# ISEC 325 Homework 10

Answer the following questions based on your reading of the text books, the module key points, and the instructor’s presentation this week.

1. [2 points] What are the two meanings of “auditing” in this section?

The first meaning is the review of processes to make sure they comply with polices and regulations. The second is a self-review for a network environment.

1. [2 points] What does log management entail?

Log management entails storing generated data, retaining log files, a baseline measurement, encryption for storage, and disposal of the log files after a certain time.

1. [2 points] What is Linux’s centralized logging facility? How does it work?

The Linux centralized logging facility is called Syslog and it will log information from the system utilities and send the information to a centralized logging facility.

1. [3 points] Compare and contrast configuration management and change management.

The configuration and change management will both look and manage changes that are implemented to the information system. The difference is that configuration management will

1. [2 points] Research the ISO/IEC 27000 series standards and the CobiT standards. How are the two similar? How are they different? Compare and contrast the two.

The two standards are both used to for overseeing their IT systems are standards available for organizations to look at to help better their own. The differences are that the COBIT is the best practice framework and defines the requirements for governance and control of the IT processes with no need for certification. The ISO is the international standard and defines the requirements for the information security and can be certified.

1. [8 points] Research two of the following network monitoring packages and describe what they do and how they do it: Nagios, ZenOSS, Cacti, or Solarwinds. Specifically address advantages and disadvantages, operating system support, and community support. What is the advantage to using a tool such as this versus manually monitoring?

Cacti has the advantage of being an open-source tool and can support some of the major operating systems like windows and linux, it also provides support for multiple people. The disadvantage is that it has trouble with SNMP handling and monitoring, it also does not have many plugins. Nagios, like Cacti, supports the major operating systems like Windows, Linux, and Unix. Nagios has the advantage of being more well known and having been in the market for a longer time meaning that it has a community with multiple plugins to its name. The disadvantage is that it is not that user friendly, and it is not making improvements to its system so it can keep up with technological advancements.

1. [6 points] Research one of the following configuration management packages and describe what it does and how it does it: Chef, Puppet, CFengine. Specifically address advantages and disadvantages, operating system support, and community support. What is the advantage to using a tool such as this versus manual configuration management?

Chef is an open-source management package that uses the Ruby language. It uses mechanisms to get the current status of the machine. It uses the operating systems Linux, Windows, macOS and several others. It has the advantages of low barrier entry and good integration with the cloud. The disadvantages are that it is harder to learn, needs constant checks, and is only a good fit for AWS cloud. Chef is big on the community aspect and takes user input into consideration.

1. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about.  In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

This week we look at monitoring network systems and how it works. During the research I was surprised with how many of the monitoring and management packages cover operating systems both linux and windows. Looking at a lot of different things in the security that involve operating systems, there are many that are only windows or only linux. The ones that have both tend to have a round about means of using them. It was interesting to see what the different packages thought would be the best information to share and use to attract users. It took some diving to find the Operating systems they use.