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

Operating System Hardening

- When we look at operating system hardening, we arrive at a new concept in information security. One of the main goals of operating system hardening is to reduce the number of available avenues through which our operating system might be attacked. The total of these areas is referred to as our attack surface. The larger our attack surface is, the greater chance we stand of an attacker successfully penetrating our defenses.
- There are six main ways in which we can decrease our attack surface, as listed here.
  - Removing unnecessary software
  - Removing or turning off unessential services
  - Making alterations to common accounts
  - Applying the principle of least privilege
  - Applying software updates in a timely manner
  - Making use of logging and auditing functions

Operating System Hardening Process

- **Remove All Unnecessary Software**: Each piece of software installed on our operating system adds to our attack surface. Some software may have a much greater effect than others, but they all add up. If we are truly seeking to harden our operating system, we need to take a hard look at the software that should be loaded on it, and take steps to ensure that we are working with the bare minimum need for a functional system.
- **Remove All Unessential Services**: In the same vein as removing unneeded software, we should also remove or disable unessential services. Many operating systems ship with a wide variety of services turned on in order to share information over the network, locate other devices, synchronize the time, allow files to be accessed and transferred, and perform other tasks. We may also find that services have been installed by various applications, to provide the tools and resources on which the application depends in order to function.
- **Making alterations to common accounts**: In many operating systems (as well as some applications), we can find the equivalent of a guest account and an administrator account. We may also find a variety of others, including those intended for the use of support personnel, to allow services or utilities to operate, and a plethora of others, widely varying by the operating system vendor, version, and so forth. Such accounts are commonly referred to as default accounts.

Operating System Hardening Process

- **Apply the Principle of Least Privilege**: As we discussed in Lesson 3, the principle of least privilege dictates that we only allow a party the absolute minimum permission needed for it to carry out its function. Depending on the operating system in question, we may find this idea put into practice to a greater or a lesser extent. In almost any modern operating system, we can find the tasks a particular user is allowed to carry out separated into those that require administrative privileges and those that do not.
- **Perform Updates**: Regular and timely updates to our operating systems and applications are critical to maintaining strong security. New attacks are published on a regular basis, and if we do not apply the security patches released by the vendors that manufacture our operating systems and applications, we will likely fall victim very quickly to a large number of well-known attacks.
- **Turn On Logging and Auditing**: Last, but certainly not least, we should configure and turn on the appropriate logging and auditing features for our system. Although the particulars of how we configure such services may vary slightly depending on the operating system in question, and the use to which the system is to be put, we generally need to be able to keep an accurate and complete record of the important processes and activities that take place on our systems.

Protecting Against Malware

- A large concern at present is the mind-boggling number and variety of malware present on the networks, systems, and storage devices around the globe. Using such tools, attackers can disable systems, steal data, conduct social engineering attacks, blackmail users, gather intelligence, and perform a number of other attacks.
- **Anti-Malware Tools**: Most anti-malware applications detect threats in the same way the IDS we discussed in Lesson 10 do: either by matching against a signature or by detecting anomalous activities taking place.
- **Executable Space Protection**: is a hardware- and software-based technology that can be implemented by operating systems in order to foil attacks that use the same techniques we commonly see used in malware. In short, executable space protection prevents certain portions of the memory used by the operating system and applications from being used to execute code

Protecting Against Malware

- **Buffer overflow:** attack works by inputting more data than an application is expecting from a particular input—for example, by entering 1000 characters into a field that was only expecting 10. Depending on how the application was written, we may find that the extra 990 characters are written somewhere into memory, perhaps over memory locations used by other applications or the operating system. It is sometimes possible to execute commands by specifically crafting the excess data.
- **Software Firewalls**: Properly configured software firewalls are a very useful additional layer of security we can add to the hosts residing on our networks. Such firewalls generally contain a subset of the features we might find on a large firewall appliance but are often capable of very similar packet filtering and stateful packet inspection.
- **Host Intrusion Detection**: HIDS are used to analyze the activities on or directed at the network interface of a particular host. They have many of the same advantages as network-based intrusion detection systems (NIDS) have but with a considerably reduced scope of operation.

Protecting Against Malware

- **Scanners**: We can use a large number of scanning tools to assist in detecting various security flaws when we are looking at hosts. Although we discussed this in Lesson 10 from a network perspective, such tools can also be used to enhance the security of our hosts. We can look for open ports and versions of services that are running, examine banners displayed by services for information, examine the information our systems display over the network, and perform a large number of similar tasks.
- **Vulnerability Assessment Tools**: which often include some portion of the feature set we might find in a tool such as Nmap, are aimed specifically at the task of finding and reporting network services on hosts that have known vulnerabilities.
- **Exploit Frameworks**: provide a variety of tools, including network mapping tools, sniffers, and many more, but one of the main tools we can find in exploit frameworks is, logically, the exploit such as Rapid7's Metasploit, Immunity CANVAS, and Core Impact provide large sets of prepackaged exploits in order to make them simple to use and to make a larger library available to us than we might have if we had to put them together individually.