Title: Individual Reflective Piece

Introduction

Reflecting on my journey through the Network Security module in the MSc Computer Science program, I find it both valuable and challenging. This module has increased my understanding of various professional terms and ethics in the field and has enriched my professional and personal development.

Summary of Learning Outcomes

During this module, I explored various aspects of network security, including legal, social, ethical, and professional issues faced by information security and risk professionals. The module covered techniques for scanning, evaluating, and mitigating network vulnerabilities, providing a solid understanding of vulnerability assessment basics, especially in web applications. Key assignments included conducting a Vulnerability Audit and Assessment, presenting the results in an Executive Summary, and reflecting on personal development.

The assignments required a deep dive into real-world applications of network security principles. For example, the first **Baseline Analysis and Plan assignment** for the Gin & Juice Shop (G&J) project taught me how to analyze network vulnerabilities in detail and develop a comprehensive plan for assessment. The subsequent **Results and Executive Summary assignment** helped me communicate technical findings to non-technical

stakeholders effectively. These tasks, though challenging, provided invaluable insights into the practicalities of network security.

The formative activities, such as the **Literature Review Activity** (Appendix 1) in Unit 2 and the **Scanning Activity** (Appendix 2) in Unit 3, provided a step-by-step approach to performing the vulnerability assessment for G&J. They also enhanced my technical skills for scanning and auditing and my understanding of compliance requirements, such as the General Data Protection Regulation (GDPR) and Web Content Accessibility Guidelines (WCAG). Before these activities and assignments, I was not aware of the accessibility requirements mentioned in WCAG. Now, it has become a practice for me when maintaining my e-portfolio during my MSc Computer Science journey.

This module also enhanced my awareness of ethical issues in vulnerability disclosure and the use of ethical hacking, emphasizing the importance of responsibility and accountability in all security practices.

Feedback from peers and tutors was crucial, enhancing my critical thinking and understanding of contemporary network security challenges. Collaborative discussions, such as those on the digital economy and log4j vulnerabilities, broadened my perspective. Tutor critiques on assignments refined my analytical and communication skills, improving my work quality.

Professional Skills Matrix and Action Plan (PDP)

All the professional skills I have gained, such as conducting network vulnerability assessments with various tools, drafting assessment reports and executive summaries, and understanding GDPR and WCAG, are invaluable. Specifically, GDPR compliance is directly transferable to real-world scenarios in my current role as Data Protection Officer, where I can implement the strategies and tools learned during this module. The knowledge of how to issue an assessment report makes it easier to facilitate communication between stakeholders and technical teams.

<u>Professional Skills Matrix</u>

Level of competence (Rewo, 2024)

◯	No Competence	◑	High Competence
◔	Low Competence	●	Expert
◐	Some Competence	⊗	Not relevant

Skills	Detail	Competence	Evidence
Time Management	Managing time to meet deadlines and balance workload.	◔	Successfully completed assignments on time during staggered module periods.
Critical Thinking and Analysis	Evaluating information to make well-informed decisions and solve problems	◐	Applied critical thinking in project evaluations and literature reviews.

Communication and Literacy Skills	Discussion and idea presentation		Participated in collaborative discussions, created a baseline analysis and plan, and issued an executive summary report.
IT and Digital	Discover various scanning tools and platforms		Used Burp Suite and other tools to complete the scanning activity.
Research	Conducting literature reviews and applying findings		Conducted vulnerability analysis literature review for assignments.
Interpersonal	Reflecting on experiences to identify strengths, weaknesses, and areas for improvement		Record all artifacts in the e-portfolio with reflections and learning outcomes.
Problem-Solving	Developing and implementing effective strategies to resolve issues		Looked for alternative solutions when the existing resource could not complete the activity requirement.

Ethical Awareness	Reflecting on ethical implications of security practices		Studied GDPR and WCAG, which enhanced my awareness of data protection and the importance of accessibility for websites.

Action Plan

Moving forward, I aim to continue enhancing my skills in network security by:

- Engaging with Advanced Topics: Exploring advanced topics in network security and data protection.

- Practical Application: Applying the knowledge gained to my current role as Data Protection Officer.

- Continuous Learning: Staying updated with the latest tools and techniques in network security through continuous education and professional development.

- Ethical Practices: Implementing ethical considerations and best practices in all security-related projects.

Conclusion

In conclusion, this module has had a profound impact on my professional and personal development during my Network Security journey. It has enriched my understanding of network vulnerabilities, ethical hacking, and compliance requirements, significantly enhancing my technical and analytical skills. The assignments and activities provided

practical insights, particularly in vulnerability assessment and effective communication with stakeholders. Moving forward, I am committed to applying this knowledge in my role as a Data Protection Officer and continuing my professional development in network security, ensuring that ethical considerations remain at the forefront of my practices.

References

Di Silvestro, F. & Nadir, H. (2021) The Power of ePortfolio Development to Foster Reflective and Deeper Learning in an Online Graduate Adult Education Program. *Adult Learning* 32(4):154-164.

Rewo. (2024) What is a skills matrix. Available from: https://www.rewo.io/skills-matrix-for-manufacturing/ [Accessed 8 June 2024].

University of Essex Online. (2024) *University of Essex Online Writing Guide Series – A short guide to Reflective Writing.* Essex: University of Essex Online.

Appendix 1 Literature Review Activity

Vulnerability Analysis – Literature Review Activity

Introduction

This activity conducts the literature review as preparation for the Assignment 1 "Vulnerability Audit and Assessment - Baseline Analysis and Plan" on Gin & Juice Shop Ecommerce.

Identified Vulnerabilities

Based on a literature search, the following potential vulnerabilities were identified for the Gin & Juice Shop website:
Sources: OWASP Top 10, CWE List.

1. **Broken Access Control (CWE-200, CWE-284):**
   - Unauthorized access and information disclosure.

2. **Cryptographic Failures (CWE-259, CWE-327, CWE-331):**
   - Exposure of sensitive information.

3. **Injection (CWE-73, CWE-79, CWE-89):**
   - Execution of malicious commands or scripts.

4. **Insecure Design (CWE-209, CWE-256, CWE-501, CWE-522):**
   - Poor security control design leading to vulnerabilities.

5. **Security Misconfiguration (CWE-16, CWE-611):**
   - Improper security settings causing information exposure.

6. **Vulnerable and Outdated Components (CWE-1104):**
   - Exploitation of known vulnerabilities in third-party components.

7. **Identification and Authentication Failures (CWE-287, CWE-297, CWE-384):**
   - Unauthorized access.

8. **Software and Data Integrity Failures (CWE-494, CWE-502, CWE-829):**
   - Attacks on software updates, data integrity, and insecure deserialization.

9. **Security Logging and Monitoring Failures (CWE-117, CWE-223, CWE-532, CWE-778):**
   - Delayed incident detection.

10. **Cross-Site Request Forgery (CSRF) and Server-Side Request Forgery (SSRF) (CWE-352, CWE-918):**
    - Unauthorized actions on authenticated users and unauthorized access to other systems.

Appendix 2 Scanning Activity

Scanning Activity

Introduction

This activity conducts the basic scan using standard tools such as Traceroute / Tracert and Nslookup as preparation for the Assignment 2 "Vulnerability Audit and Assessment - Results and Executive Summary" on Gin & Juice Shop Ecommerce.

Scanning Output

Tracert (Windows)

Nslookup