```
**************************
***  HACKING TECHNIQUES  ***
***  Typed By:  LOGAN-5  ***
***   (Hacker Supreme)   ***
***       From the       ***
***   Inner Circle Book  ***
**************************
```

1) CALLBACK UNITS:

Callback units are a good security device, But with most phone systems, it is quite possible for the hacker to use the following steps to get around a callback unit that uses the same phone line for both incomming and out going calls:First, he calls he callback unit and enters any authorized ID code (this is not hard to get,as you'll see in a moment). After he enters this ID, the hacker holds the phone line open - he does not hang up. When the callback unit picks up the phone to call the user back, the hacker is there, waiting to meet it.

The ID code as I said, is simple for a hacker to obtain, because these codes are not meant to be security precautions.The callback unit itself provides security by keeping incomming calls from reaching the computer. The ID codes are no more private than most telephone numbers. Some callback units refer to the codes as "location identification numbers," and some locations are used by several different people,so their IDs are fairly well known.I've been told that, in some cases,callback ubits also have certain simple codes that are always defined by default. Once the hacker has entered an ID code and the callback unit has picked up the phone to re-call him,the hacker may or may not decide to provide a dial tone to allow the unit to "think" it is calling the correct number. In any event, the hacker will then turn on his computer, connect with the system - and away he goes.If the however, the hacker has trouble holding the line with method,he has an option: the intercept.

The Intercept:
Holding the line will only work with callback units that use the same phone lines to call in and to call out.Some callback units use different incoming and outgoing lines, numbers 555-3820 through 555-3830 are dedicated to users' incoming calls, and lines 555-2020 through 555-2030 are dedicated to the computers outgoing calls.The only thing a hacker needs in order to get through to these systems is a computer and a little time - he doesn't even need an ID code. First,the hacker calls any one of the outgoing phone lines, which, of course, will not answer.Sooner or later, though, while the hacker has his computer waiting there, listening to the ring, an authorized

user will call one of the incomming lines and request to be called back. It will usually be less than an hours wait, but the hacker's computer is perfectly capable of waiting for days, if need be.

The callback unit will take the code of the authorized user, hang up, verify the code, and pick up the phone line to call back.If the unit tries to call out on the line the hacker has dialed, the hacker has his computer play a tone that sounds just like a dial tone.The computer will then dial the number given that matches up with the user's authorized ID. After that,the hacker can just connect his computer as he would in any other case.If he is really serious,he will even decode the touch tones that the mainframe dialed,figure out the phone number of the user the system was calling, call the person, and make a few strange noises that sound as though the computer called back but didnt work for some reason.

2) TRAPDOORS AS A POSSIBLILITY

I haven't heard of this happening, but i think it is possible that a callback modem could have a trapdoor built into it.Callback modems are run by software, which is written by programmers.An unscrupulous programmer could find it very easy to slip in an unpublicized routine, such as, "if code =*43*, then show all valid codes and phone numbers." And such a routine, of course, would leave security wide open to anyone who found the trapdoor.The obvious protection here, assuming the situation ever arises, is simply an ethical manufactorer that checks its software thoroughly before releasing it.

A trapdoor is a set of special instructions embedded in the large program that is the operating system of a computer.A permanent, hopefully secret "doorway", these special instructions enabe anyone who knows about them to bypass normal security procedures and to gain access to the computer's files.Although they may sound sinister, trapdoors were not invented by hackers, although existing ones are certainly used by hackers who find out about them.

3) THE DECOY

One of the more sophisticated hacking tools is known as the decoy, and it comes in three versions.The first version requires that the hacker have an account on the system in question. As in my case,the hacker has a low-security account,and he tries this method to get higher-security account.He will first use his low-security account to write a program that will emulate the log-on procedures of the systems in questions.
This program will do the following:

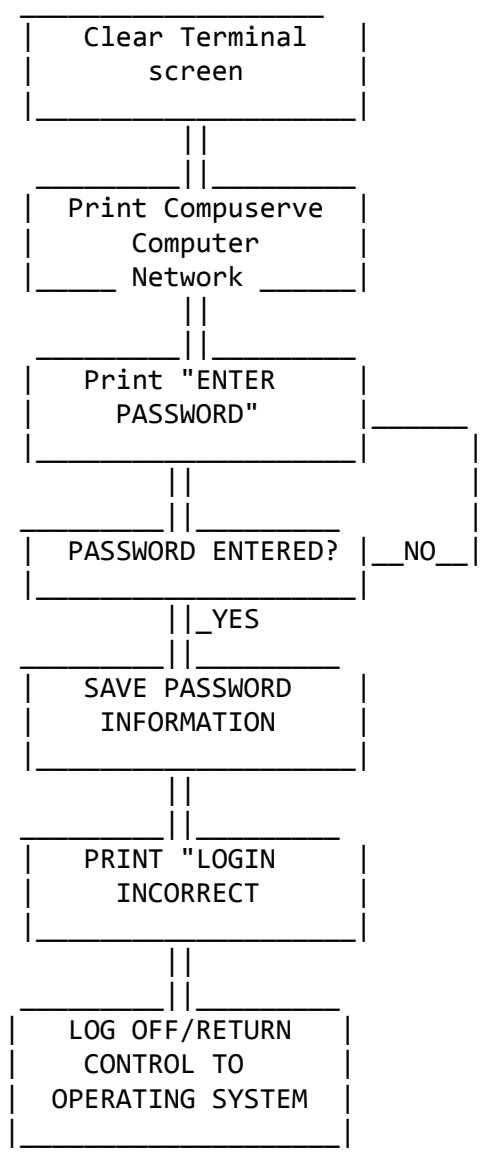
*- Clear the terminal screen and place text on it that makes everything look as if the system is in charge.

*- Prompt for, and allow the user to enter, both an account name and a password.
*- Save that information in a place the hacker can access.

*- Tell the use the account/password entries are not acceptable.

*- turn control of the terminal back over to the system.

The user will now assume that the account name or password was mistyped and will try again...this time (scince the real operating system is in control) with more success.You can see a diagram of the way these steps are accomplished



4) CALL FORWARDING

Many people use call forwarding by special arrangement with the phone company.When a customer requests call forwarding, the phone company uses its computer to forward all the customers incomeing calls to another number. Lets say, for example, that you want calls that come to your office phone to be forwarded to your home phone: A call from you to the phone company,some special settings in the phone companys computer, and all calls to your office will ring at your home instead.This little bit of help from the phone company is another tool used by hackers. Lets say you thought that the computer you were hacking into was being watched-because the sysop might have seen you and called the fed's and your sort of bugged by this nagging feeling that they will trace the next hacker that calls, just call the phone company and ask for call forwarding, pick a number, (ANY NUMBER) out of the phone book and have your calls forwarded to that number,Hea,Hea, the number you picked is the one that will be traced to, not yours, so you could be hacking away,they think that they have traced you, but actually the number you had your calls forwarded too. they enter chat mode and say (YOUR BUSTED!!!!, WE'VE TRACED YOUR PHONE NUMER THE FEDS ARE ON THE WAY!!), You could reply (Hea, SURE YA DID! I'D LIKE TO SEE YA TRY AND GET ME! GO AHEAD!) ,that wont seem very important to them at the time, but it will sure piss them off when they bust the wrong guy!

5) RAPID FIRE

Memory-location manipulation can be helpful, but there is another, more powerful,possibility, in some cases: the Rapid-fire method.To understand how this methos works, you have to know something about the way operationg systems work.When a user enters a command, the operating system first places the command in a holding area, a buffer, where it will sit for a few millionths of a second.The system looks at the command and say's "Does this person really have authorization to do this, or not?" Then, the command sits there a few thousandths of a second while the system runs off to check the user's authorization.When the system comes back to the command, it will have one of two possible answers: "OK, GO AHEAD," or "SORRY, GET PERMISSION FIRST."

Once you are on a system that handles things this way, you can use the rapid-fire method to change the command while its sitting in the buffer, waiting to be executed. If you can do this,you can do anything.You can enter a command that you know will be approved, such as "tell me the time." As soon as the system runs off to verify your right to know the time,you change the command in the buffer to something you know would not be approved-perhaps "give me a list of all the passwords." When the system comes back with an "OK, go ahead," it responds to your second command, not the first. Of course, this exchange has to be done very rapidly,but most systems existing today can be fooled by this trick. The question is,how easy is it to do, and how much authority do you need? I know of one system that let this one slip.

These are certainly not all the hacker's little secret tricks and tool's,
You will probably figure out some better, more efficiant,hacking techniques.

GOOD LUCK!!!!!!
L O G A N - 5
<-->