FTP Setup Tips

Donnie Barnes, `djb@redhat.com` V1.0, March 27, 1996

1 Preface

"Red Hat Tips" are documentation meant to help Red Hat users with specific tasks. Some of these documents are for new users, some are for advanced users. Hopefully each document will also be of help for both new and advanced users. If you have contributions to make, please send them to tech-sup@redhat.com. If you have changes that need to be made to individual Tips, send them to the author of that document.

2 Introduction

The basic text of this document was donated by Mark Cornick (thanks Mark!). This Red Hat Tips file will help you set up a secure anonymous FTP server. You'll need to be root during this entire process.

3 Getting Started

Install the NetKit-B and anonftp RPMs. NetKit-B has the FTP server daemon; anonftp has the binaries, libraries, and things that will go in the FTP directory.

/home/ftp is the root directory for your FTP server. anonftp sets most of this up for you, but there's a few things that you'll need to do yourself.

You'll want to put copies of `/etc/passwd` and `/etc/group` in `/home/ftp/etc`, so that the `ls` command will print user names and group names when it lists files. However, you should remove the encrypted passwords from the passwd file and replace them with asterisks to improve security. To copy `/etc/passwd` to `/home/ftp/etc/passwd`, replacing the passwords with asterisks, do this:

```
sed -e 's/:[^:]*:/:*:/' /etc/passwd >~ftp/etc/passwd
```

There are no passwords in `/etc/group` under Red Hat Linux, so you can just copy /etc/group as is:

```
cp /etc/group ~ftp/etc/group
```

4 Secure it up

The anonftp RPM places some binaries and libraries in the `/home/ftp` directories to allow FTP users to do things like automatically gunzip files as they are being retrieved, or retrieve whole directories as tar files.

There are a few extra files placed by the anonftp RPM that probably will never be used, and should probably be removed in the interest of security.

```
cd /home/ftp/bin
rm cpio sh zcat
cd ../etc
rm ld.so.cache
cd ../lib
rm ld.so* libtermcap*
```

Finally, you should change the permissions on these files to improve security.

```
chmod 111 ~ftp/bin/* ~ftp/bin ~ftp/etc ~ftp/lib
chmod 444 ~ftp/etc/*
chmod 555 ~ftp ~ftp/lib/*
```

When you're done, you should have the following:

```
bin:
total 164
---x--x--x   1 root     root        14776 Oct 31 09:54 compress
---x--x--x   1 root     root        45277 Oct 29 21:59 gzip
---x--x--x   1 root     root        22977 Oct 29 20:07 ls
---x--x--x   1 root     root        77873 Oct 25 17:49 tar

etc:
total 2
-r--r--r--   1 root     root          495 Mar 20 19:46 group
-r--r--r--   1 root     root          921 Mar 20 19:45 passwd

lib:
total 702
-r-xr-xr-x   1 root     root        20994 Oct 30 18:58 ld-linux.so.1
-r-xr-xr-x   1 root     root        20994 Oct 30 18:58
ld-linux.so.1.7.5
lrwxrwxrwx   1 root     root           13 Mar 20 19:43 libc.so.5 ->
libc.so.5.0.9
-r-xr-xr-x   1 root     root       669157 Oct 30 19:53 libc.so.5.0.9
```

If you're missing any of these files, re-install the anonftp RPM and try again.

Now that everything's secure, you're ready to create a pub directory where you can place files for access via anonymous FTP.

```
mkdir ~ftp/pub
chmod 555 ~ftp/pub
```

Place any files you want to make available via FTP in the `pub` directory. You can make subdirectories in `pub` as well.

For security, and to make sure anonymous users can read the files, all files in `pub` should be set to mode 444, and all directories to mode 555. Do this with:

```
chmod 444 (name-of-file)
chmod 555 (name-of-directory)
```

Some sites have an "incoming" directory, where users can drop off files to be added to your archive. I do not recommend this unless it's absolutely necessary, since such directories are inevitably abused by pirated-software traders and the like. If you want an incoming directory anyway:

```
mkdir ~ftp/incoming
chmod 333 incoming
```

The mode 333 means that people will be able to change into the directory, and place files there, but not list any files in the directory. This will deter improper use somewhat, but don't put too much faith in it - again, the best way to make sure an incoming directory isn't abused is not to have one. If you do have an incoming directory, check it daily and clean out anything you don't want around.

You're all set! For security, make sure that nothing below `/home/ftp` is writeable by anyone:

```
chmod -R a-w ~ftp
```

(You'll still be able to write to the FTP directories as root.)

5 Further Reading

See also Garfinkel and Spafford, "Practical Unix Security" (O'Reilly, 1991), pages 245-246 for more information. (This book is about to come out in a second edition and the page numbers will likely change...)

6 Copyright Notice