```
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$                                    $
$            Lex Luthor              $
$               and                  $
$    The Legion Of Doom/Hackers      $
$            Present:                $
$       Hacking Cosmos Part 2        $
$        Intermediate Course         $
$                                    $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$                                    $
$ In Part II we will explain how to  $
$ find out various information about $
$ a Telephone number.  Also, files,  $
$ paths and directories will be      $
$ explained.                         $
$                                    $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$  (C)    Written 23-Sept-84        $
$  L.O.D. Recursive Systems INC.    $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
```

NOTE: Everything shown in UPPER CASE is printed by COSMOS or typed by you.

I would like to correct a mistake I made in Part 1, I got a little carried away with the capabilties of COSMOS. You Cannot enter someones name and get thier phone #. What COSMOS is primarily used for is: To assign Central Office Equipment to cable pairs, and telephone numbers. It maintains records of all relevent facilities including subscriber cable and office equipment, process service and work orders, and it produces bulk assignments for office additions and rearrangements. In short, it automates the frame in your Central Office. It prints lists at the beggining of each day, telling what numbers to connect, and disconnect. Also, to keep track of everything going on in the frame.

HACKING ACCTS:
------- ------

Most COSMOS systems run on either a PDP 11/45 or 11/70 made by DEC, and can usually handle up to 96 terminals which are either hard-wired, or remotly dial into the system. If you don't know your local COSMOS dial-up or don't have an account you can probably bullshit 1 out of your Test Board, frame, or switch. They all should have the Dial-up, password and WireCenter in your area. Tell them you are Joe Comosolo from the COSMOS data center and youv'e noticed illegal access attempts. Ask them who is having the problem and ask them for an

account/password to do an on-line check to see what the problem is.

Typical COSMOS accts are: MF02, PA52, DP08, etc. Those 2 letter prefixes in the beggining of the acct stand for:

PA- LooP Assignment center.
DA- Network Admin center.
RS- Repair Service.
MF- Frame and Toll.
FC- Frame Control center.
GA- General Inquiries.
DC- Data Conversion.
NT- NTec.
DP- DisPatch.
CI- CIC.

The more important accounts which are used for service order entry are, in order of importance:

ROOT
SYS
BIN
PREOP
COSMOS

COSMOS is the account that the test board uses, and is now mainly found on the older versions of the COSNIX operating system. The typical COSMOS passwords are like: WETEST, MILK48, RINGIT. I have known people to guess a pass which was a color or an anmimal then they entered other account names and different colors and got other pw's, but it is very unlikely that you will guess a pw. Some accounts don't have passwords but you will rarely get that lucky.

Sometimes all you need is the dial-up to get in. Whoever was last on forgot to hit CTRL-Y to log off, and just hung up, so when you call, you get the WC% sitting there! I hate to have to rely on this method of entry, and prefer having an account/password. Well, you are now in, and can do some of the things explained in this file.

TRANSACTION CODES:
---------- ------

Once you log in you should get the prompt of WC% where WC is the Wire Center and % indicates that the system is on-line. From that prompt, you can type certain commands that will enable you to do different things. The ISH or INQ commands (Inquire about a Circuit) will print out various information about the number you do it to. From the prompt, type ISH or INQ <C/R>. You will then have to type an H which means HUNT then TN which is the Telephone Number 935-2481

and the system will print an underscore "-". You then type an "." and.....

```
WC% ISH
H TN 935-2481
-.

TN 935-2481
    ST  WK PD   DATE 07-16-78   TYPE B
  **ORD F24030161451    DD 01-20-84    FDD 01-20-84
OE  003-601-403
    ST  WK PD   DATE 07-16-78  CS  1FR US  1FR    FEA RNNL
  **ORD F24030161451    DD 01-20-84    FDD 01-20-84
    LOC WC1014    LOC W13-03L14/4-04
 CP   45-1262
    ST  WK PD   DATE 11-02-82
  **ORD F24030161451    DD 01-20-84    FDD 01-20-84
    LOC WC1010    LOC W10-06L01/3/12

HUNT SEQUENCE FOR TN 935-2481
   TN 935-2482  TN 935-2484

** ISH COMPLETED 09-24-84

WC%
```

Here is an explanation of what was just printed out about the number 935-2481:

LINE 1 --> TN 935-2481
Is the Telephone number that you inquired about.

LINE 2 --> ST WK PD   DATE 07-16-78   TYPE B
ST means STatus, WK PD is the WorK PerioD, the date following is when the TN 935-2481 was first installed, and TYPE sometimes abbreviated as TT is the Telephone number Type, where B is a POTs (Personal number) with Hunting. Hunting means that when the number 935-2481 is busy, the call will be forwarded automatically to the next number until it finds an idle line. The TT TYPE could be any one of the following:

B -- POTs hunting.
C -- Coin.
G -- Complex services, e.g., Direct
       Inward Dialing, Radio Common
       Carrier, etc.
O -- Official (company).
Q -- Centrex, WATS, large PBX's.
X -- POTs non-hunting.

LINE 3 --> **ORD F24030161451   DD 01-20-84   FDD 01-20-84

ORD stands for service or work ORDer which has a maximum of 20 Alphanumeric Characters. DD is the Due Date, and FDD is the Frame Due Date, which I assume is/was the last time the line was worked on.

LINE 4 --> OE 003-601-403
OE stands for Operating Exchange which, in this case is a #1ESS. Check HACKING COSMOS Part III for the formats of Operating Exchanges. By seeing what format the OE is, you can tell what type of CO the number is served by.

LINE 5 --> ST WK PD DATE 07-16-78 CS 1FR US 1FR FEA RNNL
ST, WK, PD were all explained in LINE 2, CS is the Customer Class of Service, 1FR stands for Flat Rate. US is the USOC (Uniform Service Order Code) which are identification codes used on Service Orders and Equipment records to identify items of service or equipment. Each code conisists of 3 or 5 characters, each one being either a letter or a number. FEA RNNL stands for Customer FEAtures. R = Rotary, N = Non-sleeve, N = Non-essential, and L = Loop started. The typical type of line is Loop started, A ground start is used on PBX's and such.

LINE 6 --> (repeat of LINE 3)

LINE 7 --> LOC WC1014 LOC 213-03L14/4-04
LOC is the LOCation.

LINE 8 --> CP 45-1262
CP is the CablePair 45-1262.

LINES 9-11 --> (Have been previously explained.)

LINE 12 --> HUNT SEQUENCE FOR TN 935-2481
            TN 935-2482 TN 935-2484

As explained earlier, when 935-2481 is busy, it will HUNT to 935-2482 if that is busy, it will goto 2483 and so on.

You can also inquire upon the Cable Pair, by:

```
WC% ISH
H CP 45-1262
-.
```

The information printed will be similar to what was printed about the TN.

PATHS, FILES AND DIRECTORIES:
------ ----- --- ------------

If you have a semi-priveledged acct., type LS /* to see what files you have access to. You will probably see something similar to:

/BIN:	/ETC:	/USR:
CP	COSNIX	BIN
DATE	INIT	COSMOS
ECHO	LINES	PREOP
LCASE	PASSWD	SO
MOTD	SYSGEN	SYS
STAT	UIDS	TMP

In actuality, these directories/files will be in "single file", I just put them in 3 columns to save space/paper.

To run a program/process just type the filename at the WC% promt. If you want to view a file in a directory, in this case we will use the /BIN directory, you would type:

```
WC% CD /BIN
```

You first Connect to the Directory then to print the file MOTD which stands for Message Of The Day, type:

```
WC% PR /MOTD

FRI APR. 10, 1984  11:37:16 MOTD  PAGE 1

ATTN: ALL USERS
MAKE SURE YOU LOG OUT PROPERLY
THANK YOU
```

Some files may have an "!" appended to the end of them on the older versions of COSNIX, those files should be text files and you should have no problem PRinting them. Other files may be encrypted, or you mistook a file for a program and all you get is garbage.

If you do not know what directory a file you are looking for is in use the FIND <file-name> command. As shown below, PERMIT is what we are looking for:

```
WC% FIND PERMIT
    /DEV/PERMIT
```

You can either connect to the /DEV directory then PRint the file or type:

```
WC% PR /DEV/PERMIT
```

The most looked up file would probably be the PASSWD file.

```
WC% CAT /ETC/PASSWD
```

```
ROOT:YXMDIMME:0::/:
SYS:YXORBMBX:1::/USR/SYS:
BIN:TMMZAKZF:3::/BIN:
PREOP::8::/USR/PREOP:
COSMOS:LEORVVB4:39::/USR/TMP:/BIN/PERMIT
PA02:ZSKD4ET:40::/USR/TMP:/BIN/PERMIT
```

99 times out of 100 the passwords will be encrypted. Notice that there are 2 colons after the PREOP account, that means that there is no password, so after entering PREOP at the ;LOGIN: it will jump to WC? then if it is a valid WC, you will get in. The way COSMOS checks to see if the pass is valid is: after you enter your account, and password, the system encrypts the pw you just typed,and compares it to the encrypted password in the PASSWD file. If it is correct, you will be in, if not, INVALID LOGIN.

In Part 3 I will have the PREFIX, FORMATS AND CODE VALUES Chart which gives all the needed definitions of the abbreviations that the system prints out when performing most transactions.

Lex Luthor
Legion of Doom!
Legion of Hackers

ACKLOWLEDGEMENTS:

SHARP RAZOR
THE WARLOCK

And last but not least, I would like to thank SOUTHERN BELL for letting me use thier COSMOS facilities to obtain the   information needed to write this phile