Nicholas Robertson

Reflective Essay

Before taking this course, I had already had a deep understanding of cybersecurity fundamentals. I had just graduated with my bachelor's degree in cybersecurity and have spent the better part of two year studying nothing but it. But as I took this course and went over the relative information provided to us, I began to rely just how much of this information I had forgotten over the past few years. Subjects like the different APs, Bluesnarfing, and the different Wi-Fi accesses are subjects that I have pretty much forgotten as time went on, due to other classes requiring us to focus on other topics within the degree. However, within this class, the Cengage learning platform and its different modules that they provided have helped with refreshening my understanding of these different topics that will help pass the 701 exam that I am planning on taking in the future. To further elaborate on my understanding of Bluesnarfing, the study guide provided by Cengage helped me understand more about how a device can be compromised in the event of a Bluesnarf attack. And how devices can still be compromised during these attacks even if they are hidden. As it is stated that, "device that is set to "hidden" may be Bluesnarfable by guessing the device's MAC address vie a brute force attack." (Pandey et al, 2017). Beyond the Cengage course, I also think that the mandatory discussion boards have helped me with my critical thinking skills as well. I especially liked discussion board four in where the topic of whether companies should continue maintain outdated software and if they continued to update their software, should consumers pay for the cost of the updates. I concluded that if consumers wanted to continue working with outdated software, then companies should have the right to charge them a monthly or yearly fee to pay for the upkeep and maintained for the software. I also came to the conclusion that if companies were to go out of business and their

software is not passed own to another company, then the software should be released to the public as opensource software so that the community can continue with updating the software. In the end this course has given me a refresher on the topics that I have forgotten as time went on and thanks to that I feel as though I am fully prepared to take the 701 exam and take the information that I have learned within this course within my future cybersecurity goals.

References

Trapti Pandey & Pratha Khare, (2017) *Bluetooth Hacking and ITS prevention*

https://www.ltts.com/sites/default/files/resources/pdf/whitepapers/2017-12/Bluetooth-Hacking-and-its-Prevention.pdf