Individual Reflective Piece

This piece reflects on my personal development during the Network Security module, and how it compares to goals set in my Personal Development Plan (PDP) created at the start of the module. Contributions towards the PDP will be evaluated next to assignments and tasks given throughout the module, before conclusions will be made on its success.

PDP Goals

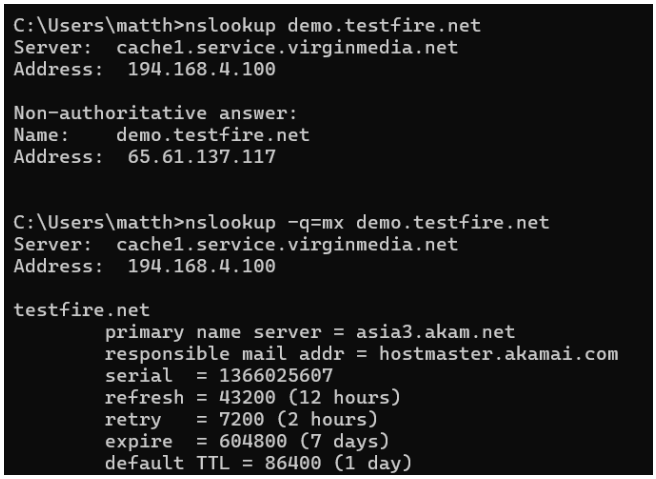
Due to my limited technical knowledge and practical experience in the field, my primary PDP goal was to gain real world applicable skills for future work and to develop my understanding of networking and network security. Further goals were to understand how weaknesses are exploited, how exploit tools are used, and how to present plans and findings in an appropriate workplace style.

Cyber Kill Chain Modelling

Week 2 referenced Lockheed Martin's cyber kill chain as a modelling tool for analysing advanced persistent threats and the concept of using institutionalised frameworks as defence against attackers (Hutchins et al., 2011). This informed my approach to both assignments by considering website vulnerabilities and baseline security competence by comparing the website to the expectations of institutions OWASP and NIST (OWASP, 2021; Scarfone et al., 2008). This achieved a key goal of my PDP by learning to analyse threats professionally. The task helped framing how I should approach analysis of threats and developed my awareness of organisations relevant to future work. The cyber kill chain showed me the process by which an attacker would attack a website.

Scanning Activity

Week 3 of the module contained a scanning activity that required students to use basic tools such as nslookup to scan a website, chosen in week 1. The main learning outcome of the task was to gather the content from various sources, for use as part of the vulnerability assessment in week 6.



(Fig 1)

Fig 1 shows one of these tests. The task was useful for developing an understanding of basic tools and their function. The results were used in reconnaissance for the website in assessment 2. It aligned with my PDP by developing technical skills and using tools that may be used in a workplace setting.

Assignment 1

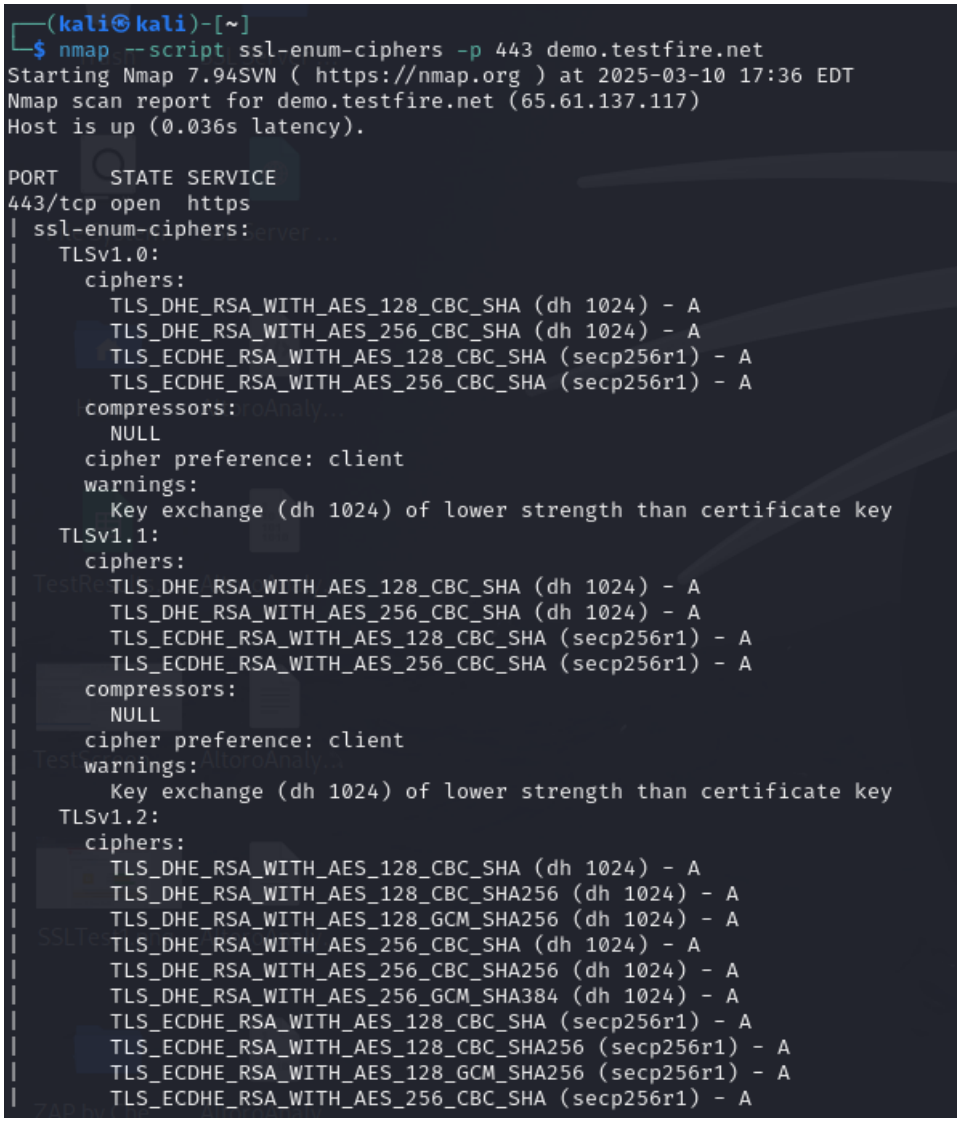
Students were tasked to create a baseline analysis and plan for a vulnerability assessment. The baseline analysis was informed by recommendations from frameworks explored when analysing the cyber kill chain. The learning outcomes for this task involved choosing suitable tools for investigating the website. The readings for the module introduced tools like Kali Linux (Hertzog et al., 2021) and Nmap (Bhingardeve and Franklin, 2018). This was significant as I had no experience using pen testing tools. This led to further research, as the readings did not cover in depth all the tools necessary to complete the assessment.

The use of these tools and developing the vulnerability assessment plan allowed me to understand cybersecurity from a new point of view; that of an attacker. Previously I had approached cybersecurity from a reactive mindset – an attack has happened; how can it be stopped. This new mindset involved being proactive, looking for vulnerabilities that can be exploited, and then thinking about how these can be mitigated. Evaluating tools and their strengths for the task aided in improving critical analysis. The assignment fulfilled all the goals of my PDP; technical knowledge was gained, and I got to experience using practical tools, leading to the creation of a workplace style report.

Assignment 2

This assignment focused on presenting the results of the vulnerability assessment. The results were to be evaluated against the baseline set in assignment 1 and measured against GDPR compliance. Recommendations for improvement were then to be given from the business viewpoint. To complete this task required use of multiple skills developed during the module. Fig 2 shows an Nmap scan using scripts to gain

information on site encryption standards. It shows my development over the module, primarily by showing a deeper understanding of tools, but also by understanding the results show outdated TLS and insufficient Diffie-Hellman key strength.



(Fig 2)

Assignment 2 had an outcome of understanding legal issues in the field. Analysing the target website for its compliance with GDPR accomplished this by focusing on the implications of weak security. GDPR considerations affect people daily, but often in an abstract way. Making recommendations for bringing the website to GDPR standards made these considerations more concrete. This helped achieve my PDP goal of developing an understanding of network security purpose.

Conclusions

On completion of this module, I feel that I have achieved my PDP goals. Alongside these goals I have improved my critical thinking, problem solving, legal awareness and research skills.

However, I believe that my goals were too narrow. An improvement would be to set goals that would closer integrate my learning with the rest of the cohort, so I could benefit from their experience. Due to time constraints, I was unable to complete all the module's formative tasks. I chose tasks that most closely reflected my goals of improving technical knowledge and workplace procedural training, resulting in predominantly independent work. In future modules I would include some goals that result in more collaboration.

Word Count - 848

References

Bhingardeve, N. and Franklin, S. (2018) 'A Comparison Study of Open Source Penetration Testing Tools.', *International Journal of Trend in Scientific Research and Development*, 2(4), pp. 2595-2597. Available at https://www.ijtsrd.com/papers/ijtsrd15662.pdf (Accessed 9 March 2025).

European Union. (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L119, 1 – 88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (Accessed 8 March 2025).

Hertzog et al. (2021) *Kali Linux Revealed*. United States of America: Offsec Press.

Hutchins et al. (2011) *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Available at https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf (Accessed 9 March 2025).

OWASP Foundation. (2021) *OWASP Top Ten*. Available at https://owasp.org/www-project-top-ten/ (Accessed 8 March 2025).

Scarfone, K. et al. (2008) Technical Guide to Information Security Testing and Assessment (National Institute of Standards and Technology, Gaitherburg, MD), NIST Special Publication (SP) 800-115. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (Accessed 16 February 2025).