My e-Portfolio's URL: https://kalina94.github.io/e-Portfolio/

e-Portfolio Documentation
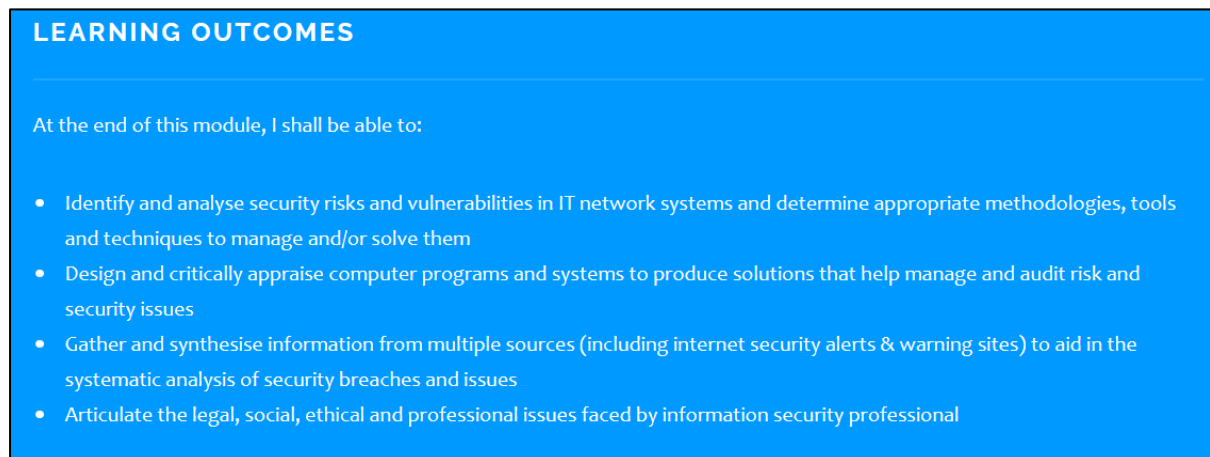
Table of Contents

My e-Portfolio's URL:

My e-Portfolio showcases the knowledge and skills I gained in the Network and Information Security Management program. The following are the different sections featured in the e-Portfolio:

Section 1 - Learning Outcomes

The learning outcomes at the end of the module are listed in this section as being enable me to:

- Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them.
- Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues.
- Gather and synthesise information from multiple sources (including internet security alerts & warning sites) to aid in the systematic analysis of security breaches and issues.
- Articulate the legal, social, ethical and professional issues faced by information security professional.

Taken from the e-Portfolio, *figure 1* shows the above-mentioned learning outcomes.

LEARNING OUTCOMES

At the end of this module, I shall be able to:

- Identify and analyse security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and/or solve them
- Design and critically appraise computer programs and systems to produce solutions that help manage and audit risk and security issues
- Gather and synthesise information from multiple sources (including internet security alerts & warning sites) to aid in the systematic analysis of security breaches and issues
- Articulate the legal, social, ethical and professional issues faced by information security professional

Figure 1 - Learning Objectives

My e-Portfolio's URL: https://kalina94.github.io/e-Portfolio/

Section 2 - Artefacts

ARTEFACTS

The continuous module assignment includes:

1. Development Team Project: Design Document
2. Development Team Project: Executive Summary
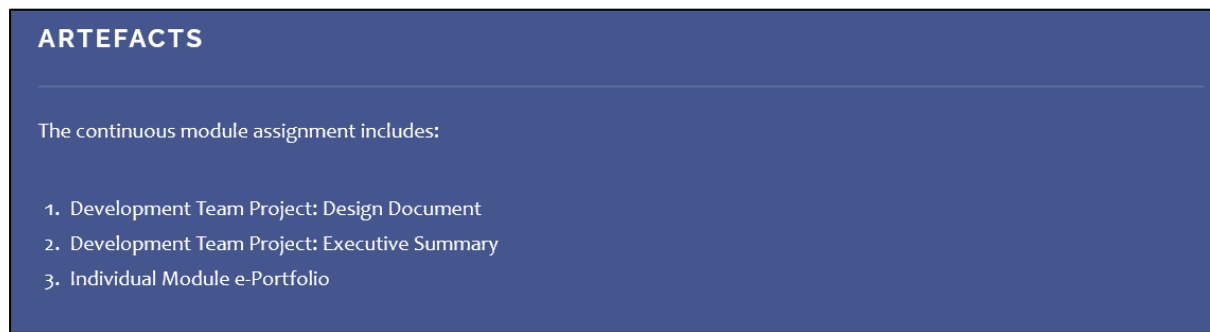3. Individual Module e-Portfolio

Figure 2 - Artefacts

Figure 2 depicts the module's summative evaluations, which comprise a group-work design document and executive summary, as well as an individual assignment. The specifics of each module's assignment are shown below.

1. Design Document

To begin this project, we created a design document that highlights the business benefits of what our team would be doing. Our team agreed to do penetration testing on a website designated as a *"e-health site"* that provides registrants with medical and fitness information and advice provided by medical professionals, as required by the first portion of the project. As a result, our eHealth site delivers medical and fitness information and assistance from medical experts to registrants, potentially enhancing the health of individuals living in rural and distant locations, according to the design document. Further, current eHealth website using the threat assessments methodologies such as STRIDE, PASTA, and TRIKE were examined, and the STRIDE methodology was chosen owing to its ease and speed of implementation. Similarly, the penetration testing tools Nmap, Nessus, ZAP, Nikto, Skipfish, Metasploit, LinPEAS, Slowloris, and LOIC were recognized and listed. The design document also included information on the commercial implications of using certain tools and methodologies, as well as our project timetable, which was subsequently implemented. A snapshot of the assignment's presentation from the e-portfolio is shown below.

My e-Portfolio's URL: https://kalina94.github.io/e-Portfolio/

DESIGN DOCUMENT

Our team was expected to evaluate the website provided by our opposite team who will provide the URL, IP address and agree access times.

Checklist for the assignment:
✓ List of security challenge
✓ Tools you will use
✓ Methodology - Selection & Discussion
✓ Limitations and assumptions
✓ Applicable citations and references

→ Design Document

FEEDBACK OBTAINED

A good report, well thought out and well supported by references and diagrams. As a development point consider adding both design patterns as well as anti-patterns to avoid – it can make development easier. Also, good attention to punctuation, defining abbreviations and referencing.

Figure 3 - Design Document

2. Executive Summary

Finally, we had to create an executive summary as a group that summarized our results, recommendations, and conclusions. We presented our executive summary by stating briefly about the, introduction to penetration testing on our eHealth website; applied methodology; sequence of applied tools; list of security issues, findings, including an assessment of how well the business meets its GDPR requirements, and summary of the conclusions and recommendations. A screenshot of the assignment's presentation from the e-portfolio is shown in *figure 4*.

EXECUTIVE SUMMARY

Our team was expected to produce an executive summary that pulls together your findings, recommendations and conclusions in a clear and unambiguous format.

Checklist for the assignment:
✓ A brief summary of the work carried out
✓ Summary findings – presented in an easy to understand, non-technical manner
✓ A section that evaluates the website against two security standards – one of which must be the GDPR directive
✓ Conclusions – with justifications
✓ Recommendations – with justifications, ordered by business priority

→ Executive Summary

FEEDBACK OBTAINED

X Feedback not yet obtained for this assignment

Figure 4 - Executive Summary

My e-Portfolio's URL: https://kalina94.github.io/e-Portfolio/

3. Individual Module e-Portfolio

This module's final evaluation is an e-portfolio that compiles all of the evidence of my work in the module. As part of the professional development element of the module, the portfolio's goal is to include the following:

- Summary of learning outcomes
- Team meeting notes
- Feedback from peers and tutors
- Professional Skills Matrix and action plan
- Other artefacts developed during the module

The presentation of the assignment on the e-portfolio website is seen below in *figure 5*.

INDIVIDUAL MODULE E-PORTFOLION

The final assessment in this module is an e-portfolio that collates all the evidence of your work in this module.

The e-portfolio should consist of:
✓ All artefacts (designs etc) demonstrating development over the duration of the module
✓ The output of the scanning and analysis tools, answers to and outputs from exercises carried out during the module, including your individual contributions to the projects.
✓ Your evaluation of the final project (Unit 11) vs. the design proposal (Unit 6).
✓ Your analysis of the data gathered, as well as your contributions to the discussion forums, showing your analytical skills.
✓ Reflections on your individual contributions and the teamwork process.
✓ A reflection of the Network and Information Security Management process based on your learnings in this module, as well as your experience as a member of a development team.

→ Individual Reflection

FEEDBACK OBTAINED

X Feedback not yet obtained for this assignment

Figure 5 - Individual Module e-Portfolio

My e-Portfolio's URL:

Section 3 - Additional Activities

ADDITIONAL ACTIVITIES

COLLABORATIVE DISCUSSION SUMMARY

As part of a software development initiative, the collaborative discussion identified and managed security threats. It also conducted a critical analysis of implementation issues in order to identify the best methodologies, methods, and strategies for resolving them.

> LEARN MORE

PENENTRATION TESTING

Evaluated the website provided by the development team. The pen-testing a report has:

- *details of possible security vulnerabilities*
- *a list of standards appropriate to their business and any non-compliance against those standards, and*
- *a summary of recommendations and potential mitigations that could be used to ameliorate any risks and comply with given standards and guidelines for the specified industry.*

> PENETRATION TESTING REPORT

Figure 6 - Additional Module Activities

This section displays the formative evaluation in which I engaged throughout the course of this module in order to enhance my knowledge. The collaborative conversations are the major formative assessment that I covered. *Figure 6* is a screenshot from my e-portfolio that shows my involvement in the formative evaluations discussed above together with the pen-tests performed on the website.

The penetration testing, I did on the tools I was assigned to, as well as the results, are listed below.

--**Penetration Testing Starts**--

NMap

- Kali Command to scan website IP Address:

    $nmap 18.168.216.191

My e-Portfolio's URL: https://kalina94.github.io/e-Portfolio/

Figure 7 - Nmap outcome 1

- Kali Command to scan website URL:

$nmap www.123easyinvite.com

Figure 8 - Nmap outcome 2

Interpretation:

The NMap scanning was completed in 14.45s - 14.57s as per above screenshots. The NMap scanning result gives us a quick overview of the host. From the scan, we can see the 2 ports (22 and 80) of the host, being opened.

SkipFish

- Kali Command to scan website IP Address:

$skipfish -o 202 http://www.123easyinvite.com

My e-Portfolio's URL: https://kalina94.github.io/e-Portfolio/

Figure 9 - Skipfish outcome 1

Figure 10 - Skipfish outcome 2

Interpretation:

The SkipFish scanning was completed in 106s as per above screenshots. This clearly demonstrate its greater consumption time that the NMap scan. The SkipFish scanning result gives us a detailed explanation about the vulnerabilities. Also, they are visually categories by their risk level, where the *'External content embedded on a page'* vulnerability has the higher risk.

ZAP

- Open the ZAP application and enter the URL for automated scan
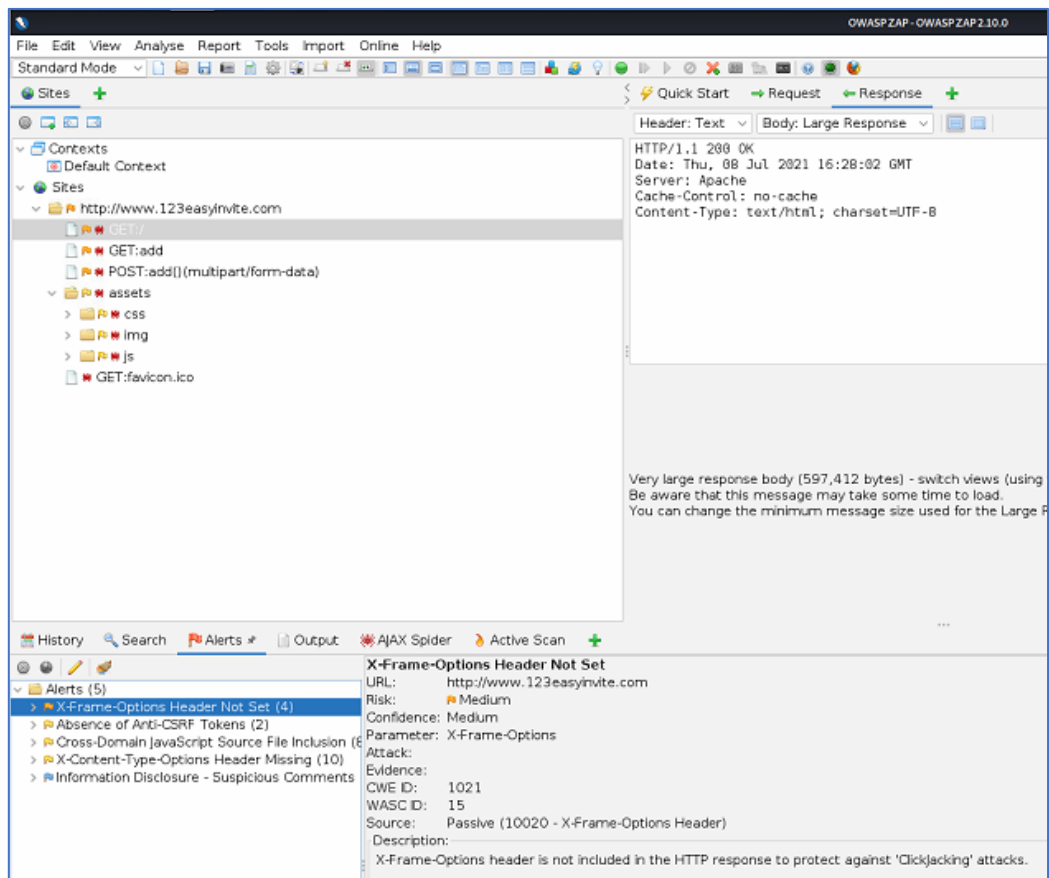
Figure 11 - ZAP outcome 1

My e-Portfolio's URL: https://kalina94.github.io/e-Portfolio/
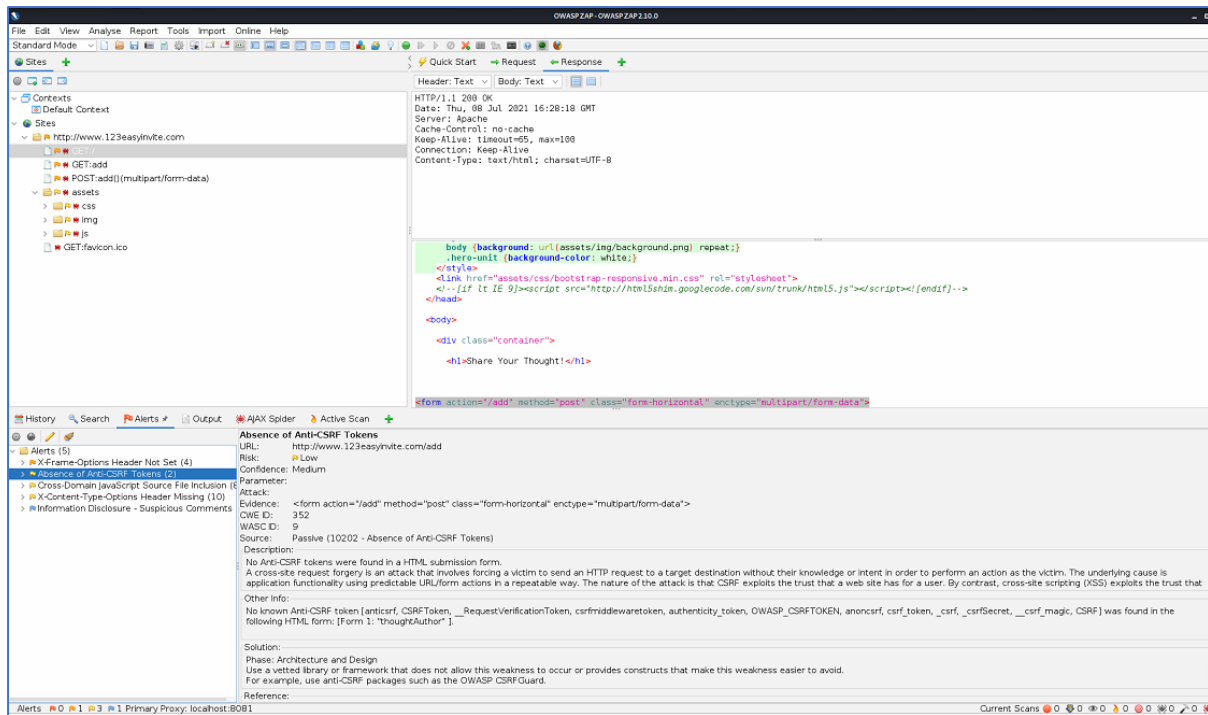
Figure 12 - ZAP outcome 2

Interpretation:

The ZAP scanning result lists down the alerts and gives us detailed information about the responses of the spider attacks to the URL, as demonstrated in the above screenshots. Similarly, to the SkipFish scanner, the alerts are visually categories by their level. The ZAP scanning also provides the solution of each alert.

Nikto

- Kali Command to scan website IP Address:

  $nikto -h www.123easyinvite.com
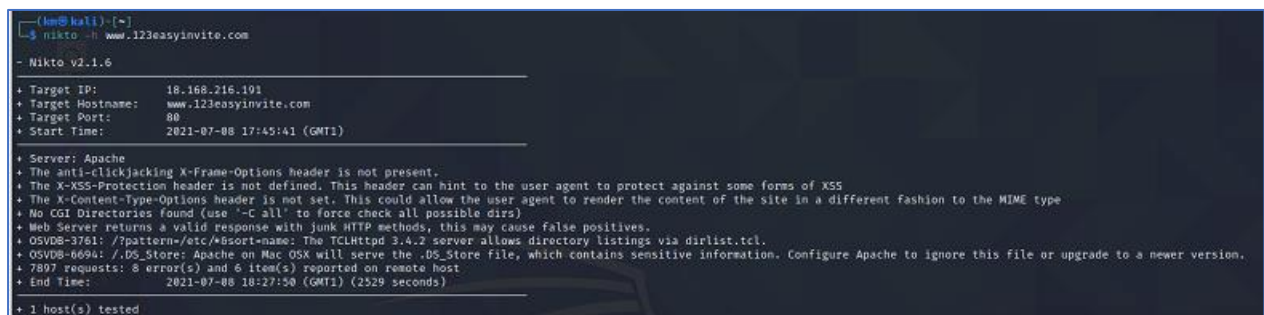
Figure 13 - Nikto outcome

My e-Portfolio's URL: https://kalina94.github.io/e-Portfolio/

Interpretation:

The Nikto scanning was completed in 2529s as per above screenshots. This clearly demonstrate its greater consumption time that the three above-mentioned scanners. The Nikto scanning result gives us information about the server, port, IP Address of the target URL.

--**Penetration Testing Ends**--

Section 4 – Reflections

Based on my knowledge gained in this module and my experience as a member of a development team, this section elaborates on my individual contributions and the collaboration process, as well as the Network and Information Security Management process. *Figure 7* shows how the reflective essay is shown in the e-portfolio.
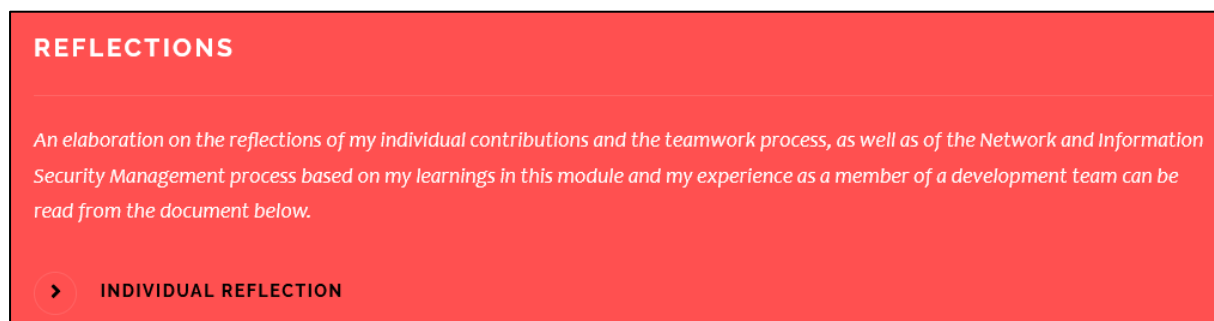
Figure 14 - Reflection

The whole reflective piece, however, may be viewed below.

--**Reflection starts**--

Our team was tasked with doing Penetration Testing in order to discover and analyze security risks and vulnerabilities on a website for the Network and Information Security Management module. The Design Document and the Executive Summary were the two components of the project. Marzio, Sebastian, Shoumik, and I were the members of our team.

However, we interacted with each other over WhatsApp as normal because we had already worked together. We agreed to keep the meetings at a particular time to be equal to each other and to discuss the project's tasks and progress on a frequent basis because Shoumik is from a different time zone. We shared our knowledge and technological talents with Shoumik to become friends, and we concluded the contract agreement at our first Google Meet meeting.

Subsequently, following our introductory meeting each team member was assigned an individual job to analyse the different proposed websites from the assignment, as well as their relevant business purpose. As a result, we were able to agree on the "e-health site that provides registrants with medical and fitness information and guidance, provided by medical professionals" as our assignment's chosen website. Our system's role and goal are to save personal information about the registrant's health and to provide medical experts with information.

Additionally, after the website was picked, we each had our own section of the Build Proposal Report to complete, and my task was to create a background summary of our eHealth website as well as design the project schedule Gantt chart. As a consequence, I looked at the existing host system, databases, and development platform, as well as any other needs that existing eHealth websites had. Figure 8 and figure 9 shows my contribution to the Design Document.

Background

Project Overview

The E-Health site provides medical and fitness information and guidance from medical specialists to registrants, potentially improving the health of those living in rural and remote areas. Within the scope of the penetration test project, a complete list of potential threats and vulnerabilities of the organisation's E-Health site and appropriate remediation plans will be provided.

Project assumptions

- Single Host System
- Database: MySQL
- Development Platform: PHP
- Currently running on a UAT environment
- UK-based system: adhere to GDPR and the Data Protection Act
- BCM/DR is absent
- The system saves personal information on the registrant's health and provides information from medical professionals
- The testing is done using VDI provided by the healthcare authority

Figure 15 - Individual Contribution for Design Document – Background

Timeline

Figure 5 depicts the timeline of the individual project phases: design documentation, penetration testing and the final executive summary.
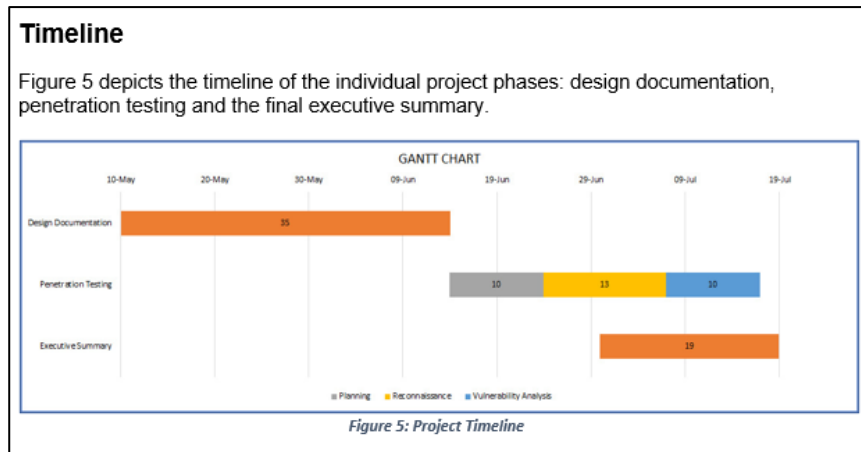
Figure 5: Project Timeline

Figure 16 - Individual Contribution for Design Document – Gantt Chart

Following the submission of the Design Document, we launched the penetration testing using the tools indicated in our Design Document, as per the project timeline. Similarly, the penetration testing phase was distributed among the team members, with Shoumik and myself assigned to NMap, Nikto, Skipfish, and ZAP. The penetration-tests done on each of the above-mentioned tools, as well as their interpretations, are shown in Figure 10.

Figure 17 - Penetration Testing
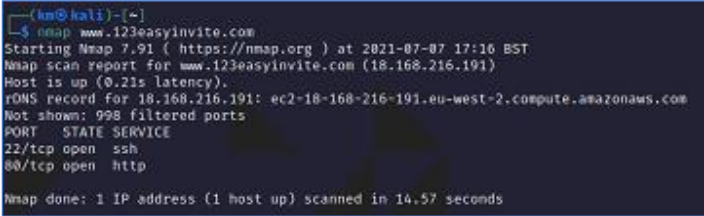
In the meantime, we began working on the executive summary for our project and kept track of its development. My job for the executive summary piece was to write about GDPR directives and show how GDPR rules were implemented to our eHealth website. This task gave me the opportunity to put my analytical thinking abilities to use in a collaborative setting. Because I finished my allocated work ahead of schedule, I was able to contribute even more to the project by taking on the responsibility of writing the analysis of the DREAD technique for threat assessment. I could picture myself honing my entrepreneurial abilities by taking charge of this. My contribution to the Executive Summary paper is represented in Figure 11 and Figure 12.

a. General Data Protection Regulation (GDPR)

The GDPR significantly altered how personal data must be legitimately processed. The E-Health industry is notably impacted by the new legislation, which establishes even tougher restrictions for so-called "special categories" of personal data, including all genetic, biometric, and health data (Burgess, 2020). As a result, under the new data protection legislation, the whole E-Health industry is crucial, and legal requirements must be thoroughly assessed.

Moreover, data processing in the E-Health sector includes data collection, organisation, and deletion. Our application aims to gather patient data and publish it on the website as medical history for doctors to review. Thus, every entity that handles personal data must verify that they comply with the GDPR's standards. The GDPR's primary obligations are as follows:

? Use of personal data in accordance with standards of integrity. Processing, for example, must have a specific function. As a result, one cannot gather personal information "just in case". Patients, in other words, have a right to know how their data is used and a say in the process.

? Breached personal data must be notified within 72 hours. If sensitive data, such as health history, is lost, it must be notified to the authorities and each affected individual within 72 hours (Burgess, 2020).

The following checklist outlines the application's objectives in relation to the GDPR directive's regulations (Burgess, 2020).

- The privacy policy includes detailed information on data processing and its legal implications.
- Users are informed about why and how their data is collected. It is explained to them how the data is processed, who has access to it, and how it is safeguarded.
- Data Subject and authorities are notified in the case of a data breach.
- In case of alteration of patient data, the supervisory authority in the jurisdiction is notified within 72 hours to prevent incorrect diagnosis of the patient.

In a nutshell, GDPR highlights the need for safeguarding the security of personal data processing at early stages as stated in Article 35 of the GDPR as "prior to the processing, carry out an assessment of the impact of envisaged processing operations on the protection of personal data" (IT Governance Ltd, 2017: 3) .

Figure 18 - Individual Contribution for Executive summary – GDPR

As a foundation, the extended CIA triad was used to evaluate the project's conformity to security. STRIDE was applied to identify potential threats. For the evaluation, a DREAD analysis was conducted to triage identified threats and rate them on an ordinal scale.

Due to the current circumstances and travel restrictions, the project's penetration testing scope had to be confined to an off-shore model. The team could not conduct the testing from within the company's location and instead ran a full suite of tests through the external network. This made the testing of certain attack vectors, such as a local area network Man-in-the-Middle (MITM) attack, impossible. Instead, the focus was shifted towards the security of the web application itself.

Figure 19 - Individual Contribution for Executive summary – DREAD methodology

Consequently, by participating in both the design document and the executive summary report has been really beneficial to me since it has allowed me to put some of the skills, I've learned in prior units to use. For instance, during discussions on the design document, I might take the initiative and lead the project by specifying the stages to be taken. In addition, I was able to comprehend the process of demonstrating several key security concepts including vulnerability assessments, penetration testing, forensic analysis, and breach management, which include:

- *Identifying and analysing security risks and vulnerabilities in IT network systems and determine appropriate methodologies, tools and techniques to manage and solve them.*

- *Designing and critically appraising computer programs and systems to produce solutions that help manage and audit risk and security issues.*

- *Gathering and synthesising information from multiple to aid in the systematic analysis of security breaches and issues.*

- *Articulating the legal, social, ethical and professional issues faced by information security professionals.*

Now I would want to focus on our team's strengths, which include being extremely communicative, well-organized, and considerate of each other's personal and professional obligations. And we completed our given work on schedule, demonstrating each individual's dedication to the project's success. Moreover, the positive feedback we received for the Design Document, which described it as "excellent demonstration of knowledge application and excellent presentation, well structured," encouraged our team to strive for greater heights and indicated that we had finally grasped the module's objectives. On the other side,

the main problem in the own team's report was that it was presented in an unstructured manner, as indicated by prior report comments that some parts were misplaced in the report, was finally cleared (Network Security for University, 2020).

Eventually, I will undoubtedly utilize the same organized method for future team development projects, which will allow myself and other team members to better monitor and comprehend the project's progress. his project has also helped me completely grasp the fundamental concepts of Network and Information Security Management methods, such as providing crucial justifications for particular actions or results to a varied audience. After completing this lesson, I am confident in my abilities to use the security vulnerability and assessment tools at my business. Rather, I will be able to help my co-workers by putting the abilities I have learned in this subject to use (Example Reflective Essay using Rolfe Reflective Model, 2021).

References

UKEssays.com. 2021. Example Reflective Essay using Rolfe Reflective Model. [online] Available at: <https://www.ukessays.com/essays/nursing/rolfe-reflective-model.php>.

UKEssays.com. 2020. Network Security for University. [online] Available at: <https://www.ukessays.com/essays/information-technology/network-security-for-university.php> [Accessed 22 July 2021].

---Reflection ends---

Section 5 - Team Meeting Notes

Figure 20 - Team Meeting Notes

This section depicts all of the meetings that were held for this module in order to complete the group tasks. As I indicated in my reflective essay, the team meeting notes might eventually reveal our team's organizational strength. *Figure 13* shows that after each meeting, each member was assigned a task to ensure that everyone participated equally in the group assignment.

Section 6 - Professional skills matrix and action plan

PROFESSIONAL SKILLS MATRIX AND ACTION PLAN

→ PROFESSIONAL SKILLS MATRIX

Skills	Level	Evidence
Time management	🟢	Define objectives and provide regular progress status
Resilience	🟠	Committed, patient and self-efficacity
Critical thinking and analysis	🟢	Recognise, build and appraise arguments
Problem-solving	🟢	Active listener and provide creative solution
Communication and Literacy skills	🟠	Show respect towards others, clarity and concision
IT and Digital	🟠	Problem-solver and model safe, legal, and ethical behavior when using technology
Interpersonal	🟠	Collaborative and clear communication skills
Team/Global Citizen & Leadership	🟢	Accept challenges and take learning into real world
Emotional Intelligence	🟢	Use active listening skills
Entrepreneurial	🔵	Creative
Critical Reflection	🟢	Use analytical thinking skills

Key Skills Level

Expert	🟠
Proficiency	🟢
Trainned	🔵
Aware	🟡

→ ACTION PLAN

What do I want to learn?	What I have to do to achieve this?	What resources support I need?	How do I measure success?	Target dates for review and completion?
Persuasion skill	To influence others to achieve the goals and objectives.	• To have high self-esteem and good emotional intelligence • Good listening skills • Motivated	Team members believing in my planning for the project	End of this module
Entrepreneurial skill	Developing my business management skills by building up my ability to multitask and delegate responsibilities to subordinates	• Leadership skills • Feedback from teammates and other colleagues	Helping co-workers develop strategies that keep them organized and on task	End of next module

Figure 21 - Professional Skills Matrix and Action Plan

This part demonstrates my professional skill level in relation to the learning goals of this module. As can be seen in *Figure 14*, my entrepreneurial talent is at a lower level, thus it is the action plan's considered skill. My action plan, on the other hand, consists of the abilities I hope to gain throughout my Master's degree and then use in my working life. Because my

employer, ICPS, has been missing leaders for the previous six months, both persuasive and entrepreneurship abilities will be quite useful in my professional function.

To summarise, I believe that the usage of an e-Portfolio for the development and management of knowledge and skills is on the rise. We have now transitioned to a knowledge society and digital culture. The rise of e-Portfolios is completely in line with this trend. We employ the technology at our disposal to better serve residents and learners; as a result, we must use e-Portfolios. As a result of using the e-Portfolio for this module, an individual will have a clear understanding of the module goals and will be able to gain critical knowledge for Network and Information Security Management. To put it another way, I would be pleased if my e-portfolio could contribute to an individual's knowledge by sharing my experiences and expertise (Eportfolio As A Tool Of Learning, Presentation, Orientation And Evaluation Skills, 2015).

References

Procedia - Social and Behavioral Sciences, 2015. Eportfolio As A Tool Of Learning, Presentation, Orientation And Evaluation Skills. pp.328 – 333.

Kalina94.github.io. 2021. *Kalina Mohonee e-Portfolio*. [online] Available at: <https://kalina94.github.io/e-Portfolio/> [Accessed 24 July 2021].