Complete At Ease Hacking
v 1.0
by Jibblit
jibblit@epix.net

Contents:

1. Overview of At Ease Hacking
2. Getting Into the Finder
3. Stealing the Prefs File
4. Using the Prefs File
5. Social Engineering Tricks
6. What To Do Once You Have Access
7. Other Ways to Get Passwords
8. Story: My First At Ease Hack

DISCLAIMER:

Don't do anything stated in this file. It is intended for admins who have forgotten their passwords or have legal access to the
system. I am not responsible fo anything idiotic you may do. Make sure you own the system or the admins know you are
doing this before you attempt anything!

****

1. Overview
****

We all should know what At Ease is and does. It is most commonly used in school computer labs to keep young hackers from doing damage. Well, we all know that by putting restrictions on it makes it much more fun to screw with.

At Ease loads at startup, and asks you to log in. Many times, there will be a "guest" or "student" login. After logining in as the
lowest level, you will be taken to a screen with a bunch of buttons. These buttons are set by the admin and restrict your usage
of the system to about nothin. It's rather secure also, getting into the Finder isn't as easy as it sounds. There are also other
levels that allow you to use the Finder. These are obviously password protected.

I wrote this file as hopefully a final collection of all of the At Ease
hacking files availble. This should be your definative guide. Send me anything I forgot and I'll probably update it. Hopefully,
this will be the last one (it needed to end somewhere). Thanks.

****

2. Getting Into the Finder
****

This section will describe how to get into the actual MacOS, the Finder. This is your ultimate goal, and is easily accomplished
many times. If you want future access to the system though, you'll need to do more. There are a variety of ways to get into the
Finder.

- Hold down the Apple or Command key and hit power (just like a restart without Control). A box will appear- this is the
debugger box, you can use this for all kinds of fun things. You want to type G FINDER in this area. If the system allows you,
you'll be floating in the Finder in no time. Sometimes, the debugger box won't appear at all (our lab is like this), and other time
doing this will just crash it. It's worth a try.

-Press Apple-Option-ESC to force a quit. If it works, you'll end up in the Finder. If it doesn't, you'll probably have to restart.

-Download At Peace (it should be easy to find). I've never actually used this, but I've heard it works.

-Download DisEase. I've used this before, and it usualy works. It gives you a menu that enables you to do a ton of crap. I
believe this only works on At Ease version 2.0 or earlier. Give it a try.

-Use Find File and you may be able to access some files on the Hard Disk, including the all important At Ease Prefs file.

-Boot up from a floppy of System CD disk. This takes longer and you'll probably get caught. There are easier ways than this.

-On earlier version, starting up without the extensions drops you into the Finder. This doesn't always work, especially on
newer versions. When I try to do it requires you type in an admin password.

-Try opening a bunch of programs. When it asks you if you want to quit At Ease to free up memory, click "Yes".

-This next section is taken from "Hack Addict 5" by the Weasel. I've never tried it, but I sounds like it works.

At startup the At Ease extension tells the computer to not start up
with the Finder and instead bring up the At Ease login sequence, or the body of At ease. From there you have several to no
choices, depending on the administrator. Each choice is an identity to login under, each identity is either assigned to the At
Ease OS (as I like to call it) or goes directly to the Finder. If the identity (weÕll call them
users... because the

access to EVERYTHING in it, including At Ease. IÕll talk more about what to do once in
the Finder later.

Now that we've become familiar with the system, let's examine it for weaknesses. A little toying around, reveals that
HyperCard allows you to launc
Finder is actually an application in disguise. it covers its self up by telling us it is a FNDR, not an APPL (application). Wrong,
the Finder may say itÕs unique but it's only unique in name. The System treats it just like any other Application. A rose by
any other name... So we fix this by changing the type to: APPL. Now we are just about ready to copy it to a floppy and try it
out. we've changed the type, but the creator is still MACS. That poses a problem, there isn't one Application I know of that has
a MACS creator. Th
enough, the macintosh will not know how to handle it and may end up crashing. This is bad. So lets fix the problem, what
creator can we use that generally is thought of as a generic application? what about HyperCard? You can make custom apps in
that. LetÕs see, open a custom app in HyperCard and the creator is WILD. How fitting,thatÕs exactly what we want. So, now
we open up (a duplicate of course) the Finder in ResEdit another program like it and choose get file info. The window lets us
change FNDR, MACS to APPL, WILD. Now we quit, save, and copy the finished product onto a disk.

Let's test it out, go to At Ease if you have it installed and launch a User that is in the At Ease OS. Once you are in insert the
disk you copied your hacked version of the Finder to and wait for it to appear on the screen (it should be it's own folder and
tab). If the program shows up in
Finder! Before you use it on any of your other computers though, check for the version number of its At Ease. If it is different
and it doesn't show up follow Plan B.

****

3. Stealing the Pref's File
****

Once you have access to the Finder, stealing the prefs file is a snap. It is in the System Folder under At Ease items. Just insert
a floppy and copy (most systems allow you to insert a floppy to save your work on). Take it home and work on it there. See
the next section to see what to do with it.

Stealing the prefs file is the most common way to get admin passwords. Make sure you have an admin account on your
system or it won't do any good. There is another way of stealing the prefs file. If you are on a network, go into Netscape and
make a new
message. Set it up to send a message to yourself. Now, when you go to attach files, you are only allowed to attach files on a
floppy, or no files at all. This can be bypassed by using the attach URL option. Every web page has a URL, as does every file
on the HD. All you need to do is find out the name of the Hard Drive. This should
be relatively easy- go into just about any program (a text editor works) and choose Save, get to the desktop, and look at the
name. Once you have it, attach this URL
to the message you are sending to yourself.

file://"HDNameHere"/System%20Folder/At%20Ease%20Items/At%20Ease %20Preferences

%20 are spaces, you must type them for Netscape to recognize they are spaces. Send the message to yourself. Then, recieve it
and save the file to disk. I've never actually tried this, but it may work.

Another way of nabbing the prefs file is writing an AppleScript. I know nothing about AppleScript, but I've heard that you can
script it so the Finder copies the file to disk.

****

4. Using the Prefs File
****

The first thing you want to do with the prefs file is take it home. If they catch you editing it there you'll get expelled (our
school's new policy). You'll also need a good HexEditor- I suggest BrainHex. You can download it from any Info-Mac
mirror, but I thought I'd include an address: ftp://wuarchive.wustl.edu//systems/mac/info-mac/disk/brain-hex-11.hqx

The encryption algorithm should be somewhere, I just can't find it now (sorry). Using the file is pretty much self explanatory.
Just copy it, create a new account, and compare.

If you really want access, just break into the finder and set a new account or set the access level high.

****

5. Social Engineering Tricks
****

Social Engineering works well also (you won't believe how stupid most admins are. Here's a few questions to ask (I used the
first one and it worked fine):

- Ask to get access to the Finder to change printers and print a file. Once they log you
in, steal the prefs.

- Tell them it won't read your disk and you need finder access to run Disk First Aid.

- Ask them for their password, something like "I'm logging into the Finder, what's your
password?" Act cool, and like you
don't care what it is.

-Think for yourself and find a way to get your admin to give you Finder access. Make up some stories, it shouldn't be that
hard.

****

6. What to do Once You Have Access
****

The first thing you should do once your in the Finder is steal the prefs file. You'll need this later. You can do a few other
things if you wish. Create a new user. Name it "Computer #25" or something inconspicuous (spelling?). Make sure it has
Finder access and set a password for it. What works even better is adding an alias of the
Finder to the At Ease buttons. I've never actually done this, but I heard you can click and be in. You may also want to install a
keystroke recorder. More on this in the next section.

Beside security features, you now can do whatever you want. Throw some things in the startup items folder, set a backgroud. I
love to install a dandy extension called "Minitors"- it shrinks the monitor one pixel every time you restart. You can pick up
this and some other fun extensions at www.machacks.com.

Even though getting into the Finder once is fun, your goal should be to maintain Finder

access for as long as you can, so you
can use it whenever you want. This means frequently nabbing the prefs file and taking it home to work on it, making an admin
account for yourself. Playing with the computers is much more fun if you can do it often. I cannot stress this point enough,
except DO NOT LOSE ACCESS, you'll have to start from scratch.

I suggest obtaining the At Ease manual (At Ease should be included w/ most Macs) and reading it cover to cover. It helps.

****

7. Other Ways to get Passwords
****

Shoulder surfing sometimes works. Watch when the admin types the password. If s/he does it slow, look closely. I did this in
Kinko's once. They logged me in under the name "Jib". I stayed under that account for a few minutes. Logged out, created a
new account with the password I got, did all of my work under that, and went to pay.
I only was charged for the 2 minutes under "Jib" and not the 30 under another account.

A better way to get the password is to install Invisiable Oasis on the system. Drop into the finder and install it. Make sure the admin logs in on that system, or get them to somehow. This utility records everything typed on the computer since installation. Leave it on the computer for a few days, come back and take the log it
saves. Delete the log and the utility, and take the log home. You'll have to read through letters to mom and reports, but eventually the password will show up.

****

8. Story
****

This is a description of my first At Ease hack. Read it, and feel free to use any ideas.

I asked our teacher for a pass to go to the lab during study hall. I did this because everyone in my class gathers around my
computer to see what kinda crap I'm up to today. No one was suspicious, including the teach. I went to work on what I said
was

a report- I slapped together a two sentence report on the KGB. I went to print it, and found that the printer only did B&W. I
asked her if any printers printed color. There was one, but the computers weren't set up to use it. I asked if I could use the
server

to print, and she flashed a dirt look my way. So, I waited a few minutes and asked her to log into the Finder so I could use the

chooser and change the printer. She did, and she carefully watched me as I changed printers in the chooser, and started to
print. She then went to look at the printer. I navigated through the HD and stole the prefs. I took it home and went to work.