UNIVERSITY OF UTAH
STUDENT COMPUTING LABS

Integrating Mac OS X on Campus Seminar

Mac OS X Lab Security
University of Utah - Student Computing Labs by James Reynolds

More info and scripts at http://www.macos.utah.edu/macosx_security.html

Physical Security:
Alarms:
http://www.worldsecuritycorp.com/LGBasisList_li.htm LightGard Fiber optic cables
Security Cameras:
http://www.netbotz.com NetBotz
http://www.axis.com Axis
Tamper Detection:
http://www.intermapper.com/ InterMapper
System Profiling:
http://www.apple.com/remotedesktop/ Apple Remote Desktop
“system_profiler”

Boot Security:
http://www.macosxlabs.org/documentation/firmware_security/intro.html
http://docs.info.apple.com/article.html?artnum=120095 Open Firmware Password
http://users.ez-net.com/~jasonb/secureit.html SecureIt
“nvram security-mode”
http://www.bombich.com/software/shadowclassic.html ShadowClassic

Published Exploits:
See: http://www.macos.utah.edu/macosx_security.html

Password:
http://www.openwall.com/john/ John the Ripper
http://newsforge.com/newsforge/03/02/26/1639212.shtml?tid=2 Strong password guide
http://www.smat.us/sanity/pwdilemma.html Password dilemmas
Search http://www.versiontracker.com for the latest password generators
Remove world read/execute for:
- NetInfo Manager
- nicl, nidump, nifind, nigrep, niload, nireport, niutil
- /var/db/netinfo/local.nidb

Admin System Changes;
http://nob.cs.ucdavis.edu/~bishop/secprog/1997-ns/index.htm Writing Safe SetUID Programs
Cron
- “chmod -R o-rx”
- /etc/crontab
- /etc/periodic
- “echo root > /var/cron/allow”

World Writable
http://www.radmind.org Radmind
http://www.skytag.com/filebuddy/ File Buddy
"sudo find / -perm -2"
http://www.sayware.com/ Who Owns What

http://www.macos.utah.edu/Documentation/Crappyapps/crappyapps.html Fix apps that want world writable

SUID Root
http://www.sans.org/rr/mac/default_install.php Improving the Secuirty of a Default Install of Mac OS X
http://nob.cs.ucdavis.edu/~bishop/secprog/1997-ns/index.htm Writing Safe SetUID Programs
"find / -perm -4000 -user 0"

Logout:
“killall -u $1”
KillSumApps script:: http://www.macos.utah.edu/macosx_security.html (Logout)

Services:
https://grc.com/x/ne.dll?bh0bkyd2 Scan yourself
sudoers (see man visudo)
sshd edit /etc/sshd_config: Add “AllowUsers username”, change “Protocol 2,1” to “Protocol 2”
http://www.hmug.org/HowTos/tcpwrappers.html TCP-Wrappers how to

The Unknown:
http://www.radmind.org Radmind
http://faktory.org/m/software/nmap/ Nmap
http://deepquest.code511.com/nessus_faq_OSX.html Nessus
http://www.hmug.org/HowTos/logcheck.html LogCheck

Process Accounting
mkdir /var/account
touch /var/account/acct
accton /var/account/acct or reboot
chmod o-rx /usr/bin/lastcomm

Other Links:
http://www.princeton.edu/~psg/unix/osx/osxsecurity.html
http://homepage.mac.com/macbuddy/SecurityGuide.html
http://osx.hyperjeff.net/mac/
http://conferences.oreillynet.com/presentations/macosx02/towns_leon.pdf