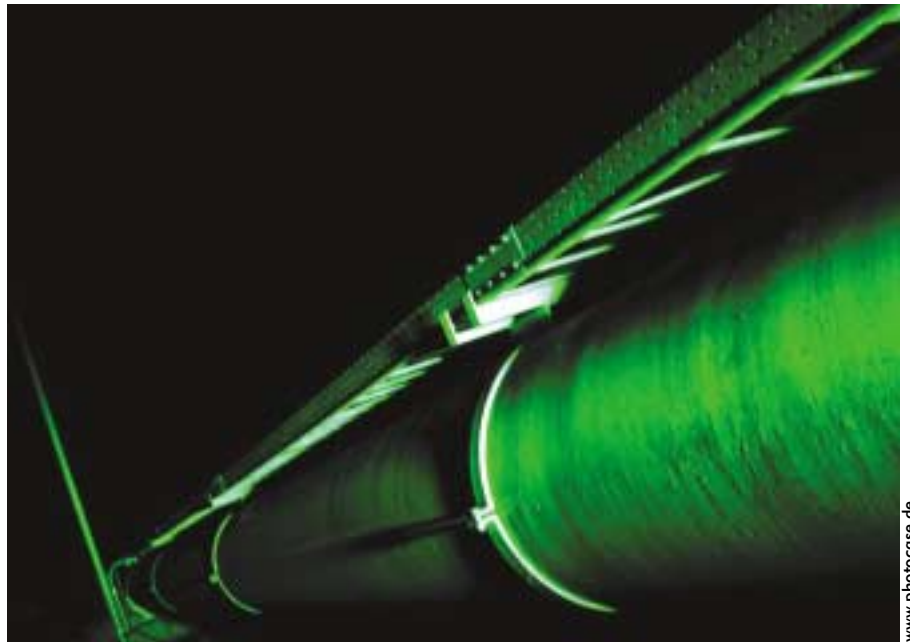


Ograniczanie dostępu do SSH przy pomocy SCPonly

Bezpieczna linia

Większość administratorów cieszy się na wieść o zastąpieniu protokołu FTP bezpieczniejszą alternatywą, jaką jest SCP/SFTP. Niestety, pakiet ten w domyślnej instalacji umożliwia dostęp do systemu z poziomu powłoki. Możemy jednak skorzystać z SCPonly, który umożliwia uwięzienie użytkowników w chroot.

MARTIN WERTHMÖLLER



www.photocase.de

Protokół FTP jest z nami od trzydziestu lat, umożliwiając pobieranie i przekazywanie plików na serwer. Co dziwne, FTP jest nadal chętnie używanym protokołem, mimo że nie jest w ogóle zabezpieczony. Cały proces przesyłania danych i haseł jest jawny, co ułatwia potencjalne ataki.

Poza tym zasada działania FTP komplikuje konfigurację zapór sieciowych. Protokół wymaga dwóch jednoczesnych połączeń TCP. W zależności od trybu pracy, połączenie ustanawiane jest przez serwer lub klienta na przypadkowym porcie po drugiej stronie połączenia. Kiedy zapora sieciowa napotka żądanie połączenia tego typu, musimy podać jej informacje na temat źródła połączenia FTP.

Protokół FTPS jest bezpieczną i kompatybilną odmianą protokołu FTP. Zasady FTPS określono w RFC 2228 [1]; wykorzystuje on również dwa połączenia TCP, podobnie jak protokół FTP, ale stosuje szyfrowanie danych

w zbliżony sposób do protokołu HTTPS. Niestety, FTPS nie przeszedł nigdy etapu wstępnego RFC i nie jest powszechnie używany na świecie.

Brak alternatywy

Rozszerzenie protokołu WebDAV HTTP (RFC 2518, [2]) umożliwia przekazywanie i bezpośrednie modyfikacje plików na serwerze. Kanał transmisji danych TLS/SSL zajmuje się szyfrowaniem danych. Niestety, WebDAV ma kilka wad. Moduł serwera Apache nie obsługuje zmian identyfikatorów użytkowników. Innymi słowy, wszyscy użytkownicy WebDAV posiadają w systemie plików ten sam identyfikator użytkownika, a zatem nadawanie szczegółowych uprawnień na serwerze Apache WebDAV jest niemożliwe. Większość produkcyjnych serwerów WWW nie posiada w dodatku zainstalowanego modułu WebDAV lub nie jest on skonfigurowany.

Bezpieczne zastępstwo

Pakiety narzędzi SSH, SCP oraz SFTP są w systemach Unix alternatywą dla protokołu FTP. SCP zapewnia szyfrowane przekazywanie plików przy pomocy tune-

lowania SSH. Użytkownicy określają po prostu z poziomu wiersza poleceń pliki, które należy skopiować. Nie można tutaj mylić protokołu SFTP z protokołem FTPS – nie mają one ze sobą nic wspólnego. Protokół SFTP wymaga tylko jednego połączenia TCP, gdyż korzysta z SSH – tak samo jak protokół SCP. Jednakże, w przeciwieństwie do SCP, możemy z niego korzystać interaktywnie – tak jak z klienta FTP.

Oba rozwiązania nie wymagają skomplikowanej konfiguracji serwera czy klienta. Wiele komputerów ma już uruchomiony serwer SSH, a większość zapór sieciowych umożliwia połączenia SSH bez dodatkowej ingerencji ze strony użytkownika. Niestety, podana metoda ma swoje wady:

- Nie wszystkie systemy operacyjne posiadają oprogramowanie SCP z graficznym interfejsem użytkownika.
- Programy SCP i SFTP z pakietu OpenSSH są zbyt skomplikowane dla większości użytkowników.
- SCP wymaga interaktywnej sesji SSH. Oznacza to, że użytkownicy SCP mogą także wykonywać polecenia powłoki.
- W przeciwieństwie do wielu serwerów FTP, demon SSH nie posiada własnej

AUTOR

Martin Werthmöller mieszka wraz z żoną i dwoma synami w Niemczech, nieopodal Munster. Jest niezależnym projektantem i administratorem sieci.

obsługi konfiguracji chroot.

Rozwój OpenSSH jest nastawiony głównie na obsługę OpenBSD, chociaż istnieją próby przeniesienia go na inne systemy, m.in. Linux, Cygwin czy Mac OS X. Dzięki przeniesieniu programu na platformę Cygwin, możemy zainstalować OpenSSH nawet w systemie Windows. Dla tego systemu lepszym rozwiązaniem będzie jednak Putty [3]. Poza programami klienta OpenSSH, scp i sftp, dla systemów Linux, Windows i Mac OS X dostępne są także nakładki z graficznym interfejsem użytkownika (GUI) (patrz Ramka „Programy SCP typu klient z interfejsem GUI”). Większość tych programów-klientów jest bezpłatna.

Istnieje wiele sytuacji, w których użytkownicy nie potrzebują lub wręcz nie powinni korzystać z powłoki systemu (shell) – na przykład, gdy dostawcy Internetu obsługują kilkanaście serwisów internetowych na jednym serwerze. Pełny dostęp do interpretera poleceń mógłby być fatalny w skutkach...

Ograniczanie dostępu

Protokoły SCP i SFTP zakładają korzystanie z powłoki – dobre rozwiązanie będzie jednak wymagać ograniczenia dostępu do powłoki, przy jednoczesnym gwarantowaniu pełnej funkcjonalności, jaką dają nam SCP i SFTP. Mamy do wyboru dwie metody: przygotować osobną powłokę logowania, aby użytkownicy mogli uruchamiać swoje pliki wykonywalne wyłącznie dla SCP i SFTP, bądź uwięzić użytkowników w chroot po zalogowaniu

do systemu, pozwalając jedynie na dostęp do wymaganych programów. W ten sposób zabezpieczamy się dodatkowo, uniemożliwiając dostęp do plików innych użytkowników.

Powłoka logowania musi gwarantować automatyczne uruchomienie polecenia chroot. Pod adresem [8] znajduje się poprawka, która nakazuje demonowi SSH wywołanie chroot().

Najlepsze rozwiązanie: SCPonly

Ulepszona wersja demona SSH nie jest dostępna jako pakiet RPM czy Debiana, a więc nie będzie także uznawana przez dystrybutora aktualizacji zabezpieczeń naszego systemu. Oznacza to konieczność ręcznej modyfikacji wersji instalacyjnej OpenSSH na serwerze po każdej aktualizacji zabezpieczeń.

RSSH [9] wraz ze SCPonly [10] oferują najlepsze z możliwych rozwiązań. Blokują użytkownika w „klatce chroot” i umożliwiają dostęp wyłącznie do ograniczonej liczby poleceń. Jedną z zalet wyróżniających SCPonly w stosunku do RSSH jest kompatybilność SCPonly z popularnym klientem WinSCP. Ponadto, aby uruchomić rsync przez SSH, również możemy użyć SCPonly, a kolejne wersje mają obsługiwać także CVS przy pomocy protokołu SSH.

Obecnie żadna z głównych dystrybucji Linuksa nie zawiera pakietów SCPonly. Programiści Debiana posiadają taki pakiet, jednak jest to wersja testowa (niestabilna). Do momentu wydania pakietu użytkownicy nie mają innego wyboru, jak po-

branie plików źródłowych i samodzielna kompilacja programu. Pliki znajdują się pod adresem [10].

Autor SCPonly pracuje nad pakietem programu dla systemu FreeBSD, który posiada inną strukturę zarządzania hasłami i użytkownikami. Starsze wersje mogą wymagać pewnych modyfikacji skryptów instalacyjnych, szczególnie, jeśli będziemy korzystać z automatycznej konfiguracji klatki dla użytkowników (chroot). W obecnej wersji 3.11 takie czynności nie są już konieczne.

Kolejną pułapką może być polecenie groups, które w Linuksie często występuje jako skrypt powłoki. Skrypt instalacyjny setup_chroot.sh kopiuje między innymi do klatki dla użytkowników plik /usr/bin/groups. Kiedy wywołamy polecenie groups, jądro systemu będzie chciało przekazać skrypt do powłoki /bin/sh.

Aby uniknąć instalowania pełnej wersji interpretera poleceń w klatce dla użytkowników (chroot), administratorzy nie mają innego wyboru, jak zastąpić /usr/bin/groups poleceniem dostarczonym wraz z dystrybucją SCPonly. Niektóre programy SCP z interfejsem GUI mogą być prawdziwym powodem do zmartwień. Zalecamy skorzystać ze wskazówek umieszczonych w ramce „Programy SCP typu klient z interfejsem GUI”.

Instalacja

Po rozpakowaniu źródeł SCPonly uruchamiamy skrypt configure z wybranymi opcjami, np. chrobot z funkcjonalnością rsync lub chroot. Aby uzyskać pełną listę możliwości, wpisujemy polecenie ./confi-

Programy SCP typu klient z interfejsem GUI

Dla systemów Linux, Windows i Mac OS X istnieje wiele klientów SSH z interfejsem GUI. Niektóre z tych programów, np. gFTP [4] (patrz Rysunek 1), to przede wszystkim klienci FTP umożliwiające obsługę SCP i SFTP. Inne programy to typowi klienci SCP, jak np. WinSCP [5] dla platformy MS Windows. Podobnie sprawa wygląda z nakładkami. Wszystkie te aplikacje posiadają okno główne podzielone na dwie równe części (jeden panel dla komputera lokalnego, a drugi – dla komputera zdalnego), dzięki czemu użytkownicy mogą przeciągać i upuszczać pliki do kopiowania w obie strony.

W większości przypadków kliknięcie prawym przyciskiem myszy na pliku spowo-

duje ustawienie atrybutów tego pliku.

Menu kontekstowe często posiada dodatkowe funkcje np. dodawanie zakładek czy zarządzanie hasłami. Użytkownicy WinSCP powinni skorzystać z wersji 3, ponieważ usunięto w niej błędy poprzednich wersji. Dzięki temu unikniemy komunikatów błędów mówiących o brakującym poleceniu groups na serwerze po wyłączeniu w programie WinSCP opcji lookup user groups. Alternatywą dla WinSCP może być w MS Window klient Filezilla [6].

Dużo prościej sprawa wygląda dla użytkowników KDE, chcących korzystać z SCP. Aby skopiować pliki, wpisujemy po prostu na pasku adresu przeglądarki Konqueror fish://server. Dla systemu Mac

OS X istnieje program Fugu [7]. Fugu jest dostępny w postaci kodu źródłowego i obsługuje protokoły FTP, SFTP i SCP.



Rysunek 1: Sesja SCP z programem gFTP. Jako że SCPonly pracuje na komputerze zdalnym, użytkownik zostaje automatycznie „uwięziony” w chroot.

5

ZALET PRENUMERATY



UŻYWASZ LINUKSA? CZYTAJ LINUX MAGAZINE!

1

NISKA CENA

W prenumeracie rocznej – 3 numery ZA DARMO! W półrocznej – 1 numer ZA DARMO! Linux Magazine to najtańsze polskie czasopismo o Linuksie.

2

STAŁA CENA

Gwarancja stałej ceny Linux Magazine przez cały okres trwania prenumeraty.

3

GWARANCJA ZWROTU PIENIĘDZY

Jeśli będziesz chciał zrezygnować z prenumeraty, otrzymasz zwrot pieniędzy za numery, których jeszcze nie otrzymałeś.

4

BĄDŹ PIERWSZY

Do naszych prenumeratorów pismo Linux Magazine dociera, zanim ukaże się w sprzedaży detalicznej. Prenumeratory otrzymują Linux Magazine w specjalnej kopercie, chroniącej pismo przed uszkodzeniem.

5

PRENUMERATA NA PRÓBĘ

Wypróbuj prenumeratę Linux Magazine. TRZY KOLEJNE NUMERY za jedyne 30 zł.

Zamów przez Internet: www.linux-magazine.pl/Subs

WWW.LINUX-MAGAZINE.PL/SUBS

gure --help. Poniżej podaliśmy przykład, w którym uruchamiamy kompatybilność rsync, tworzymy binaria chroot i instalujemy program:

```
./configure --enable-rsync
--compat --enable-chrooted-binary
make
make install
```

Aby zainstalować klatkę dla użytkowników (chroot), administratorzy muszą przygotować wymagane biblioteki i umieścić je w odpowiednich miejscach w drzewie katalogów chroot. W dalszej części artykułu omówimy skrypt setup_chroot.sh, który zajmuje się tym zadaniem. Domyślnie nie ustawiono dla tego skryptu bitu wykonywania programów (execute). Można to łatwo zmienić – zamiast make install wpisujemy make jail i inicjujemy w ten sposób kolejne kroki wymagane do uruchomienia tego skryptu.

Uruchomienie skryptu instalacyjnego

wymaga uprawnień użytkownika root. Będziemy musieli posiadać te uprawnienia do uruchomienia polecenia configure, które generuje plik setup_chroot.sh z setup_chroot.sh.in. Ponadto potrzebujemy jeszcze kilku plików z udostępnionych ścieżek dostępu, np. /usr/sbin/. Podczas pierwszego uruchomienia setup_chroot.sh zostaniemy poproszeni o nazwę dla nowego użytkownika SCPonly oraz podanie nazwy katalogu domowego. Po zalogowaniu się przez SFTP użytkownik zostanie umieszczony w klatce dla użytkowników (chroot). Użytkownik otrzymuje prawa do zapisu w katalogu ~/incoming (lub innym katalogu przydzielonym przez administratora).

Zastosowanie

Aby uprościć użytkownikom zadanie, wystarczy jako katalog domowy użytkownika wpisać katalog /home/user/incoming. W ten sposób SCPonly przejdzie do katalogu ~/incoming zaraz po zalogowaniu się użytkownika. ■

INFO

- [1] FTPS RFC: <http://www.ietf.org/rfc/rfc2228.txt>
- [2] WebDAV RFC: <http://www.ietf.org/rfc/rfc2518.txt>
- [3] Putty: <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- [4] gFTP: <http://www.gftp.org>
- [5] WinSCP: <http://winscp.sourceforge.net/eng/>
- [6] Filezilla: <http://filezilla.sourceforge.net>
- [7] Fugu: <http://rsug.itd.umich.edu/software/fugu>
- [8] OpenSSH-Chroot-Patch: <http://chrootssh.sourceforge.net/index.php>
- [9] RSSH: <http://www.pizzashack.org/rssh/index.shtml>
- [10] SCPonly: <http://sublimation.org/scponly/>

PRENUMERATA Linux Magazine

Nie przegap TAKIEJ okazji



■ Zamawiając prenumeratę oszczędzasz!

■ Płacisz jak za 9 numerów, a otrzymujesz 12!

■ Z każdym numerem DVD lub płyta CD-ROM.

Najszybszy sposób zamówienia prenumeraty:

<http://www.linux-magazine.pl> Infolinia: 0801-800-105