Week 3 Playbook Entry: Endpoint device security

* Hands-On Project 5-6

This project was about protecting yourself against ransomware, recommending the use of VPNs on public networks if you have to use them at all. The project from there veers into website for the No More Ransomware Project, a website that hosts information on ransomware, as well as the various ways to deal with ransomware, the site hosts multiple ransomware decryption programs, I looked at the manuals for the decrypters for Emsisoft, Rakhni, DoNex, and the Micro Ransomware File Decryptor. All of these were very simple, run the program on the affected machine and let it do the magic.

* Hands-On Project 6-1

This project looks at the security of QR codes. Started off by making a QR code that linked back to the cengage website. The code made was actually a link that redirects to the website that you listed, so what is on the code is obscured until you go to that link. You could in theory do that intentionally and link to a malicious website. We also made a link to a random location on google maps, this could in theory be used to misdirect someone, regardless of how likely that is, it is worth considering that when scanning random qr codes.

* Hands-On Project 6-2

In this project, we look at Security bulletins and CVE numbers, we start by looking at Microsoft's bulletin, the board is a little bit difficult to navigate at first but once I realized what I was looking at I didn’t have any issues at all. Every issue listed is very clear and well written, by it’s nature it is a tad dry but that is just how it has to be. Unlike Apple’s which is much more neglected, While it should be expected that Apple would have fewer security issues due to the size of their market share, it is still quite barren and lacks a lot of the features Microsoft’s has.