Rooting OS X With Physical Access
Version 1.0.2

Kuno
Nexus9 - http://www.Nexus9.org
February 1, 2005

DISCLAIMER: I (Kuno) or Nexus 9 take NO responsibility for your actions before/during/after reading this paper. You are your own person and we refuse to be held responsible for what you may or may not do as a result of reading this paper. This story is COMPLETELY FICTIONAL, it is for your reading entertaingment purposes only. The concept however, is non-fictional.
NOTE: This has not been tested on a computer that does not have root enabled.

I have a C in the class and I need a B to bring my GPA up to 3.0. My school uses all Macs with OS X(Panther). The systems administrator at school has a grudge against me because I kept shutting down her computer remotely, so she watches my every move. The only possible way to change my grade would be to break in psychically and change it. The only thing stopping me is I do not know the root password for my teachers computer.

Friday I put tape on the door, so the door opens even though it is locked. I flip on the lights and let the fun begin.

Her computer is on and I see the dreaded login window. I pull out my laptop and firewire cable, turn on my laptop, shutdown her computer, and plug-in the firewire cable to both of our computers. I turn on her computer while holding 't' down, which will mount her drive on my laptop via the firewire cable. Let the rooting begin.

My heart is beating faster because I know I am only a few steps away from changing my grade and finally being ungrounded. I quickly open up Terminal and type sudo -s to log into root. Then I type cd /var/db/shadow/hash which is the directory where OS X keeps the password hashes. I am not going to use any of those files, because some of my account passwords are different than the other ones, so I create a temporary account. The account name I enter is "temporaryaccount" and the password I use is "owned". Now that I have her computer mounted on mine, and the password file I want to use, it is time to change hers.

To do this I open her hash folder first with, open /Volumes/g4/var/db/shadow/hash/,(Note that the "g4" is just the name of her computer, it could be anything, so look at your desktop to see what the mounted drive is called) and open all of the files that do not have the extension ".state" with my text editor. Then I copy those files to my desktop, so I can change her password back later. Now I am back in Terminal and I type: cd /var/db/shadow/hash; ls -l. I look at the date and look for the one that is the most recent and copy the password text from my newest account hash file with: cat PO5D16F9-16FZ-64H8-3B16-123F3412P154, which would output something like: 8497FAD8FD8V89ASIP34U98DFJHQ897AS8DF9H2H8DSF973847UFHADS98VU98DSAFH WQPUIADNKJ983298AG98FA98F8732HJDFA545. Then I paste the output into all of her files that I have open in my text editor, save, quit, close my terminal windows, unmount her drive, and reboot her computer.

I am now back at the dreaded login screen. My heart is pounding again. I type in "root" for the user name and "owned" as the password and hit login. I stare at the login screen hoping it will not shake(a sign that the password is wrong), and it doesn't! I am logged in! I add some points to get my B, and reboot her computer holding 't' down again. This time I just drag, drop, and replace her modified hash files with the ones I copied to my desktop earlier. I unmount again, reboot her computer, and make sure that the password "owned" doesn't work anymore. I unplug my computer and leave with a smile and a better grade.

If you have any questions or comments, please send them to kuno@nexus9.org or you can find me on the KDX server: kdx.nexus9.org.