zaimponują początkującym hakerom.

## Hasła BIOS-u

Hasła BIOS-u należą do podstawowych ustawień komputera, takich jak liczba dysków, informacja o tym, które dyski są dostępne i które służą do uruchamiania systemu. Te ustawienia są zapisane w pamięci CMOS na płycie głównej. Jest ona zasilana małą baterią i dzięki temu pamięta dane również po wyłączeniu zasilania całego systemu.

Wejście do BIOS-u następuje zwykle po naciśnięciu klawisza Del podczas uruchamiania systemu. Inne możliwe metody to naciśnięcie kombinacji klawiszy Ctrl+Alt+Esc lub Ctrl+Esc. W większości komputerów BIOS można skonfigurować tak, aby pytanie o hasło pojawiało się zaraz po włączeniu komputera. Jeżeli uaktywniona jest opcja Ask Password (Pytaj o hasło), po włączeniu zasilania systemu pojawi się okno dialogowe z pytaniem o hasło. Nie można wówczas obejść tego pytania, ponieważ zmiana tego ustawienia wymaga wejścia do BIOS-u. Co w takim razie można zrobić? Wyłączyć tę opcję, wchodząc do ustawień BIOS-u. Najczęściej stosowaną w tym przypadku metodą jest wypróbowanie domyślnych haseł BIOS-u. Oto niektóre z nich:

lkwpeter  
j262  
AWARD\_SW  
AWARD\_PW  
Biostar

AMI  
Award  
bios  
BIOS  
setup

cmos  
AMI!SW1  
AMI?SW1  
password  
hewittrand



Pełna lista haseł BIOS-u jest zamieszczona w rozdziale 8.

Hasło „j262” otwiera większość wersji BIOS-u firmy Award; działa w około 80 przypadkach na 100. Na niektórych komputerach skuteczne są hasła „AWARD\_SW” i „AWARD\_PW”. Czasem działa kombinacja klawiszy Shift+s y x z. Najlepszym sposobem dotarcia do haseł domyślnych jest przeszukanie witryny <http://astalavista.box.sk>. Na rynku znajdują się różne BIOS-y w różnych wersjach. W poszukiwaniu haseł można także zajrzeć do witryn firm oferujących BIOS, m.in. [award.com](http://award.com), [megatrends.com](http://megatrends.com) i [mrbios.com](http://mrbios.com).

Nazwa firmy i wersja BIOS-u jest wyświetlana na ekranie przy każdej próbie uruchomienia systemu.

Jeżeli hasło domyślne nie zadziałało, trzeba spróbować czegoś poważniejszego. Spróbuj przywrócić ustawienia fabryczne BIOS-u, aby pytanie o hasło w ogóle się nie pojawiało. W tym celu należy postąpić w następujący sposób:

Najpierw otwórz obudowę komputera i poszukaj okrągłej baterii litowej, która zwykle wygląda jak srebrna moneta. Usuń baterię i po pół minuty umieść na poprzednim miejscu. W niektórych komputerach konieczne jest także zresetowanie zworki. Najczęściej zwarte są końcówki 1 i 2. Jeżeli przesuniesz zworkę do końcówek 2 i 3 i pozostawisz ją w tej pozycji na dłużej niż pięć sekund, spowoduje to przywrócenie ustawień fabrycznych CMOS-u.

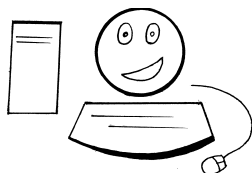


Za pomocą ustawień BIOS-u można również przyspieszyć taktowanie zegara w komputerze (overclocking). Więcej informacji na ten temat oferuje witryna <http://www.overclocking.com>.

Po uruchomieniu komputera BIOS może wyświetlić komunikat o błędzie informujący, że zmieniły się ustawienia BIOS-u lub zostały przywrócone ustawienia fabryczne, ale nie należy się tym przejmować.



Błąd podczas manipulacji chipsetem CMOS i zworki jest bardziej niebezpieczny niż wprowadzanie zmian w plikach systemowych. Czynności te należy wykonywać z najdalej idącą ostrożnością.



Na wielu komputerach seryjne naciśnięcie klawiszy może doprowadzić do awarii programu obsługującego wczytywanie hasła.

Aby to wypróbować, uruchom komputer i zaczekaj na pojawienie się pytania o hasło, po czym naciśnij klawisz Esc od 50 do 100 razy. Spowoduje to awarię programu obsługującego hasło i komputer będzie kontynuował proces uruchamiania. Jednak ta operacja udaje się jedynie na niektórych komputerach.

Jest jeszcze inne łatwe rozwiązanie problemu hasła BIOS-u: program KillCMOS, który można wczytać z witryny [www.koasp.com](http://www.koasp.com) lub poszukać w [astalavista.box.sk](http://astalavista.box.sk). Istnieje także sporo programów do łamania haseł CMOS, które można pobrać z różnych witryn hakerskich. Oczywiście korzystanie z cudzego oprogramowania, aby później udawać hakera, nie ma sensu.

## Hasła logowania Windows

Hasło BIOS-u zostało złamane. Okazało się, że jest to bardzo łatwe. Ale po chwili na ekranie pojawia się ekran logowania Windows.

Nie ma się czego obawiać. Ten kłopot jest jeszcze mniejszy niż poprzedni. Kiedy się z nim uporasz, zrozumiesz, dlaczego haker posługujący się systemem Windows nie wzbudza szacunku i dlaczego hakerzy się głośno śmieją, słysząc wymawiane w jednym zdaniu słowa „Microsoft” i „security”.

Aby obejść hasło logowania do systemu Windows, uruchom system ponownie i poczekaj na ukazanie się komunikatu

„Uruchamianie systemu Windows 9x...”

W tym momencie naciśnij klawisz F8. Pojawi się menu uruchamiania systemu. Wybierz opcję 7 – uruchomienie w trybie MS-DOS. Następnie przejdź do katalogu systemowego Windows, wpisując polecenie:

```
C:\>cd windows
```



Na uruchamianie komputera mają wpływ klawisze F4, F5, F6, F8, Shift+F5, Control+F5 oraz Shift+F8. Wypróbuj je i zobacz, co się stanie!!!

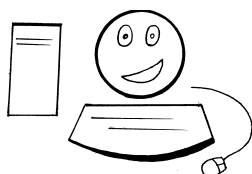
Następnie zmień nazwy wszystkich plików z rozszerzeniami .pwl za pomocą następującego polecenia:

```
C:\windows>ren *.pwl *.xyz
```

Można je także usunąć:

```
C:\windows>del *.pwl *.xyz
```

Kiedy pojawi się ekran logowania Windows, można zamiast hasła wpisać cokolwiek. Ponieważ po zmianie nazw plików z hasłami (lepiej nie usuwać ich, aby ofiara nie wiedziała, że ktoś „dłubał” w komputerze), Windows nie może odnaleźć pliku hasła, akceptuje dowolny ciąg znaków.



Można wyłączyć klawisz F8 lub klawisz rozruchu w następujący sposób:

1. Igraszki z plikami systemowymi są bardzo niebezpieczne. Zanim do tego przystąpisz, wykonaj na wszelki wypadek kopie zapasowe plików systemowych z dysku twardego...

lub przynajmniej z dyskietki uruchamiającej system, aby w razie popełnienia błędu można było naprawić plik msdos.sys.

2. Znajdź plik msdos.sys (zwykle znajduje się w c:\msdos.sys). Ponieważ jest to ukryty plik systemowy, należy zmienić atrybut zapisywania do tego pliku. W oknie DOS-u wykonaj następujące polecenie:

```
\Windows>cd\
```

Następnie dodaj atrybut zapisywania i wyłącz opcję ukrywania pliku, wpisując:

```
\>attrib msdos.sys -h -w
```

3. Otwórz plik msdos.sys w edytorze WordPad.
4. Jego zawartość ma postać podobną do następującej:

```
;FORMAT
[Paths]
WinDir=C:\WINDOWS
WinBootDir=C:\WINDOWS
HostWinBootDrv=C
[Options]
BootMenu=0 (default)
BootMulti=1
BootGUI=1
DoubleBuffer=1
AutoScan=1
WinVer=4.10.1998
;
;The following lines are required for compatibility with other
programs.
;Do not remove them (MSDOS.SYS needs to be >1024 bytes).
;xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Aby wyłączyć klawisze funkcji podczas uruchamiania systemu, w wierszu poniżej [Options] wstaw następujący fragment kodu:

```
"BootKeys=0."
```

(Oczywiście bez cudzysłowu).

Zamiast polecenia BootKeys można także wstawić następujące polecenie:

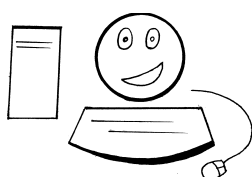
```
"BootDelay=0."
```

Mało kto wie o istnieniu polecenia BootDelay=0, które w połączeniu z poleceniem BootKeys uczyni komputer bardziej bezpiecznym. Po wprowadzeniu zmian zapisz plik msdos.sys na dysku.

5. Ponieważ msdos.sys jest ważnym plikiem systemowym, należy ponownie zmienić atrybuty do poprzedniej postaci:

```
C:>attrib msdos.sys +h +r
```

Jeżeli na komputerze, który nie jest włączony do sieci LAN, uruchomiony jest system Windows 95 lub Windows 98, nie ma potrzeby wykonywania opisanych czynności. Wystarczy kliknąć przycisk Anuluj w oknie logowania do systemu Windows. Haker oczywiście powinien znać wszystkie te możliwości. Do systemu operacyjnego Windows dołączany jest także program pwledit usuwający niektóre hasła Windows. Aby go uruchomić, należy wykonać polecenie: Start→Programy→Akcesoria→Narzędzia systemowe→PWLedit. Można go też zainstalować z dysku instalacyjnego Windows 95. Znajduje się on w katalogu d:\admin\apptools\pwledit. Być może jest też dołączany do Windows 98.



Nie masz dysku instalacyjnego? Oto, jak go sporządzić.

Włóż czystą dyskietkę do napędu i otwórz Panel sterowania. Kliknij ikonę Dodań/Usuń programy, po czym kliknij kartę Auto-start, a następnie kliknij przycisk Utwórz dysk.



Dokładniejsze informacje na temat plików .pwl dostępne są pod adresem <http://hackingtruths.box.sk/pwl.htm>.

## Zmiana wyglądu Windows

Ponieważ wiemy już, jak włączyć się do komputera lokalnego, pora nauczyć się przydatnych trików w Windows. Jeżeli komputer jest normalnie skonfigurowany, to przy uruchamianiu systemu pojawia się nieciekawy ekran z napisem: System Windows 95 – zapraszamy. Czy nie masz ochoty zmienić go na inny, bardziej zaskakujący z czaszkami i rozmazaną krwią? Oto dokładna instrukcja, jak zmienić ekrany pojawiające się w chwili uruchamiania i zamykania systemu.

Poszukaj pliku c:\logo.sys. Ze względu na rozszerzenie .sys plik może być niewidoczny dla Windows Explorera. Aby obejrzeć wszystkie pliki systemowe .sys, wykonaj w oknie MS-DOS najpierw polecenie cd\, a potem wpisz:

```
C:\>Attrib *.sys
```

Na ekranie może pojawić się:

```
SHR C:\MSDOS.sys
SHR C:\IO.sys
A SHR C:\CONFIG.sys
A SHR C:\logo.sys
```

Atrybuty SHR oznaczają, że logo.sys jest plikiem systemowym, jest ukryty i przeznaczony tylko do odczytu.

Jeżeli pliku logo.sys nie ma w katalogu głównym na dysku c:, można skopiować plik logow.sys z katalogu systemowego Windows:

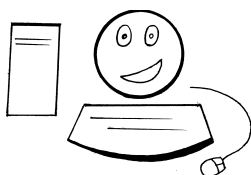
```
C:\>cd windows
C:\Windows>copy logow.sys c:
```

Plik logo.sys jest plikiem tylko do odczytu. Aby umożliwić zapis, zmień atrybuty w następujący sposób:

Krok 1. Otwórz okno MS-DOS.

Krok 2. Wpisz następujące polecenia:

```
C:\Windows>cd\  
C:\>attrib logo.sys -s -h -r
```



Jest jeszcze inny sposób zdobycia hasła systemu Windows. Zamiast przytrzymywać klawisz F8, wystarczy nacisnąć klawisz F5, który uruchamia komputer w trybie bezpiecznym. Komputer wówczas nie pyta o hasło logowania. Czasem można zastosować także następujący trik. Jeżeli klawisze F8, F5 są wyłączone w czasie startu systemu, przydatna jest dyskietka startowa. Po uporaniu się z hasłem wejdź do BIOS-u (zwykle trzeba w tym celu nacisnąć klawisz Del podczas rozruchu komputera) i włącz opcję uruchamiania z dyskietki A:. Następnie włóż dyskietkę i zaczekaj na znak zgłoszenia DOS-u. Potem wystarczy tylko wpisać odpowiednie polecenia.

Teraz można przystąpić do zmiany pliku zawierającego logo. Oto kolejne czynności, które należy wykonać:

Krok 1. Otwórz program MS Paint.

Krok 2. Wybierz polecenie Plik→Otwórz.

Krok 3. Otwórz plik c:\logo.sys.

Krok 4. Przygotuj własny ekran powitalny.



Zapisz plik na dysku pod nazwą `c:\logo.sys`. Ponownie zmień atrybuty na fabryczne, wpisując w wierszu poleceń:

```
C:\>attrib logo.sys +h +r +s
```

Uruchom komputer ponownie i podziwiaj efekty swojej pracy. W podobny sposób można zmienić okno Zamykanie systemu. W tym przypadku zmień atrybut zapisu pliku `logow.sys`, otwórz plik w programie MSPaint, zmień go i zapisz pod nazwą `c:\windows\logow.sys`. Przywróć poprzednie atrybuty pliku za pomocą polecenia `c:\>attrib c:\windows\logow.sys +h +s +r`. Voilà, nawet ekran pożegnalny nabrał charakteru.

## Zacieranie śladów

Co dzieje się po wpisaniu adresu URL konkretnej witryny? Przeglądarka łączy się ze stroną internetową, pobiera obrazy, tekst i zapisuje na dysku twardym, tj. w podręcznej pamięci na dysku. Każdy, kto ma dostęp do dysku komputera, może dowiedzieć się, które witryny były odwiedzane. Powiedzmy, że chcesz zmienić pracę. Przeglądasz w tym celu witryny pośrednictwa pracy. Jeśli szef sprawdza, jak podwładni korzystają z Internetu, dowie się, że szukasz nowej pracy. Daję głowę, że nie wróży to nic dobrego. Jak zatrzeć za sobą ślady? Zarówno Netscape Navigator, jak i Microsoft Internet Explorer zapisują adresy ostatnio odwiedzanych witryn, obrazy i pozostałe pliki w pamięci podręcznej.

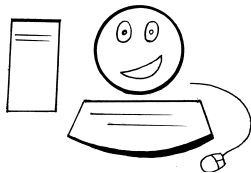
## Dla użytkowników Internet Explorera

Aby usunąć wszystkie pozycje historii Internet Explorera, wykonaj następujące czynności:

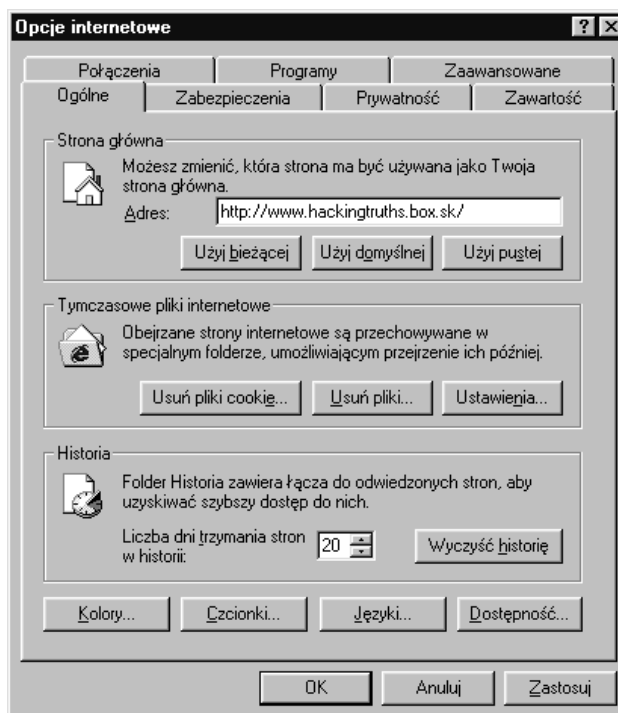
1. Otwórz okno programu Internet Explorer i wybierz menu Widok.
2. Z listy rozwijanej wybierz Opcje internetowe.
3. Na karcie Historia kliknij przycisk Wyczyść historię.

Wszystkie pozycje historii IE zostaną usunięte. Jeżeli trzeba usunąć tylko niektóre wpisy, wykonaj następujące czynności:

1. Uruchom program Internet Explorer.
2. Kliknij przycisk Historia.
3. Po lewej stronie pojawi się ramka z historią połączeń.
4. Aby usunąć konkretny wpis, kliknij go i w menu kontekstowym wybierz polecenie Usuń lub kliknij lewy przycisk myszy i naciśnij klawisz Del.



Każdy komputer połączony z Internetem ma przypisany adres IP. Trzeba go znać, aby nawiązać kontakt. Adresy IP są dość długie i trudne do zapamiętania. Lepiej używać nazw DNS. Aby połączyć się z witryną hotmail.com, wystarczy podać adres słowny (hotmail.com). Po wpisaniu w przeglądarce nazwy łączy się ona z jednym z serwerów DNS (Domain Name Server). Przechowują one nazwy hostów i adresy IP. Więcej na ten temat można dowiedzieć się z rozdziału 5.



Wszystkie strony pochodzące z danej witryny zostaną usunięte z pamięci podręcznej.

W witrynie może znajdować się wiele obrazów, apletów i innych komponentów multimedialnych. Przeglądarka pobiera je na dysk twardy lub do pamięci podręcznej. Przy powtórnej wizycie w witrynie program sprawdza, czy zmieniła się zawartość strony. Jeśli pozostała bez zmian, przeglądarka wczytuje kopię witryny przechowywaną lokalnie. W przeciwnym razie pobierze nową kopię. W ten sposób treść pamięci podręcznej zdradza upodobania sieciowego podróżnika.

Aby wyczyścić pamięć podręczną Internet Explorera na dysku, wykonaj następujące czynności:

1. Uruchom Internet Explorer.
2. Wybierz polecenie Widok → Opcje internetowe.
3. W ramce Tymczasowe pliki internetowe kliknij przycisk Usuń pliki.

Opcje zapisu stron WWW w pamięci podręcznej można wyłączyć, choć jest to niewygodne, gdy komputer przy każdym połączeniu na nowo pobiera z sieci pełną zawartość strony, bez względu na to, czy zmieniła się ona od ostatniej wizyty. W celu wyłączenia pamięci podręcznej wykonaj następujące czynności:

1. Uruchom Internet Explorer.
2. Wybierz polecenie Widok→Opcje internetowe.
3. Na karcie Pliki programów kliknij przycisk Ustawienia.
4. Za pomocą suwaka ustaw wartość parametru Ilość miejsca na dysku na 0 MB.

### Ciasteczka (cookies)

Czym są ciasteczka?

Według witryny Maximum Security ciasteczko działa podobnie jak stemplowanie rąk przy wejściu na dyskotekę. Można się bawić, zamawiać drinki, a nawet wyjść na zewnątrz na kilka minut. Dopóki na ręce jest stempel, nie trzeba drugi raz płać za wejście na salę. Jednak ciasteczko pełni jeszcze inną rolę. Zapisuje dane charakterystyczne dla konkretnego użytkownika. Kiedy ponownie wybiera daną stronę, serwer WWW pobiera te dane stanu (ang. *state information*). Problem tkwi nie w samym fakcie pobierania informacji, ale w tym, z którego obszaru dysku twardego pochodzi. Ciasteczka (w Netscape noszą nazwę *persistent client state HTTP cookies*) służą najczęściej do przechowywania danych użytkownika podczas przeglądania strony.

Zespół Netscape'a wyjaśnia to w ten sposób:

Ten prosty mechanizm otwiera drogę do tworzenia nowego rodzaju aplikacji działających w środowisku WWW. Aplikacje obsługujące zakupy online mogą przechowywać dane o wybranych towarach, a w przypadku kolejnych połączeń umożliwiają stosowanie uproszczonej procedury logowania do serwisu. Preferencje użytkownika mogą być zapisane po stronie klienta i przekazywane w momencie połączenia z witryną.

W Internet Explorerze ciasteczka są przechowywane w oddzielnych plikach w katalogu `c:\windows\cookies`. Aby je usunąć, należy usunąć odpowiednie pliki.



Ciasteczka są ważnym narzędziem zdobywania informacji o użytkowniku. Można je wykorzystać w celu monitorowania zachowania i upodobań internauty. Każdy, kto chce chronić swoją prywatność, powinien wyłączyć opcję uruchamiania ciasteczek.

Aby wyłączyć ciasteczka, wykonaj następujące czynności:

1. Uruchom Internet Explorer.
2. Wybierz polecenie Widok→Opcje internetowe.

3. Wybierz kartę Zaawansowane.
4. Przewiń do sekcji zabezpieczeń. Wybierz odpowiedni przycisk opcji.

## Pasek adresów URL

Każdy nowo wprowadzony adres URL jest zapisywany w rozwijanym menu. Jeżeli wyczyścisz historię Internet Explorera, usunięte zostaną również wszystkie pozycje z listy Pasek adresów.

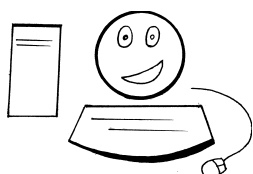
## Dla użytkowników Netscape Navigatora

Historię można usunąć w następujący sposób:

1. Uruchom Navigator i kliknij przycisk Communicator.
2. Kliknij przycisk Tools.
3. Kliknij przycisk History.
4. Usuń poszczególne pozycje lub naciśnij klawisz Shift i wybierz zakres usuwanych pozycji.

Pamięć podręczna (cache) na dysku może być wyczyszczona w następujący sposób:

1. Uruchom Navigator i kliknij przycisk Edit.
2. Wybierz opcję Preferences.
3. Wybierz opcję Advanced.
4. Kliknij przycisk Clear Disk Cache.



Przedstawię teraz metodę usuwania adresów URL z paska adresowego za pomocą Rejestru.

Manipulowanie Rejestrem Windows wymaga dużej ostrożności. Nie powinny tego robić osoby, które niewiele wiedzą o Rejestrze. Modyfikacji Rejestru każdy dokonuje na własną odpowiedzialność. W kluczu `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer` znajduje się folder `Typed URLs`. Aby usunąć historię adresów URL, należy usunąć odpowiadające im klucze.

W celu wyłączenia opcji `Disk Caching` należy wykonać następujące czynności:

1. Uruchom Navigator i wybierz opcję Edit.
2. Wybierz opcję Preferences.
3. Wybierz kartę Advanced.
4. Kliknij opcję Cache.
5. Ustaw opcję `Disk Cache` na 0 MB.

## Ciasteczka

Ciasteczka programu Netscape są przechowywane w pliku cookies.txt.

Aby wyłączyć ciasteczka, wykonaj następujące czynności:

1. Po uruchomieniu Navigatora wybierz opcję Edit.
2. Wybierz opcję Preferences.
3. Wybierz kartę Advanced.
4. Wybierz opcję Disable Cookies.

## URL History

Aby wyczyścić historię URL, otwórz plik: C:\Program Files\Netscape\Users\  
<username>\pref.js w programie Notepad i usuń wybrany wiersz, na przykład:

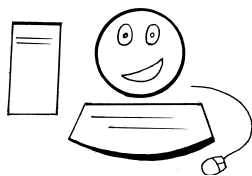
```
user_pref("browser.url_history.URL_13", "www.perl.org/");
```

Spowoduje to usunięcie konkretnej pozycji, w tym przypadku jest to perl.org-13. w kolejności adres URL.

Aby w sposób trwały zabezpieczyć się przed zapisywaniem stron do pamięci podręcznej, ustaw wartość parametru History na 0.

## Rejestr

Rejestr ma kluczowe znaczenie dla całego systemu operacyjnego. Jeżeli popełnisz błąd podczas modyfikacji wpisów Rejestru, może się okazać, że konieczna jest ponowna instalacja systemu operacyjnego. Dlatego dyskiety instalacyjne powinny być zawsze pod ręką. Jeżeli uporasz się z modyfikacją wpisów w Rejestrze, zdobędziesz władzę nad całym komputerem, a nawet nad siecią LAN. Modyfikacja wpisów w Rejestrze Windows jest tym, czym jest dostęp do konta root na stacji Unix. Windows 98 ma wbudowane narzędzie przywracania Rejestru do stanu początkowego. Przed dokonaniem zmian należy wykonać kopię zapasową Rejestru na dyskietce.



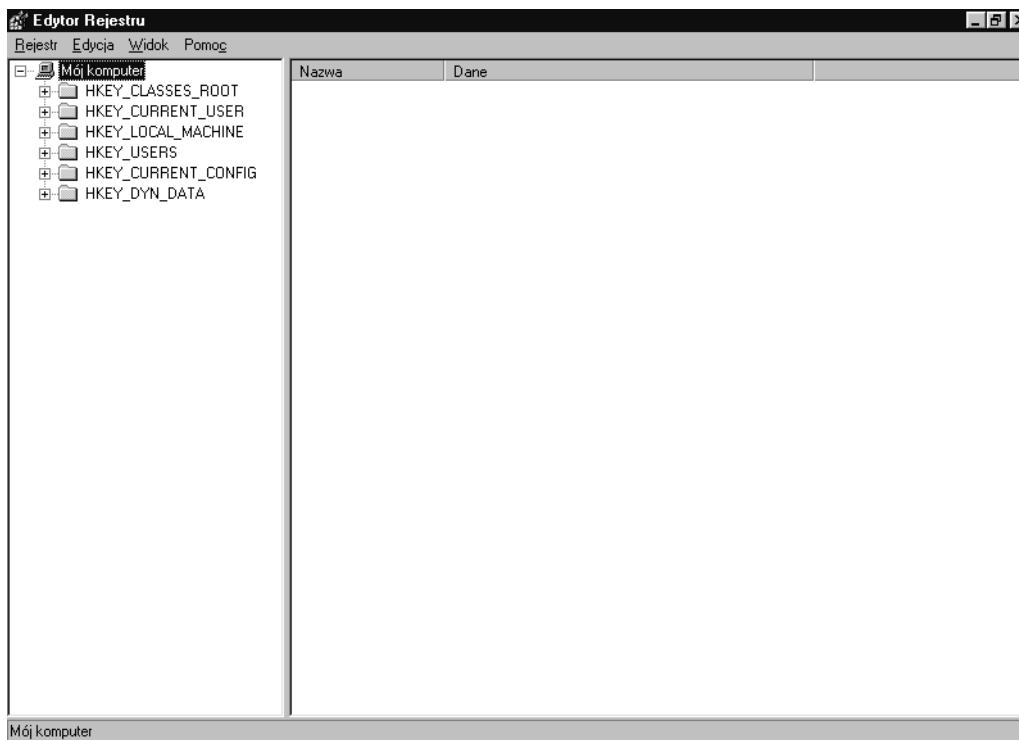
Netscape również wykonuje operacje zapisu w Rejestrze. Aby usunąć wpisy Rejestru, kliknij gałąź HKEY\_CURRENT\_USER. Kliknij Software. W lewym oknie pojawi się pozycja Netscape. Po prawej widoczna będzie historia URL. Usuń ją.

Aby otworzyć Rejestr Windows, wybierz polecenie Start→Uruchom, a następnie wpisz polecenie regedit. Jeżeli nie spowoduje to otwarcia Rejestru, w polu Uruchom wpisz polecenie c:\windows\regedit.exe. Można także kliknąć ikonę Mój komputer, wybrać dysk C, potem katalog Windows i uruchomić program, klikając dwukrotnie ikonę regedit.

Po otwarciu Rejestru w lewym oknie widoczne są zwykle następujące pozycje:

```
HKEY_CLASSES_ROOT  
HKEY_CURRENT_USER  
HKEY_LOCAL_MACHINE  
HKEY_USERS  
HKEY_CURRENT_CONFIG  
HKEY_DYN_DATA
```

W Microsoftzie wyznają zasadę bezpieczeństwa przez pogmatwanie. Wydaje się im, że zapobiegają modyfikacji Rejestru przez użytkowników, ukrywając go w katalogu Windows i nadając mu dziwną nazwę. Zawartość Rejestru ma zapewne odstraszać przeciętnego użytkownika niezrozumiałymi nazwami. Po bliższym poznaniu okazuje się, że nie taki diabeł straszny, jak go Microsoft maluje.



Rejestr składa się z dwóch plików, user.dat i system.dat (NIE PRÓBUJ ICH ZMIENIAĆ). Zawierają wszystkie istotne informacje o systemie operacyjnym, od wyglądu pulpitu do hasła telefonicznego dostępu do Internetu. Najpierw pobaw się trochę gałęziami Rejestru. Szybko dojdiesz do wniosku, że tą metodą nie można pojąć jego zawartości. Hakerzy wybierają inną drogę.

Aby obejrzeć menu danej gałęzi Rejestru, rozwiń ją, klikając znak +. Nazwy menu dają pewne pojęcie o tym, co się w nim znajduje. Aby zmienić sposób działania

konkretnego programu, należy odszukać odpowiedni wpis w menu software. Kliknij HKEY\_CURRENT\_USER. Kliknij Software. W lewym oknie pojawi się lista zainstalowanych programów. Po prawej widoczne są dane w niezbyt zrozumiałej postaci. Aby stały się bardziej czytelne, kliknij wybrane menu lub jedną z jego pozycji i przejdź do nagłówka Rejestr na pasku menu edytora Rejestru. Kliknij go, po czym wybierz opcję Eksportuj plik Rejestru. Pojawi się pytanie o nazwę i ścieżkę, do której dane mają być eksportowane. Wpisz wybraną przez siebie nazwę.



Wygląd i inne cechy człowieka wynikają z jego kodu genetycznego. Podobnie Rejestr Windows definiuje wygląd i sposób działania systemu Windows.

Uruchom edytor tekstu WordPad i otwórz plik wyeksportowany z Rejestru. Do nazwy tego pliku trzeba dodać rozszerzenie .reg. Teraz zawartość Rejestru ma bardziej zrozumiałą postać. Łatwo zmienić wpisy Rejestru i dostosować do własnych potrzeb. W ten sposób można poprawić wydajność pracy systemu i zmienić jego wygląd. Oto niektóre przykłady:

1. W miejsce nazwy przycisku Start można wpisać swoje imię.
2. Zmień logo Internet Explorera.
3. Zmień nazwę Kosza.
4. Zmień sposób działania programu.

Pełna lista możliwości jest zamieszczona w instrukcji Advanced Windows Hacking Manual.



Informacjom i poradom na temat Rejestru poświęcona jest witryna [www.regedit.com](http://www.regedit.com). Jest dobrze zaprojektowana i zawiera wiele zdumiewających trików.

## Programy cenzorskie

Czy denerwują Cię głupie programy nadzorujące Twoje zachowanie w sieci? Czy blokują dostęp do niektórych witryn? Czy chcesz zmienić funkcjonowanie takiego programu, aby poruszać się w sieci bez przeszkód?

Nie namawiam do udostępniania dzieciom pornografii, nie zachęcam też do nieprzestrzegania reguł obowiązujących w firmie. Chcę jedynie powiedzieć, że żaden program cenzorski nie odfiltruje z sieci całego brudu. Ludzie zupełnie niepotrzebnie kupują programy tego typu. Można je unieszkodliwić kilkoma metodami.

Jedna z nich polega na uruchomieniu Menedżera zadań za pomocą kombinacji klawiszy Ctrl+Alt+Del. Jeżeli na liście działających w danym momencie programów znajduje się program cenzorski, kliknij go lewym przyciskiem myszy, po czym kliknij przycisk Zakończ proces.

Programy cenzorskie z założenia mają startować podczas każdego uruchamiania systemu. Bywa, że uruchamiają się automatycznie, umieszczając wzmiankę o sobie w pliku `c:\autoexec.bat`. Ten plik i zapisane w nim polecenia są wykonywane podczas każdego startu systemu. Otwórz plik w edytorze Notepad i usuń wszystkie wpisy odnoszące się do tego programu. Bezpieczniej jest wstawić słowo REM na początku wiersza związanego z danym programem. Zapisz je i uruchom system ponownie, aby zmienić ustawienia.

Innym miejscem, do którego wpisują się programy uruchamiane automatycznie, jest folder `c:\windows\Start Menu\Programs\Start up`. Wszystkie wpisane w nim programy startują automatycznie podczas uruchamiania systemu. Jednym ze sposobów blokowania tych programów jest naciśnięcie wtedy klawisza Shift. Aby trwale zapobiec ładowaniu programów, usuń z tego katalogu skróty do wybranych programów.

Informacje o programach uruchamianych automatycznie podczas startu Windows są umieszczane także w pliku `win.ini`. Aby usunąć z niego wszystkie ślady programu cenzorskiego, otwórz plik w edytorze Notepad i poszukaj w sekcji [Windows] wiersza zawierającego `'load='` lub `'run='`. Usuń wszystkie wzmianki programu.

Prawie wszystkie programy uruchamiane automatycznie wykorzystują w tym celu informacje z Rejestru Windows. Oto klucze, w których umieszczone są referencje do tych programów:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\RunServices
HKEY_LOCAL_MACHINE\DEFAULT\SOFTWARE\Microsoft\Windows\Current Version\Run
HKEY_LOCAL_MACHINE\DEFAULT\SOFTWARE\Microsoft\Windows\Current Version\
RunServices
```

Usuń z tych kluczy referencje, które mogą być odpowiedzialne za uruchamianie dokuczliwych programów.

W celu uzyskania informacji o tych programach użytkownicy Windows 98 mogą skorzystać z narzędzia `msconfig.exe`, znajdującego się na CD-ROM-ie instalacyjnym.

Internet Explorer ma wbudowany Klasyfikator treści, który (jeśli jest włączony) pyta o hasło zawsze wtedy, kiedy napotka witrynę bez certyfikatu. Na przykład, aby wejść do witryny Yahoo, trzeba wpisać hasło Klasyfikatora treści, ponieważ Yahoo nie ma certyfikatu.

Oto, jak usunąć to hasło. Wszystkie ustawienia klasyfikatora treści są zapisane w następującym kluczu Rejestru:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
Ratings
```

Aby zapobiec pytaniom Internet Explorera o hasło, usuń powyższy klucz z edytora Rejestru Windows (`c:\windows\regedit.exe`).