Intruder Alert!

BY JOHN E. JOHNSTON

I recently interviewed a young man for a job opening in my department. During the interview, "Jerry" and I discussed hacking computer networks. Jerry admitted that he was very knowledgeable about hacker techniques and the ways to combat intruders. (I didn't ask how he acquired this "hacker" knowledge — some things are better left unsaid!)

> Jerry told me that he could hack into my network in less than four hours if left unattended at a network-attached workstation. Not only did he say he could hack in, but he said he could gain administrator access to our NetWare 4.x servers and create a backdoor administrator level account that my network administrators could not detect or delete.

Jerry told me that he could hack into my network in less than four hours if left unattended at a network-attached workstation. Not only did he say he could hack in, but he said he could gain administrator access to our NetWare 4.x servers and create a backdoor administrator level account that my network administrators could not detect or delete.

I was intrigued by this young man and decided to take him up on his challenge. We set up a date and time when I would allow Jerry to have full access to a Windows 95 Workstation configured exactly like the ones we deploy for our users. I didn't allow Jerry to be left unattended, however; I made sure I was by his side every minute that he was visiting my company.

When Jerry sat down at his Windows 95 workstation, he immediately opened a DOS box, switched to the F: drive (which was mapped to SYS:LOGIN) and typed DIR. He mumbled, "Good, I'm attached to a NetWare 4 server." Next, he entered the following command:

```
CX /T/A/R
```

I was amazed when I saw my entire NDS tree displayed on Jerry's screen. "You should really lock down your NDS a bit tighter," Jerry said as he began navigating through my NDS tree using the CX command. Jerry set his context to different areas in the NDS tree and entered the following commands:

```
NLIST USER /D
NLIST SERVER /D
NLIST GROUPS /D
NLIST /OT=* /DYN /D
```

From these commands, he learned a great deal about the structure of the NDS tree, including user names, group names and server names. Remember, Jerry wasn't even logged into the network and he already had a list of valid user accounts that he could use to begin his attack.

While scanning through the NDS structure using the CX command, Jerry found a couple of test accounts named TESTSUSER and TESTNURS. He tried logging in as TESTUSER with no password, and sure enough, he was logged in. One of the network administrators had set up this account to test an application and had never deleted it. Once Jerry was logged in, he went back to the CX and NLIST commands to see if he could obtain more information about the network.

Next, he began searching to see what volumes and files he could see with the TESTUSER account. Jerry found that he had full access to a directory named SYS:DCARE. He found a file in this directory named DCARE.NCF, which is used to start a database application on one of our NetWare 4.11 servers. Jerry added the following lines to the end of this file:

```
UNLOAD RSPX
UNLOAD REMOTE
LOAD REMOTE JERRY
LOAD RSPX
```

Then he told me it was time to reboot the server to see if his change to DCARE.NCF would allow him to access the RCONSOLE utility. He told me that he could crash the system for me using some "tools" he had picked up along the way, but he thought that I might want to bring it down gracefully instead.

I agreed, and went into the computer room to ask one of the operators to re-boot the server. I watched the operator re-boot the server. When she was finished, she said, "Oh, I almost forgot to start DCARE." She went to the server console and entered DCARE. I watched Jerry's commands execute and knew he had won.

I went back into the office and Jerry already had RCONSOLE up on his screen. "You do realize that I have full control of your console, right?" he asked me. I simply nodded. "Do you also realize that there are many NLMs available on the Internet that allow me to reset passwords from the console?" I nodded again. "I assume you have a favorite one that you just happen to have with you," I said, feeling a bit upset with myself and more than a little embarrassed.

I then called off the exercise. I realized that with full access to the system console, Jerry owned my NetWare network. I asked him what steps he would have taken next. He outlined the following steps:

1. Change the password of the Admin account.
2. Login as Admin.
3. From NWAdmin, add a new container inside an existing container.
4. Create a new user in this container with no home directory.
5. Grant the new user full Trustee Rights to its own user object.
6. Grant the new user full Trustee Rights to the new container.
7. Grant the new user account full access to the root of the NDS tree.
8. Modify the ACL of the new user so it cannot be seen.
9. Modify the Inherited Rights filter on the new container so the container is hidden.

Upon accomplishing these steps, Jerry would have a back door account that could not be seen and would be difficult for the network administrators to remove.

Jerry, acting a bit brazen, asked me, “So, we still have three-and-a-half hours left, do you want me to hack your Windows NT network?”

If you have any questions or comments on this material, or have suggestions for future topics, please feel free to email me at johnj@fast.net.

NaSPA member John E. Johnston is manager of technical support and communications for a major hospital in Pennsylvania. He designs and maintains cross-platform local and wide area networks utilizing NetWare, OS/2, DOS, and Windows.