Fedora Core. Ćwiczenia

Autor: Piotr Czarny
ISBN: 83-7361-512-1
Format: B5, stron: 152

Linux już dawno przestał być zabawką dla informatyków-pasjonatów. Dzięki pracy setek programistów z całego świata stał się doskonałą alternatywą dla systemu Windows, zwłaszcza w zastosowaniach sieciowych. Jego podstawową przewagą nad konkurencją jest fakt, że jest dostępny nieodpłatnie. Kolejne wersje najpopularniejszych dystrybucji są coraz łatwiejsze w instalacji, konfiguracji i obsłudze. Dla Linuksa powstaje coraz więcej aplikacji, co stopniowo wzmacnia jego pozycję jako systemu operacyjnego do zastosowań domowych i biurowych. Coraz częściej sięgają też po ten system ogromne korporacje, takie jak Boeing czy NASA. Znajomość Linuksa jest dużym atutem na rynku pracy dla informatyków.

Fedora Core to następca jednej z najpopularniejszych dystrybucji Linuksa – RedHata. Podobnie jak poprzednik, cechuje się łatwością instalacji, rozbudowanymi możliwościami obsługi urządzeń multimedialnych, korzystaniem z technologii Plug&Play i bogatym pakietem aplikacji, które można łatwo zainstalować za pomocą pakietów RPM. Wykonując ćwiczenia zawarte w tej książce, poznasz podstawy obsługi systemu Fedora Core.

Nauczysz się:

- Instalować system
- Logować do systemu
- Korzystać z menedżera okien
- Wykorzystywać wszystkie funkcje pulpitu
- Odczytywać dane z dyskietek i CD-ROM-ów
- Korzystać z internetu
- Instalować nowe oprogramowanie
- Zabezpieczać system przez niepowołanym dostępem

Poznaj system Fedora Core Linux. Przekonaj się, że nie trzeba być komputerowym guru, aby w pełni wykorzystać jego potencjał.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 13.

Bezpieczeństwo systemu

Objawem włamania do komputera nie musi być sformatowanie dysku twardego. Oczywiście zdarzają się również takie przypadki — są one jednak mało groźne, gdyż łatwo je wykryć.

Znacznie większe niebezpieczeństwo stanowi np. utworzenie przez włamywacza folderu i udostępnienie go w sieci. Właściciel komputera będzie ponosił odpowiedzialność za treść plików, które znajdują się na jego sprzęcie. Sprytny włamywacz może pozostać bezkarny.

Komputer przyłączony do sieci można wykorzystać do rozsyłania *spamu*. Oczywiście dzieje się to bez wiedzy właściciela sprzętu. O celu, do jakiego wykorzystano jego sprzęt, dowiaduje się, gdy rozesłano już kilkaset tysięcy listów.

Komputery są wykorzystywane do przechowywania cennych informacji. Numery kart kredytowych, hasła, projekty przedsięwzięć — to tylko niektóre z nich. Dostanie się takich informacji w niepowołane ręce może spowodować poważne straty.

Niebezpieczeństwo zwiększają łącza stałe. Dzięki nim użytkownik ma stały dostęp do internetu, a inni użytkownicy internetu mają również stały dostęp do tego komputera.

Nie da się całkowicie wyeliminować ryzyka włamania. Można natomiast przedsięwziąć kroki, które zmniejszą jego prawdopodobieństwo i wydłużą czas niezbędny do pokonania zabezpieczeń.

Wszelkie szyfrowania i hasła działają tylko po uruchomieniu systemu. Jeśli włamywacz wejdzie w posiadanie komputera, wymontuje z niego dysk twardy i podłączy do komputera uruchomionego z innego dysku systemowego, może bez trudu zapoznać się z danymi. Za podstawową zasadę należy zatem przyjąć fizyczną ochronę sprzętu. Komputer powinien znajdować się w pomieszczeniu zabezpieczonym przed dostępem osób niepowołanych.

Po opublikowaniu systemu wykrywane są w nim błędy i luki, a autorzy publikują poprawione wersje wadliwych programów. Z punktu widzenia bezpieczeństwa istotne jest, aby w systemie były zainstalowane najnowsze poprawki.

Ćwiczenie 13.1.

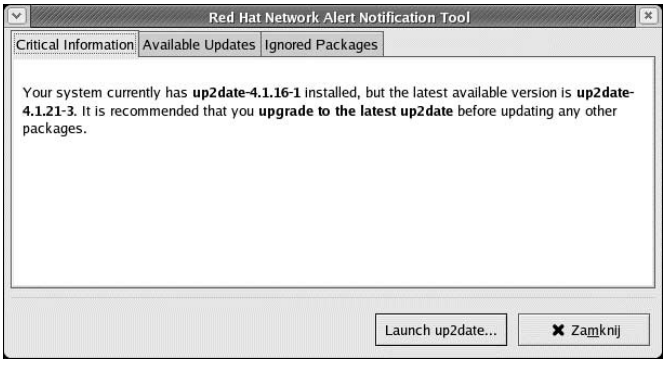
Zaktualizuj system Fedora Core.

1. W prawym rogu panelu znajduje się kółko. Jeśli na czerwonym tle widoczny jest wykrzyknik, oznacza to, że w sieci mogą być dostępne aktualizacje (rysunek 13.1).

Rysunek 13.1. *Wskaźnik aktualizacji systemu*

2. Dwukrotnie kliknij wskaźnik aktualizacji.
3. Wyświetlone zostało okno *Red Hat Network Alert Notification Tool* (rysunek 13.2). Kliknij przycisk *Launch up2date...*

Rysunek 13.2. *Okno Red Hat Network Alert Notification Tool*

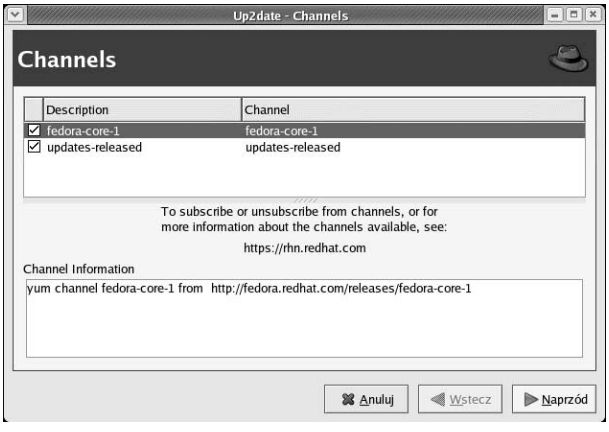


4. Przez proces instalacji poprawek użytkownik prowadzony jest przez kreatory. Po wyświetleniu okna *Red Hat Update Agent* kliknij przycisk *Naprzód* (rysunek 13.3).

Rysunek 13.3. *Okno kreatora aktualizacji*

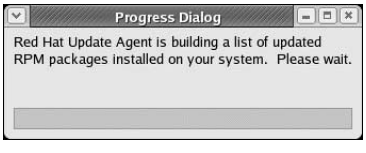
5. Po wyświetleniu okna *Up2date* zaznacz aktualizację wszystkich kanałów (rysunek 13.4). Kliknij przycisk *Naprzód*.

Rysunek 13.4. *Lista aktualizowanych kanałów*



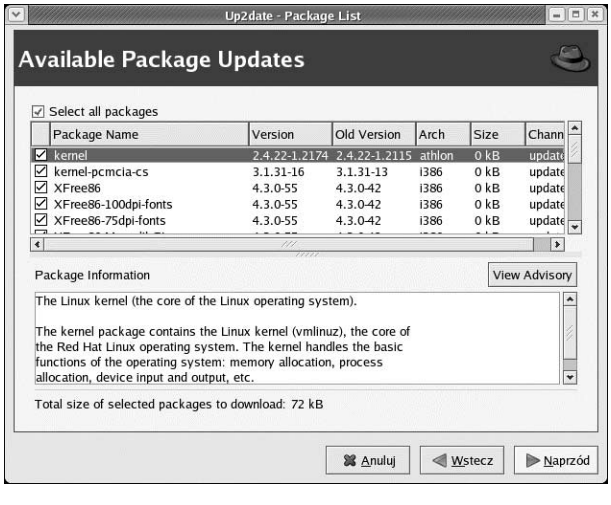
6. Przez chwilę agent aktualizacji będzie generował listę pakietów RPM, które są zainstalowane w systemie. Zaawansowanie operacji jest wyświetlane w formie paska postępu (rysunek 13.5).

Rysunek 13.5. *Agent aktualizacji zbiera informacje o zainstalowanych w systemie pakietach*

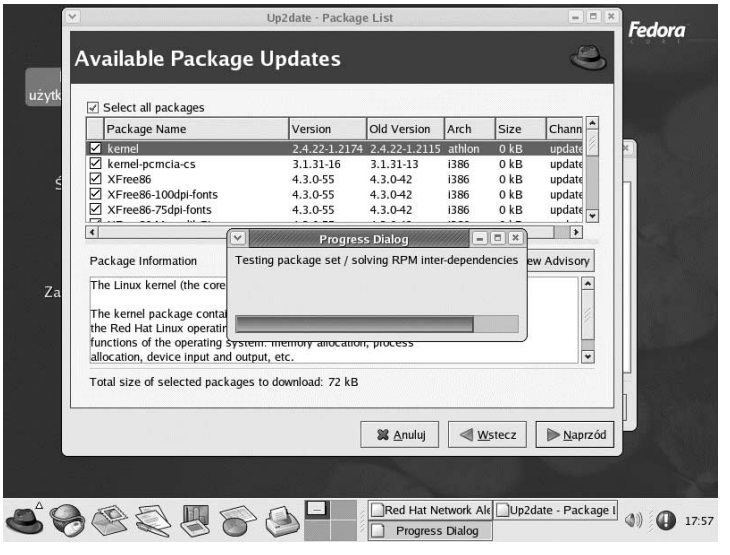


7. Wyświetlone zostało okno z listą pakietów (rysunek 13.6). W kolumnie *Version* podana jest wersja aktualizacji do pobrania z sieci. W kolumnie *Old Version* widoczny jest numer wersji zainstalowanej w komputerze. Zaznacz aktualizacje, które chcesz zainstalować. Jeśli korzystasz z łącza stałego — zaznacz wszystkie. Jeżeli korzystasz z modemu — zaznacz nazwy tylko tych programów, które działają nieprawidłowo. Kliknij przycisk *Naprzód*.

Rysunek 13.6. *Porównanie wersji programów zainstalowanych i poprawek*



8. Rozpoczęła się aktualizacja systemu (rysunek 13.7).



Rysunek 13.7. *Duża liczba poprawek i wolne łącze wymagają sporo cierpliwości*

Po aktualizacji systemu należy go przeładować.

Hasła pozwalają na dostęp do wybranych zasobów komputera tylko uprawnionym osobom. Nie powinny być one zbyt skomplikowane — w takim przypadku będziesz zapewne je zapisywał, aby uniknąć ich zapomnienia. Dostanie się notatek w niepowołane ręce narazi system na utratę bezpieczeństwa. Zbyt proste hasła również nie stanowią dobrej ochrony. Komputerowi włamywacze używają bowiem programów łamiących hasła, które stosują tzw. atak słownikowy. Polega on na wpisywaniu kolejnych słów z słownika. Tym samym jako hasła zdyskwalifikowane są:

- nazwy osób i rzeczy,
- słowa i skróty z języków polskiego i angielskiego,
- kolejne klawisze na klawiaturze (np. QAZWSX),
- przykładowe hasła znalezione w publikacjach,
- powyższe sekwencje znaków zapisane w odwrotnej kolejności, małymi literami, wielkimi literami itp.

Drugą metodą jest atak siłowy, polegający na generowaniu przez program kolejnych sekwencji znaków. Aby wydłużyć czas łamania hasła, nie należy:

- używać haseł składających się z samych cyfr,
- używać informacji związanej z kontem, osobą właściciela, numerem telefonu, numerem pokoju itp.

Zalecane jest częste zmienianie haseł. Gdy włamywacz mimo wszystko wejdzie w posiadanie hasła, to czas, przez jaki korzysta z niego, powinien być maksymalnie krótki. W hasłach należy stosować:

- małe litery, wielkie litery, cyfry i znaki interpunkcyjne,
- sekwencje liczące minimum osiem znaków,
- przypadkowe kombinacje znaków, które są łatwe do zapamiętania przez właściciela.

Mimo przestrzegania podanych reguł można odczytać hasło, które jest zapisane w pliku */home/nazwa_konta/.bash_history*. Zapisywane są w nim polecenia wydawane w oknie terminala. Jeśli po wpisaniu polecenia `su` nie naciśniesz klawisza *Enter*, lecz wpiszesz hasło, zostanie ono utrwalone w pliku *bash_history*.