Keith Bagley

Review / Familiar Topics

Security+

I'm somewhat familiar with the installation and configuration of systems to secure applications, networks and devices. In Community College we learned some basics of VMWare, and how it is used in the network environment. I have also researched CompTIA and what they have to offer. It is important to have certificates in this area. I also remember learning about Risk Management. Risk Management is important because it helps to avoid and reduce financial risks. Familiar terms on this exam are Worm, Viruses, Trojan, Rootkit, Keylogger, Adware, Spyware, Bots, and Backdoor. Many of the types of attacks I found here are also very familiar. I have looked through a book on Certified Ethical Hacking previously and a lot of the things mentioned here look familiar.

Black box, White box, and Gray box is familiar. It goes along with the "hats". The technologies and tools section reminds me of some of the things that we encounter at work in telecommunications. There is a very large amount of things here that I am not familiar with, but I do recognize a lot of things as well. Identity and Access Management controls such as Smart cards, multiple types of recognition, hardware, software, and MAC/DAC are familiar here.

Risk management, again, is something I remember from Community College. It focuses a lot on the ways that, without risk management, could negatively affect the work and lives of employees or people in general. I am not very familiar with Cryptography and PKI. There are a ton of Acronyms listed here. Just to name a few I recognize are CCTV, DNS, ICMP, FTP, IoT, IP, IPSec, LAN, HTML, HTTPS, HVAC, URL, USB, and more. The hardware/software list I would say that I recognize at least half of it.

Certified Ethical Hacker

I am very interested in this one! It is a very exciting part of the field. I recently got a book off of Amazon to kind of explore the idea of Ethical Hacking. I was not aware that there are two different certifications, the ANSI and the Practical. I know what IoT hacking means, and I see a few mentions of Malware here that I am familiar with. The course outline is large, and I know a lot of the terms here, although I do not know them anywhere near as in depth as I would like to. Sniffing seems to be a very important thing here. It seems it will take a lot of hard work to eventually reach the Master level of the CEH. I am excited to learn about all of these new things.