

Zugriff zum Datenaustausch per sponly

Warum sponly?

In der Grundkonfiguration der Musterlösung ist es notwendig, dass ein Benutzer, der die Möglichkeit haben soll von außen Dateien mit dem Server auszutauschen, einen Zugriff auf Shellebene benötigt. Das bedeutet, der Benutzer kann sich am Server anmelden und unter Linux dort Befehle ausführen, was die Systemsicherheit beeinträchtigen kann.

Mit sponly kann man

- Dataaustausch von außen machen
- Der Benutzer hat keinen Shellzugang
- Wenn man möchte: Der Benutzer kann sein Heimatverzeichnis nicht verlassen

Aus dem letzten Punkt folgt auch ein kleiner Nachteil: Die Tauschverzeichnisse sind von Zuhause nicht erreichbar, und Linux Clients sind nicht mehr einsetzbar.

Etwas Theorie

Die hier vorgestellte Möglichkeit besteht aus zwei Komponenten:

1. Der Zugang wird nicht mehr mit einer Shell wie der in Linux übliche bash realisiert, sondern mit einer Shell namens sponly, die nur noch Befehle zur Verfügung stellt, die zum Dataaustausch per scp notwendig sind. Der Benutzer darf aber auch mit dieser Shell immer noch in alle von System erlaubten Verzeichnisse wechseln und kann somit alle für seine Benutzerkennung lesbaren Dateien auch nach Hause kopieren. Sollten irgendwelche Zugriffsrechte nicht korrekt gesetzt sein, kann auf diese Weise auf sensible Informationen zugegriffen werden.

Man kann an dieser Stelle aufhören und hat bereits ein erhebliches Sicherheitsplus gegenüber dem für gewöhnlich notwendigen Shellzugang gewonnen.

2. Wenn man nun das Programm sponly und alle von ihm benötigten Teile (Bibliotheken u.ä.) innerhalb jedes Homeverzeichnisses installiert, kann man den Zugang so konfigurieren, dass der Benutzer als Stammverzeichnis sein Heimatverzeichnis sieht – er kann also nicht in Verzeichnisse unterhalb seines Heimatverzeichnisses wechseln.
Nachteile: Speicherplatzbedarf (Kann man durch Hardlinks vermeiden) und kein Zugriff auf die Tauschverzeichnisse.

Installation

Um die Übungen durchzuführen, muss es auf dem System den im ersten Teil der Fortbildung angelegten Benutzer *remote* geben. sollte dieser nicht existieren, legen Sie ihn bitte an oder übertragen Sie die Anweisungen auf einen Testbenutzer ihrer Wahl.

Übung und Schritt 1: sponly auf dem Server installieren

Laden Sie die Datei `lml22-sponly-0.1.tgz` von <http://www.gtr-wiki.de/> herunter. Packen sie die Datei mit dem Befehl `tar xPzvf lml22-sponly-0.1.tgz` aus.

Damit der Benutzer nur noch Zugang per `sponly` hat, muss man ihm in der Datei `/etc/passwd` als Shell das Programm `/usr/local/bin/sponly` zuweisen. Vor allen Änderungen an der Passwort- Datei empfiehlt es sich diese zu sichern, z.B. mit der Anweisung

```
cp /etc/passwd /etc/passwd.sponly
```

Jede Zeile der Passwortdatei folgt demselben Schema:

```
remote:x:1000:100:::/home/remote:/bin/bash
```

Durch Doppelpunkte getrennt finden sich

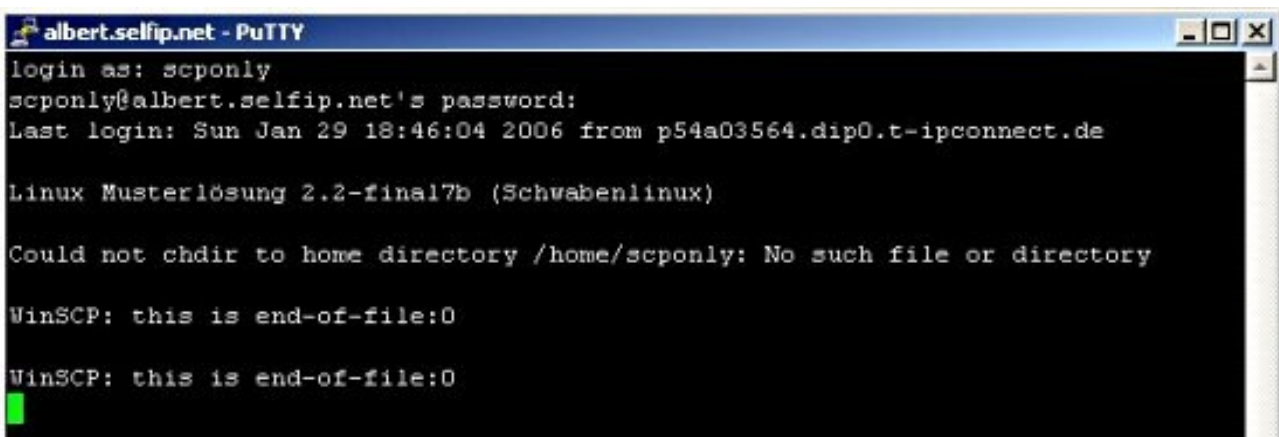
```
Benutzername:UserID:GruppenID:Bemerkungen:Heimatverzeichnis:Shell
```

Beachten Sie, dass die Bemerkungen in diesem Fall leer sind – es folgen zwei Doppelpunkte direkt aufeinander. Ändern Sie bitte den Eintrag für die Shell (am Zeilenende) beim Benutzer `remote` in `/usr/local/bin/sponly`

Nun muss die Shelländerung dem System noch mitgeteilt werden, dazu führen Sie bitte den Befehl

```
/etc/init.d/nscd restart
```

aus. Dies muss nach jeder Änderung an der Passwort Datei geschehen.



```
albert.selfip.net - PuTTY
login as: sponly
sponly@albert.selfip.net's password:
Last login: Sun Jan 29 18:46:04 2006 from p54a03564.dip0.t-ipconnect.de

Linux Musterlösung 2.2-final7b (Schwabenlinux)

Could not chdir to home directory /home/sponly: No such file or directory

WinSCP: this is end-of-file:0

WinSCP: this is end-of-file:0
```

Versuchen Sie dann sich von einem Client- PC aus per `putty` als Benutzer `remote` am Server anzumelden. Sie sollten ein Ergebnis wie das im Screenshot dargestellte erhalten, wenn Sie nach der Anmeldung mit Passwort die Return Taste drücken. Sie haben also keine Kommandozeile zur Verfügung.

Testen mit WinSCP

Laden Sie sich die Anwendung WinSCP von <http://winscp.net/eng/download.php> herunter. Wenn Sie das Paket „Standalone Application“ wählen, muss das Programm nicht installiert werden, liegt aber auf Englisch vor. Für zu Hause empfiehlt sich die Installierbare Version auf Deutsch.

Diese Beschreibung bezieht sich auf die nicht installierbare Standalone Version des Programms. Durch einen Doppelklick startet es, sie werden aufgefordert, die Daten zu Zielsever und Konto einzugeben.

Host name: Hier kommt der DNS-Name oder die IP-Adresse des Servers rein

Port number: 22 (ssh)

User name: Benutzername...

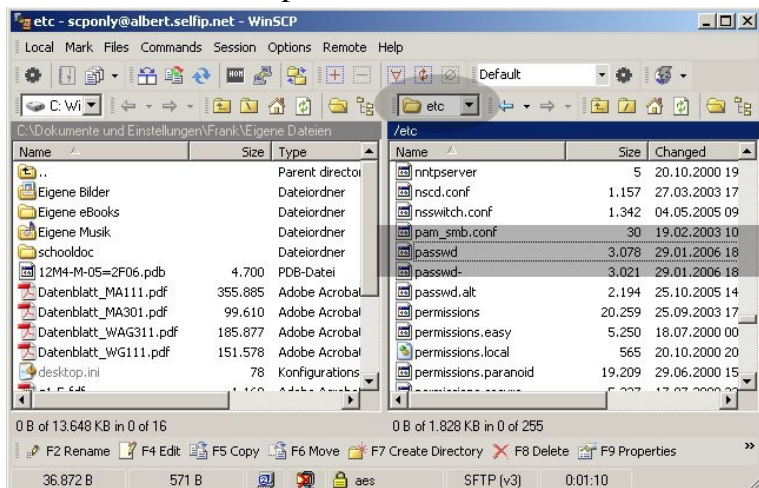
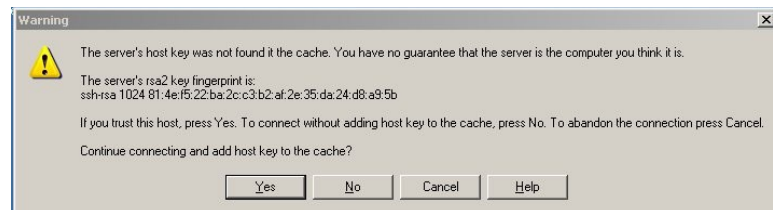
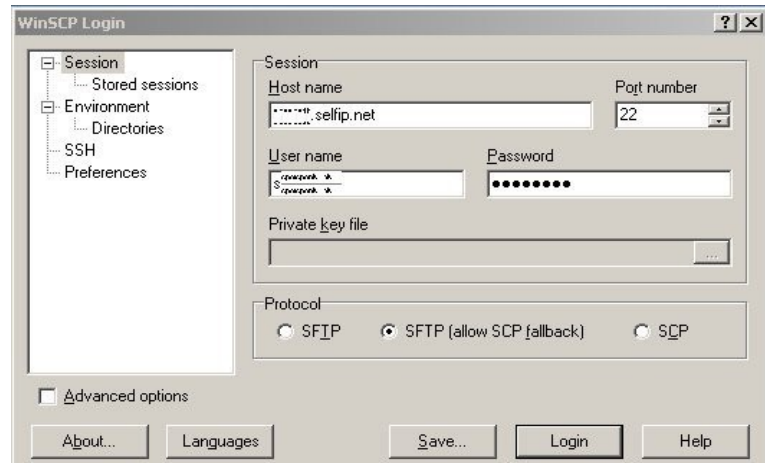
Password: Ebendas...

Beim Protocol können Sie die Voreinstellung SFTP(allow SCP fallback) belassen.

Wenn Sie alles richtig gemacht haben und das Passwort zum Benutzer passt, erscheint zunächst eine Sicherheitswarnung, die man abnickt, bevor sich der Hauptbildschirm öffnet.

Wichtig ist, zu erkennen, dass man immer noch in alle für den Unix-Benutzer *remote* erlaubten Verzeichnisse wechseln darf. Im Screenshot befindet sich der Testbenutzer im Verzeichnis `/etc/` und könnte sich problemlos die Passwortdatei herunterladen, da diese für jeden Benutzer lesbar ist.

Zwischenbilanz: Die Benutzer können sich zwar nicht mehr direkt am Server anmelden, dennoch Dateien austauschen, aber mit Hilfe von WinSCP noch immer in Bereiche vordringen, von denen man sie möglicherweise gerne fernhalten würde.



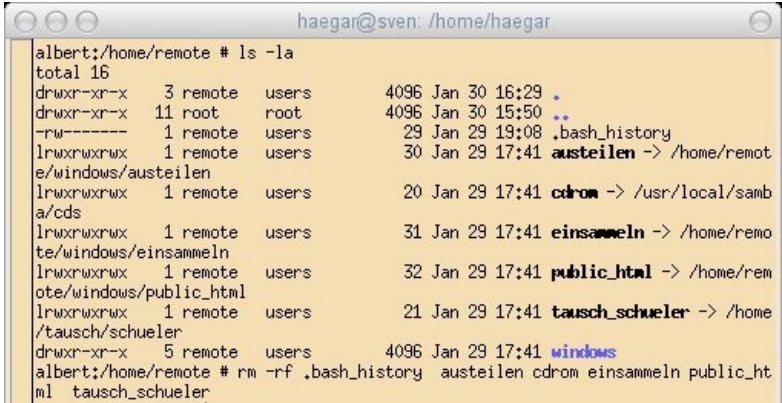
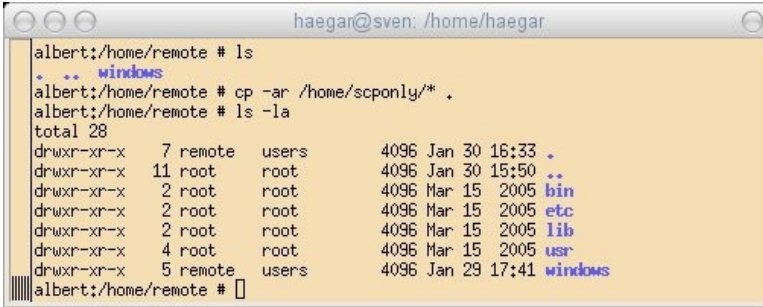

Übung und Schritt 2: Die Changeroot Umgebung

Laden Sie die Datei [lml22-sponly-changeroot-env-0.1.tgz](http://www.gtr-wiki.de/lml22-sponly-changeroot-env-0.1.tgz) von <http://www.gtr-wiki.de/> herunter. Diese Datei enthält alle für die Changeroot- Umgebung nötigen Bestandteile. Wenn sie die Datei mit `tar xPzvf lml22-sponly-changeroot-env-0.1.tgz` entpacken, wird die Changeroot- Umgebung nach `/home/sponly` entpackt, es sollte keinen Benutzer mit diesem Namen auf dem System geben!

Wechseln Sie nach dem Auspacken in das Verzeichnis `/home/sponly/` Sie finden die Unterverzeichnisse `etc/` `usr/` `bin/` und `lib/`

Von Hand einrichten

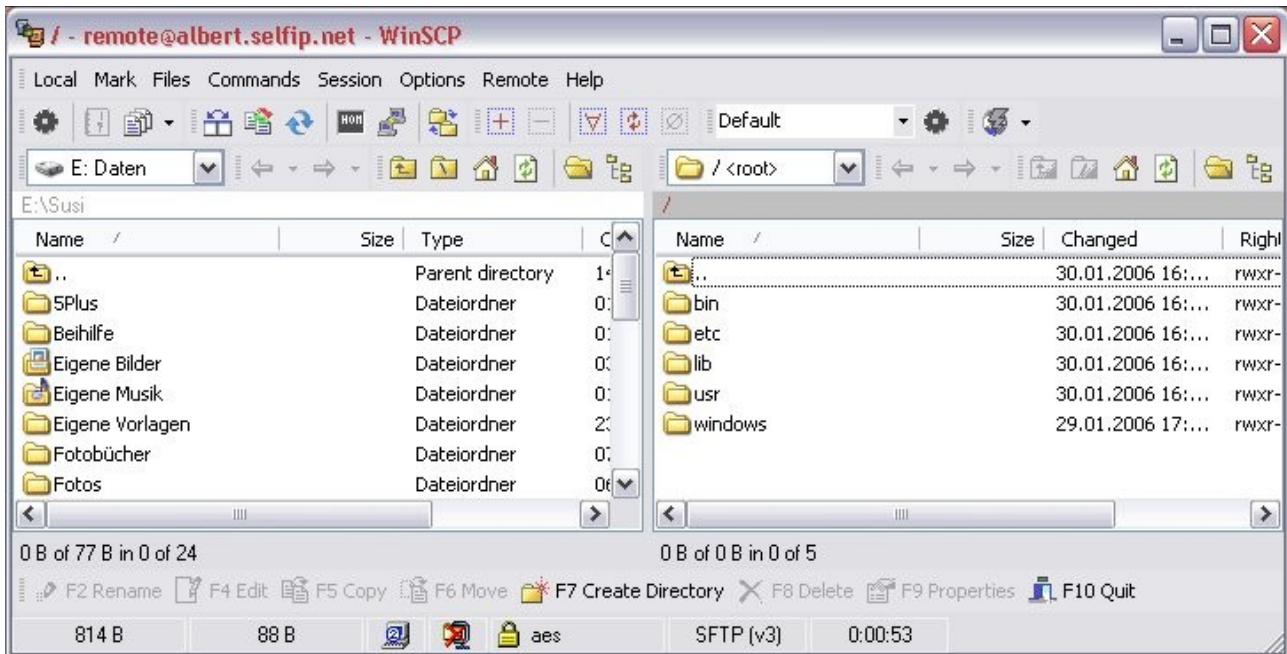
Um die Changeroot Umgebung für einen Benutzer „von Hand“ einzurichten, muss man folgendes tun (Übung: Machen Sie es am Inserver!)

1. Im Verzeichnis des Benutzers alle Dateien und Verzeichnisse mit Ausnahme des `windows`-Verzeichnisses löschen (Achtung: Kollision mit Linux Clients!)
 
2. Alle Unterverzeichnisse der Changeroot- Vorlage aus `/home/sponly` in das Home des Benutzers kopieren. Kontrollieren Sie anschließend, dass alle Unterverzeichnisse mit Ausnahme von `windows` root gehören, wenn nicht muss das mittels `chmod` angepasst werden.
 
3. Die zum Benutzer gehörige Zeile aus der Datei `/etc/passwd` muss in die Datei `/home/<benutzer>/etc/passwd` kopiert werden, sonst darf die Passwortdatei in der Changeroot Umgebung leer sein. Außerdem muss als Shell jetzt in beiden Passwort Dateien `/usr/local/sbin/scponlyc` stehen, das „c“ steht für die Changeroot Version.
 

Jetzt nochmals mit

`/etc/init.d/nscd restart`

die Änderungen wirksam werden lassen. Das wars, nun kann man dass funktionieren testen, indem man sich mit WinSCP am Server anmeldet, man sollte nicht mehr aus seinem Homeverzeichnis herauswechseln können. Man sieht auch am Bildschirmfoto, dass der Benutzer in seinem Heimatverzeichnis ist, dort die Dateien der Changeroot Umgebung und sein Windows Homeverzeichnis sieht, WinSCP aber als aktuelles Verzeichnis /<root> anzeigt. Man kann im Verzeichnisbaum nicht mehr nach oben wechseln.



Automatik

Das mitgelieferte Shellskript `/usr/local/sbin/addscpaces.sh` erledigt die Schritte oben automatisch für den Benutzer der als Argument übergeben wird:

```
addscpaceess.sh hallo
```

richtet einen Changeroot- SCP-Zugang für den Benutzer *hallo* ein. Außerdem kopiert das Skript die Dateien der Changeroot Umgebung nicht sondern legt harte Links an, was den Platzbedarf reduziert, da die Dateien so nur einmal vorgehalten werden müssen.

Bemerkung zum Skript: Ich habe mich um Sorgfalt bemüht, die passwd- Datei wird auch gesichert, aber Garantien für das Skript gebe ich keine.