Unit 7 Activity

Step 1

1. **Organize the nine events that can be audited into order of severity, by explaining which events pose the greatest risk for a security breach.**
   - Account logon events
   - Account management
   - Directory service access
   - Logon events
   - Object access
   - Policy change
   - Privilege use
   - Process tracking
   - System events
2. **What are the three audit policy settings, and which one is the most important in terms of security analysis?**
   - Success
   - Failure
   - No Auditing

The most important one in terms of security analysis is all of them combined (in my opinion). They all work off each other and can help security analysis.

Step 2

1. **Scan through the Task Category column and locate the rows where the user interacted with the File System. (These will be labeled "File System.") Look in the Information cell corresponding to these rows to locate the following:**

   a. **Where the user wrote data to the system (Search for WriteData or AddFile in the expanded Information cell). What objects did the user attempt to create?**
   It looks like they really kept trying at this. It looks like the user attempted to add a file called "backgroundTaskHost.exe". Looks like they had some trouble with this.

   b. **Write a short report, listing the Object Names (which will look like file paths, such as "C:\User\Documents\etc" listed in the expanded Information cell) and whether the user was successful in writing this data. Include the row number where you found this information in the original file (If you "sort by rows" for any reason, be sure to unsort before recording row numbers).**
   - C:/Windows/WinSxS/FileMaps/$$_system32_ (Row 533)
   - C:/Users/tipki/Documents/PROTECTED FOLDER (Row 250)

   (This is what I could find)

c. Where the user attempted to access and delete an audited file (by looking for DELETE). Again, report these, listing the object names, whether the user was successful in deleting the data, and the row number where you found the information.

For me, I see this under Registry and Other Object Access Events tasks. The tasks had to do with Drobox and Microsoft Office. They were successful in doing these tasks, I found this information in the rows around 416 and the rows around row 435.

2. How many events returned a "Failure"? What type(s) of events were they (identify them by row number as well)? What was the reason for this failure? How concerned should you as the administrator be about these failures?

11 events returned a "Failure." The failures are listed under Logon, which means these were failed login attempts. As the administrator, I would be concerned because that means someone is trying to intrude into my system.