PREFACE
#######

This instruction tutorial was written to help members of the hacking community by giving them useful information about HEWLETT-PACKARD's HP3000 series of mainframe computers.

The following abbreviations will be used throughout the entirety of this file:

```
<CR>              -   CARRIAGE RETURN, RETURN, ENTER, ETC.
^Y                -   CONROL CHARACTER (CONTROL-Y IN EXAMPLE)
CAPITAL LETTERS   -   COMPUTER OUTPUT AND USER INPUT
```

SYSTEM INFORMATION
############

Unlike its predecessor, the HP2000, the HP3000 runs on the MPE V operating system which can support up to 101 LDEVs (Logical Devices) in a time-sharing environment. MPE V allows the 3000 to access many more software/database packages than the 2000, as it is =not= a TSB (Time Shared Basic Environment). The systems usually run on various levels of MPE V, although I have heard that Hewlett-Packard is now beginning to upgrade the CPU and systems design of their machine in order for a better chance at competing with other large mainframe computers (The 3000 was put together in 1979!)

LOGON PROCEDURE
#########

HP3000s are distinguishable from other systems merely by their initial

logon message which you get after a couple of <CR>'s, ^F's, or ^E's:

:EXPECTED :HELLO, :JOB, :DATA (CIERR 1402)

MPE is easily recognized by its : prompt. Once you have received the : prompt, you are then allowed a chance at logging on. The logon process will contain the following pieces of data:

JOB ID : This is used to allow users to distinguish terminal sessions that are being run on the same group name. It consists of 1 letter followed by up to 7 characters (not ','). My favorite ones to use are MANAGER, OPERATOR, and some nasty ones when I get frustrated or bored. The first time hacker may not wish to use these as they draw unwanted attention if they are not used in the right ways.

USER NAME : The user name consists of up to 8 letters, (e.g.) GEBHARDT

GROUP NAME : The group name consists of up to 8 letters and is often times the same as the account name, but not always! (We'll discuss determination of all of these later..)

ACCOUNT NAME : The account name consists of 1 letter followed by up to 7 letters or digits (I may have seen more, but usually these account names are kept as short as possible...)

PASSWORD : The passwords are from 1 to 8 printing and/or non-printing (CONTROL) characters. As with the 2000, the following characters will never be found in any PW's so don't bother: LINE DELETE (^X), NULL (^@), RETURN (^M), LINEFEED (^J), X-OFF (^S), X-ON (^Q), UNDERSCORE (_)

LOGON FORMAT
######

:HELLO (JOB ID),(USER NAME)/(USER PW).(ACCOUNT NAME),(GROUP NAME)/(GROUP PW)

The passwords may not be typed in at the same time as the user/group/acct names, as the 3000 will prompt for them afterwards, but that is up to your discretion. A simpler example would be:

HELLO MANAGER.SYS,PUB (Remember, the JOB ID is not needed! Optional!)

The computer will then respond with...

ENTER USER PASSWORD:

..if the user/group/account all exist. Once past this one, you might
have to hack a group pw as well (usually not...)

LOGON NOTE: User and Group PW's are =NOT= necessary! If you get lucky,
             the sysop might not have implemented one onto the them!
             If this is the case, you will be automatically logged on!

A final comment on the logon sequence: The only USER NAMES/GROUP NAMES
that are =always= going to be found on the 3000 are:

MANAGER.SYS,PUB (or maybe just plain MANAGER.SYS)
FIELD.SUPPORT

If you hack these, then you have PRIVs and will be able to make your own
accounts and/or use others. So, you the hacker, will try:

:HELLO MANAGER.SYS,PUB (if it works, then good!)
:HELLO MANAGER.SYS
:HELLO FIELD.SUPPORT

The HP3000 system is usually set to allow you one try at hacking a certain
user-account, and you will have three tries at the PW before it cans you.
Hewlett-Packard has stepped up its security from the 2000!

USERS
#####

The various users are identified by their USER ID (GEBHARDT), their group
name (GEBHARDT), their ACCOUNT NAME (SBA), and their PASSWORD. USER ID's
have an allocated CPU time, connect time, and user privileges ranging from
SYSTEM MANAGER capability down to just being able to run BASIC or PASCAL.
GROUP ID's are allocated file space on the disks, and are able to support
many #'s of USER ID's on them (e.g.) 5 USERS with USER ID's of:

NELSON, GEBHARDT, SEKHON, DEGNAN, and JEBIAN are all attached to the same
GROUP NAME of CSCI. Each of them is able to have different CPU allocations
and logon time, but all of their files are stored in the same group (CSCI)
and they share the same file directory. Thus, say user JEBIAN wants to
logon. Let's say his ACCOUNT NAME is ADVANCED. His logon process would be:

:HELLO JEBIAN.ADVANCED,CSCI

..and then he would enter his PASSWORD(s)...

The 3000 has ACCOUNT MANAGERS for each of its accounts (there may be up to
24 different ACCOUNT NAMES, each supporting up to 150 or so GROUPS, which
in turn can support 12 USER NAMES...) Unlike the 2000, there may be more than

one MANAGER for every account, all with the same powers. ACCOUNT MANAGERS
do not have full system privs like the MANAGER.SYS does, but they may still
create their own USER and GROUP names, so if you hacked one of these, then
you essentially control an account and may make your own user accounts for
future use or trading. The 3000 may also have other system managers besides
the MANAGER.SYS, so once you have hacked his PW, you can create other
system manager accounts, and even make non-privileged accounts have privs!
(We will discuss this later...)

NON-PRIVILEGED COMMANDS
########

SHOWJOB - Lists =ALL= users and their respective acct/group info as well
as their session # and their message reception status. If the
word QUIET is printed, then that particular session will not
receive messages from you.

SHOWME - Lists everything you might want to know about your current job
session. (i.e.) job #, LDEV #, time on, your USER/GROUP/ACCOUNT
ID's, and more...

SHOWTIME - Lists the time and date.

REPORT - Lists allocated disk space for the group, as well as total disk
volume for the ACCOUNT ID. Also shows allocated CPU and total
used CPU seconds. System manager may do a REPORT @.(ACCT NAME)
which will tell info on the specified account.

LISTF @.(GROUP NAME).(ACCOUNT NAME)

This command (LIST FILES) allows the user the list the files in any group
directory in any account. Say you wanted to see the files in GEBHARDT.HS,
you would do this:

LISTF @.GEBHARDT.HS

If you wanted more information on the files in his account, then you would do:

LISTF @.GEBHARDT.HS,2 (this will take longer, but it tells file sizes etc.)

Account and system managers may do a LISTF @.(GROUP ID).(ACCT ID),-1
This will show any LOCKWORDS that might have been placed on some files
for added security. LOCKWORDS consist of 8 letters.

TELL (JOB ID),(USER ID).(ACCT ID);[Desired message up to 255 characters]

This command allows you to send a message to any logged in user, as long

as he is not specified as QUIET as discussed in the SHOWJOB command.
Many users dislike receiving these, so I do not recommend heavy use of this
unless someone else you know is logged onto another account.

SETMSG OFF/ON - Refuses/Accepts transmission of user sent messages.

SHOWCATALOG - Shows some system defined commands that will allow you to
further your prospective hacking directions. Some I have
encountered are: BASIC (Puts you into BASIC), ED (Goes into
file editor, TDP (Enters more advanced editor), DISPLAY
(Displays text files for user reading), just to mention a
few. There are unlimited possibilities here...

DSCOPY (FILE NAME).(GROUP ID).(ACCOUNT ID)

Copies specified file from named group and account to yours. Account
and system managers may copy files from one group to another by doing:

DSCOPY (FILE NAME).(GROUP ID).(ACCOUNT ID) TO (FILE NAME).(GROUP ID).(ACCT ID)

It is important to remember that account managers' powers are limited to
only their account and it's group members, and are not system wide as are
the system manager's!

Another thing that you should know: GROUP ID's may be exchange with an @
(at sign) symbol to allow for more expansive command usage. For example,
to send a message to =every= user on the system, do a...

TELL @.@;{Message}

I highly discourage this though as your account will probably be investigated
and/or purged immediately after use of such a message routine. Other uses:

LISTF @.@.@ (Lists all files on every group in the system)
LISTF @.@   (Lists all files on every group on your logged account)
LISTF @   (Lists all files on your group)

Don't forget the ,2 option added after this command, as it will give much
more file information. To get a list of every user on the system (this is
the only way I know of...) do a:

LISTF @.@.@,2 (This will list all files, and will also tell their group
and account that they are under....so if you go through all of them and
write them down as they pass by, you should get a very complete listing...)

TELLOP - This command sends a message to the operator's terminal
(I never use it...)

BYE - Logs current session off.

PRIVILEGED COMMANDS
########## ########

NEWGROUP (GROUP ID) [Creates a new group name for file allocation]
NEWUSER (USER ID);HOME=(GROUP ID);PASS=(8 CHARACTER PASSWORD)
PURGEUSER (USER ID)
PURGEGROUP (GROUP ID)
LISTF @.(GROUP ID).(ACCT ID),-1

These are just a few of the many nice privileged commands that you might want to use...

FILE COMMANDS
########

PURGE (FILE NAME).(GROUP NAME).(ACCT NAME)

This is the format for system management purging of other users' files. To purge ones own file, simply do PURGE (FILE NAME)

RENAME (OLD FILE NAME),(NEW FILE NAME)/(LOCKWORD-OPTIONAL)

This is how to rename files, and is also how to place lockwords on designated files for private security. Managers may:

RENAME (OLD FILE).(GROUP).(ACCT),(NEW FILE).(GROUP).(ACCT)/(LOCKWORD)

.if they want to change other users' file names and lockwords. If the original file had a LOCKWORD, then the 3000 will first prompt with:

LOCKWORD (OLD FILE)?

Which must be responded to correctly before the command will be executed. Manager Accounts bypass this security with the LISTF,-1 option and may find out others' LOCKWORDS.

SUBSYSTEMS
##########

All subsystems and systems programs are located in the public library of the 3000. To see a listing of files located in this directory, do:

LISTF @.PUB.SYS (Optional ,2)

Programs with the MACH designation in the ,2 directory are run-able from the MPE : Prompt and are machine language. Trial and error may have to be used with some forms of source code programs. The format for running a specified file is:

RUN (FILE NAME).(GROUP ID).(ACCT. ID)

For example, if the file BASIC was on the PUB.SYS directory, and you wanted to run it, you would type RUN BASIC.PUB.SYS, and the system would place you into the BASIC interpreter. Commands for the BASIC interpreter are:

SAVE (PROG NAME) [Optional ,RUNONLY,FAST added for protection of listing
and faster runtimes]
GET (PROG NAME)
RUN (PROG NAME)
CAT/CATALOG (Optional ALL added at end for entire group file catalog)
PURGE (FILE NAME)
LIST (PROG NAME)

The BASIC is =very= extensive with many of the commands found on the 2000, plus a very large number of special features. It is assumed that you know how to program in BASIC. Many neat little programs can be written to screw the system, and will be discussed in later volumes.

==========

There are a few bugs in the system that allow the stubborn hacker to bypass some group security, and defeat the purpose of passwords. If any of you out there come across any, please inform me on an aforementioned BBS.

There also exists on the 3000 the ability to link together two or more systems (I have seen two). The user is able to switch between each, provided he has account capabilities on both.

COMING IN NEXT VOLUMES:
#######

SYSTEMS CRASHING and NEAT THINGS TO DO TO THE 3000
BASIC PROGRAMS and MACHINE LANGUAGE COMPILING
USER DEFINED COMMANDS (UDC)
FILE I/O
MORE PRIVILEGED COMMANDS
SYSTEMS TAKEOVER

==========

Here's a dialup to an HP3000 system: [415] xxx-xxxx

Happy Hacking...

```
 _________/
/ DE BUG 00
\_\_\_\_\_>
/ \ / \ /
```


If you need help on an HP3000 or find any other systems, feel free to consult me. Any comments, corrections, and/or questions are welcome.

Note: This tutorial was typed in UPPER & lower case.

PS: Other BBS sysops are welcome to post this material on their boards
    provided that they don't change anything.