Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

Instructor intro

- Contact info: Arthur.Moore@wgu.edu
- Number: 1-877-435-7948 Ext. 1554
- Office Hours:
- Monday: 8AM-5PM
- Tuesday: 8AM-5PM
- Wednesday: 8AM-5PM
- Thursday: 8AM-12PM AND 7PM-10PM
- Sunday: 6PM-10PM

As a reminder

- This web series is only to enhance/supplement the course material not to replace it please follow the guidelines as posted below.
- ***It's Highly recommended that you Don't schedule the first assessment until all the materials are covered***.
- -take the preassessment until constantly passing
- -review lessons 1-14 readings (pay close attention to chapters 1 – 6.)
- -complete lessons 1-14 quizzes.
- -complete lessons 1-14 exercises (pay close attention to chapters 1 – 6)
- -watch the videos that are posted in the course tips
- -go over the PowerPoints that are posted in the course tips

Accountability

- Accountability provides us with the means to trace activities in our environment back to their source. In addition, it provides us with a number of capabilities, when properly implemented, which can be of great use in conducting the daily business of security and information technology in our organizations. In particular, organizations need to carefully maintain accountability in order to ensure that they are in compliance with any laws or regulations associated with the types of data they handle or the industry in which they operate.
- Accountability depends on identification, authentication, and access control being present so that we can know who a given transaction is associated with, and what permissions were used to allow them to carry it out

Nonrepudiation, Deterrence, & Admissibility of records

- Nonrepudiation: refers to a situation in which sufficient evidence exists as to prevent an individual from successfully denying that he or she has made a statement or taken an action.
- Deterrence: Accountability can also prove to be a great deterrent against misbehavior in our environments. If those we monitor are aware of this fact, and it has been communicated to them that there will be penalties for acting against the rules, these individuals may think twice before straying outside the lines.
- Admissibility of records: When we seek to introduce records in legal settings, it is often much easier to do so and have them accepted when they are produced from a regulated and consistent tracking system.

Intrusion detection and prevention

- Intrusion detection and prevention: One of the motivations behind logging and monitoring in our environments is to detect and prevent intrusions in both the logical and physical sense. If we implement alerts based on unusual activities in our environments and check the information we have logged on a regular basis, we stand a much better chance of detecting attacks that are in progress and preventing those for which we can see the precursors.

- Intrusion detection: (IDSes) An IDS performs strictly as a monitoring and alert tool, only notifying us that an attack or undesirable activity is taking place.

- Intrusion prevention: (IPSes) An IPS can actually take action based on what is happening in the environment. In response to an attack over the network, an IPS might refuse traffic from the source of the attack.

Auditing

- Auditing: One of the primary ways we can ensure accountability through technical means is by ensuring that we have accurate records of who did what and when they did it. In nearly any environment, from the lowest level of technology to the highest, accountability is largely accomplished through the use of auditing.
- When we perform an audit, there are a number of items we can examine, primarily focused on compliance with relevant laws and policies. In the information security world, we tend to look at access to or from systems as a primary focus, but often extend this into other fields as well, such as physical security.

Logging & Monitoring

- Logging: gives us a history of the activities that have taken place in the environment being logged. Without this evidence, audits and investigations are not practical. It is key to any organization to determine the correct level of logging to support their needs.
- Monitoring: is a subset of auditing and tends to focus on observing information about the environment being monitored in order to discover undesirable conditions such as failures, resource shortages, security issues, and trends that might signal the arrival of such conditions. Monitoring is largely a reactive activity, with actions taken based on gathered data, typically from logs generated by various devices.

Assessments

- Assessments: audits may take a more active route toward determining whether everything is as it should be and compliant with the relevant laws, regulations, or policies.
- We can take two main approaches to assessments: vulnerability assessments and penetration testing. While these terms are often used interchangeably, they are actually two distinct sets of activities.
- Vulnerability assessments: generally involve using vulnerability scanning tools, such as Nessus in order to locate such vulnerabilities. Such tools generally work by scanning the target systems to discover which ports are open on them, and then interrogating each open port to find out exactly which service is listening on the port in question.
- Penetration testing: although it may use vulnerability assessment as a starting place, takes the process several steps further. When we conduct a penetration test, we mimic, as closely as possible, the techniques an actual attacker would use.