Hack a Mac

With only 30 minutes of physical access.

by
Jeff Browning
Evan Savage
and
Alex Galvin

Published by hackmac

Disclaimer:
The information contained in this guide is for informational purposes only. Any instructions in this guide are intended to be performed on a machine that you have permission to use, as well as permission to execute the following commands and procedures upon. We take absolutely no responsibility for any damages of any kind resulting from the use of any knowledge in this guide. By reading further, you agree release HackMac.org from any and all liability, and assume all responsibility for your own actions.

Users of this guide are advised to use their own due diligence when it comes to making any sort of decisions and all information, products, and services that have been provided should be independently verified by your own qualified professionals. By reading this guide, you agree that HackMac.org and its authors are not responsible for the success or failure of your decisions relating to any information presented in this guide.

Table of Contents

Chapter 1: The Admin Hack

Approximate time: 24 minutes

Boot into Single-User Mode

Turn on the computer. When you hear the startup chime hold down the keys CMD+S. This key combination boots the computer into Single-User Mode (SUM), giving you temporary root access. It is important to note that this can be blocked by a firmware password. If that's the case, take a look at our guide on how to get into single-user mode while locked.

Mount the Hard Drive

Once you've booted into SUM (it should look like a black screen with white text) we need to mount the hard drive to be able to modify files. To do so, type in the following after the prompt:

```
/sbin/mount -uw /
```

Remove the "Setup has been completed" File

Now that the drive is mounted and we can edit the file system, we need to delete a file that tells your computer that you have completed setup. Mac OS X checks for this file every time it boots up, and by deleting it, we will effectively trick the computer into believing it's brand new and you need to set up an administrator account. To delete the file, type in:

```
rm /var/db/.applesetupdone
```

This deletes the afore mentioned file (aptly named ".applesetupdone"), which is stored in the /var/db/ directory.

Reboot

This step is pretty self explanatory. We need the system to exit SUM and reboot so that it can check for the file we just deleted and not find it. Type in the following and press return:

```
reboot
```

Watch the Video

Your computer will reboot. A setup window should pop up asking what language you would like to set up your computer in, just as if you were turning on your computer for the first time. After you select a language, a welcome video plays. We'd recommend some headphones for this bit (you can't access the volume controls yet), unless there's nobody around or you're performing this procedure on your own computer, in which case you can enjoy a little music.

Continue Setup

Continue through the rest of the setup process. See the next step for setting up the administrator account.

Heads Up: Be sure to select "DO NOT TRANSFER MY DATA."

Don't worry, all of your old files will still be on the computer, you just don't have any files from an older computer to be transferred.

Set up the Administrator Account

Near the end of the setup you will be asked to create an administrator account for your computer.

Heads Up: Be sure to make the name of the admin account different from any existing accounts.

You can name the account anything that you want, **except for the name of the old administrator account**. If the new account is given the same name as the old one it will overwrite the old account, causing all the account's files to be deleted. **That is not optimal.**

Finish Setup and Log In

Complete the setup and the computer should automatically log you into your new administrator account.

Some important notes:

1. This administrator account is exactly like any other account.
2. It is not hidden in any way, and it does not have any special privileges.
3. With this account you will be able to change the password on the old administrator account, and access the files of any account stored locally on the computer.

Chapter 2: Enable The Root User

Approximate time: 2 minutes

Option 1: Enable Root Via GUI

Enabling the Root User through the GUI is different depending on your version of Mac OS X.

*If you're using **Tiger**, follow these steps:*

1. Open **NetInfo Manager**, located in **Applications > Utilities**.

2. Choose **Security > Enable Root User** and type a password for the root account. You may need to type the password you set for the new administrator to make these changes.

*If you're using **Leopard**, follow these steps:*

1. Open **Directory Utility**, located in **Application > Utilities**.
   - You may need to unlock the application to use it. Unlock the application by clicking the padlock icon and entering the password you set for the new administrator.

2. Choose **Edit > Enable Root User**, and then type in a password for your root user.

*If you're using **Snow Leopard,** follow these steps:*

In **Snow Leopard**, the instructions are the same as Leopard except that Directory Utility has moved to **System > Library > CoreServices**.

If the root account is already enabled, don't worry; you can change the password by using **Option 2** in Terminal, which is on the next page.

Option 2: Enable / Change Root Password Via Terminal

Fire up **Terminal** (located in **Applications > Utilities**), and enter in the following command:

```
sudo passwd root
```

When prompted, you'll be asked to enter your administrator password. Do so. It may not look like you're typing when you're doing it, but trust me, you are. Hit enter after you type your password.

The system will then ask you to enter in a root password twice. Pick a new password, type in it and press enter. Enter the same password for confirmation.

Chapter 3: Removing Traces

Approximate time: 3 minutes

Log Out and Login as Root

To log out of the administrator account, click on the Apple logo in the top left-hand corner, and then click **Log Out**. If the Login window features Username and Password fields, enter "**root**" as the username and then your selected root password from **Chapter 2**. If the Login window has a list of users, choose "Other" in the Login window, type root in the Name field, and the root password in the Password field.

Delete The Administrator Account

The root account is a "hidden" account, and won't show up in the list of users under the Accounts pane in System Preferences, but the administrator account you created in **Chapter 1** will. We'll go ahead and delete that, now that you can log in as the root user.

Fire up System Preferences, and go into the Accounts Pane, unlocking the lock icon in the left hand corner if need be (click it and enter your root password to unlock). Then, select the administrator account you created in **Chapter 1** on the left, and then the minus (-) button. Confirm, and this will delete the user.

While you're much less likely to do something wrong if you delete the account via System Preferences, it can also be done in the Terminal. If you want to do this via Terminal, the command would be:

```
dscl . -delete /Users/username
```

Chapter 4: Enable SSH

Approximate time: 1 minute

Option 1: Enable SSH Via GUI

Open System Preferences again (if you've closed it), and click on the Sharing preference pane. Unlock the lock if necessary, and then ensure that "Remote Login" is checked.

To turn it off, just uncheck it.

Option 2: Enable SSH Via Terminal

Fire up **Terminal** (located in **Applications > Utilities**), and enter in the following command:

```
sudo /sbin/service ssh start
```

You'll have to enter your root password, but then Remote Login/SSH will be enabled.

If you want to stop it from Terminal, replace `start` with `stop`, as so:

```
sudo /sbin/service ssh stop
```

With SSH enabled, you can send Bash commands (you can take a look at our Bash 101 series to learn more about Bash) or AppleScript commands from the Terminal of another computer.

To learn more about how to log in using SSH, and other SSH basics, please see our article on it: Remotely Control a Computer: A Basic SSH Tutorial

That's It.

You've gained root access and the ability to command the computer remotely with SSH.

You have complete access to the computer.

Chapters 5 & 6

Chapters 5 & 6 follow this page and explain how to **recover any user's password in cleartext** on that computer. That means actually **viewing the unencrypted password** of any account on the computer.

Chapter 5: Obtain The Password Hash

Approximate time: 7 minutes

Log in and open Terminal.

Log into any account on the computer and open up the Terminal application. This application can be found in **Applications > Utilities > Terminal.app**

Finding the GUID (Globally Unique Identifier)

You first need to find out the Globally Unique IDentifier. This identifies the user to the Mac OS X authentication system, and is the name of the shadow file in which the password is contained. Depending on your version of OS X, enter one of the following commands:

If you are using **10.5 Leopard or 10.6 Snow Leopard** enter this command:

```
dscl localhost -read /Search/Users/<username> | grep
GeneratedUID | cut -c15-
```

If you're on a **10.4 Tiger** machine, enter this command:

```
niutil -readprop . /users/<username> generateduid
```

In both cases replace `<username>` with the shortname of the account you want to find the password for. (i.e. `admin` or `root`). The shortname is the name that the system refers to the account by, and can be found by looking in the **Users** folder on your hard drive.

You should get a value that looks like `A66BCB30-2413-422A-A574-DE03108F8AF2`. This is the GUID. Write it down, we'll need it later on.

The Password Hash

Password hashes are the encrypted form of the user's password. When the user enters their password to log in, the computer encrypts it using an encryption scheme to create a salted SHA1 hash, which it checks against the stored hash in the computer. If they match, the computer logs you in. We will be using the same method the computer uses to authenticate the login in order to crack the password.

To enter these commands to retrieve the hashes, you'll need root access. Make sure you're logged into the root account before entering any of the commands.

Obtaining the Hash

Enter the following into the command line, replacing <*GUID*> with the GUID you wrote down from Step 2.

```
cat /var/db/shadow/hash/<GUID> | cut -c169-216
```

After running the command, it should spit back out a hash that's formatted like this: 3`3BA7C74C318F5D3EF40EB25E1C42F312ACF905E20540226.`

Chapter 6: Decrypting The Hash

Approximate time: Depends On The Complexity of the Password

At this point, you no longer need physical access to the target computer, and can perform the rest of the commands on another computer. We'll use the application "**John the Ripper**" ("John") to decrypt the hash. John will use '**brute force**' to determine what the password is in cleartext. That means that the application will systematically generate passwords, encrypt them into the **salted SHA1 hash** (the encryption scheme that Apple uses for its passwords), and check them against the hash you found to see if the password matches. If it matches, then John has found the password.

You can download John the Ripper for Mac OS X here, and for Windows here.

Open up the zip file (Nowadays, Mac OS X will usually unzip it for you) and drag the "**John the Ripper**" folder into your **base directory** (also known as your home folder). This can get a little tricky so be sure to follow the instructions correctly.

Create a Text File Containing the Hash

Create a text file and save it in your John the Ripper folder as sha1.txt. Inside this file you should have the username and the hash. So if I wanted to find the password for the account crackMe, I would put the following inside sha1.txt:

```
crackMe:33BA7C74C318F5D3EF40EB25E1C42F312ACF905E20540226
```

Navigating to John the Ripper

Now you need to open up **Terminal** (**Applications > Utilities**) and navigate into the directory of your **John the Ripper** folder. If you followed the directions and put the folder into your base directory the command should be:

```
cd /name_of_your_john_folder/.
```

If you decided to be a rebel and leave the John the Ripper folder in a different directory, you just need to type in the full path to the directory from your home folder.

Cracking the Password with John the Ripper

All we have left is to load the hash into John. To do so, type in the following terminal command:

```
./run/john sha1.txt
```

If John is successful in loading the hash, you'll get a message that'll look like this:

```
Loaded 1 password hash (Mac OS X 10.4+ salted SHA1 [32/64]
```

Depending on the complexity of the password this process could take anywhere from a second to a day, so be patient. When John is successful at cracking the hash, it will display something along the lines of:

```
password (crackMe) guesses: 1 time: 0:00:00:00 100% (2) c/s:
153000 trying: password
```

Any text after `trying:` should be the password. In this case, the user account crackMe has the password: “`password`”

We hope you enjoyed the guide!

Check out our website for the latest and greatest security exploits, news, application reviews, scripting guides, and more!

If you have any questions, comments, or feedback of any kind regarding the guide, please feel free to send an email to feedback@hackmac.org, or jeff@hackmac.org to let us know how we did!

We hope we've expanded your knowledge of the security systems that protect the latest versions of Mac OS X, and trust that you will utilize the knowledge responsibly.

Thanks for downloading and subscribing!

-Jeff, Evan, and Alex