Identify 3 important learning points acquired from Week 1 and 2 lessons.

* Security is heavily attacker sided as only one vulnerability needs to be found and exploited however the defender must guard against all possible attacks.
* I need to be more careful when doing work as carelessness can cost me
* I learnt about the different area’s hackers can attack, the application, the host, or the network. The most common point of attack is the application because that is where a hacker can try and find a vulnerability or exploit from anywhere and it will not be considered illegal.

What do these learning points imply? Or what conclusions could you draw?

* It implies that the defender has to take extra precautions and must never be complacent as nothing is ever fully 100% secure.
* It implies that I need to be more focused on my work and not be distracted when I’m doing it as it can take a long time trying to find careless mistakes especially when coding.
* The application layer has to be the most heavily guarded as that is where hackers will start from to penetrate into a network.

What will you do more of, less of, start or stop the next time? (In the context of the learning acquired thus far)

* I will do less procrastination
* I will try and understand what is required of me before I start my work