VTHACK2.TXT

VT Hacker #2

courtesy of
The Mad Hermit

Well, there's some old news, so let's get it out of the way. The Novice menu stuff has changed slightly. Options 8-12 are no longer active. in addition, poking around above there gives you a simple error message.

With that taken care of, we move on to:

-------- COMMUNICATIONS NETWORK SERVICES --------

There are ways to hack into this, but I'll do an overview of general info for those neophytes out there. CNS is running a ROLM phone system. Rolm created a telephone system a few years back, and IBM used it for voice messages & the like. It had bugs. It had security holes the size of Wisconsin. While it lasted, phreakers had a free message and conferencing system that IBM could do nothing about. IBM ended up buying out Rolm, and the company survived long enough to put out a beta version of the current Tech system at the University of New York.

Problems arose as the illustrious hackers there showed Rolm that gross abuses of the system were possible. They showed Rolm the hard way.
The Pick-Up function which isn't enabled on our system is capable of picking up someone else's phone, if you know their extension number. Devious people were answering other people's calls and transferring them to Topeka and other parts unknown. If they were really cruel, they Parked them there. As far as I know, just about all bugs left are harmless (well, mostly harmless). One thing to note: whenever you call CNS, the phone you are calling from is displayed immediately on a monitor in front of the operator.

The data line has a different story. Though a few bugs exist, they aren't exploitable. They merely irritate. Expect them to disappear soon, as the technical people at CNS are very helpful and know what to do in most circumstances. The "Call, Display, or Modify?" prompt is your ticket to fun and weirdness. Normal functions include tweaking your dataline's parameters and speed, displaying commonly used services, and calling these services by typing:

C VTLAN (or whatever name you want)

Recently, a hack was discovered at this prompt. All numbers that you called from here went like this: #XXXX, where # is the start number, and XXXX is the four-digit extension. Here is a list of current start numbers:

1 - On Campus (not hooked up yet. Will replace 961-XXXX)

2 - On Campus (normal dataphones)
3 - Long Distance
4 - Special
9 - Off Campus Local

The 4XXXX numbers are basically for CNS use, and for special mainframe connections. If you call VTCOSY, for example, you get a message stating that you are calling VTCOSY, and what modem number. These modem numbers can be dialed directly, leading to some interesting discoveries. Scanning these numbers without a program can be very time consuming, especially when you hit several numbers that all connect to the same mainframe. In addition, every "No Answer" takes one minute to do, because the Net waits that long before telling you it hasn't connected. Below, "Dead End" means that a connection was made, but no keypresses have any effect.

	40000-40049	Not A Dataline.
	40050-40052	Not Accessible
	40053-40055	Originate Only
	40056-40057	Group Closed
	40058-40059	No Answer
	40060-40061	Originate Only
¥	40062	Node Router (see below)
	40063	Dead End
	40064-40068	No Answer
	40069-40071	Not A Dataline
	40072	Not Accessible
	40073-40089	Not A Dataline
¥	40090-40093	VTLS
	40094	No Answer
	40095-40098	Connection Failed
	40099	No Answer
	40100	Not A Dataline
	40101	No Answer
	40102-40104	Dead End
	40105-40113	No Answer
¥	40114	CoSy Maintenance Port (00)
	40115-40120	No Answer
	40121-40132	Not A Dataline
	40133-40134	No Answer
	40135-40136	Even Parity lines (????)
	40137-40141	No Answer
	40142-40150	Not A Dataline
	40151	No Answer
	40152-40168	Not A Dataline
	40169	Dead End
	40170-40199	Not A Dataline

	40200-40220	Originate Only
	40221-40243	Not A Dataline
	40244-40263	Originate Only
	40264-40276	Not Accessible
¥	40277	64000 BAUD !!!
	40278-40281	Characteristics Mismatch
	40282	Not A Dataline
¥	40283	64000 BAUD !!!
	40284	Originate Only
	40285-40299	No Answer
¥	40300-40306	VTVMS
	40307	Not Functional
¥	40308-40323	CoSy (02-17)
	40324-40339	Busy
	40340-40363	Not A Dataline
	40364	No Answer
	40365-40399	Not Accessible
	40400-40403	Not Accessible
¥	40404-40433	VTVM1
	40434-40435	Not Functional
¥	40436-40457	VTVM2
	40458-40459	Not Functional
¥	40460-40499	VTLAN
¥	40500-40506	VTLAN
	40507	Dead End
¥	40508-40539	VTCC1
	40540-40551	Originate Only
¥	40552-40559	"Request:" (VTDSW)
	40560	Connection Failed
¥	40561-40567	"Request:" (VTDSW)
	40568-40569	Not A Dataline
	40570-40573	1200 BAUD lines
	40574	Not A Dataline
	40575	Busy
	40576-40578	Dead End
	40579	Busy
	40580	No Answer
	40581-40592	Originate Only
¥	40593-40599	VM/XA VT
¥	40600-40624	VM/XA VT
	40625-40699	Not A Dataline

40700-40799 Not A Dataline

40800-40899 Not A Dataline

40900-40999 Not A Dataline

Note that these numbers can also be dialed on the voice line. Who knows WHAT you'll find...

You might notice that there are only 1,000 numbers of 10,000 represented. If you find anything else above there, let me know. Finally, there are a couple of ways to mess up your trail if you're paranoid or just like feeling secure. Call VTLAN, and then CALL 9000. This brings you back to the Net, through a short loop. If you really want things messed up, call 9-232-2020. This calls off-campus, then calls the link for getting back on the Net. Enjoy!

The Node Router appears to be a CNS computer. The prompt is "Node[20] Enter Destination:" and there are 64 numbers you can type in. Some have passwords, some are dead ends, and others connect to other locations in the Net.

Here's a list:

Passworded nodes:	0,32,50
Dead Ends:	3,4,22,28,33
Calls the Net back:	34
"Request:" prompt:	15
VTLAN:	1
Net/One:	27

The Net/One prompt is the most interesting thing found yet. It's just about the only friendly interface ever located in CNS's part of the Net. You get to look at various nodes in the Net, and make connections between lines. Don't get your hopes up, though. My sources have only found one open link, but in order to figure out what it could do, they ended up closing it.

Here's a list of the commands you get on the 'help' screen:

The Net/One commands are:
    CONNECT Resource Name<CR>
    GET Resource Name<CR>
    LIST<CR>
    RESUME Connection Number<CR>
    ABANDON Connection Number<CR>
    EXAMINE Resource Name<CR>
    IDENTIFY Node ID<CR>
    SET DISCONNECT /New Disconnect Sequence/<CR>

```
    SET HOLD /New Hold Sequence/<CR>
    SET ECHO ON<CR> or OFF<CR>
    SET LINEFEEDS ON or OFF[ FOR ECHOES or INPUT or OUTPUT]<CR>
    SET BINARY ON<CR> or OFF<CR>
    SET FLOW NONE/CHARS/ENQ-ACK/SIGS/CTS-RTS/DSR-DTR/XON-XOFF[ NIU/DEVICE]<CR>
    LOGOUT<CR>
    QUIT<CR>
```

'Get' requests a particular line, 'Connect' opens it for use, and 'Resume' allows you to use it. The last command also seems to lock up the terminal...

When you 'List', you get something like this:

```
  You are using port 4 of Net/One NIU-180 number 57106A, on network number 1.
  Port 4's name is "57106A4".  NIU 57106A's name is "acc30".

  Connection 1 is unused.

  Your Hold Sequence is: --none--
  Your Disconnect Sequence is: <FS>OFF

  The Net/One command editing keys are:
      Cancel whole line: <DEL> or ^<BS>   Delete last character: <BS> or ^h
      Delete last word:  <CAN> or ^x      Complete current word: <SP>
      Repeat last line:  <SOH> or ^a

  ECHO mode is turned OFF.
  Automatic insertion of linefeeds after carriage returns is turned OFF.
```

Recently (as of 10/19/88), the number 40062 has gone out of service due to use by certain individuals (heh heh heh). There is another way of getting to it, which will be detailed in the forthcoming VT Hacker #3. The above data was gathered using a script file for Red Ryder. Don't try to comprehend what it does. It works. The Net kicks you off after five unsuccessful attempts at connection, making this simple incremental scanner procedure slow, and painful. A scanner for LocalNet is in the works, and will definitely be faster due to the unlimited tries LocalNet allows you. We're looking for 20+ tries per minute, but in the meantime, here's the CNS-CBX scanner:

```
COPYINTO ~8,ENTER NUMBER TO START AT
(GET1)
QUERY1 ~1
EMPTY ~1
IF YES JUMPTO (GET1)
LET EQUAL `1,~1
LET EQUAL `3,`1
COPYINTO ~8,ENTER LENGTH OF SEARCH
(GET2)
```

```
QUERY1 ~2
EMPTY ~2
IF YES JUMPTO (GET2)
LET EQUAL `2,~2
ADD `3,`2
COPYINTO ~3,`3
SUBTRACT `1,1
(NEXT)
ADD `1,1
TEST `1=~3
IF YES JUMPTO (QUIT)
TYPE C
TYPE `1
TYPE ^M
ALERT1 THIS DATALINE/JUMPTO (NNUM)
ALERT2 NOT A DATALINE/JUMPTO (NNUM)
ALERT3 BUSY/JUMPTO (BUSY)
PANICAFTER 10
PROMPT CONNECTED
PAUSE
BELL
BELL
JUMPTO (QUIT)
(BUSY)
BELL
(NNUM)
ONPANIC JUMPTO (QUIT)
PANICAFTER 10
ALERT1 DISCONNECTED/JUMPTO (HOLD)
TYPE ^M
PROMPT MODIFY?
PAUSE
JUMPTO (NEXT)
(HOLD)
PAUSE
PAUSE
PAUSE
ONPANIC JUMPTO (QUIT)
PANICAFTER 10
TYPE ^M
PROMPT MODIFY?
PAUSE
JUMPTO (NEXT)
(QUIT)
END
```