**Discuss what security measures you have implemented or will implement as a result of this unit**

The Operating System virtualizes memory, not only to make processes run efficiently, but also to keep potentially dangerous processes from disrupting other processes or even taking over the system (Arpaci-Dusseau & Arpaci-Dusseau, 2012). Considering the extent to which devices are networked, “it is no surprise that developers have implemented a variety of defensive countermeasures to halt those wily hackers from gaining control of systems” (Arpaci-Dusseau & Arpaci-Dusseau, 2012). One method to thwart hacking, is to monitor systems and networks for malicious activity and benign events that could leave systems vulnerable to attack (NSA/CSS ,2013). In other words, logging system activity for proactively monitoring the custom views of the logs on a daily basis or plugging the logs into a Security Information Event Management (SIEM) system can help an administrator determine if a system is at risk or if it has already been compromised so that action can be taken to rectify the situation. According to the NSA/CSS (2013), the first step in logging system activity should be to deploy a clean, and therefore uncorrupted, dedicated server whose sole use it is to collect and archive log data from both itself and the network machines it is monitoring. In addition to a machine which collects log data, all of the “source” machines being monitored will have to periodically send pertinent logs that they create to the “collector” machine. Moreover, the transmission of logs should be encrypted as well as follow an assortment of authentication policies to “Harden” the collection of event logs against malicious activity (NSA/CSS, 2013). Windows OS already has built-in features that allow for the logging of events and for their transmission to a collector device; and by isolating important logs on an otherwise unused collector machine, the risks of those logs being erased to hide nefarious activity is reduced and the benefits of logging as a way to detect vulnerabilities can be achieved (NSA/CSS, 2013).

References

Arpaci-Dusseau, R. & Arpaci-Dusseau, A. (2012). *Operating Systems: Three Easy Pieces.* Madison, WI: University of Wisconsin-Madison. Retrieved from <http://pages.cs.wisc.edu/~remzi/OSTEP//>

NSA/CSS (2013). Spotting the Adversary with Windows Event Log Monitoring, Revision 2. *United States of America National Security Agency.* Retrieved from <https://my.uopeople.edu/pluginfile.php/322781/mod_forum/attachment/3094792/U8%20Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf>

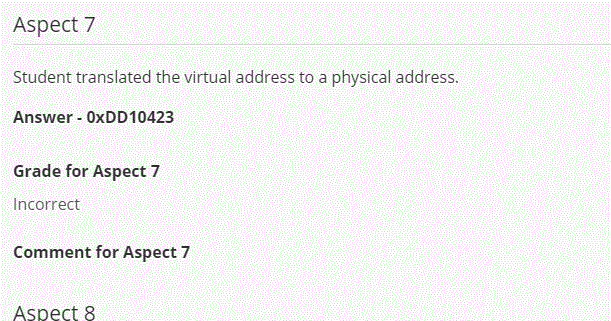
**Discuss the weeks activities and your observations**

I would not call the the NSA document we were provided ‘light reading’, but it was very informative. In it we learned that Windows OS already has the features necessary to perform event logging securely as well as how to configure machines in the network to send log files to a collection machine (or even a networked storage drive) for administrative viewing, log management software, or archiving. Aside from reading and writing the above learning journal entry, there was not much to do this week. I did not mention it in the last learning journal, but the question about Shell32.dll, was helpful for me to answer. By answering it, I got a glimpse into the actual files in the OS and how they could be modified….BUT SHOULDN’T--at least not to create a vanity desktop. lol Naturally the review quiz (and previous unit quizzes) will need to be studied thoroughly, but that should not pose a problem. I hope to take the second part of this course next term, while everything is still fresh in my head. I hope our paths cross again someday as your dedication to the class and our learning is outstanding. Lastly, I wish you well as you write your dissertation and defend it. Best of Luck!!! -Angela

**Request for a grade change**

Apologies for the hassle, and thank you for your time in advance. One of my graders for the Unit 7 Assignment seems to have made an error in grading. If it can be corrected, I would be most appreciative. Here are the details:

This shows Aspect 7 marked as incorrect. The answer is supposed to be DD10423.



The next screen capture is of my response to the question, showing that I did in fact have the correct answer, namely that the physical address would be DD10423 in hex (see bottom row of table showing how I came to the right answer).

