Lab 02: Common Locations of Windows Artifacts

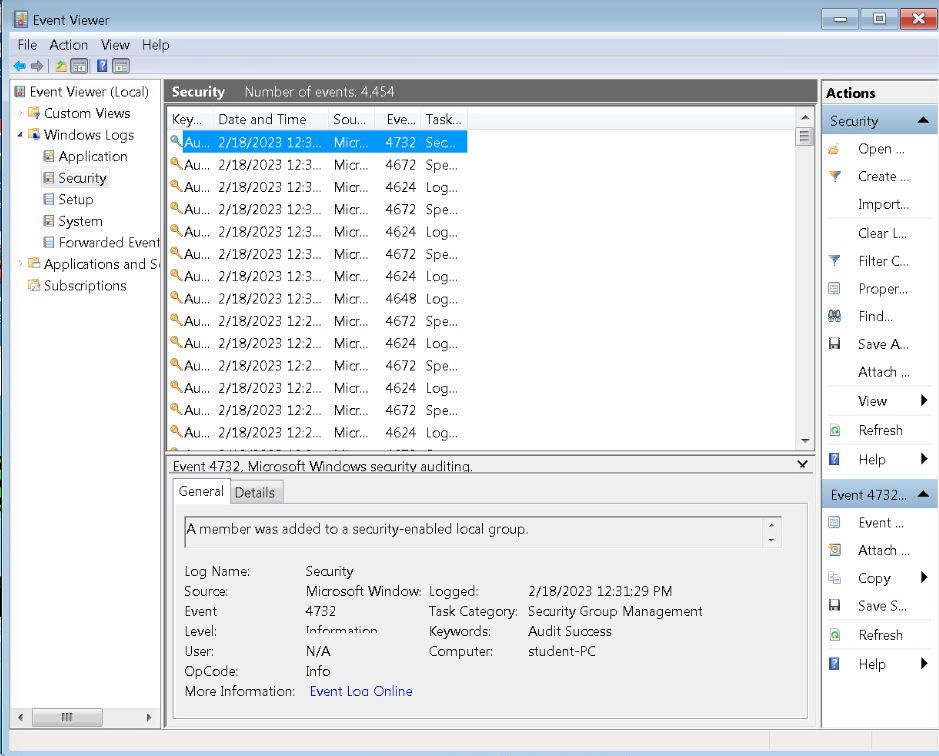
Lab 02 report Name: Kevin Ubilla

This Lab is required for Unit 5. It is worth 15 points. The Challenge Flags are worth 2.5 Extra Credit points.

1. **Examining Windows Event Logs, IIS Logs, and Scheduled Tasks, Step 5.** One of the first tasks you are asked to do on a Windows system is to add a guest operator to the Backup Operators group in your localgroup. What is the advantage of being able to manage localgroups like this one in Windows? Please tell me in three sentences or less below:

**→** This may help in case the system becomes compromised. Being able to add a guest operator means we can SSH from another computer and thus effectively maintain our management principles. It is our job to organize and assign permissions for different users, among other functions in order to effectively perform duties. **←**

1. **Examining Windows Event Logs, IIS Logs, and Scheduled Tasks, Step 10.** You have made your way to the Security Log and found the record of your change to add the guest operator to the Backup Operators group. Please capture the window in which that event is detailed and paste it below.

**→  ←**

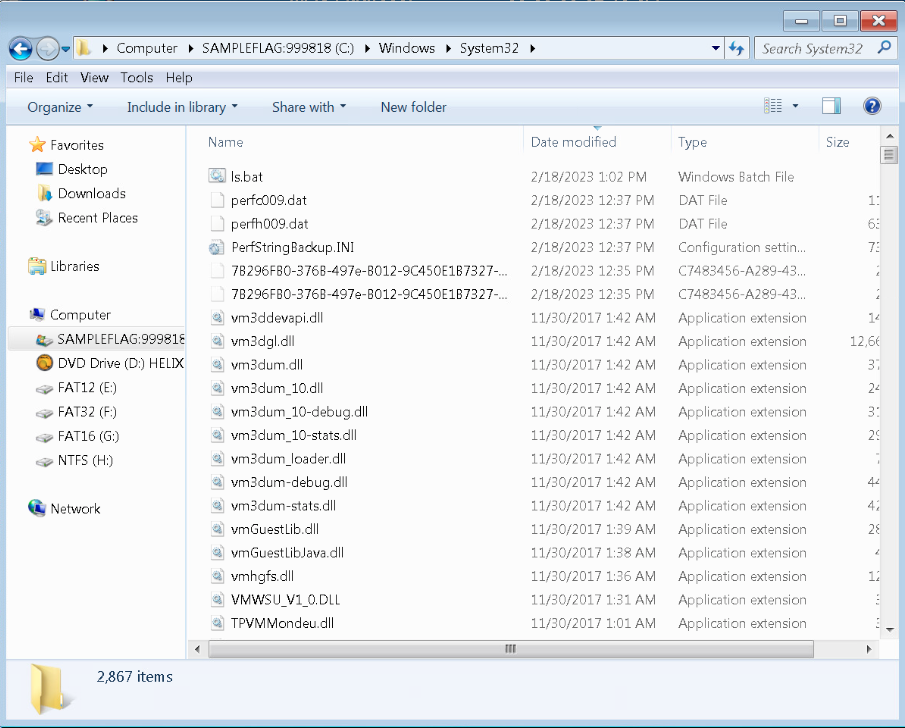
1. **Examining Windows Event Logs, IIS Logs, and Scheduled Tasks, Step 19.** Now that you are headed to this address on the Web, just what IS Ice Weasel, anyway, and what machine is 216.5.1.200? Please note you answer in no more than several sentences below.

**→**The 216.5.1.200 url is the webpage for the Windows 7 machine we are running. We are using IIS logs to examine activity on another machine**.** Ice weasel is an open-source web browser that came about as a fork from the more popular FireFox web browser. **←**

1. **Examining the Startup, Windows, and System32 Folders, Step 11.** You have just tried to execute a command (‘**ls**’)while in the Windows folder, only to have it be unrecognized. Why is it not recognized? Please place your brief but concise explanation in no more than 3 sentences below.

**→** The default list command on Windows id “cmd”, not “ls” which is for Linux or Mac. ‘ls’ was not a command installed on the system. It wasn’t until we copied in the batch file including the command on Step 12 that we are able to access its features. **←**

1. **Examining the Startup, Windows, and System32 Folders, Step 20.** Now that you have sorted the Windows\System32 folder according to date modified, arrange the list so the most recently modified is at the top and capture the window, making sure that the most recently modified item is clearly readable., and paste it below.

**→  ←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**