

HACK2.TXT

Hacking

HACK AND PHREAK

=====

FILE #2

BY: THE HYAENA

PLEASE BE CAREFUL WHO YOU GIVE THIS FILE TOO...

THE FOLLOWING IS AN EXTENDER LIST...

1-800-221-1950
1-800-221-5430
1-800-221-5665
1-800-221-5670
1-800-221-8190
1-800-223-7854
1-800-243-7650
1-800-255-2255
1-800-321-0327
1-800-321-0424
1-800-321-0845
1-800-323-4313
1-800-327-0005
1-800-327-0326 4444-9
1-800-327-2703
1-800-327-6713
1-800-327-9136
1-800-327-9895
1-800-328-1224 088759
1-800-331-4100
1-800-343-1319
1-800-343-1844
1-800-348-1800
1-800-356-0001 1-2-3...2-3-4
1-800-368-4222
1-800-368-5963
1-800-424-9826
1-800-521-8400
1-800-527-3511
1-800-543-7168
1-800-547-1784
1-800-547-6017
1-800-547-6754
1-800-553-8432
1-800-621-1506
1-800-621-1703
1-800-637-4663

HACK2.TXT

1-800-638-6402
1-800-641-4713 3WAY 8-1-AC
1-800-654-8494
1-800-682-4000
1-800-843-0698
1-800-858-9000

AND NOW A LITTLE TUTORIAL ON PHREAKING...
REMEBER THAT IT IS ILLEGAL IN CANADA AND THE UNITED STATES TO MAKE USE OF LONG
DISTANCE LINES WITHOUT PAYING FOR THE SERVICE. I AM NOT TELLING YOU HOW TO
BREAK INTO, NOR WILL I SUGGEST THAT YOU SHOULD TRY IT, BUT IF YOU ARE STUPID
ENOUGH TO BREAK THE LAW, THEN YOU DESERVE TO BE CAUGHT FOR YOUR IGNORANCE OF
THE LAW.

HOW TO PHREAK WESTERN UNION'S EASYLINK.
FIRST A LITTLE INFORMATION ABOUT EASYLINK. EASYLINK IS A SERVICE PROVIDED BY
WESTERN UNION FOR THOSE PEOPLE WHO WANT A TELEX, BUT DON'T WANT TO GET A
SEPERATE LINE OR MACHINE FOR IT SINCE THEY HAVE A COMPUTER. ANY COMPUTER WITH
A COMMUNICATIONS PACK CAN USE IT.
THE SYSTEM IS VERY HARD TO PHREAK, BUT I WILL INCLUDE A SAMPLE ACCOUNT FOR
YOUR TESTING USE.

FIRST GET YOUR COMPUTER READY TO COMMUNICATE. NOW DIAL 1-800-325-4112. IT
SHOULD RING ONCE OR TWICE. AFTER IT PICKS UP YOU WILL HEAR A HIGH PITCHED
SOUND. ESTABLISH CARRIER.
IT SHOULD RESPOND:

EASYLINK
ID?

AT THIS POINT YOU ARE TO ENTER YOUR CODE.
THE CODE IS IN THE FORMAT:

01 ESL##### PASSWORD.PASSWORD

01 - SAYS THAT YOU ARE USING FULL DUPLEX.
ESL - SAYS YOU ARE USING EASYLINK.
- A 6 DIGIT ACCOUNT CODE.
PASSWORD - A NEEDED PASSWORD.

ONCE YOU GET A CODE TO WORK, IT WILL RESPOND WITH A CONNECTION NUMBER, DATE
AND TIME. THEN YOU WILL GET:

PTS

THAT MEANS PROCEED TO SELECT. ENTER IN A TELEX NUMBER THAT YOU WANT IT TO GO
TO, FOLLOWED BY A "+". THE SYSTEM WILL RESPOND WITH A GA. <GO AHEAD.> NOW
ENTER THE TEXT OF THE MESSAGE. IT CAN BE UP TO 80 CHARACTERS LONG. WHEN YOU

HACK2.TXT

ARE DONE ENTER:

MMMM

IT WILL THEN GIVE YOU AN ACCEPTANCE NUMBER, EASYLINK, THEN THE CONNECTION NUMBER, DATE AND TIME AGAIN. THEN IT WILL HANG UP. YOUR MESSAGE HAS BEEN SENT.

WHAT'S THAT YOU SAY? YOU'VE TRIED EVERYTHING YOU CAN THINK OF, AND YOU CAN'T GET ON? WELL WHAT KIND OF A PERSON WOULD I BE IF I DIDN'T INCLUDE SOME SAMPLE INFORMATION?

ID : 01 USR999999 TEST.TEST
SAMPLE TELEX # : 62901234,624123
SAMPLE TWX # : 7101234567

NOW WHAT?! WANT TO SEND A MAILGRAM? WELL, THEN TRY THIS LITTLE PROCEDURE. AT THE PTS ENTER:

/ZIP
WHO TO
STREET ADDRESS 1
STREET ADDRESS 2
CITY,STATE ZIP +

AT THE GA, JUST TYPE IN THE MESSAGE AND TERMINATE IT WITH THE "MMMM".

WHAT? YOU WANT TO SEND AN OVERSEAS TELEGRAM NOW. GEE ARE YOU EVER CURIOUS. TO SEND AN OVERSEAS TELEGRAM, THE FORMAT IS:

/INT NAME
ADDRESS
CITY (COUNTRY)+

BEFORE YOU ASK MORE QUESTIONS, I MIGHT AS WELL GIVE YOU THE FOLLOWING HINTS.

- * USE CTRL-H TO BACKSPACE
- * USE CTRL-X TO DELETE ENTIRE LINE
- * TYPE EEEE TO DELETE ENTIRE TEXT AND ADDRESS; EEEE MUST BE TYPED AT THE LEFT HAND MARGIN FOLLOWED BY A C/R.
- * END-OF-MESSAGE INDICATOR <MMMM> MUST BE TYPED IN AT THE LEFT HAND MARGIN FOLLOWED BY A C/R.

WELL, I'VE TOLD YOU ENOUGH ON EASYLINK NOW, SO DO WHAT YOU WANT, AND MOST OF ALL DON'T GET CAUGHT.

AND NOW THE FOLLOWING WILL TELL YOU HOW TO CRASH SOME BBS'.

HACK2.TXT

THE FOLLOWING TUTORIAL WILL TELL YOU WAYS OF CRASHING GBBS II SYSTEMS AND ALSO GIVE THE SOLUTIONS ON HOW THE SYSOP CAN PROTECT HIS BOARD AGAINST THE CRASH.

<A> THE MOST COMMON AND MOST ELEMENTARY METHODS OF CRASHING A GBBS II SYSTEM IS BY WHAT IS KNOWN AS "THE OLD SPACE TRICK". WHAT IS DONE IS THAT A PERSON ENTERS AS A "NEW" USER AND USES THE SYSOP'S NAME WITH A SPACE BEFORE THE FIRST NAME. THIS BYPASSES ALL THE "NAME IN USE" CHECKS BUT AWARDS THE PERSON A SYSOP SECURITY OF 64 UPON ENTRY. THE SIMPLE REMEDY WOULD BE TO NOT ALLOW SPACES IN A NAME THAT AREN'T INBEDDED. FOR EXAMPLE:

```
510 0$=EL$+"LAST NAME-->":GOSUB 7000:GOSUB 8200:A2$=I$...ETC.
```

AND THE LINE:

```
515 IF LEFT$(I$,1)=" " THEN 510
```

THIS SHOULD ALSO BE ENTERED ON A LINE AFTER THE FIRST NAME IS INPUTTED.

 ANOTHER COMMON METHOD IS TAKING ADVANTAGE OF THE SYSOP'S MODS, ESPECIALLY THE ONERR GOTO STATEMENTS. WHAT A PERSON CAN DO IS TO PURPOSELY MAKE AN ERROR TO GET HIM TO WHERE THE ONERR GOTO STATEMENT IS POINTING. THIS MIGHT BE AN AREA THAT THE USER DOES NOT NORMALLY HAVE ACCESS TO. TO PREVENT THIS, NULLIFY ALL YOUR ONERR GOTO STATEMENTS AFTER YOU'RE DONE WITH THEM WITH A "POKE 216,0". WHEN THE ONERR FLAG IS RESET WITH THIS STATEMENT ALL ERRORS WILL RESULT IN A PROMPT LOGOFF.

COMMON MENTHODS OF CREATING ERRORS ARE:

- 1) WHEN THE PROGRAM ASKS FOR A NUMBER, ENTERING A "99E99".
- 2) WHEN ASKING FOR A PASSWORD, ENTERING A NEGATIVE NUMBER IMBEDDED IN THE LETTERS. (IE. G-99FFF, OR A-01AAA)
- 3) THEN THERE ARE THE FATAL ERRORS THAT WILL BE COVERED IN SECTION C.

<C> NOW HERE IS THE GOOD PART. THE GBBS II DRIVER IGNORES THE ENTRY OF ALL CHARACTERS WITH AN ASCII EQUIVALENT OF HEXADECIAMAL (\$20) AND BELOW, EXCEPT... A BIG EXCEPT...FOR A FEW. NOW THESE FEW CHARACTERS WHEN ENTERED, GOES UNNOTICED, THAT IS, UNLESS ENOUGH OF THEM ARE ENTERED. IF A SUFFICIENT NUMBER OF THEM IS ENTERED, (WHICH WOULD TAKE A LONG TIME WITH OUT A REPEAT KEY), THEN THE BUFFER SUFFERS WHAT CAN BE CALLED A "FATAL ERROR" WHICH WILL PROMPTLY PUT THE USER INTO MACHINE LANGUAGE WITH DOS INTACT. OH NO! BUT THERE IS GOOD NEWS. IF THE FOLLOWING POKES ARE ENTERED DIRECTLY AFTER THE GBBS II DRIVER IS LOADED, LET'S SAY ON LINE 60, THEN IT WILL TREAT THOSE CERTAIN CHARACTERS LIKE ALL THE REST OF THE TRASH AND IGNORE THEM.

```
60 POKE 36942,37:
   POKE 36943,208:
   POKE 36944,35:
   POKE 36945,76:
   POKE 36946,95:
   POKE 36947,255:
   POKE 36948,234
```

AND THAT'S IT. ALL OF THE ABOVE HAS BEEN CAREFULLY TESTED AND RETESTED SO THE INFORMATION IS VALID.

THE FOLLOWING IS A METHOD ON HOW TO CRASH GBBS 'PRO'.

FIRST, I SUGGEST THAT YOU LOG ON AS A NEW USER AND USE A GARBAGE NAME, SINCE YOU DON'T WANT THE CRASH TO BE TRACED BACK TO YOU. GOOD NOW THAT YOU HAVE ACCESS TO THE SYSTEM, GOTO EITHER THE MESSAGE BASE TO POST A MESSAGE, OR SEND

HACK2.TXT

FEEDBACK, OR IN E-MAIL. THEN JUST TYPE IN A FEW LINES OF GARBAGE. THEN TYPE IN THE WORD "DONE" AND EDIT ONE OF THE LINES. NOW THAT YOU ARE ABOUT TO EDIT ONE OF THE LINES, JUST PRESS CTRL-I AND HOLD IT DOWN AND YOU WILL BEGIN TO SEE THE CURSOR GOTO THE RIGHT OF THE SCREEN AND THEN BEGIN TO BEEP LIKE CRAZY WITHOUT AN END. SO NOW YOU HAVE SUCCESSFULLY CRASHED A GBBS "PRO" BBS, AND THE SYSOP HAS TO REBOOT HIS SYSTEM. IF WHEN YOU PRESS CTRL-I AND NOTHING HAPPENS, THEN THE SYSOP HAS ALREADY PROTECTED HIS BOARD AGAINST THE CTRL-I CRASH, SO GO PHONE UP ANOTHER GBBS 'PRO' BBS AND SEE IF YOU CAN CRASH THAT ONE.

NOW FOR THE SYSOP, IF YOU WANT TO PROTECT YOUR COPY OF GBBS 'PRO' FROM THE CTRL-I CRASH THEN DO THE FOLLOWING:

BLOAD ACOS.OBJ

CALL -151

528E

IF THE RESULT GIVES YOU 528E- 09 THEN TYPE 528E:FF

BSAVE ACOS.OBJ,A\$1800,L\$4900

OTHERWISE

TYPE 528B

THE RESULT SHOULD BE 528B- 09 THEN TYPE 528B:FF

BSAVE ACOS.OBJ,A\$1800,L\$4900

NOTE: MAKE ONLY ONE OF THESE MODS, BUT NOT BOTH. THE 528E AND 528B ARE ONLY USED TO CHECK WHICH VERSION OF ACOS YOU ARE USING.

NOW THIS IS A TUTORIAL ON HOW TO CRASH NET-WORKS.

NICK NAIMO (THE AUTHOR OF NET-WORKS) LEFT QUITE A FEW BUGS IN HIS PROGRAM, AND HERE ARE A FEW OF THEM.

TO MILDLY ANNOY THE SYSOP, TYPE "G" AT THE MAIN MENU PROMT. WHEN IT ASKS YOU FOR A NUMBER, ENTER A VALID NUMBER PLUS A DECIMAL. FOR INSTANCE, 3.5. THIS WILL CREATE A ONE SECTOR FILE CALLED "J.3.5.SYS" WHICH WILL NEVER BE ERASED UNLESS THE SYSOP HIMSELF CATALOGS THE DISK AND DELETES THEM ALL BY HAND.

TO DESTROY ALMOST ANY SYSTEM FILE, THERE MUST BE A BOARD SHARING DRIVE 1, WHERE MOST OF THE SYSTEM FILES ARE KEPT. POST A MESSAGE CALLED:

USERS.SYS

TITLES OR TITLES1 OR TITLES.1

MENU.SYS

WITH A SPACE IN FRONT OF IT. FOR INSTANCE, TO DESTROY THE PASSWORD FILE, POST A MESSAGE CALLED " USERS.SYS", THE SPACE IN THE FRONT IS LOST WHEN THE FILE IS RE-READ. NOW GOTO ANOTHER BOARD, AND THEN BACK TO THE BOARD YOU POSTED ON, THEN REMOVE THE MESSAGE THAT YOU JUST POSTED. THIS WILL DELETE "USERS.SYS" AND LEAVE " USERS.SYS" ALONE.

IF YOU WANT TO GET INTO MONITOR (THIS IS THE BEST CRASH THERE IS, I THINK).

IF THE BOARD YOU ARE CRASHING HAS NOT BEEN PROTECTED FROM IT, THEN IT WILL ALWAYS A) HANG TOTALLY OR B) GO INTO THE MONITOR. WHAT YOU WANT TO DO IS TYPE "E" AT THE MAIN MENU PROMT, AND THEN WHEN IT ASKS YOU FOR A NAME, ENTER GARBAGE, OR A REAL NAME, IT REALLY DOESN'T MATTER. WHEN IT SAYS "50 LINES MAX., TO END TYPE --> /EX <--" YOU DO THE FOLLOWING:

A) HIT <RETURN> ONCE.

B) TYPE /EX

HACK2.TXT

C) TYPE 'F' AT THE CHOICES.

D) ENTER "99E99" FOR THE LINE NUMBER TO FIX.

E) GOTO STEP A WHEN IT SAYS "50 LINES...ETC" AGAIN.

AFTER ABOUT 6-10 TIMES OF DOING THIS, YOU WILL HEAR A BEEP AS IT GOES INTO THE MONITOR. IF CTRL-C WORKS, THEN YOU'RE INTO BASIC. IF IT DOESN'T WORK, THEN YOU'LL JUST HAVE TO WAIT FOR THE SYSOP TO COME ALONG AND RE-RUN HIS BOARD. NOW IF YOU GET INTO BASIC, THEN CHECK TO SEE IF HE HAS HIS PROGRAM SAVED ON HIS DISK. IF HE DOES, THEN MAKE A FEW "BACKDOORS" SO YOU CAN GET INTO BASIC ANYTIME YOU WANT TO, AND THEN SAVE IT ONTO HIS DISK, AND THEN TYPE RUN. YOU'LL LOSE CARRIER, AND HE'LL NEVER KNOW WHAT HIT HIM, WHEN SUDDENLY HIS PASSWORD FILE GETS DELETED EVERY NIGHT.

ANOTHER USEFUL THING TO KNOW IS, IF YOU ENTER A SYSOP PASSWORD, YOU CAN GET VERY HIGH ACCESS. FOR INSTANCE, LET'S SAY YOU LOG ON AND SEE THE NORMAL LOG ON:

CONNECTED TO: SNIFFLES' BBS

ENTER ACCOUNT NUMBER OR THE WORD 'NEW'.

--->

AT THAT POINT, YOU SHOULD ENTER SOMETHING LIKE: E1EL (THAT IS A COMMON SYSOP PASSWORD). WHEN IT SAYS "INVALID PASSWORD", YOU SHOULD TYPE THE WORD "NEW". ENTER WHATEVER YOU WANT FOR THE NAME, AND WHEN IT ASKS YOU FOR A PHONE NUMBER, JUST HIT <RETURN>, IT WON'T ASSIGN YOU A PASSWORD, BUT WHO CARES. WHEN YOU GET INTO THE BBS, TYPE "Y". YOU SHOULD EITHER HAVE A LEVEL OF 9 OF SPECIAL DOWNLOAD ACCESS (ON T-I-M-E-C-O-R YOU GET SPECIAL DOWNLOAD ACCESS). THE ONLY PROBLEM IS THAT YOU ARE NOT VALIDATED. IF THE SYSOP IS STUPID ENOUGH, HE MAY VALIDATE YOU IF YOU CHAT SO YOU CAN JUST "LOOK AROUND". THE MAIN USE FOR THIS SMALL TIP, IS TO LOOK AT A HIGH LEVEL "G" SECTION THAT YOU DON'T NEED TO BE VALIDATED TO LOOK AT.

NOTE: ON BOARDS REQUIRING ACCOUNT NUMBERS, YOU SHOULD ENTER 1 AS THE ACCOUNT NUMBER.

END OF FILE #2...

[Time Left 00:40] 1. the_NeoPsychedelic_UnderGround_ Computer Philes:
Command ? I DRIVER IS
LOADED, LET'S SAY ON LINE 60, THEN IT WILL TREAT THOSE CERTAIN CHARAC
Downloaded From P-80 International Information Systems 304-744-2253