Linux Internet Server. Czarna księga

Autorzy: H. Tsuji, T. Watanabe, Acrobyte
Tłumaczenie: Dariusz Boratyn
ISBN: 83-7197-357-8
Tytuł oryginału: Setting Up A Linux Internet Server Visual Black Bo
Format: B5, stron: 256

W bogato ilustrowanej książce „Linux Internet Server" opisano system operacyjny Red Hat Linux w roli serwera internetowego obsługującego za pomocą sieci TCP/IP połączenia ze światem – czyli Internetem.
Dzięki niej można nauczyć się zarówno podstaw Internetu, jak i konfiguracji różnych typów serwerów dostępnych w Linuksie. Układ treści jest zrozumiały i przejrzysty dzięki czytelnym diagramom technicznym, wydzielonym sekcjom wiersza poleceń i bogato opisanym zrzutom ekranów.
Zagadnienia poruszane w książce obejmują między innymi:

- rejestrację domeny,
- uzyskanie dedykowanej linii dzierżawionej,
- informacje dotyczące ruterów,
- instalację i konfigurowanie serwerów DNS, poczty, WWW, Proxy.

Ta książka pomoże:

- Nauczyć się wszystkiego, co trzeba wiedzieć, aby uruchomić serwer internetowy.
- Zrozumieć wymagania niezbędne do uruchomienia serwera internetowego.
- Pomyślnie utworzyć środowisko z dedykowanym dostępem do Internetu.
- Przygotować strukturę sieci lokalnej.
- Zainstalować dystrybucję Red Hat Linux.
- Zaimplementować serwer DNS.
- Skonfigurować serwer poczty elektronicznej.
- Uruchomić serwer WWW.
- Zrozumieć i skonfigurować serwer Proxy.
- Odkryć i wykorzystać wirtualne hosty.
- Zapewnić bezpieczeństwo serwera.

Ilustrowany podręcznik uruchamiania i obsługi internetowego serwera pod Linuksem jest przeznaczony dla użytkowników początkujących i średnio zaawansowanych.

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

Spis treści

Rozdział 10.

Bezpieczeństwo serwera internetowego

Praca bynajmniej nie kończy się wraz z uruchomieniem serwera internetowego. Prowadzenie serwera internetowego wymaga od administratora skupienia uwagi na zagadnieniach związanych z bezpieczeństwem i zastosowania odpowiednich środków do eliminacji wszelkich problemów, jakie mogą się pojawić. W tym rozdziale opisano minimum tego, co każdy administrator wiedzieć powinien.

W tym rozdziale znajdziesz:,

Zabezpieczanie serwera internetowego przed nieuprawnionym dostępem

Zabezpieczenia

Ponieważ serwer internetowy jest na stałe połączony z Internetem, jest narażony na ataki ze strony *crackerów* (ludzi nielegalnie uzyskujących dostęp do cudzych komputerów). W szczególności brak dostatecznej dbałości o sprawy związane z bezpieczeństwem, z uwagi na łatwe w Linuksie zdalne wykonywanie operacji, może spowodować, że dany serwer zostanie wykorzystany jako przyczółek do ataku na inne serwery.

W tym podrozdziale opisano wiele zagadnień, od ogólnych informacji do metod faktycznego ograniczania dostępu w celu zabezpieczenia serwera internetowego przed atakami intruzów.

Rodzaje ataków

Obsługując każdy komputer lub inne urządzenie podłączone do Internetu trzeba, mieć na uwadze jego bezpieczeństwo. Szczególnie jest zagrożony serwer internetowy, ponieważ jest on stale dostępny z każdego miejsca w Internecie. Ataki na serwery mogą przybierać różną postać i nasilenie:

Włamanie

Ten typ ataku obejmuje kradzież prywatnych lub poufnych informacji, dowolną zmianę lub usunięcie danych i zmianę ustawień konfiguracyjnych. Podczas ataku tego typu może również zostać zablokowane konfigurowanie zabezpieczeń, na przykład poprzez zmianę programów konfiguracyjnych, w celu ułatwienia następnych włamań.

Wykorzystanie serwera do ataku na inny serwer

Aby ukryć swoją tożsamość, intruzi często planują atak na określony serwer poprzez wiele innych serwerów, które już opanowali. W ten sposób nie pozostawiają śladów, które umożliwiłyby ich wykrycie lub powodują, że pozostawiony ślad jest tak złożony, iż nie można nim podążyć.

Blokada usług (ang. Denial of Service, DoS)

Atak tego typu ma na celu zatrzymanie usług. Istnieje kilka rodzajów ataków DoS. Zwykle skutkiem ataku jest nienormalny stan systemu i paraliż serwera.

Dziury w zabezpieczeniach

Intruz często atakuje, wykorzystując słaby punkt konfiguracji zabezpieczeń serwera. Ten słaby punkt nazywa się często dziurą w zabezpieczeniach (ang. *security hole*). Dziury w zabezpieczeniach można ogólnie podzielić na dwa rodzaje: spowodowane zaniedbaniami administratora lub błędną konfiguracją i dziury spowodowane problemami z oprogramowaniem.

- Dziury związane z administrowaniem i konfiguracją

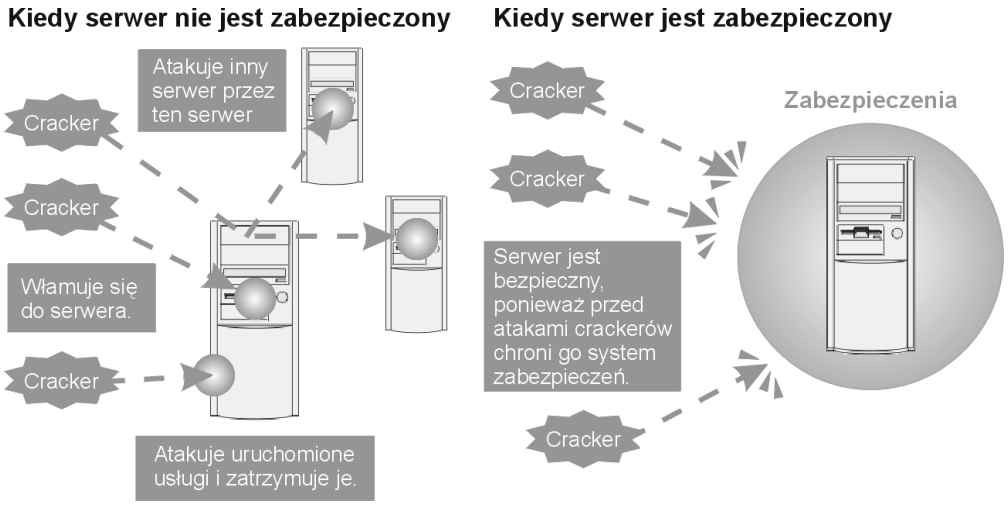
  Działanie: Ponowne sprawdzenie plików konfiguracyjnych, wyłączenie nieużywanych usług.

- Dziury związane z oprogramowaniem

  Działanie: Śledzenie bieżących informacji o aktualizacjach, aktualizowanie oprogramowania natychmiast po wykryciu problemu.

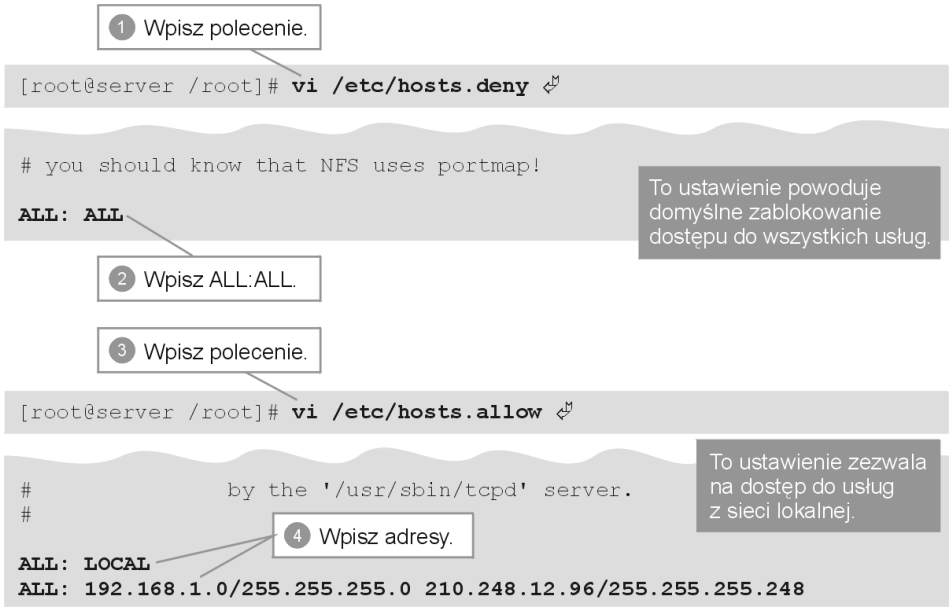
Należy zwrócić uwagę na wyłączenie nieużywanych a uruchomionych usług. Przemawia za tym zwykły zdrowy rozsądek. Byłoby stratą czasu martwić się o ochronę nieużywanych serwerów i usług. Prawdopodobnie nikt nie bawiłby się w nieustanne aktualizacje takich serwerów, nawet gdyby znane były dziury w ich zabezpieczeniach. Być może nawet nie będzie trzeba uruchamiać wszystkich serwerów opisanych w tej książce. Administrator serwera powinien wprowadzać środki bezpieczeństwa następującymi metodami:

- Ograniczanie dostępu (uniemożliwianie dostępu do serwera).
- Szyfrowanie haseł (uniemożliwienie dostępu osobie podszywającej się za użytkownika).
- Aktualizację wersji oprogramowania (eliminacja dziur związanych z błędami w oprogramowaniu).
- Śledzenie plików dziennika (monitorowanie podejrzanych zachowań).

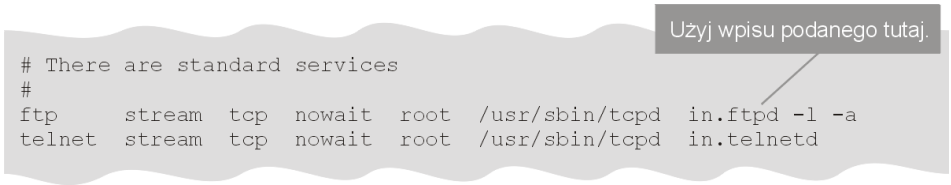


Ograniczanie dostępu przy użyciu tcpd

Efektywnym środkiem bezpieczeństwa jest ograniczenie dostępu do działających serwerów. Serwery korzystające z demona *inetd* (takie jak *qpopper*, *ftpd* i *telnetd*) są konfigurowane poprzez plik *inetd.conf* w taki sposób, aby mógł interweniować ograniczający dostęp program rezydentny o nazwie *tcpd* (*tcp_wrapers*). A zatem do ograniczenia dostępu należy użyć funkcji demona *tcpd*. Demon ten korzysta z dwóch plików konfiguracyjnych, o nazwach */etc/hosts.allow* i */etc/hosts.deny* (z ang. *allow* — zezwolić, *deny* — zabronić). Dla maksymalnego bezpieczeństwa spróbujmy skonfigurować te pliki tak, aby wszystkim zabronić dostępu do wszystkich usług, z wyjątkiem użytkowników z sieci lokalnej.



Po lewej stronie dwukropka (:) znajduje się to samo słowo, które znajduje się również na końcu wiersza w pliku *inetd.conf*. Na przykład w przypadku ustawienia dla serwera protokołu POP byłoby to słowo *popper*, a dla usługi telnet byłoby to *in.telnetd*. Nazwy poleceń obsługujących te serwery to również *popper* i *in.telnetd*. Należy dokonać wpisów odpowiadających nazwie następującej po fragmencie `/usr/sbin/tcpd` z każdego wiersza pliku *inetd.conf*.



Wpisanie ALL na początku wiersza spowoduje, że wpis będzie dotyczył wszystkich serwerów. Po prawej stronie dwukropka można wpisać nazwę komputera lub adres IP, adres i maskę sieci i tym podobne.

Co można wpisać przed dwukropkiem?

Nazwę serwera (ostatnie słowo z każdego wiersza pliku *inetd.conf*).

ALL	Odpowiada wszystkim serwerom.
EXCEPT	Wpisy następujące po tym słowie kluczowym odpowiadają komputerom, których wiersz nie dotyczy.

Co można wpisać po dwukropku?

Adres (nazwę hosta lub adres IP) komputera, którego dotyczy dany wiersz.

ALL	Odpowiada wszystkim adresom.
LOCAL	Dotyczy komputerów z domeny, w której znajduje się serwer.
Specyfikację sieci	(**210.248.12.96/255.255.255.248**)
Skrótowe określenie sieci	(**192.168.1.**)
Nazwę domeny	(**.dekiru.gr.jp**)
EXCEPT	Wpisy następujące po tym słowie kluczowym odpowiadają komputerom, których dany wiersz nie dotyczy.

Aby sprawdzić ustawienia, należy użyć poleceń `tcpdchk` i `tcpdmatch`. Polecenie `tcpdchk` umożliwia stwierdzenie błędów składniowych w plikach *hosts.allow* i *hosts.deny*.

```
[root@server /root]# tcpdchk
warning: /etc/hosts.allow, line 7: 192.168.1.0/255.255.0: bad net/mask pattern
[root@server /root]# _
```

Taki komunikat informuje o błędnej masce sieci.

Popraw maskę sieci w pliku *hosts.allow* na **255.255.255.0**.

Taki komunikat oznacza, że wiersz numer 7 w pliku */etc/hosts.allow* jest nieprawidłowy. Jeśli składnia jest prawidłowa, wykonaniu polecenia `tcpdchk` nie towarzyszy żaden komunikat.

```
[root@server /root]# tcpdmatch popper 192.168.1.1
client:   address   192.168.1.1
server:   process   popper
matched:  /etc/hosts.allow line 7
access:   granted
[root@server /root]# _
```

To jest test dostępu do serwera POP spod adresu **192.168.1.1**.

Słowo granted (ang. przyznany) wskazuje, że dostęp jest dozwolony.

```
[root@server /root]# tcpdmatch in.ftpd 192.168.2.1
client:   address   192.168.2.1
server:   process   in.ftpd
matched:  /etc/hosts.deny line 9
access:   denied
[root@server /root]# _
```

To jest test dostępu do serwera FTP spod adresu **192.168.1.1**.

Słowo denied (ang. zabroniony) wskazuje, że dostęp jest zablokowany.

Po co hasła?

Hasło jest ważną informacją potwierdzającą tożsamość użytkownika. Jeśli hasło wpadnie w ręce crackera, będzie on mógł zrobić to samo co może zrobić użytkownik (a nawet trochę więcej, ponieważ zwykle dysponuje większa wiedzą niż przeciętny użytkownik – *przyp. tłum.*). Dlatego niezwykle istotne jest zabezpieczenie hasła przed możliwością ujawnienia go.
Hasło jest przesyłane w sieci w różnych sytuacjach. Dlatego najpierw należy dowiedzieć się co się dzieje z hasłem przy wykonywaniu różnych czynności. Mając tę wiedzę, można myśleć o ochronie i podjęciu odpowiednich środków zapobiegawczych.

Usługi używające haseł i te, które ich nie używają

Większość spośród opisywanych w tej książce serwerów, które używają haseł (na przykład FTP i POP), przesyła je jawnym tekstem (niezaszyfrowane). Warto więc ograniczyć do nich dostęp również z komputerów pracujących w sieci lokalnej.

Telnet lub FTP (File Transfer Protocol)

Nazwa użytkownika i hasło są przesyłane w postaci niezaszyfrowanej. Ponieważ wprowadzane polecenia i wyświetlane znaki również są przesyłane w ten sam sposób, korzystanie z tych usług z zewnątrz jest niebezpieczne. Należy ograniczyć dostęp wyłącznie do użytkowników w sieci LAN.

Anonimowe FTP

Nazwa użytkownika i hasło są przesyłane w postaci niezaszyfrowanej. Ponieważ jednak nazwa użytkownika w tym przypadku to *anonymous*, a hasłem jest adres poczty elektronicznej, przejęcie tych informacji nie stwarza zagrożenia. Chociaż polecenia (takie jak `ls` i `cd`) i pliki danych są również przesyłane w jawnej postaci, to dopóki serwer jest dostępny publicznie poprzez anonimowe FTP, nie ma powodu do obaw.

POP (Post Office Protocol) lub IMAP (Internet Message Access Protocol)

Nazwa użytkownika i hasło są przesyłane w postaci niezaszyfrowanej. Poczta jest przesyłana w postaci możliwej do bezpośredniego odczytania. Korzystanie z tych serwisów z lokalizacji zewnętrznych jest niebezpieczne. Należy ograniczyć dostęp do tych usług wyłącznie do połączeń z komputerów podłączonych do sieci lokalnej.

APOP

Nazwa użytkownika jest przesyłana w postaci jawnej, ale hasło jest zaszyfrowane. Poczta jest przesyłana w postaci możliwej do bezpośredniego odczytania. Jest to jednak rozwiązanie bezpieczniejsze niż zwykły protokół POP.

SMTP (Simple Mail Transfer Protocol)

Protokół SMTP nie przesyła nazw użytkowników ani ich haseł. Poczta jest wysyłana i odbierana w postaci możliwej do bezpośredniego odczytania.

HTTP (HyperText Transfer Protocol)

Zwykle protokół HTTP nie korzysta z nazw użytkowników ani haseł. W przypadku dostępu do strony WWW o ograniczonym dostępie z koniecznością podania hasła, jest ono przesyłane w postaci jawnej. Uwierzytelnianie poprzez hasło w protokole HTTP powinno być zatem stosowane z pełną świadomością tego faktu.

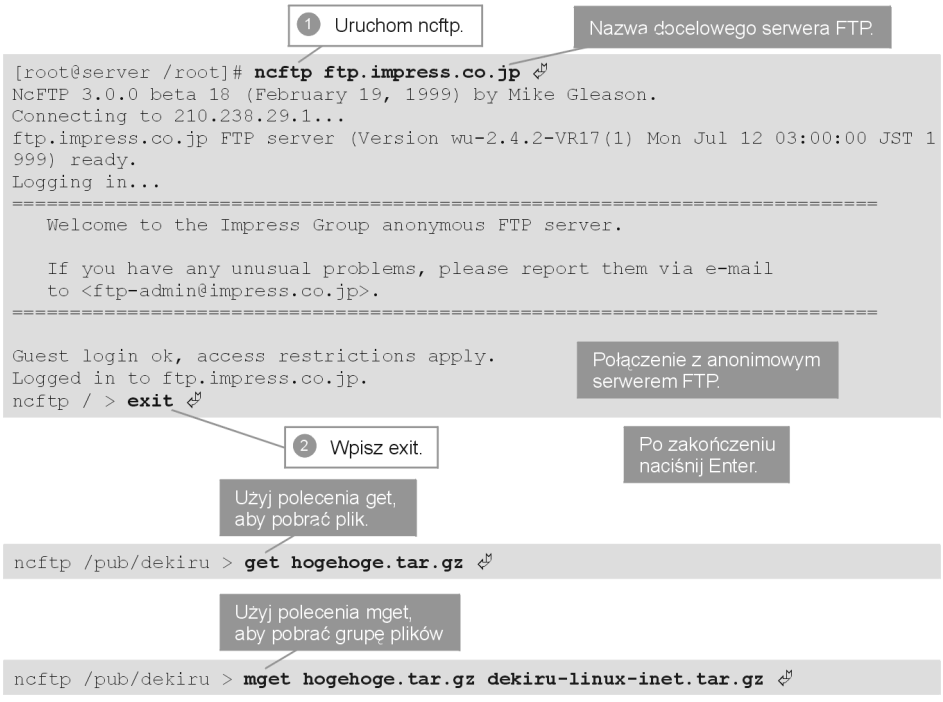
DNS (Domain Name Service)

Wymieniane informacje nie są szyfrowane. Nie rodzi to jednak zagrożenia, ponieważ usługa ta nie korzysta z nazw użytkowników ani haseł.

Aktualizacja wersji oprogramowania

Poprzez zmianę ustawień konfiguracyjnych nie da się wyeliminować dziury w systemie bezpieczeństwa, której przyczyna tkwi w samym oprogramowaniu. W takim przypadku najwyższego znaczenia nabiera codzienne śledzenie informacji o oprogramowaniu.
Dziura spowodowana błędami oprogramowania rzadko jest odkrywana podczas ataku na system. W rzeczywistości większość ataków następuje po upowszechnieniu informacji o słabościach danego oprogramowania, a przed zastosowaniem przez administratora odpowiednich środków zaradczych.
Uniknięcie takich ataków jest możliwe poprzez szybką aktualizację oprogramowania do najnowszej wersji, w której poprawiono znane błędy.
Poniżej opisano popularnego klienta FTP — program ncftp, za pomocą którego można pobierać z serwerów FTP najnowsze wersje oprogramowania.

Jak używać programu ncftp?



Opis programu ncftp

Metody uruchamiania

`ncftp`	Uruchamia *ncftp*.
`ncftp` *`nazwa_hosta`*	Uruchamia *ncftp* i łączy się z podanym serwerem FTP.
`ncftp –u` *`nazwa_użytkownika nazwa_hosta`*	Loguje się, używając podanej nazwy użytkownika.

Polecenie open

`open` *`nazwa_hosta`*	Łączy się z serwerem FTP.
`open –u` *`nazwa_użytkownika nazwa_hosta`*	Loguje się, używając podanej nazwy użytkownika.

Zmiana trybu

`ascii`	Przechodzi w tryb tekstowy
`binary`	Przechodzi w tryb binarny.

Zmiana lub sprawdzenie bieżącego katalogu

`cd`	Zmienia katalog.
`ls`	Wyświetla listę plików
`dir`	Wyświetla szczegółową listę plików.
`pwd`	Wyświetla nazwę katalogu bieżącego.

Zmiana lub sprawdzenie katalogu lokalnego

`lcd`	Zmienia katalog.
`lls`	Wyświetla listę plików
`lpwd`	Wyświetla nazwę katalogu bieżącego.

Operacje na plikach

`get`	Pobiera plik.
`mget`	Pobiera grupę plików.
`page`	Przegląda plik, strona po stronie.
`put`	Przesyła plik do serwera.
`mput`	Przesyła do serwera grupę plików.

Polecenie help

`help`	Wyświetla listę dostępnych poleceń
`help` *`polecenie`*	Wyświetla pomoc dla danego polecenia.

Koniec pracy

`quit`, `exit` lub `bye`	Kończy działanie *ncftp*.
`close`	Przerywa połączenie.

Wykrywanie nieuprawnionego dostępu

Przeglądanie systemowych plików dziennika nie musi prowadzić do wykrycia włamania do systemu. Jeśli zdarzenie takie faktycznie miało miejsce i zostały przejęte uprawnienia administratora, intruz prawdopodobnie pozacierał za sobą wszystkie ślady. Także w plikach dziennika nie pozostały zapisy o tym zdarzeniu. Przeglądanie plików dziennika może być jednak pomocne w odkryciu nielegalnego dostępu, który wystąpi zanim jeszcze zostanie dokonane włamanie i zostaną przejęte uprawnienia administatora. W razie jakichkolwiek podejrzeń, należy najpierw przejrzeć pliki dziennika.

/var/log/boot.log	Plik dziennika zawierający dane o uruchamianiu i zatrzymywaniu programów rezydentnych.
/var/log/cron	Plik dziennika demona *crond* (wykonującego skrypty o zadanych godzinach).
/var/log/dmesg	Komunikaty jądra.
/var/log/maillog	Plik dziennika serwera *Sendmail* i demona *imapd*.
/var/log/messages	Plik dziennika programu *BIND*, jądra, polecenia *su*, itp.
/var/log/secure	Plik dziennika zawierający dane o logowaniu i informacje demona *tcpd*.

/var/log/xferlog	Plik dziennika demona *ftpd*.
/usr/local/www/logs/access_log	Plik zawierający informacje o próbach dostępu do serwera *Apache*.
/usr/local/www/logs/error_log *Apache*.	Plik zawierający informacje o błędach serwera
/var/log/squid/access.log	Dane o próbach dostępu serwera *Squid*.
/var/log/squid/cache.log	Dane o działaniu serwera *Squid*.
/var/log/squid/store.log	Plik z danymi o wykorzystaniu pamięci podręcznej serwera *Squid*.

Ponadto można użyć polecenia `last`, podającego informacje o ostatnich logowaniach użytkowników do systemu.

```
[root@server /root]# last ⏎
watanabe tty1                  Mon Jul 12 04:03   still logged in
watanabe pts/5                 Mon Jul 12 04:03 - 04:03  (00:00)
watanabe pts/3                 Mon Jul 12 04:03 - 04:03  (00:00)

wtmp begins Thu Jul  1 04:03:36 1999
[root@server /root]# _
```

Serwisy WWW poświęcone zabezpieczeniom

Red Hat, Inc.

www.redhat.com

Serwis zawiera informacje o błędach (errata) znalezionych w dystrybucji Red Hat Linux oraz odnośniki do aktualnych informacji. W erracie opisano również metody eliminowania dziur w systemie zabezpieczeń.

CERT/CC

www.cert.org

Oprócz różnych informacji dotyczących zabezpieczeń, serwis zamieszcza raporty z rzeczywistych ataków i umożliwia wzięcie udziału w dyskusji poświęconej zagadnieniom bezpieczeństwa.

Linux Online

www.linux.org

W serwisie można znaleźć łącza do innych serwisów związanych z Linuksem.

FreeBSD

www.freebsd.org

Macierzysty serwis systemu FreeBSD, który jest alternatywnym do Linuksa uniksowym systemem operacyjnym dla komputerów PC. Jednak pomimo różnic między systemami, wiele pakietów programowych jest takich samych, stąd zamieszczane w serwisie informacje są cenne także dla użytkowników Linuksa.

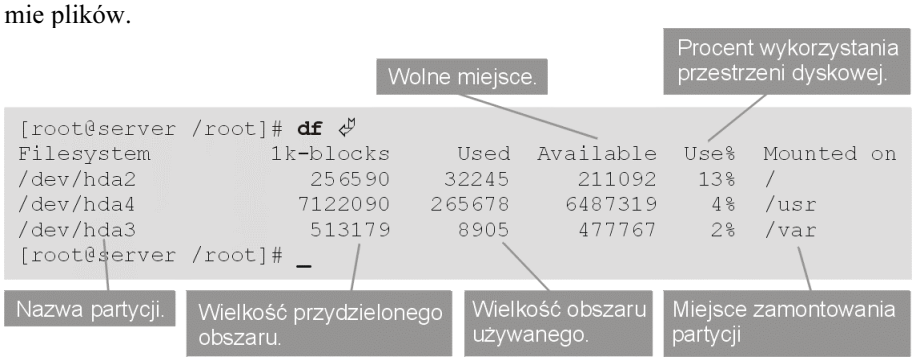
Jak unikać kłopotów?

Kopie zapasowe

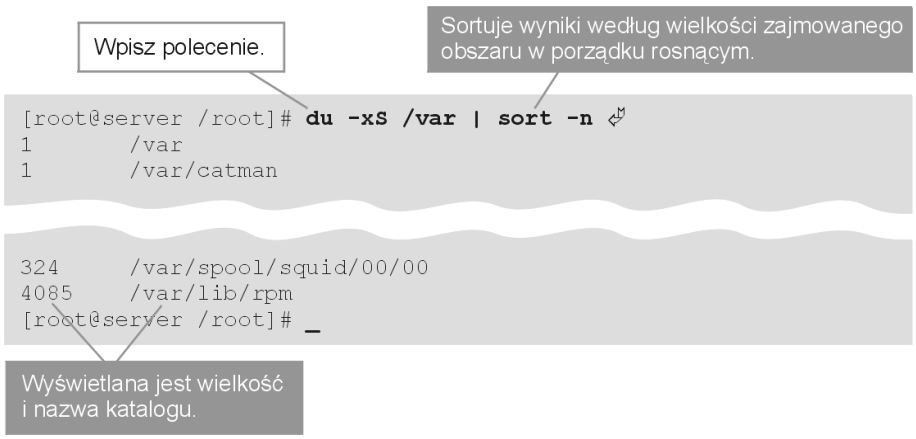
W przypadku wystąpienia problemu, który prowadzi do unieruchomienia serwera, prawdziwym zbawieniem mogą być kopie zapasowe. Rutynowa archiwizacja plików konfiguracyjnych może być przydatna przy ponownej instalacji systemu lub w przypadku nieumyślnej modyfikacji plików konfiguracyjnych, w wyniku której serwer przestaje działać. Archiwizacja danych użytkowników lub zawartości serwisu WWW minimalizuje także straty powstałe wskutek uszkodzenia serwera.

Jak sprawdzić wielkość systemu plików?

Polecenie `df` służy do sprawdzania ilości dostępnego miejsca w zamontowanym systemie plików.



Jeśli rezultaty polecenia `df` wskazują na to, że kończy się miejsce na dysku, należy najpierw usunąć niepotrzebne pliki. Polecenie `du` pokazuje wielkość obszaru zajmowanego przez poszczególne katalogi.



Kopia zapasowa plików konfiguracyjnych

Wygodną metodą archiwizacji plików konfiguracyjnych jest sporządzenie listy nazw tych plików i użycie polecenia `tar` do zarchiwizowania ich w postaci pojedynczego pliku.

Odtwarzanie plików konfiguracyjnych

Odtworzenie zarchiwizowanych plików konfiguracyjnych wymaga rozpakowania ich z archiwum i skopiowania. Jeśli w przypadku jakiegoś problemu zajdzie potrzeba instalacji serwera od początku, użycie zarchiwizowanego pliku konfiguracyjnego zapewnia odtworzenie tej samej konfiguracji serwera co poprzednio.

Archiwizowanie plików danych

Dane z katalogów osobistych użytkowników i ich strony WWW znajdują się odpowiednio w katalogach */home* lub */usr/local/www*. Archiwalna kopia danych obejmuje wszystkie pliki z tych katalogów.

```
[root@server /root]# cd /usr/local/src ⏎
[root@server src]# tar cvfz home-bak.tar.gz /home ⏎
tar : Removing leading '/' from absolute path names in the archive
home/

home/hide/.bashrc
[root@server src]# cd /usr/local ⏎
[root@server local]# tar cvfz src/www-bak.tar.gz www ⏎
www/

www/proxy
 [root@server local]# _
```

Za pomocą opisanych poprzednio poleceń dane z katalogów */home* i */usr/local/www* zostały zapisane w plikach kopii archiwalnych o nazwach *home-bak.tar.gz* i *www-bak.tar.gz* w katalogu */usr/local/src*. Na wszelki wypadek można skopiować te pliki do innych lokalizacji. Każda jest dobra, jeśli tylko pozwoli na rozpakowanie plików w przypadku awarii serwera. Jednak prawdopodobnie najlepszy wyjściem będzie przesłanie ich z serwera do innego komputera PC za pomocą serwera FTP.

Instalowanie serwera FTP

Jeśli serwer FTP nie został jeszcze zainstalowany, trudno będzie przesłać pliki kopii archiwalnych do innego komputera. Za pomocą polecenia `rpm` należy zainstalować serwer FTP w systemie Linux.

Wpisz polecenie.

Zainstaluj serwer o nazwie *wu-ftpd*.

```
[root@server /root]# rpm -i /mnt/cdrom/RedHat/RPMS/wu-ftpd-2.4.2vr17-3.i386.rpm ⏎
[root@server /root]#
```

Aby zalogować się do serwera FTP, należy podać nazwę użytkownika i hasło używane w Linuksie. Nie można jednak zalogować się jako użytkownik root, trzeba użyć swojego zwykłego konta.

Odtwarzanie plików danych

Bezpośrednie odtwarzanie zarchiwizowanych plików danych może spowodować nadpisanie nowych danych. Aby temu zapobiec, należy przed rozpakowaniem plików zmienić nazwę oryginalnego katalogu.

Zmień nazwę istniejącego katalogu, aby go zabezpieczyć.

Rozpakuj zarchiwizowane pliki.

```
[root@server /root]# cd / ⏎
[root@server /]# mv home home.old ⏎
[root@server /]# tar xvpfz /usr/local/src/home-bak.tar.gz ⏎
```

Bezproblemowe administrowanie pocztą

Poczta elektroniczna

Podczas eksploatacji serwera internetowego mogą wystąpić różne problemy. Jednak serwer jest wyposażony w przydatną funkcję powodującą automatyczne przesyłanie na określone konta (użytkownika root lub administratora poczty) poczty informującej o wystąpieniu problemu. Ponadto konto root lub administratora poczty używane jest jako centrum obsługi skarg i wniosków napływających od administratorów innych systemów lub użytkowników. Z tych powodów należy tak skonfigurować serwer poczty, aby poczta adresowana na specjalne konta była przekazywana na normalne konto administratora, co umożliwi jak najszybszą reakcję.

Gdy poczta nie dociera do celu

Jeśli ustawienia w pliku konfiguracyjnym *sendmail.cf* powodują nadmierne ograniczenie dostępu z sieci do serwera poczty, może to być przyczyną niedostarczania poczty do zewnętrznych lokalizacji. W takim przypadku w programie pocztowym użytkownika jest wyświetlany komunikat o błędzie. Wyeliminowanie problemu wymaga powrotu do rozdziału 7. i ponownego sprawdzenia ustawień konfiguracyjnych.

W innych wypadkach, kiedy serwer sendmail nie może dostarczyć poczty pod adres docelowy, wysyła do nadawcy komunikat o błędzie z krótkim opisem okoliczności. Komunikaty o błędach pojawiające się względnie często to „User Unknown" (nieznany użytkownik) i „Host Unknown" (nieznany host). Oznacza to, że wysłana wiadomość została niewłaściwie zaadresowana.

Komunikat o błędzie wysyłany do nadawcy zawiera pełny tekst wysłanej wiadomości. Jednocześnie ten sam komunikat, ale już bez treści wiadomości wysyłany jest na konto administratora poczty. Dlatego ustawienie domyślnego przesyłania poczty adresowanej do administratora poczty na jego normalnie używane konto pozwala mu na bieżąco śledzić problemy z serwerem poczty.

Gdy nie dochodzi poczta od nadawcy spoza sieci lokalnej

Jest kilka przyczyn niedostarczania poczty od nadawcy spoza sieci lokalnej.

Przepełnienie kolejki

Poczta jest tymczasowo przechowywana w kolejce poczty w katalogu */var/spool/mail*. Jeśli wyniki polecenia `df` wskazują na brak miejsca w systemie plików */var*, należy za

pomocą polecenia `du` zlokalizować pliki zajmujące najwięcej miejsca i usunąć je (patrz podrozdział 10.2).
W przypadku dużej objętości wiadomości przechowywanych w katalogu kolejki, powodującej jego nadmierną wielkość, należy usunąć całkowicie nieużywane konta użytkowników. Jeśli użytkownik będzie chciał zatrzymać jedynie adres nieużywanego konta pocztowego, można przekazywać pocztę na jego normalne konto, modyfikując plik */etc/aliases*.

Zdalny serwer nie może określić serwera SMTP lokalnej domeny

Jeśli rekord typu MX w konfiguracji serwera DNS jest nieprawidłowy, zdalny serwer nie będzie mógł zidentyfikować lokalnego serwera poczty i tym samym dostarczyć mu poczty. Należy wówczas sprawdzić rekordy MX poleceniem `nslookup` (patrz rozdział 6.).

Nieprawidłowa konfiguracja serwera *Sendmail*

Skutkiem nieprawidłowej konfiguracji programu *sendmail* jest brak możliwości odbierania poczty. W takiej sytuacji trzeba wrócić do procedur opisanych w rozdziale 7. i sprawdzić w ustawieniach w pliku *sendmail.cf*, czy program *sendmail* został skonfigurowany do odbierania poczty adresowanej do domeny lokalnej.

Poczta adresowana na konta specjalne

Poczta adresowana na konta specjalne o nazwach *postmaster*, *webmaster*, *root* i *MAILER-DAEMON* może zawierać ważne informacje. Poczta taka powinna być przekazywana na normalne konto administratora poprzez odpowiednie ustawienia w pliku */etc/aliases*. Informacje o tym pliku zawiera rozdział 7.

Poczta od innych administratorów lub użytkowników

Pełniąc funkcje administratora serwera, otrzymuje się wiadomości adresowane na konta *postmaster* lub *webmaster* wysłane przez innych administratorów lub użytkowników. Wiadomości te mogą zawierać uwagi dotyczące działania serwera. Obsługa takiej poczty to ważna funkcja administratora. Należy próbować odpowiadać na wszystkie wiadomości, oczywiście z wyjątkiem spamu lub innej wątpliwej poczty.

Rozwiązywanie problemów

Problemy z siecią

Jeśli działanie serwera lub łączy sieciowych wydaje się podejrzane, administrator powinien przedsięwziąć kroki w celu przywrócenia normalnego stanu rzeczy. W tym podrozdziale opisano techniki radzenia sobie z niektórymi problemami z siecią.

Należy unikać restartowania serwera, chyba że nie ma innego wyjścia. Należy raczej restartować programy podejrzewane o sprawianie problemów (takie jak serwer DNS lub serwer WWW), bez ponownego uruchamiania systemu operacyjnego.

Gdy nie można podłączyć się do sieci

Przyczyną niemożności podłączenia się do sieci może być awaria sprzętowa. Trzeba wówczas sprawdzić kable łączące z routerem i koncentratorem.

- Czy kabel się nie poluzował?

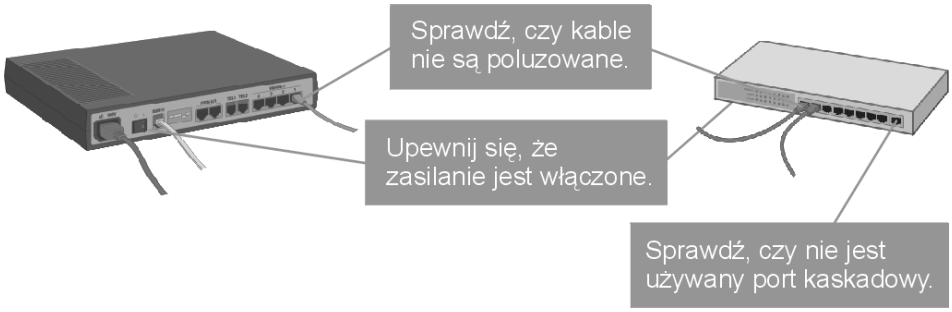
  Przy podłączaniu wtyczki kabla sieciowego do gniazda na karcie lub w koncentratorze czy w routerze powinno być słyszalne kliknięcie. Należy także sprawdzić diody LED w kartach sieciowych, w routerze i w koncentratorze.

- Czy router i koncentrator są włączone?

  Należy sprawdzić kontrolki zasilania w ruterze i w koncentratorze.

- Czy nie jest używany port sąsiadujący z portem kaskadowym koncentratora?

  Podłączenie kabla do portu koncentratora, który nie może być używany z uwagi na wykorzystanie portu kaskadowego, spowoduje brak dostępu do sieci dla wszystkich maszyn podłączonych do tego koncentratora.



- Czy nie jest używany kabel skrośny?

  Kabel skrośny jest wykorzystywany do bezpośredniego połączenia dwóch komputerów wyposażonych w karty sieciowe. Nie można użyć takiego kabla do podłączenia komputera do koncentratora.

Sprawdzanie, czy sieć jest podłączona

Polecenie `ping`, używając protokołu IP, pozwala określić, czy jest możliwa komunikacja z innym urządzeniem w sieci. Dlatego właśnie administratorzy często określają sprawdzanie połączenia z inną maszyną za pomocą polecenia `ping` terminem *pingowanie*.

Sprawdzanie połączeń internetowych poleceniem ping

Uruchom polecenie ping z komputera z systemem Windows.

Wpisz polecenie.

```
C:\WINDOWS>ping www.impress.co.jp ↵

Pinging impgw.impress.co.jp [210.238.29.1] with 32 bytes of data:

Reply from 210.238.29.1: bytes=32 time=39ms TTL=242
Reply from 210.238.29.1: bytes=32 time=36ms TTL=243
Reply from 210.238.29.1: bytes=32 time=36ms TTL=243
Reply from 210.238.29.1: bytes=32 time=36ms TTL=243

Ping statistics for 210.238.29.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 39ms, Average = 36ms

C:\WINDOWS>_
```

Otrzymanie odpowiedzi oznacza,że komputer ma połączenie z Internetem.

Sprawdzanie połączeń LAN poleceniem ping

Wpisz polecenie.

```
C:\WINDOWS>ping 192.168.1.1 ↵

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\WINDOWS>_
```

Otrzymanie odpowiedzi oznacza, że komputer ma połączenie z siecią lokalną.

Nietypowe wyniki działania polecenia ping

Jeśli wyniki polecenia `ping` wskazują na dziwne działanie systemu, należy ponownie przejrzeć rozdział 9. i sprawdzić, czy w poniższych plikach znajdują się prawidłowe dane:

/etc/conf.modules
/etc/sysconfig/network
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/sysconfig/network-scripts/ifcfg-eth1

Po dokonaniu ewentualnych zmian należy ponownie inicjować ustawienia.

```
[root@server /root]# /etc/rc.d/init.d/network restart ↵
Shutting down interface eth0                               [  OK  ]
Shutting down interface eth1                               [  OK  ]
Disabling IPv4 packet forwarding                           [  OK  ]
Enabling Ipv4 packet forwarding                            [  OK  ]
Bringing up interface lo                                   [  OK  ]
Bringing up interface eth0                                 [  OK  ]
Bringing up interface eth1                                 [  OK  ]
[root@server /root]# _
```

Jeśli pakiety wysyłane poleceniem `ping` z sieci lokalnej nie przechodzą do Internetu, być może błąd tkwi w konfiguracji translacji adresów sieciowych (NAT). Trzeba wtedy ponownie skonfigurować translację NAT.

```
[root@server /root]# /etc/rc.d/init.d/ipmasq restart ↵
```

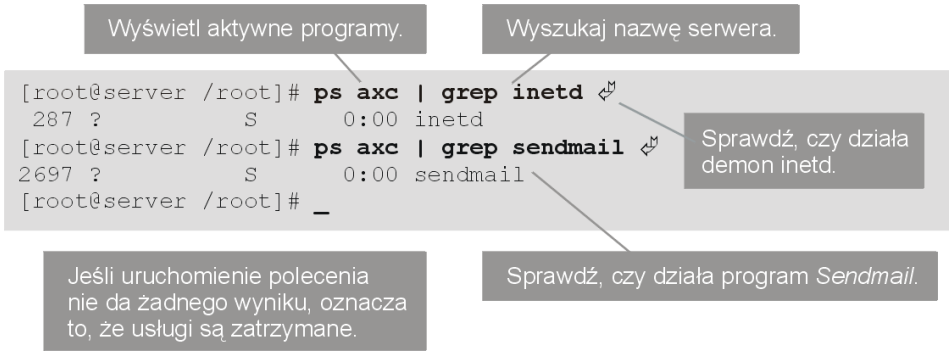
Restart demonów

Jeśli usługi nie działają prawidłowo pomimo poprawnego działania sieci, należy spróbować restartować serwery. Być może zmiany dokonane w konfiguracji nie zostały uaktywnione, ponieważ serwer nie został zrestartowany.

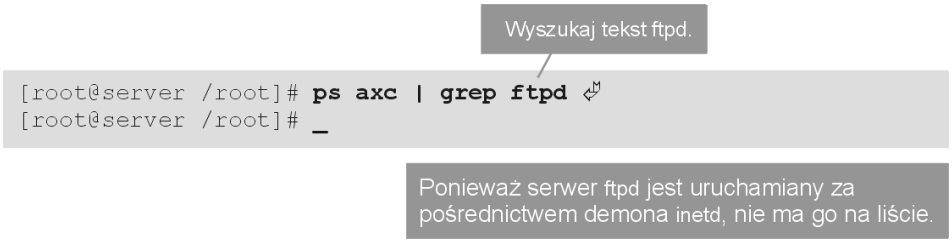
Usługa	Metoda restartu
BIND	`ndc restart`
Apache	`/etc/rc.d/init.d/httpd restart`
sendmail	`/etc/rc.d/init.d/sendmail restart`
Qpopper	`/etc/rc.d/init.d/inet restart`
FTP	`/etc/rc.d/init.d/inet restart`
Dhcpd	`/etc/rc.d/init.d/dhcpd restart`
Squid	`/etc/rc.d/init.d/squid restart`
NAT	`/etc/rc.d/init.d/ipmasq restart`

Lista działających programów

Za pomocą polecenia `ps` można sprawdzić, jakie programy są uruchomione w systemie Linux. Dzięki temu można stwierdzić, czy programy serwerów są uruchomione.



Metoda ta umożliwia sprawdzenie, czy działają serwery uruchamiane przez demona `inetd` (takie jak `qpopper` czy `ftpd`), ale tylko wtedy, gdy obsługują one jakieś połączenie. Ponieważ translacja NAT działa na innych zasadach, niż pozostałe serwery, jej działania nie da się sprawdzić poleceniem `ps`.



Kto decyduje o tym, jak działa Internet?

W Internecie wykorzystuje się wiele różnych protokołów, konwencji i mechanizmów, z których kilka przedstawiono w tej książce. Kto decyduje o tym, w jaki sposób są one wdrażane? Komitet o nazwie Internet Engineering Task Force (IETF — Zespół Zadaniowy ds. Inżynierii Internetu). Każdy zainteresowany może uczestniczyć w jego spotkaniach, których rezultaty są publikowane w postaci dokumentów o nazwie *Internet Draft*. Gdy dokument Internet Draft zostanie zaaprobowany przez komitet Internet Architecture Board (IAB) staje się formalnym dokumentem noszącym nazwę Request for Comments (RFC). Zarówno dokumenty Internet Draft, jak i RFC, są dostępne dla wszystkich na serwerach anonimowego FTP i serwerach WWW. Dokumentom RFC przypisywane są numery seryjne, na przykład dokument RFC 2068 zawiera specyfikację protokołu HTTP w wersji 1.1, używanego obecnie w sieci WWW. Oprócz różnych rodzajów specyfikacji internetowych dokumenty RFC zawierają streszczenia innych dokumentów oraz podstawowe informacje nazywane FYI (*For Your Information* — do twojej wiadomości) z objaśnieniami, pytaniami i odpowiedziami (ang. *Question and Answer, Q&A*) i historią Internetu. W dokumentach RFC można znaleźć ponadto tzw. standardy specjalistyczne (ang. *Specific Standard — STD*), które zostały przyjęte w Internecie. Standardy te również mają swoje numery seryjne. Odpowiedzi na wszelkie pytania dotyczące Internetu oraz inne poszukiwane informacje można na pewno znaleźć czytając dokumenty RFC.

Dokumenty RFC i STD są uważane za formalne specyfikacje mechanizmów internetowych głównie dlatego, że programy i urządzenia faktycznie działają w zgodzie z tymi specyfikacjami, bez względu na to, czy specyfikacje te są logiczne. Standardem może być tylko to, co jest powszechnie stosowane i działa prawidłowo. Ilustruje to często wykorzystywany zwrot: „jest to de facto standardem w Internecie".

IAB *www.iab.org*
IETF *www.ietf.org*