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 known as systems monitoring which is the ongoing review of a system or network of systems to determine if the operational results and events are within the bounds established as proper functioning which will include processes to detect potential incidents and ensure compliance with systems policies. The second is a periodic review of program or system functions to determine compliance with a set of established standards. In network security it entails examining all the systems, policies, personnel, and operations associated with protecting the organizations information and networking devices and making sure they are operating and being used in accordance with the will or intent of management.

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

   In order to be effective log management must entail the following five points. Storage you must prepare the system to handle the amount of data generated by logging and that the rotation of log entries is acceptable rather than merely accept system defaults. Retention is the period that log files or log file data should be maintained, different organizations may have different requirements on the retention of data requiring remote locations for the storage of data. Regulations may also dictate how and when to rotate or destroy data. A baseline must be determined which is the measurement of activity that represents the normal state of routine conditions. The baseline is used to measure ongoing events against. Encryption must be used if the organization plans to archive logs, if so, the logs should be encrypted for storage. Disposal is the last thing for consideration and disposal of log files should be routinely and securely destroyed.

3. [2 points] What is Linux's centralized logging facility? How does it work?

   Linux's centralized logging facility is named syslog which stands for system logger. Syslog allows multiple system utilities to log using the same mechanism. Syslog can be used to log messages from Linux applications and tools such as web servers and email programs. Syslog also allows organizations to store logs on a separate system so that you can keep logs from attackers who may try to alter them. Syslog has its own daemon syslogd which runs as a backup process. It uses a configuration file to determine the type and extent of logging to perform which can be configured to report on different levels and different ways.

4. [3 points] Compare and contrast configuration management and change management.

Configuration management is the identification, inventory, and documentation of the current information system's status- the hardware, software and networking configurations. Configuration management also involves version numbers, revision dates and other features that allow the changes made to them to be monitored and administered. Terms involved with configuration management include configuration item which is the hardware or software item to be modified or revised, version is the recorded state of a particular revision of a software or hardware configuration item, major release is a significant revision to a previous state, minor release is an update or patch, build is a snapshot of a particular version of software, build list is a list of the versions of components that make up a build, configuration is a collection of components that make up a build, revision date is the date associated with a particular version or build, software library is a collection of configuration items that is usually controlled and that developers use to construct revisions and to issue new configuration items. The configuration management process helps avoid confusion, problems and unnecessary spending.

Change management addresses the modifications to the base configuration. Change management is used to prevent changes that could detrimentally affect the security of a system. It reduces the risk that if changes made to a system like insertions, installations, deletions, uninstallations, or modifications will result in a compromise to system data, confidentiality, integrity or availability. It provides a repeatable mechanism that effects system modifications in a controlled environment. Change management must be tested prior to implementation to minimize risk of any adverse effects. The change management process also identifies the steps required to ensure that all changes are properly requested, evaluated and authorized. It also entails a step by step procedure for identifying, processing, tracking and documenting changes. The steps may include first identifying the change that may be needed, then the change must be evaluated to see if it is viable, correct, if system security will be affected, the cost of the change and if security components will be affected. The decision to implement the change will either be approved, denied or deferred to a later time. A change request is then implemented if the change is approved and finally the change is monitored continuously to ensure there are no negative consequences.

5. [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.

   ISO 27000 provides recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in interorganizational dealings. It is also designed to serve as a metric for the assessment of good security management within the organization, as defined in the ISO series. It is designed as an assessment tool more than an implementation framework. It covers
   risk assessment and treatment, security policy, organization of information security, asset management, human resource security, physical and environmental security, communications

and operations, and access control. It provides some implementation information specifying what must be done but not how to do it.

COBIT provides advice about the implementation of sound controls and control objectives for information security. This document can be used not only as a planning tool for information security but also as an auditing framework controls model. COBIT has 34 high-level objectives that cover 215 control objectives, the control objectives are grouped into four areas plan and organize, acquire and implement, deliver and support and monitor and evaluate. COBIT was designed to be an IT governance structure it also provides a framework to support information security requirements and assessment needs.

ISO 27000 and COBIT are both used to set up guidelines for systems and information security and both have recommendations. COBIT can be used as a framework whereas ISO 27000 is used more for recommendation and assessment not a framework.

6. [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?

SolarWinds is a whole system of different tools to help monitor and log systems. I focused on the security event manager alone for the sake of simplifying and comparing to show the difference between this and cacti. Advantages of SolarWinds are it provides the software with a centralized log collection and automation, automated threat detection and response, integrated compliance and reporting tools, intuitive dashboard and user interface, built in file integrity and monitoring and “affordable licensing”. The disadvantages are that it would certainly have a learning curve which may be supported by SolarWinds perhaps for a price and the cost although it may be cheaper than other intrusion event monitors it still costs $4800 to obtain a license. SolarWinds supports a bunch of operating systems including Windows, Linux, Cisco and Palo Alto networks as well as a whole dedicated web page on other systems supported. SolarWinds has a large community of support including THWACK, Orange Matter, Logical read blog, SolarWinds certified professional as well as customer support. The advantage of using SolarWinds over manually monitoring is that SolarWinds is very convenient and consolidated. Security makes things more expensive and slows things down the tools SolarWinds offers would help mitigate some of the loss of speed by saving time.

Cacti is a user developed freeware tool for consolidating log data. The advantage of Cacti is it consolidates your log data into easy to read charts and graphs that can then be sorted and organized to help more easily identify problems. The disadvantages of Cacti are that it would have a learning curve that may not be as supported as something paid like SolarWinds, Cacti has a limited amount of systems that it works on just Windows and Linux, it also has a steep application dependency needing a LAMP stack listing MySQL, PHP, RRDTool, net-SNMP and an Apache or IIS server. Community support includes the software documentation, forums, mailing

lists, FAQ, and a Wiki page. The advantage of using a tool like this vs manually monitoring is that the tool can neatly organize your data for sorting which will make going through massive logs much easier.

7. [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?

   CFengine is a configuration management tool used to automatically roll out updates and changes to every node in your infrastructure. It does it by consolidating and running the update through one program. The advantages of using CFengine are that it quickly can update up to 50,000 nodes of servers automatically. Cfengine is lightweight and fast as it is coded in C, it is secure, stable and scalable. The disadvantages are that it has a very steep learning curve. It supports a variety of Operating systems including Linux, Windows, AIX and Solaris. Its community support includes a community support page with mailing lists, official support for the enterprise edition with direct customer contact, it has a link with useful documentation and a link with blogs for support as well. Having software to consolidate and roll out update server nodes would be a big advantage to using remote updating through windows server which would save time and resources.

8. [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.

   With the cyber security events I have attended they brought to my attention several times the same thing you have told us several times in our lectures. Logs are only good if you look at them. The thing that kept getting said in those conventions frequently is there is always a struggle with management over how many people that they need in security. You need people to look at these logs and all the data in them. This again talks to your point about security being expensive. From the things that I noticed as well it takes a special person to be able to go through those logs and do it well.

   I found it interesting to see how the process of collecting and configuring the logs and how it all fits in with your organizations security policy. I think I got the most out of the last two questions on the homework that had us research some of those tools and how they work. The thing I kept thinking is how difficult it can be to learn something new like

Linux and when you do apply programs to Linux can be difficult as well. Windows can also be very finicky. Adding any of these programs must make your job easier as a security professional, if you don't have anyone proficient in them it seems like it could be a real weak point until you get past the learning curve. It makes me wonder what it would be like trying to get something like this to run on a test server while management pushes you to have it rolled out to production the whole time. I am sure there are times in security where it feels like you are at ends with production trying to keep things secure.

Some of the employers I talked to mentioned they were hurting for people badly and they were even using auditors to help fill the gap. I can understand how they would do well in the cyber security field now.

References

Cacti the complete rrdtool-based graphical solution. (2004-2020). Retrieved from cacti.net: https://www.cacti.net/

CFEngine. (2020). Retrieved from cfengine.com: https://cfengine.com/

Solarwinds. (2020). Retrieved from solarwinds.com: https://www.solarwinds.com/

Whitman, M. E. (2012). *Guide to Network Security, 1e.* Cengage Learning.