**Please make a copy of this document and save to your computer prior to editing. This document should not be directly modified by anyone other than the Standards and Practice Team. Remove this note prior to submitting to DAMS.**

# Transcript: IT Podcast - Ep 114 - C836 Lesson 11 - with Arthur Moore and Jessica Galterio

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker # 1: Arthur Moore

WGU's IT Audio Series, flexible, portable, profound.

Hey everybody. This is Arthur with WGU. I'm one of the course instructors on C836, Fundamentals of Information Security. As a quick note, this series is meant to enhance the learning material, not meant to replace it. For this particular chapter, let's go on ahead and get our notes together because this is very technology acronym driven for Chapter 11, so let's go on ahead and jump into it. Operation system hardening. Well, 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 evidence through which our operating system might be attacked. In other words, it reduces the attack surface or attack vector, and there are six main ways to decrease our attack surface as listed here. Remove 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, and making use of logging and auditing functions. Remove all unnecessary software. Each piece of software installed on our operating system adds to the attack surface. Some software might have a greater effect than others, but all add up. If we are truly seeking to harden our operating system, we need to take a look at the software that should be loaded on it and what is loaded on it and make sure that we are only working with the bare minimum. Remove all unessential services. In the same vein as the unneeded software, we should remove or disable any unused services to lessen that attack surface. Making alterations to common accounts.

In many operating systems, you usually ship with two default accounts, which is the guest account and the administrator account. The first thing that you want to do is going on ahead and either disable, change the name or apply a password to these particular default accounts, so that way there isn't a vulnerability for those accounts.

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 minimum amount of permission needed to carry out its function. No more than the minimum. If you don't need Internet browser to do your job, you should not have an Internet browser installed on your PC. This is applying the principle of least privilege. Perform updates in a regular and timely manner.

This can vary from organization to organization because the updates are really published to patch and fix software and hardware vulnerabilities that are in our production environment. But we have to balance performing updates with the regulation of the organization. What I mean by that is there will always be a small gap in between getting updates and applying updates because there needs to be a period where there is testing going on to make sure that the update applied doesn't break anything in the production environment. Turning on logging and auditing. Last but not least, this is in my opinion, probably the most important is to make sure that there is appropriate auditing and logging features turned on your system, and what this does is it creates a digital trail of who, what, how, when and why.

Services, software and other items that are running on the PC are functioning logged on access and things of those nature. The biggest thing that mal actors go against is the auditing and logging system because that's how they hide their tracks.

Protecting against malware. There is no short or easy way to say this. There is a mind-boggling amount of software that is considered malware coming out on a daily basis. Tools that hackers use to attack, disable, steal data, perform social engineering attacks, and blackmail users, and all other very malicious attacks.

Anti-malware tools are any software or application that detects and prevents threats that you would have to deal with malware either by matching signature or by detecting anomalous activities. The executable space protection is hardware and software based technology that

can be implemented by the operating systems in order to follow attacks that use the same techniques we commonly see in malware. In short, executable space protects certain portions of the memory, while the operating system and applications are being used from executing that particular code. A great way to say that is, think of Macros from Microsoft Office.

You're normally asked, "Hey, there's a Macro attached to this, do you still want to run it?" It warns you about not trusting unknown Macros. The Buffer Overflow Attack. Buffer Overflow works by inputting more data than an application is expecting from a particular input. For example, let's say we're inputting data for which state we are from, this particular application just wants the abbreviation of the state. Well, it's only meant to take two characters, so anything over those two characters, let's say 4, 5, 6, or even 10,000 characters they have to be written somewhere in memory. Once it's written to memory, the mal actor can actually take that overflow in use code with that to execute attacks.

That's why you have to do input validation and vulnerability checks on your software to make sure that you're actually sanitizing the input. Software firewalls. These are the same as our hardware firewall [inaudible 00:07:55] but they are ran on the actual PC or device that you're using. It's not dedicated hardware and it's a more scaled down version of the firewall and normally comes in either stateful or a packet filtering type of firewall, excuse me, there. Host Intrusion Detection, HIDS. HIDS are used to analyze the activities on or direct it at the network interface of a particular host and they have many of the same advantages as Network-based Intrusion Detection Systems, NIDS, but with a considerably reduced scope of operations. One, we have just for maybe a particular production server, that server that probably has all of the credit card data on it, and then the Network-based Intrusion Detection System actually performs these particular scans for the whole network, not just one device.

Scanners, just like we talked about in the last lesson, scanners are used to look at the ports and services that are running on our devices while we're using them. Vulnerability assessment tools, same as before we're looking for vulnerabilities that are on our systems in order to patch and configure them correctly to remove these vulnerabilities in that tenable nessus. Exploit Frameworks really it's like a Swiss Army knife of hacking tools.

They're just all varieties of these tools that are put into a nice little package. Rapid7, Metasploit, Immunity Canvas, Corps Impact, the Burp Suite to Kali Linux. All of these are Exploit Frameworks that have all of these items put into it. Let me correct myself. Kali Linux is more of a operating system that has all of these different tools audit, it's not just a single Exploit Framework. But when I think of these frameworks, one good place that I go to have a model is the Kali distribution of the Linux. With that, I bring this particular lesson to a close. If you have any questions or concerns, please, feel free to email me at arthur.moore@wgu.edu. Thank you all. Have a nice day.

Schedule time with your course instructor to explore more deeply. WGU, a new kind of you.