HACKRSTS.TXT

Hacking RSTS Systems

So, you've decided that you'd like to try to down an RSTS system? Well, here's a beginner's guide: The RSTS system has two parts, the Priviledged accounts, and the User accounts. The Priviledged accounts start with a 1 (In the format [1,1], [1,10], etc. To show the Priv. accounts we'll just use the wildcard [1,*].) The priviledged accounts are what every RSTS user would love to have, because if you have a priviledged account you have COMPLETE control of the whole system. How can I get a [1,*] account? you may ask....Well, it takes A LOT of hard work. Guessing is the general rule. for instance, when you first log in there will be a # sign: # (You type a [1,*] account, like) 1,2 It will then say Password: (You then type anything up to 6 letters/numbers Upper Case only) ABCDEF If it says ?Invalid Password, try again' then you've not done it YET...Keep trying.

Ok, we'll assume you've succeeded. You are now in the priviledged account of an RSTS system. The first thing you should do is kick everyone else off the system (Well, maybe just the other Priviledged users)....You do this with the Utility Program. UT KILL (here you type the Job # of the user you'd like to get ut of your way). If the system won't let you, you'll have to look for the UTILTY program. Search for it by typing DIR [1,*]UTILTY.* Now, you've found it and kicked off all the important people (If you want you can leave the other people on, but it's important to remove all other [1,*] users, even the Detached ones). To find out who's who on the system type SYS/P-(That will print out all the privileged users). Or type SYS to see Everyone.

Next on your agenda is to get all the passwords (Of course). Do this by run $MONEY (If it isn't there, search for it with DIR[1,*]MONEY.* and run it using the account where you found it instead of the $.)

There will be a few questions, like Reset? and Disk? Here's the Important answers. Disk? SY (You want the system password) Reset? No (You want to leave everything as it is) Passwords? YES (You want the passwords Printed) There are others, but they aren't important, just hit a C/R. There is ONE more, it will say something like Output status to? KB: (This is important, you want to see it, not send it elsewhere.)

Ok, now you've got all the passwords in your hands. Your next step is to make sure the next time you come you can get in again. This is the hard part.

First, in order to make sure that no one will disturb you, you use the UTILTY pr/gram to make it so no one can login. Type UT SET NO LOGINS. (also you can type UT HELP if you need help on the program.)

Next thing you want to do is LIST the program and find out where The input of the Account # is. To get this far you have to knwo a lot about programming and what to look for...

Here is generally the idea, an idea is all it is, because I have not been able to field test it yet:

Add a conditional so that if you type in a code word and an account # it will respond with the password. This will take a while to look for, and a few minutes to change, but you can do it, you've got that RSTS system in your back pocket. Let's say you've (Somehow) been able to change the program. The next thing you want to do is replace it, so put it back where you got it (SAVE Prog-name), and the put it back to the Prot Level (The # in the <###> signs) by typing PIP (Prog name)<232>=Progname (Note, in all of this, don't use the ()'s they are just used by me to show you what goes where.)

Now you've gotten this far, what do you do? I say, experiment! Look at all the programs, since you have Privilged status you can analyze every program. Look around forthe LOG program, and find out what you can do to that.

The last thing to do before you leave is to set the date back to what it was using the UTILTY program again UT DATE (and the current date).