

## Lab Experiments using Sysinternals Tools

Comp 3410 Lab 10

Not to be passed in

### **Chapter 1**

1. [Windows Operating System] Download and run the *AutoRuns* utility from <http://www.microsoft.com/technet/sysinternals/utilitiesindex.mspx>. Find out what programs are configured to run during system bootup or login. Do you recognize these programs? Identify the programs not provided by Microsoft that automatically start when you bootup or login.

### **Chapter 2**

2. [Windows Operating System] Download and run the *Process Explorer* utility from <http://www.microsoft.com/technet/sysinternals/utilitiesindex.mspx>. Find out what processes are currently running on your system. Choose a process, e.g. winword.exe and find out which DLLs it has loaded. Now click on the *System Information* button (Ctrl+I) to see details of CPU activity in your system. Now start a new program, e.g. Microsoft Excel. Describe how CPU usage changes when you start this program, a minute after you have started this program, and when you terminate this program. Click on System Information button (Ctrl+I) to see this information in detail. Provide an explanation for this CPU usage pattern.

### **Chapter 3**

3. Run the *Process Explorer* utility (Available at <http://www.microsoft.com/technet/sysinternals/utilitiesindex.mspx>). Click on the *System Information* button (Ctrl+I) to see details of memory usage activity in your system. Provide information about the usage of physical memory, kernel memory and paging in your system. Now start a new program, e.g. Microsoft Excel. Describe how this usage pattern changes when you start this program, a minute after you have started this program, and when you terminate this program. Provide an explanation for this usage pattern.

### **Chapter 4**

4. [Windows Operating System] Download and run the *NTFSInfo* utility from <http://www.microsoft.com/technet/sysinternals/utilitiesindex.mspx>. Explain the details of your hard drive organization (typically Drive C:) using this utility. To run this utility, open a command window, go to the directory where you have stored ntfsinfo.exe, and enter ntfsinfo.exe C:\.

## **Chapter 9**

5. [Windows Operating System] Download and run the *Rootkit Revealer* utility from <http://www.microsoft.com/technet/sysinternals/utilitiesindex.mspx>. What information does this tool produce? It has been stated that this tool has been updated to execute its scan from a randomly named copy of itself. Provide a detailed reason for this update.