**ePortfolio:** <https://alesteka.github.io/essexPublic/>

**REFLECTIVE PIECE OF WORK**

We started our six-week module with a brief overview of cybersecurity history, which is the baseline to understand advanced concepts including networking, penetration testing, and standards relevant to Information Communication Technology. One of these was CIA (Confidentiality, Integrity, Availability) which allowed me to hold onto during my learning and scanning activities since it is designed to convey basic principles of information security. Through understanding the standards, including GDPR and appropriate tools, we were able to use different models that helped us to approach and eventually detect various vulnerabilities and threats emerging in the contemporary cybersecurity field. One of these was the Cyber Kill Chain model, which allowed us to understand the SolarWinds breach case study, which was also the topic for our second seminar.

The Case Study was particularly interesting, since the steps taken by adversaries, were well described through the model. The intrusion example confirmed that no one can be safe in the cybersecurity world, since human error appears to be often the weakest chain of the attack. What was even more interesting is, that the employees managed to detect unusual events, yet they decided to not pay additional attention to it since the intrusions were so well concealed. Additionally to the Seminar, we participated in our first collaborative discussion about Digitalization. This activity was also interesting since the discussions opened well. It is inevitable for companies to adapt to changes if they want to endure their positions in the market. Therefore the main conclusion was that some companies are still reluctant to make digital transition, due to costs, which are often the main factor.

In the week that followed, we focused on the practical examples of scanning and penetration testing, to detect, monitor and eventually mitigate possible threats. Through the simple command line tools and the advanced network scanning approaches, we were able to capture some initial data of the website, that we chose in the first week. I particularly liked the third week, since it was the first time I delved into practical examples of the tools that we utilized to perform penetration testing. However, to conduct such activity one has to be familiar with the networking protocols, security management, and other website-specific functionalities.

Toward the end of the third unit, we submitted our first assignment, which was the outline for the final assignment. The latter included extensive vulnerability scanning using different tools, for example, WireShark, Nessus, and Kali Linux. In that week I, enjoyed working with Kali Linux, due to its diverse and advanced functionalities that enabled me to conduct penetration testing. At first, I struggled to establish the environment, since I had to consider multiple network and setup-related configurations. However, this was also my first time conducting such activity, hence I had been learning with enthusiasm.

In unit 5 we discussed the use of logging in Linux and Windows environments (namely Syslog-ng, Nagios, Snort, log4j tools), together with the security protocols, which were also part of a final discussion topic about the different types of networking approaches. We had seen that there wasn't a unique answer to which of the types should prevail in the future, as all have their pros and cons. However, from the standpoint of the current infrastructure, IPv6 will probably prevail in the future since it would be a struggle to restructure the entire network with the new approach, such is a peer-to-peer overlay network.

The last six weeks were intense in terms of activities, yet I thoroughly liked the process, since the topics were interesting. Using different software allowed me to explore and understand different vulnerabilities and it gave me the scope of future learning. Therefore, I enjoyed using Nessus as well, yet it lacks the functionalities that are provided by Kali Linux, which is optimized for manual testing. Therefore, I can say with high confidence, that Kali Linux would be my first choice in future scanning and penetration testing activities. I learned a lot and the knowledge already helps me in my current job where I use AWS services (in particular, how to use VPC functionalities, together with other services). In addition, I will strongly consider the options for future learning in networking as such.