Network Security Reflection

What?

The brief but powerful network security module was interesting and thought-provoking. It was my first 6-week module, and it made a big impression. As someone with experience in software development, I've always understood how crucial security is to system development. Nevertheless, the majority of the frameworks and tools we employ have a tendency to handle security implementation by default and abstract away a large portion of it. This module inspired me to stand back and consider security more thoughtfully. It introduced me to the different vulnerabilities that can occur during development due to simple carelessness or presumptions we frequently make, rather than sophisticated attacks.

What also set this module apart was its unique, hands-on structure. Unlike other modules, we were asked to choose a live demo website right at the start and then carry out a series of related activities in each unit. These tasks were interconnected and fed directly into our summative assessments. That meant there was no skipping ahead or completing things out of order; each unit had to be completed sequentially. I had never approached learning in this way and certainly never with network security as the central focus. All of the steps from choosing a website in Unit 1 to the last summative assessment in Unit 6 presented some level of difficulty and unfamiliarity. It challenged me to think like both a software engineer and an attacker, pushing me beyond my

comfort zone. I've included my e-portfolio, which documents my learning from this module, [here](#) before I go into the specifics of my journey.

So what?

Because the module was brief, I deliberately chose to get ahead of the game right away. I started early and made sure to always be at least 1 unit ahead of schedule, whether it was reading, watching lecturecasts, watching seminar recordings, contributing to forum discussions or completing formative activities. This method allowed me to delve deeper into the network security without feeling rushed by impending deadlines.

One of the most valuable outcomes of this early involvement was the chance to test out various vulnerability assessment tools. I began exploring both desktop and online versions of the tools mentioned in the module, getting hands-on experience with how they function and what kind of insights they provide. Being a Linux user, I'm already familiar with tools like Nmap, Traceroute, and Netstat, which helped me feel more at ease when exploring network scanning and analysis during the module. This hands-on experience gave me the self-assurance to assess which tools would best support my analysis for the Unit 6 summative assessment.

The scanning activities were especially enjoyable to me. These activities revealed internal details of the website I had chosen in Unit 1, helping me become familiar with its structure and vulnerabilities in a short amount of time. Seeing how tools could reveal

potential security vulnerabilities that aren't always apparent at first glance was fascinating. I even experimented with injecting basic malicious scripts just to observe how the website might respond, a safe and educational way to understand how real-world attacks might play out. Additionally, browsing through various security articles and resources added another layer of depth. I found our module tutor, Doug, to be especially interesting and thought-provoking because he frequently shared real-life security incidents during seminars.

However, my journey through the module wasn't without difficulty. Unit 5 coincided with a personal bereavement, which made it emotionally challenging to keep up with academic work. Thankfully, because I had started early and stayed ahead, I was in a position where the only major task left was to scan the website using pre-selected tools and analyse the resulting reports. It was still difficult to focus, but my earlier planning gave me the space I needed to cope and continue. That experience reinforced the value of pacing myself and building buffers into my schedule.

Now what?

Network security has always felt like a weak area for me, a subject I often avoided, possibly because I never found it particularly engaging in the past. However, this module served as a turning point. It helped me recognise that understanding security isn't just a nice-to-have skill but a necessity for a software engineer today. The hands-on activities, scanning tasks, and exposure to real-world vulnerabilities gave me a practical way to approach what had previously felt like an abstract topic.

While I didn't particularly enjoy the forum discussions, especially the first one, I've come to understand their importance. These conversations, even when challenging, exposed me to different perspectives and helped me realise that security concerns are not limited to specialists or infrastructure teams. As a software engineer, I have a responsibility to ensure that the code I write and the configurations I apply are secure by design. Going forward, I plan to explore more security-focused content, stay updated with the latest threats and mitigation strategies, and apply this mindset in my day-to-day development work. This module shifted how I view my role in building secure systems.