```
*********************** bioc agent 003's tutorial in ***********************
*                                                                          *
*                          ====================                            *
*                          =hacking the 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 systems usually run a version of hewlett packard's timeshared/basic 2000 (various levels).

logon procedure

once connected to a hp2000, type a nume ral 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 characters 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 used in passwords (bu t 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, a100 through a199 is another group, & z900 through z999 is the last possible grous@"!2%IMQ*MIJJ9*!:I=UA5R`is designated as the group master & he has 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 password. 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). t he 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 c an use these programs. these are viewed
by typing group. for example, user s50 0 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 privi leged commands. they are: protect & unprotect. with protect, the group mas ter can render a program so it cannot be
listed, saved, csaved, punched to pa per 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 sys tem library. all users have access to these files by typing library to view t hem. only the system master can modify these
files since his private library & group library constitute the system library. the sm a6)o has access to oth er privileged commands such as:

```
directory:  this command will printout all files and programs stored on the
            sysBem according to users.
 dir will print out the entire directory.  dir-s500 will s
```

tart 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 boc es ed 1. the date of the printout is the 53rd day of 1984 (053/84) and the t ime is 12:43 (24-hr). the files appearing under a000 are those in the s ystem library. the date associated with the program is the date it was last ref erenced. the length is how long it is in words. disc refers to its storage b lock 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 pr ogram, 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 the0example. the a bove example is an abridged version of a 43 page directory! the <break> key wil l stop the listing if necessary.

report

the report command will show the user i d, how much terminal time they have

used
since the last billing period (in minut es), and how much disc space they are using.

example:

```
report
     boces ed 1 055/84    1905

 id  time  space     id  time  space     id  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 passw ord 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 pe netrate the system.

port

this command tells the character size a nd baud rate at which each of the 32 ports are configured. it is in the for mat 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 t o 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 info rmation 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
alonNY:%Q!zQ!I5R`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. t here is only 1 system library & any
user
can access it.
example:

```
library
 name    length    name    length    na me    length    name    length
alpha       498   bckgmn     4564   fpr int      567   stock      4332
tfile  f     28   wumpus p   2636
```

this uses the same notation as the priv ileged directory command.

to retrieve a program from the system l ibrary, you would type:

```
     get-$name   (to load the stock pro gram, you would type get-$stock)
```

you can then run or list it. if you at tempted 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
command.

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 acters
csave-name      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)
scratch         clears users swap area (new)
key             transfers control to ke yboard
time            informs user of total c onnect time & ,M[9ole 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 because they don'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

REwlett-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 must." 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 the 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 multiplexer would 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/xxx-xxxx]
[203/xxx-xxxx]
[312/xxx-xxxx]

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-=>>

(>rrecti ons, and/or threats are also welcome.

Downloaded from..

```
   The Lost City of Atlantis
  .     _ . __ |\  _  .
.   .__ =| |[] |# |# ._  .
  ...##.=|.|[].|#:|#.|=|...
- -- --- ------------ --- -  -
        703 - xxx - xxxx
```

Downloaded From P-80 International Information Systems 304-744-2253