# Final Reflective Piece: Network Security Management

**Student Name:** Lauren Pechey

**Student ID:** 12696823

**Course:** Masters of Computer Science

**Module:** Network Security Management

**Professor:** Beran Necat

**Word Count:** 804

**Submission Date:** 21 July 2025

## Introduction

This reflection delves into my learning experience throughout the Network Security module, guided by Rolfe et al.'s (2001) 'What? So What? Now What?' reflective framework. This module challenged me to develop and apply technical and professional skills in vulnerability assessment, threat modelling, penetration testing, critical analysis, effective technical communication, time management, and ethical awareness. These competencies align directly with the real-world legal, social, and professional responsibilities that information security professionals navigate daily (Aslan et al., 2023).

## What?

The most impactful part of this module was completing two linked Vulnerability Audit and Assessment assignments: the first on planning and baseline analysis, and the second on executing scans and summarising results with clear recommendations. This was my first time independently planning a full vulnerability audit for an e-commerce site, selecting open-source tools, designing a scan strategy, analysing findings, and making evidence-based recommendations. These skills align with industry best practices that emphasise risk prioritisation and clear communication beyond technical scanning alone (Admass et al., 2024; ISO, 2022).

Technically-speaking, I gained practical experience with tools such as Nmap, Nikto, OWASP ZAP, Wfuzz, and Burp Suite. While Burp Suite was initially daunting, repeated use built my confidence and exposed me to the persistence needed in real-world penetration testing (Alhamed & Rahman, 2023). An unexpected challenge was Wfuzz's incompatibility with my MacBook due to MacOS Python and dependency issues (Beggs, 2014), requiring a switch to Windows. This reinforced adaptability and troubleshooting as essential cybersecurity skills (Miller, 2022).

I also engaged actively in peer discussions and contributed to the Module Wiki, discussing topics like digitalisation and the log4j vulnerability, which all broadened my understanding of evolving security threats (Shoemaker et al., 2019). Seminar debates deepened my grasp of threats and defences; applying the Cyber Kill Chain model (Hutchins et al., 2011) to the SolarWinds exploit (Temple-Raston, 2021) clarified how advanced persistent threats (APTs) gradually bypass layered defences—a pattern that is increasingly prevalent. The Generative AI debate challenged me to consider how emerging technologies both bolster and threaten network security, illustrating AI's dual-use nature (Abedin, 2022). These collaborative experiences, supported by my peers and guided by my module tutor, highlighted teamwork's vital role in cybersecurity problem-solving (Strode et al., 2022).

**So What?**

Reflecting on these experiences, I see the module enhanced both my technical competence and my understanding of network security's legal, social, and ethical dimensions. I learned that effective vulnerability scanning demands critical analysis and clear communication to enable proactive risk management (Admass et al., 2024).

The Cyber Kill Chain framework proved crucial for anticipating attacker tactics and reinforcing layered defences (Fadzil et al., 2023). Working with tools like Burp Suite and ZAP underscored the importance of patience and time management, as practical testing is rarely straightforward (Aslan et al., 2023). Collaborative discussions strengthened my ability to translate complex technical data into clear, actionable insights suitable for varied audiences (Strode et al., 2022).

The Generative AI debate illuminated complex ethical issues around privacy, bias, and misuse (Abedin, 2022). These concerns closely relate to professional integrity and

alignment with regulations such as GDPR and ISO/IEC 27001, which set the legal and ethical framework for security professionals (European Union, 2016; ISO, 2022).

Emotionally, the module was demanding but rewarding. Initial uncertainty transformed into confidence as I developed the skills to plan and execute scans, interpret real vulnerabilities, and engage critically with advanced topics like AI. Balancing this learning with full-time work reinforced the importance of disciplined time management and persistence.

**Now What?**

Looking ahead, I plan to expand my technical proficiency by exploring more advanced vulnerability scanning features in tools like Burp Suite and ZAP and experimenting further with the broader Kali Linux toolkit. To formalise my learning, I aim to pursue a recognised professional certification, such as CompTIA Security+ or Certified Ethical Hacker (CEH), which will strengthen my technical credibility (Chapple & Seidl, 2023).

I will update my Professional Development Plan (PDP) to focus on refining my time management for complex tasks like multi-step scanning and reporting. I also intend to keep applying frameworks like the Cyber Kill Chain in practice, as recommended by Lachkov et al. (2022), to develop deeper threat modelling expertise.

Finally, the debate on AI emphasised the importance of staying current with new research, emerging threats, and evolving compliance obligations, such as GDPR and ISO/IEC 27001 (European Union, 2016; ISO, 2022). My long-term goal is to build a career grounded in secure, ethical, and legally compliant practice, contributing to a safer digital landscape.

## Conclusion

Drawing on Rolfe et al.'s (2001) reflective framework has enabled me to connect what I learned, why it matters, and how it shapes my future development. This Network Security module has strengthened my technical foundation, sharpened my critical thinking about vulnerabilities, and deepened my understanding of the legal, social, and ethical responsibilities that define effective and responsible information security practice.

**References:**

Abedin, B. (2022). Managing the tension between opposing effects of explainability of artificial intelligence: a contingency theory perspective. *Internet Research* 32(2): 425–453. DOI: https://doi.org/10.1108/INTR-05-2020-0300

Admass, W., Munaye, Y. and Diro, A. (2024) Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications 2*(1): 1-9. DOI: https://doi.org/10.1016/j.csa.2023.100031

Alhamed, M., & Rahman, M. (2023) A systematic literature review on penetration testing in networks: Future research directions. *Applied Sciences* 13(12): 6986. DOI: https://doi.org/10.3390/app13126986

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023) A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics 12*(6): 1-42. DOI: https://doi.org/10.3390/electronics12061333

Beggs, A. (2014) *Mastering Kali Linux for Advanced Penetration Testing.* 1st ed. Birmingham, United Kingdom: Packt Publishing.

Chapple, M., & Seidl, D. (2023) *CompTIA Security+ Certification Kit: Exam SY0-701 (Sybex Study Guide)*. 7th ed. Hoboken, NJ: Wiley.

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 from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 16 July 2025].

Fadzil, L.M., Manickam, S. and Al-Shareeda, M.A. (2023) 'A review of an emerging cyber kill chain threat model', *2023 Second International Conference on Advanced Computer Applications (ACA)*, Misan, Iraq, 2023. 157–161.

Hutchins, E., Cloppert, M., & Amin, R. (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research* 1(1): 1–14.

ISO. (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Available from: https://www.iso.org/standard/27001 [Accessed 16 Jul 2025].

Lachkov, P., Tawalbeh, L., and Bhatt, S. (2022) Vulnerability assessment for applications security through penetration simulation and testing. *Journal of Web Engineering* 21(7): 2187–2208. DOI: https://doi.org/10.13052/jwe1540-9589.2178

Miller, A. (2022) *Cybersecurity Career Guide*. 1st ed. Shelter Island, NY: Manning Publications Co.

Rolfe, G., Freshwater, D., & Jasper, M. (2001) *Critical reflection for nursing and the helping professions: A user's guide*. 1st ed. Palgrave Basingstoke: Pearson Education Limited.

Shoemaker, D., Kohnke, A., & Sigler, K. (2019) What the profession of cybersecurity needs to know and do. *EDPACS 59*(2): 6–18. DOI: https://doi.org/10.1080/07366981.2019.1565106

Strode, D., Dinsoyr, T., & Lindsjorn, Y. (2022) A teamwork effectiveness model for agile software development. *Empirical Software Engineering* 27(56): 1-50. DOI: https://doi.org/10.1007/s10664-021-10115-0

Temple-Raston, D. (2021) 'The SolarWinds attack: The story behind the hack', *NPR*, 20 April. Available at: https://www.npr.org/2021/04/20/989015617/the-solarwinds-attack-the-story-behind-the-hack (Accessed: 19 July 2025).