```
****************** BIOC AGENT 003
'S TUTORIAL IN ************************
*
                                      *
*                            ==========
==========                            *
*                            =HACKING T
HE HP2000=                            *
*                            ==========
==========                            *
*
                                      *
***************************************
****************************************
```

PREFACE

THE PURPOSE OF THIS TUTORIAL IS TO GIVE POTENTIAL HACKERS USEFUL INFORMATION ABOUT HEWLETT-PACKARD'S HP2000 SYSTEMS. THE FOLLOWING NOTATION WILL BE USED THROUGHOUT THIS TUTORIAL:

<CR> - CARRIAGE RETURN, RETURN, ENTER, ETC.
^C   - A CONTROL CHARACTER (CONTROL-C IN EXAMPLE)
CAPITAL LETTERS - COMPUTER OUTPUT & USER INPUT

SYSTEM INFORMATION

EACH HP2000 SYSTEM CAN SUPPORT UPTO 32 USERS IN A TIMESHARED BASIC (TSB) ENVIRONMENT. THE SYSTEM**MU11ERUN A VERSION OF HEWLETT PACKARD'S TIMESHARED/BASIC 2000 (VARIOUS LEVELS).

LOGON PROCEDURE

ONCE CONNECTED TO A HP2000, TYPE A NUMERAL FOLLOWED BY A <CR>. THE SYSTEM SHOULD THEN RESPOND WITH: PLEASE LOG I

N. IF IT DOES NOT IMMEDIATELY
RESPOND KEEP ON TRYING THIS PROCEDURE U
NTIL IT DOES (THEY TEND TO BE SLOW
TO RESPOND).

USER ID: THE USER ID CONSISTS OF A LET
TER FOLLOWED BY 3 DIGITS, EG, H241.

PASSWORD: THE PASSWORDS ARE FROM 1 TO
6 PRINTING AND/OR NON-PRINTING (CONTROL)
CHARACTERS. THE FOLLOWING C
HARACTERS WILL NOT BE FOUND IN ANY
PASSWORDS SO DON'T BOTHER TR
YING THEM: LINE DELETE (^X), NULL (^@),
RETURN (^M), LINEFEED (^J),
X-OFF (^S), RUBOUT, COMMA (^L), SPACE
(^@), BACK ARROW (<-), & UND
ERSCORE (_). HP ALSO SUGGESTS THAT ^E
IS NOT USE IN PASSWORDS (BUT
I HAVE SEEN IT DONE!).

THE LOGON FORMAT IS: HELLO-A123,PASSWD

WHERE: HELLO IS THE LOGI
N COMMAND. IT MAY BE ABBREVIATED TO
HEL. A123 IS THE
USER ID & PASSWD IS THE PASSWORD.

THE SYSTEM WILL RESPOND WITH EITHER ILL
EGAL FORMAT OR ILLEGAL ACCESS DEPENDING
UPON WHETHER YOU SCREWED UP THE SYNTAX
OR IT IS AN INVALID USER ID OR PASSWORD.
THE MESSAGES: PLEASE LOG IN, ILLEGAL F
ORMAT, & ILLEGAL ACCESS ALSO HELP YOU
IDENTIFY HP2000 SYSTEMS.

THE SYSTEM MAY ALSO RESPOND WITH ALL PO
RTS ARE BUSY NOW - PLEASE TRY AGAIN
LATER OR A SIMILAR MESSAGE. ONE OTHER
POSSIBILITY IS NO TIME LEFT WHICH MEANS
THAT THEY HAVE USED UP THEIR TIME LIMIT
WITHOUT PAYING.

UNLIKE OTHER SYSTEMS WHERE YOU HAVE A C
ERTAIN AMOUNT OF TRIES TO LOGIN, THE
HP2000 SYSTEM GIVES YOU A CERTAIN TIME
LIMIT TO LOGON BEFORE IT DUMPS YOU.
THE SYSTEM DEFAULT IS 120 SECONDS (2 MI

NUTES). THE SYSOP CAN CHANGE IT TO BE
ANYWHERE BETWEEN 1 AND 255 SECONDS, THO
UGH. IN MY EXPERIENCE, 120 SECONDS IS
SUFFICIENT TIME FOR TRYING BETWEEN 20-3
0 LOGON ATTEMPTS WHILE HAND-HACKING &
A MUCH HIGHER AMOUNT WHEN USING A HACKI
NG PROGRAM.

USERS

THE VARIOUS USERS ARE IDENTIFIED BY THE
IR USER ID (A123) & PASSWORD. USERS
ARE ALSO IDENTIFIED BY THEIR GROUP. EA
CH GROUP CONSISTS OF 100 USERS. FOR
EXAMPLE, A000 THROUGH A099 IS A GROUP,
AL"!I=U!A199 IS ANOTHER GROUP, &
Z900 THROUGH Z999 IS THE LAST POSSIBLE
GROUP. THE FIRST USER ID IN EACH GROUP
IS DESIGNATED AS THE GROUP MASTER & HEJHAS CERTAIN PRIVILEGES. FOR EXAMPLE,
A000, A100,...H200..., & Z900 ARE ALL G
ROUP MASTERS. THE USER ID A000 IS KNOWN
AS THE SYSTEM MASTER & HE HAS THE MOST
PRIVILEGES (BESIDES THE HARDWIRED SYSOP
TERMINAL). THE LIBRARY ASSOCIATED WITH
USER Z999 CAN BE USED TO STORE A HELLO
PROGRAM WHICH IS EXECUTED EACH TIME SOM
EONE LOGS ON.

SO, THE BEST THING TO HACK ON AN HP2000
SYSTEM IS THE SYSTEM MASTER (A000)
ACCOUNT. IT IS ALSO THE ONLY USER ID T
HAT MUST BE ON THE SYSTEM. HE LOGS ON BY
TYPING: HEL-A000,PASSWD. YOU JUST HAVE
TO HACK OUT HIS PASWORD. IF YOU DECIDE
TO HACK Z999, YOU CAN CREATE OR CHANGE
THE HELLO PROGRAM TO GIVE EVERY USER
YOUR OWN PERSONAL MESSAGE EVERY TIME HE
LOGS ON! THIS IS ABOUT ALL YOU CAN DO
WITH Z999 THOUGH SINCE IT IS OTHERWISE
A NON-PRIVILEGED ACCOUNT.

LIBRARY ORGANIZATION

EACH USER HAS ACCESS TO 3 LEVELS OF LIB
RARIES: HIS OWN PRIVATE LIBRARY, A
GROUP LIBRARY, AND THE SYSTEM LIBRARY.

TO SEE WHAT IS IN THESE LIBRARIES YOU WOULD TYPE: CATALOG, GROUP, & LIBRARY RESPECTIVELY (ALL COMMANDS CAN BE ABBREVIATED TO THE FIRST 3 LETTERS). THE INDIVIDUAL USER IS RESPONSIBLE FOR HIS OWN LIBRARY AND MAINTANING ALL THE FILES. IF A PROGRAM IS IN YOUR CATALOG, THEN YOU CAN CHANGE IT.

[GROUP MASTERS]

GROUP MASTERS (GM) ARE RESPONSIBLE FOR CONTROLING ALL PROGRAMS IN THE GROUP LIBRARIES. ONLY MEMBERS OF THE GROUP CAN USE THESE PROGRAMS. THESE ARE VIEWED BY TYPING GROUP. FOR EXAMPLE, USER S500 CONTROLS ALL PROGRAMS IN THE GROUP LIBRARY OF ALL USERS BEGINNING WITH ID S5XX. OTHER USERS IN THE GROUP CANNOT MODIFY THESE PROGRAMS. ALL PROGRAMS IN THE GROUP LIBRARY ARE ALSO IN THE GROUP MASTERS PRIVATE LIBRARY (CATALOG), THEREFORE HE CAN MODIFY THEM! THE GROUP MASTER ALSO HAS ACCESS TO 2 PRIVILEGED COMMANDS. THEY ARE: PROTECT & UNPROTECT. WITH PROTECT, THE GROUP MASTER CAN RENDER A PROGRAM SO IT CANNOT BE LISTED, SAVED, CSAVED, PUNCHED TO PAPER TAPE, OR XPUNCHED. FOR EXAMPLE, IF THE GM TYPED PRO-WUMPUS, OTHER USERS IN THE GROUP WOULD BE ABLE TO RUN WUMPUS BUT THEY WOULD NOT BE ABLE TO LIST IT. THE GM CAN REMOVE THESE RESTRICTIONS WITH THE UNPROTECT COMMAND.

[SYSTEM MASTER]

THERE IS EXACTLY ONE SYSTEM MASTER (SM) AND HIS USER ID IS A000. HE CAN PROTECT & UNPROTECT PROGRAMS IN THE SYSTEM LIBRARY. ALL USERS HAVE ACCESS TO THESE FILES BY TYPING LIBRARY TO VIEW THEM. ONLY THE SYSTEM MASTER CAN MODIFY THESE FILES SINCE HIS PRIVATE LIBRARY & GROUP LIBRARY CONSTITUTE THE SYSTEM LIBRARY. THE SM ALSO HAS ACCESS TO OTHER PRIVILEGED COMMANDS SUCH AS:

DIRECTORY: THIS COMMAND WILL PRINTOUT ALL FILES AND PROGRAMS STOED ON THE SYSTEM ACCORDING TO USERS. DIR WILL PRINT OUT THE ENTIRE DIRECTORY. DIR-S500 WILL START LISTING THE DIRECTORY WITH USER S500.

EXAMPLE:

```
DIR
   BOCES ED 1   053/84   1243

 ID    NAME    DATE    LENGTH   DISC
   DRUM
A000  ALPHA   043/84    00498  001384
      BCKGMN  053/84    04564  001526
      FPRINT  053/84    00567  002077
      STOCK   038/84    04332  002753
      TFILE   020/83 F  00028  002804
      WUMPUS  053/84  P 02636  003142
B451  BLJACK  316/75    03088  011887
      GOLF    316/75    02773  011911
S500  GIS     050/84 C  03120  019061
      GISCL4  050/84 F  03741  022299
Z999  HELLO   021/84    00058  011863
```

IN THIS EXAMPLE, THE SYSTEM NAME IS BOCES ED 1. THE DATE OF THE PRINTOUT IS THE 53RD DAY OF 1984 (053/84) AND THE TIME IS 12:43 (24-HR). THE FILES APPEARING UNDER A000 ARE THOSE IN THE SYSTEM LIBRARY. THE DATE ASSOCIATED WITH THE PROGRAM IS THE DATE IT WAS LAST REFERENCED. THE LENGTH IS HOW LONG IT IS IN WORDS. DISC REFERS TO ITS STORAGE BLOCK LOCATION ON ONE OF THE HARD DRIVES. DRUM REFERS TO ITS LOCATION ON THE DRUM STORAGE UNIT. ONLY SANCTIFIED PROGRAMS ARE STORED ON A DRUM TO INCREASE THEIR ACCESS TIME. THE LETTERS AFTER THE DATE REFER TO F IF IT IS A FILE, P MEANS IT IS PROTECTED, AND C MEANS THE PROGRAM IS COMPILED. IN THE EXAMPLE THE SYSTEM PROGRAM, WUMPUS, WAS LAST USED ON THE 53RD DAY OF 1984 (2-22-84); IT IS CURRENTLY UNLISTABLE (PROTECTED) AND IT OCCUPIES 2636 WORDS OF MEMORY STARTING AT DISC B

LOCK 3142. THE COMMAND SDIRECTORY WILL PRINT OUT PROGRAMS THAT ARE ONLY STORED ON DRUM. MOST SYSTEM DIRECTORIES ARE USUALLY LONGER THAN THE EXAMPLE. THE ABOVE EXAMPLE IS AN ABRIDGED VERSION OF A 43 PAGE DIRECTORY! THE <BREAK> KEY WILL STOP THE LISTING IF NECESSARY.

REPORT

THE REPORT COMMAND WILL SHOW THE USER ID, HOW MUCH TERMINAL TIME THEY HAVE USED SINCE THE LAST BILLING PERIOD (IN MINUTES), AND HOW MUCH DISC SPACE THEY ARE USING.

EXAMPLE:

```
REPORT
     BOCES ED 1 055/84    1905

 ID  TIME  SPACE     ID  TIME  SPACE
   I  TIME  SPACE
A000 01150 12625    B451 00003 05861
  B864 00000 00000
S500 00235 06861    S543 00421 00000
  Z999 00000 00058
```

THE ADVANTAGE OF HACKING THE A000 PASSWORD FIRST IS THAT YOU CAN USE THE PRIVILEGED COMMANDS TO SEE WHICH WHICH USER ID'S EXIST AND WHAT PROGRAMS ARE STORED WHERE SO THAT YOU CAN FURTHER PENETRATE THE SYSTEM.

PORT

THIS COMMAND TELLS THE CHARACTER SIZE AND BAUD RATE AT WHICH EACH OF THE 32 PORTS ARE CONFIGURED. IT IS IN THE FORMAT C-BBB, WHERE C=CHARACTER SIZE & BBB=BAUD RATE. IT IS SET UP IN COLUMNS OF 8. THE FIRST ROW CORRESPONDS TO PORTS 0-7, THE SECOND ROW CORRESPONDS TO 8-15, ETC. THIS IS GENERALLY USELESS IN MY OPINION. ALSO, THE PORTS ARE USU

ALLY ONLY CONFIGURED SEPARATELY IF THE TERMINALS ARE ALL HARD-WIRED.

STATUS

THIS COMMAND ALLOWS THE SM TO VIEW INFORMATION CONCERNING THE MASS-STORAGE DEVICES. IT GIVES CURRENT LOCATIONS OF THE ID TABLE, USER SWAP AREAS, LINE PRINTER STATUS, ETC. IT TENDS TO HOLD ALOT OF INFO IF IT IS READ CORRECTLY. UNFORTUNATELY, I DON'T HAVE THE ROOM TO FULLY DISCUSS IT HERE.

SINCE ALL LOGINS & LOGOUTS ARE PRINTED AT THE SYSTEM CONSOLE ALONG WITH OTHER PERTINENT INFORMATION, I WOULD STRONGLY SUGGEST THAT YOU AVOID EXTENSIVE USE OF AN A000 PASSWORD IF YOU FIND ONE.

THE SYSTEM OPERATOR HAS ACCESS TO ALOT OF OTHER COMMANDS. UNFORTUNATELY, HE IS SITUATED AT THE SYSTEM CONSOLE WHICH IS HARD-WIRED TO THE COMPUTER. IF ANYONE FIGURES OUT A WAY TO GIVE A REMOTE USER SYSOP PRIVILEGES, LET ME KNOW & I CAN HELP YOU WITH HIS COMMANDS.

NON-PRIVILEGED COMMANDS

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=

LIBRARY - LISTS THE SYSTEM PROGRAMS. THERE IS ONLY 1 SYSTEM LIBRARY & ANY USER CAN ACCESS IT.
EXAMPLE:

LIBRARYTO RETRIEVE A PROGRAM FROM THESYSTEM LIBRARY, YOU WOULD TYPE:

```
     GET-NAME   (TO LOAD THE STOCK PROGRAM, YOU WOULD TYPE GET-STOCK)
```

YOU CAN THEN RUN OR LIST IT. IF YOU ATTEMPTED TO LIST WUMPUS WHICH IS

```
PROTECTED (P), IT WOULD SAY RUN ONLY.
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

GROUP - LISTS ALL FILES IN YOUR GROUP.
 IT IS IN THE SAME FORMAT AS THE LIBRARY
      =5599

TO RETRIEVE A PROGRAM FROM YOUR GROUP L
IBRARY, YOU WOULD TYPE:

     GET-*NAME
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

CATALOG - LISTS ALL FILES IN YOUR PERSO
NAL LIBRARY.  IT IS ALSO IN THE SAME
          FORMAT AS THE LIBRARY COMMAND
.

TO RETRIVE A PROGRAM IN YOUR PERSONAL L
IBRARY, YOU WOULD TYPE:

     GET-NAME
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

OTHER COMMANDS YOU CAN USE WITH YOUR PE
RSONAL FILES (OR SYSTEM FILES IF LOGGED
ON AS A000) INCLUDE:

RUN             RUNS THE PROGRAM IN THE
 USER SWAP AREA (MEMORY)
LIST            LISTS THE PROGRAM IN TH
E USER SWAP AREA
SAVE-NAME       NAME MAY BE UPTO 6 CHAR
ACTQ**HHMY5NAME      SAVE IN COMPILED FORM
NAME-NAME       ASSIGN A NAME TO IT
KILL-NAME       DELETES A FILE FROM YOU
R LIBRARY
PUNCH           PUNCHES A PROGRAM ONTO
PAPER TAPE
TAPE            INPUT A PAPER TAPE
APPEND-NAME     ATTACHES THE FILE NAME
TO CURRENT PROGRAM IN MEMORY
LENGTH          TELLS THE CURRENT LENGT
H OF PROGRAM IN MEMORY
LPRINTER        DESIGNATES THE LINE PRI
```

```
NTER AS USER OUTPUT DEVICE
OPEN            CREATES A FILE [OPEN-FI
LE,# OF RECORDS, (RECORD LENGTHS)]
RENUMBER        RENUMBERS STATEMENTS
                [REN-(1ST STATEMENT #),
(INTERVAL BETWEEN STATEMENTS),(# TO
                 START RENUMBERING AT),
(# TO END RENUMBERING)]

NOTE:  ALL COMMANDS CAN BE ABBREVIATED
TO THE FIRST 3 DIGITS.  THE MAIN COMMAND
       IS SEPARATED FROM THE FIRST PARA
METER BY A DASH (-), THE FIRST PARAMETER
       IS SEPARATED BY THE SECOND PARAM
ETER BY A COMMA (,), AND ALL FURTHER
       PARAMETERS ARE SEPARATED BY COMM
AS.  EG, HEL-A000,^C(I DID ACTUALLY
       FIND A SYSTEM WHERE THE SM PASSW
ORD WAS ^C).

OTHER USEFUL COMMANDS
---------------------

BYE             LOGS USER OFF
ECHO-ON         HALF-DUPLEX
   -OFF         FULL-DUPLEX (DEFAULT)
SCRATCH1IMUSERS SWAP AREA
(NEW)
KEY             TRANSFERS CONTROL TO KE
YBOARD
TIME            INFORMS USER OF TOTAL C
ONNECT TIME & CONSOLE TIME
MESSAGE         SENDS A MESSAGE TO SYSO
P CONSOLE [MES-(TEXT UPTO 68 CHARS)]


TSB 2000
--------

THE PROGRAMMING OF THE SYSTEM IS ABOVE
THE SCOPE OF THIS TUTORIAL.  IF YOU DO
MANAGE TO GET INTO THE A000 OR Z999 ACC
OUNTS, THERE IS SUFFICIENT INFO
PROVIDED IN THIS TEXT TO HELP YOU MANIP
ULATE THE DATA.  THE BASIC IS RATHER
EXTENSIVE. THE FILE COMMANDS ARE EXCELL
ENT & YOU CAN MASK FILES SO THAT NOBODY
CAN READ THEM WITHOUT THE PROPER MASK (
```

I HAVE ALREADY CRACKED THIS CODE,
THOUGH!). BRIEFLY, IT IS SIMILAR TO MOS
T OTHER BASIC'S. IF YOU WANT, ORDER
THEIR PROGRAMMING MANUAL. IT IS CALLED
 20854A TIMESHARED BASIC/2000, LEVEL F
(PART # 02000-90073).

NOTE: THERE ARE DIFFERENT LEVELS (VERS
IONS) OF TSB/2000. THIS ARTICLE IS
       BASED PRIMARILY ON LEVEL F. MOS
T OF THE LEVELS ARE SIMILAR IN THEIR
       COMMANDS SO THE DIFFERENCES SHOU
LD NOT AFFECT THE HACKER. ALSO, SOME
       SYSTEMS ARE CUSTOMIZED. EG, ONE
 SYSTEM I KNOW DOESN'T HAVE THE MESSAGE
       COMMAND BECAU*_"!EDON'T WANT
THE OPERATOR BOTHERED WITH MESSAGES.
       ANOTHER SYSTEM SAYS ??? INSTEAD
OF PLEASE LOG IN AND ILLEGAL INSTEAD OF
       ILLEGAL ACCESS. THESE ARE ONLY
TRIVIAL PROBLEMS, THOUGH.
PROGRAMS

HEWLETT-PACKARD OFTEN SUPPLIES PROGRAMS
 FROM THEIR TSB LIBRARY FOR THE SYSTEMS.
UTILITIES SUCH AS ASCII*, FPRINT, & OTH
ERS ARE ALMOST INEVITABLY FOUND ON
EVERY SYSTEM. STANDARD GAMES SUCH AS W
UMPUS, STOCK, LUNAR, & MANY OTHERS ARE
ALSO A "SYSTEM OUST." OTHER COMPANIES
OFFER VERY LARGE PROGRAMS FOR THE
HP2000 ALSO. GIS (GUIDANCE INFORMATION
 SYSTEMS) IS A DATABASE TO HELP GUIDANCE
COUNSELORS HELP STUDENTS TO SELECT COLL
EGES, JOBS, FINANCIAL AID, ETC. GIS IS
USUALLY FOUND IN TH S5XX GROUP LIBRARY
(ANYONE WITH AN S5XX PASSWORD CAN USE
IT). UNFORTUNATELY, SOMETIMES THESE PR
OGRAMS ARE SET SO THAT A CERTAIN
PASSWORD WILL AUTOMATICALLY RUN THEM.
IN SOME CASES YOU CAN ABORT BY PRESSING
THE <BREAK> KEY. THERE IS A BASIC FUNC
TION [X=BRK(0)] THAT DISABLES THE
<BREAK> KEY. IN THIS CASE, ONLY THE SY
SOP OR THE PROGRAM CAN THROW YOU INTO
BASIC.

THERE ARE MANY ALLEGED BUGS ON THE HP20
00 THAT ALLOW USERS TO DO ALL SORTS OF
THINGS. IF YOU RUN ACROSS ANY OF THESE
 BE SURE TO LET ME KNOW.

I HAVE SEEN ONE SYSTEM THAT CONSISTED O
F 2 HP2000'S RUNNING TOGETHER. IN THIS
CASE, THE MULTIEAIWOULD FIRST ASK T
HE USER SYSTEM 1 OR SYSTEM 2? BEFORE
LOGGING IN. YOU WOULD THEN TYPE SYS1 O
R SYS2.

MOST OF THE HP2000 SYSTEMS ARE USED BY
SCHOOLS, SCHOOL DISTRICTS, BOCES,
AND VARIOUS BUSINESSES. THIS WAS AN ID
EAL SYSTEM FOR SCHOOLS BEFORE MICRO-
COMPUTERS EXISTED. THE HP2000 SYSTEM H
AS BEEN IN EXISTANCE SINCE AROUND 1973.
IT HAS BEEN REPLACED BY THE HP3000 BUT
THERE ARE STILL MANY HP2000 SYSTEMS IN
EXISTANCE & I BELIEVE THAT THEY WILL ST
AY THERE FOR AWHILE.

HERE ARE THE DIAL-UPS TO A FEW HP2000 S
YSTEMS TO GET YOU STARTED:

[314/645-1289]
[203/622-1933]
[312/398-8170]

IF YOU NEED HELP WITH ANYTHING ON AN HP
2000 OR FIND OTHER HP2000 SYSTEMS, FEEL
FREE TO ASK ME. ANY COMMENTS, CORRECTI
ONS, AND/OR THREATS ARE ALSO WELCOME.

YOURS TRULY,

*****BIOC
*==*AGENT
*****003

<<=-FARGO 4A-=>>

(P) APRIL 8, 1984 [THE YEAR OF BIG BRO
THER]

SHERWOOD FOREST][- (914) 359-1517
 RACS III - (914) 942-2638

PS SYSOPS OF OTHER BBS'S ARE WELCOME TO
 USE THIS MATERIAL ON THEIR BOARD
   PROVIDING THEY DO NOT ALTER ANYTHING
.

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Downloaded from P-80 Systems.....