How do you find the culprit when unauthor…

By rjben Author

Apr 19, 2017 10:49 AM in response to rjben

I found a login in system.log

This was on a laptop running El Capitan:

screensharingd [5791]: Authentication: SUCCEEDED :: User Name: XXX Viewer Address :: 172.xx.xx.xx :: Type DH

So search system.log on the attacked computer for some of these things and you will at least get the ip address, and if you are fast you could relate that back to the computer that it was done from. In this case they had shoulder surfed the password from the attacked computer, so they were logging in with what they know is a local user of the victim computer.

May 30, 2012 8:23 PM in response to rjben

the secure.log includes logs of computers that remote into the computer VIA ARDAgent. This includes the time date, account, and IP address of a computer they used to remote into the computer. The secure log is found in /var/logs/secure.log.

If they're using some thing other then the built-in remote fetures of the mac. Then your not going to see any thing in the secure log.

of corse you could just have all the passwords updated on the mac. Make sure ARDAgent is restricted. So they hopefully can't remote into the computer.

Also keep in mind an IP address has limitations. IE if I remote into a computer on 1/2/12 and then you check the log on 4/2/12, by that time some one else may have that IP address.

May 31, 2012 9:57 AM in response to TeenTitan

You may also want to completly change the password on YOUR ARD sever. If someone has comprimised YOUR system, you may find out that it was your system doing the "illegal" mosue movements. You may also want to check to be sure to NOT allow your system to be controlled by ARD from someone else. The Setting is in the ARD (Server) Preferences Menu under the Security tab.
