Network Security - Reflection

https://tbrays.github.io/e-Portfolio/

The module covered network security fundamentals including vulnerability assessments, security protocols and cyber threat mitigation. This reflection follows the What, So What, Now What format suggested by Rolfe et al. (2001).

What?

At the start of this module, I had little experience with cybersecurity tools and vulnerability assessments. The assignments focused on scanning and reporting website vulnerabilities. I chose to evaluate the Gin and Juice Shop, an e-commerce platform which was designed to test Burp Suite, a paid security tool. I did not initially realise this limitation and later found that many required scanning activities such as identifying the operating system and software running on the server were not possible. If I took this module again, I would scan all test sites briefly before selecting one.

I struggled with discussion posts often overthinking them. Relating them to real companies helped but I misunderstood how replies should be structured treating them as evaluations rather than personal viewpoints. Salmon (2011) argues that effective online discussions require concise, structured engagement rather than excessive detail. Applying this approach will help me contribute more effectively while saving time. Referencing was difficult especially identifying source types. The literature review was broad so I focused on three key areas to narrow it down.

Exploring cybersecurity tools was new to me. I first tried installing tools on Windows but most were designed for Linux. To make tools more accessible I set up Kali Linux (Kali.org, no date) on VirtualBox (Oracle, no date). I started with command-line tools then configured Burp Suite Proxy to intercept requests but scanning required a paid version. I attempted to use OWASP ZAP but

struggled with installation and found it harder to use. Eventually I trialled the professional version of Burp Suite which allowed me to complete automated scans.

Balancing work and coursework was difficult due to increased commitments. With no prior experience using cybersecurity tools I felt that a practical demonstration perhaps in a seminar would have been helpful. Without structured guidance learning how to install and use these tools was time consuming. Many classmates had professional cybersecurity experience which made me feel out of my depth.

So What?

As the module progressed, I realised that I needed to change my approach to discussion posts and practical tasks. I had been treating discussion posts as formal evaluations instead of engaging in discussions and expressing my own views. This made them more time-consuming and difficult to complete. I started focusing on whether I agreed or disagreed with a post and provided concise explanations instead of overanalysing every aspect.

The lack of practical demonstrations made it difficult to gain confidence with security tools. Burp Suite (PortSwagger, no date) and OWASP ZAP (OWASP, no date) required extensive self-learning and a trial-and-error approach that was frustrating as I did not know what to expect. The Gin and Juice Shop was hosted behind an AWS Elastic Load Balancer (ELB), which hid much of the information required for the exercises, making some tasks more difficult (Amazon, no date). Independent research and practice helped me become more comfortable with these tools. Installing Kali Linux and experimenting with Burp Suite improved my confidence. Learning to intercept requests and examine headers was valuable but not being able to perform full scans without a paid licence was frustrating.

Managing time in a six-week module was challenging. Research suggests that intensive courses require structured study schedules to prevent cognitive overload (Biggs & Tang, 2011). Moving forward, I will implement structured study blocks to manage workload more efficiently.

Now What?

To improve my technical skills, I will work with cybersecurity tools and carry out the test on the other websites. I plan to explore additional functionality of Burp Suite by following the tutorials on the PortSwigger website.

To improve referencing I will continue using structured tools and attend support lectures from the study skills team. I will also refine my discussion post approach focusing on concise opinion driven responses instead of lengthy evaluations.

In future modules I will research how tools work before using them to reduce the trial-and-error learning curve. Managing my time more effectively will also be a priority ensuring I allocate dedicated periods for both theoretical study and hands-on practice.

Conclusion

This module was a steep learning curve but provided a strong foundation in network security and vulnerability assessments. Initially I struggled with using security tools and managing my time but through independent learning and practical experimentation I developed more confidence. By refining my skills and seeking structured learning opportunities I aim to build a solid foundation in cybersecurity.

Reference

Amazon Web Services, (no date) *Elastic Load Balancing (ELB).* Available at: https://aws.amazon.com/elasticloadbalancing/ [Accessed 10 March 2025].

Biggs, J and Tang, C., (2011) *Teaching for Quality Learning at University.* Maidenhead: McGraw-Hill Education

Kali Linux, (no date) *Kali Linux Documentation.* Available at: https://www.kali.org/ [Accessed 10 March 2025].

Oracle. (no date) *VirtualBox: Virtualisation for Everyone.* Available at: https://www.virtualbox.org/ [Accessed 10 March 2025].

PortSwigger, (no date) *Burp Suite: Application Security Testing Software.* Available at: https://portswigger.net/ [Accessed 10 March 2025].

OWASP, (no date) *OWASP ZAP - The Zed Attack Proxy.* Available at: https://www.zaproxy.org/ [Accessed 10 March 2025].

Rolfe, G., Freshwater, D. and Jasper, M., (2001) *Critical reflection in nursing and the helping professions: a user's guide.* Basingstoke: Palgrave Macmillan.

Salmon, G., (2011) *E-moderating: the key to teaching and learning online.* New York: Routledge