# System Security Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

In this lab you will explore some of the security measures that are provided by your operating system.

1. Login as Comprep for this lab, you will need administrative access. Why does the Windows OS provide different levels of access for different users?
2. Go to the control panel and be sure your view is set as Category. For this lab which category do you want to look at?
3. List the sub categories found in this section that are related to Security.
4. Click on the Windows Firewall link. What is the function of a firewall? (read the description).
5. What are the recommended settings for Windows Firewall?
6. When we setup FTP in Dreamweaver Windows Firewall was blocking our connection so we simply turned off Windows Firewall. What would have been a better approach? (see the FAQs )
7. Click on the Windows Update link and list the current settings for Windows Update on your system. Why is having automatic updates checked important for system security?
8. In the Administrative Tools section click on the View Event Logs link. Once the Event Viewer window opens click on the Window Logs and then the Security link. How many security events are listed in this log file? Click on one of the events and list some of the information displayed.
9. Are there any events that seem to be threats? What are most of the entries?
10. Exit the control panel and now press Cltr + Alt + Delete and select Start Task Manager. Most of the time you would use this application to close any applications that locked up your system. You can also use this window to see what applications are currently running on your system. Click on the Applications tab. What applications are currently running on your system?
11. Next click on the Processes tab. These are applications and processes that typically start up and run in the background and you don’t even know they are there. List three different processes and give a description of each.
12. If you think your system might be infected with a specific virus or worm you could check to see if that application was running here. What button is in the lower right of the window?
13. Click on the performance tab. What is your current CPU usage? Why do you have two CPU monitor windows?
14. If your system is idle and you do not have many tasks running then your CPU usage should be low. If you find the CPU usage high when you don’t have any applications running this could be an indication of a virus/worm but it could also be a legitimate program running in the background.
15. Click on the Networking tab. What is true about CPU usage is also true here, if you find a lot of network usage when your system is idle it could be an indication of a problem. What is your current network utilization value?

1. Close the Task Manager and click on the Sophos Protection icon in the task bar (a blue S) to open the AV program installed on your system. When was this software last updated?
2. Why should you always update your software before performing a scan?
3. Do you have any files in Quarantine? How does quarantine work? If you are not sure search the help function to find out.
4. Begin a scan of your system and show your instructor the scan screen (don’t wait for it to finish) to your instructor for teacher check.