Week 2 Discussion

**Explain why it is best for administrators to use two different accounts when working on a computer. Explain the difference between the two accounts.**

Accounts with administrative access have the power to make changes to a system. Turn of logging. Shutdown or reboot the system. Modify any user resources like files or configuration settings. In other words, modify critical components of the underlying current security model we use. This heightened access is contrasted with regular accounts more limited access. They can modify items specific to themselves unless explicitly given access to other users process or system settings. So a user account shouldn't and very often can't do damage except to their own account.

With this level of control/access great care must be done to ensure that no unwanted or unexpected changes are done when actions are taken by a sysadmin. To compartmentalize this, sysadmins are encouraged to only access their administrator account to run their specific tasks that need that higher level access. Once that specific task is done the best practice is to then revert back to a normal level account. That way if you inadvertently run a "bad" command as a regular user the OS will stop you from doing any harm since a regular account doesn't have the privileges to modify system resources. This compartmentalization also shows up with security threats. Attackers looking to compromise a system will often use exploits targeted at sysadmins hoping to gain access to their accounts. If that sysadmin isn't practicing good compartmentalization of their accounts you can have a google chrome exploit parlayed into full administrator ownership of the system.