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

# *e-Portfolio Documentation*

## Table of Contents

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

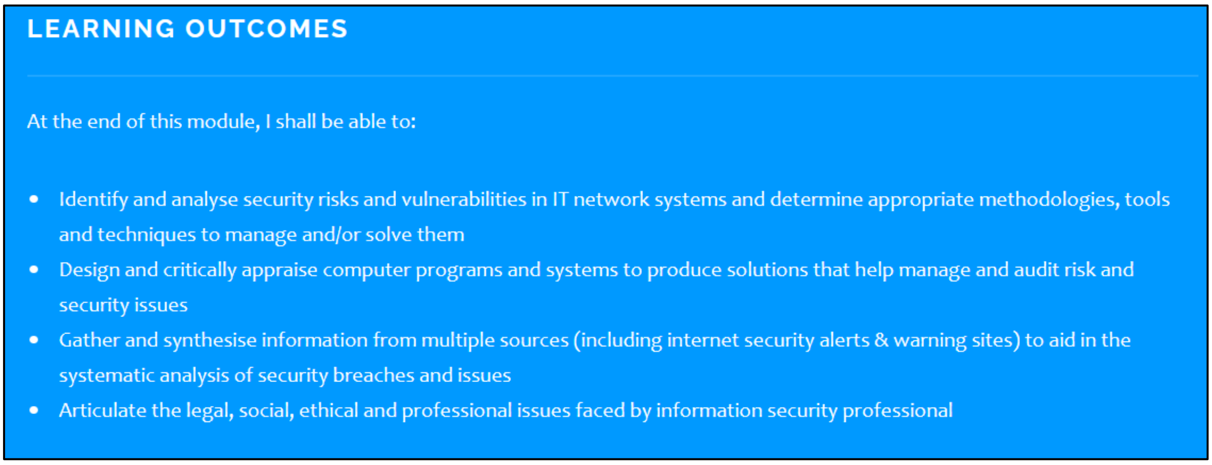
My e-Portfolio showcases the knowledge and skills I gained in the Network and Information Security Management program. The following are the different sections featured in the e-Portfolio:

## 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.



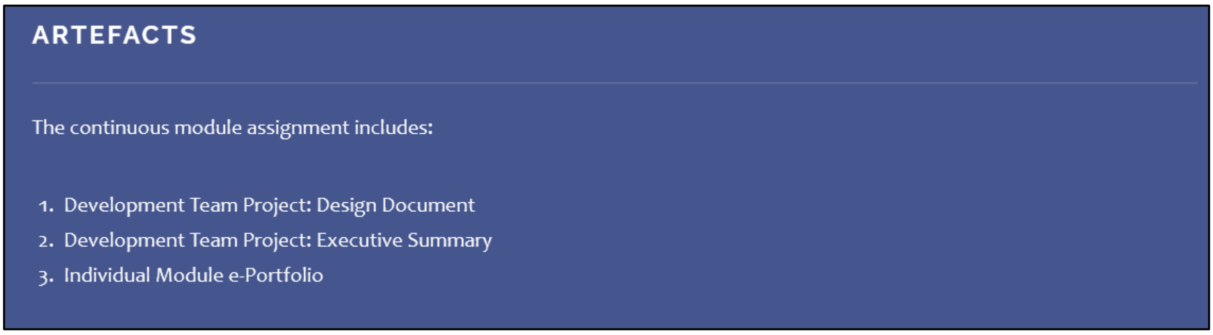
LEARNING OUTCOMES

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*

## Section 2 - Artefacts



ARTEFACTS

The continuous module assignment includes:

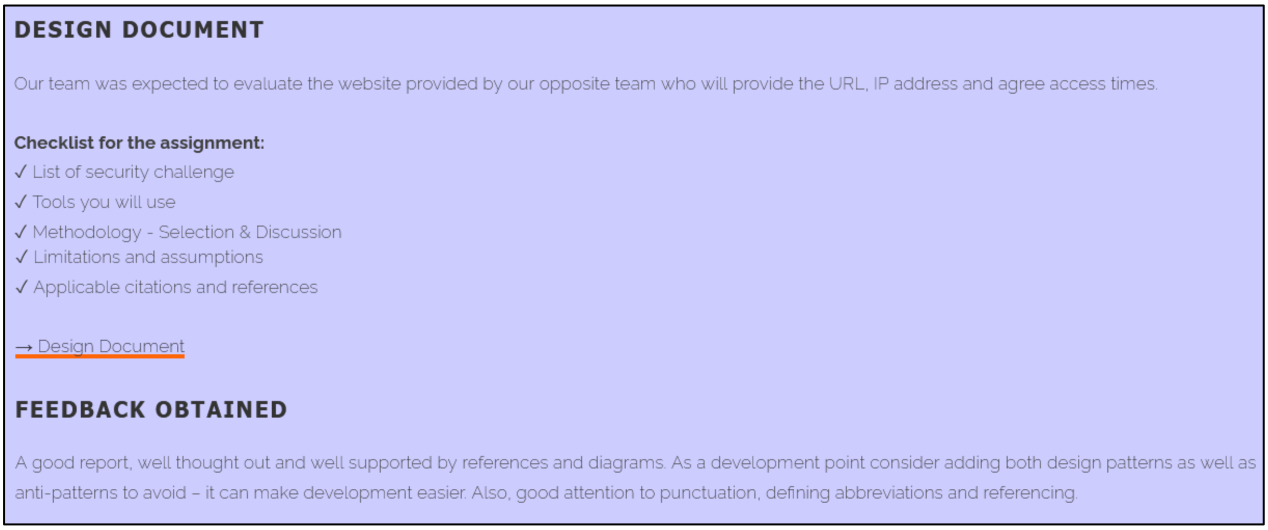
1. Development Team Project: Design Document
2. Development Team Project: Executive Summary
3. Individual Module e-Portfolio

*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. *Figure 3* shows the assignment's presentation from the 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

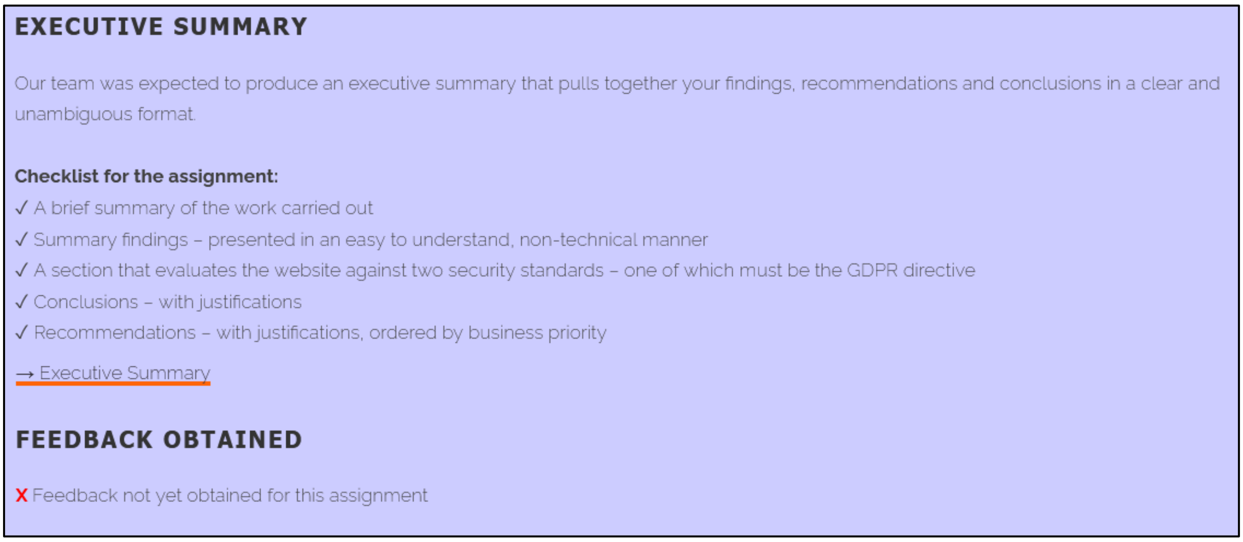
**FEEDBACK OBTAINED**

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

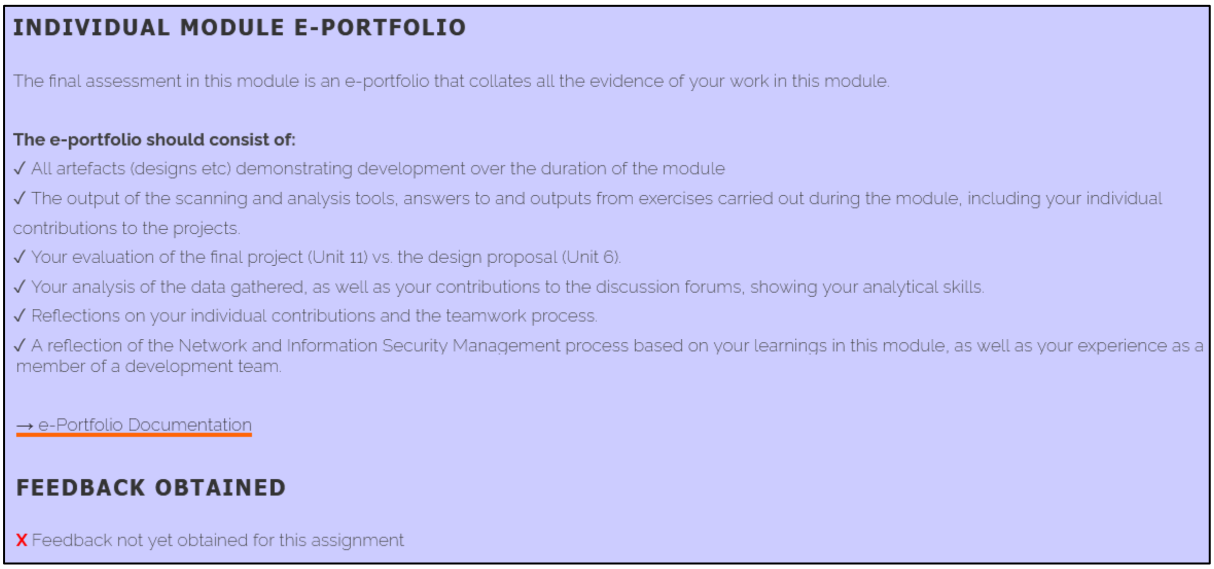
*Figure 4 - Executive Summary*

## 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-PORTFOLIO

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.

→ e-Portfolio Documentation

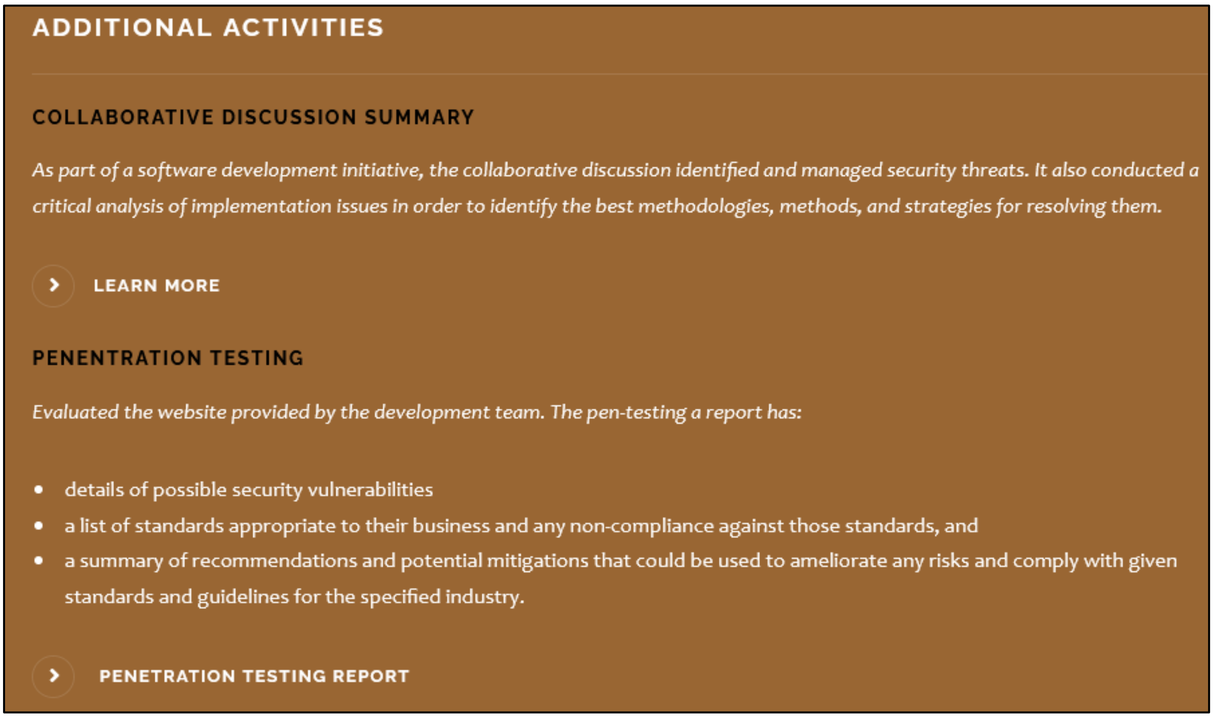
FEEDBACK OBTAINED

X Feedback not yet obtained for this assignment

*Figure 5 - Individual Module e-Portfolio*

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

## 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.*

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.

*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.

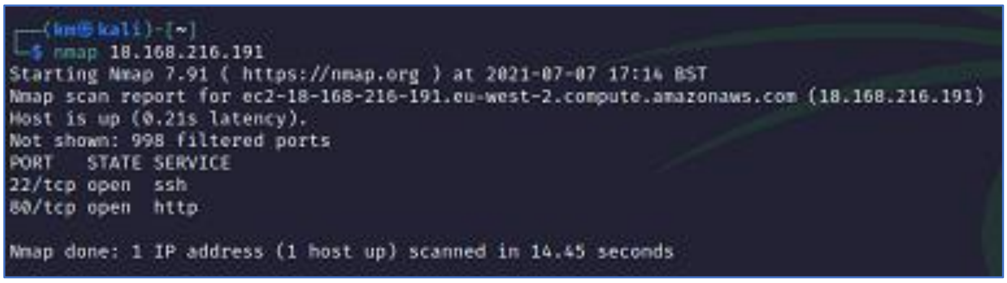
The penetration testing, I did on the tools I was assigned to, as well as the results, are listed below.

**---------------------------------------Penetration Testing Starts--------------------------------------**

**NMap**

- Kali Command to scan website IP Address:

```
$nmap 18.168.216.191
```

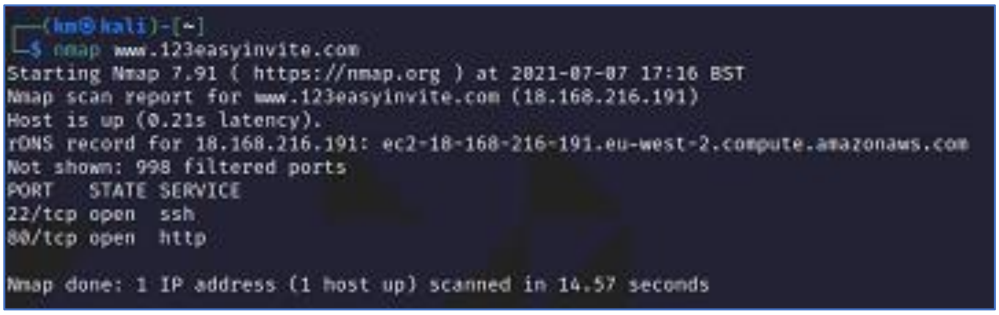


```
┌──(km㉿kali)-[~]
└─$ nmap 18.168.216.191
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-07 17:14 BST
Nmap scan report for ec2-18-168-216-191.eu-west-2.compute.amazonaws.com (18.168.216.191)
Host is up (0.21s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds
```

*Figure 7 - Nmap outcome 1*

- Kali Command to scan website URL:

$nmap www.123easyinvite.com



```
┌──(km㉿kali)-[~]
└─$ nmap www.123easyinvite.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-07 17:16 BST
Nmap scan report for www.123easyinvite.com (18.168.216.191)
Host is up (0.21s latency).
rDNS record for 18.168.216.191: ec2-18-168-216-191.eu-west-2.compute.amazonaws.com
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.57 seconds
```

*Figure 8 - Nmap outcome 2*

**Interpretation:**

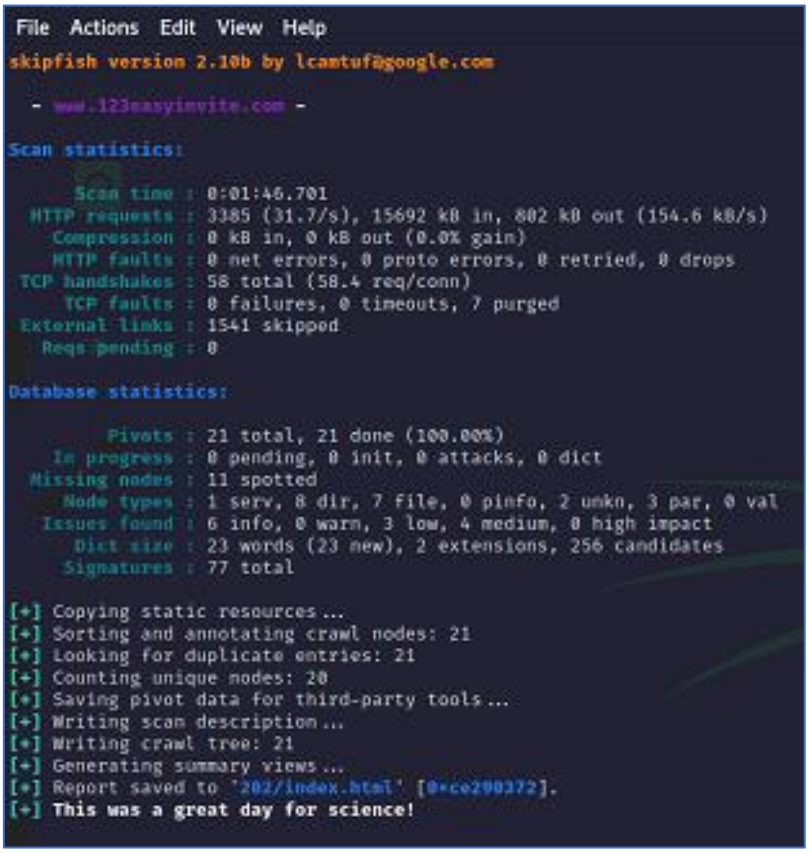
The NMap scanning was completed in 14.45s - 14.57s as per above screenshots. The NMap scanning result gives us a quick overview of the host. From the scan, we can see the 2 ports (22 and 80) of the host, being opened.

**SkipFish**

- Kali Command to scan website IP Address:

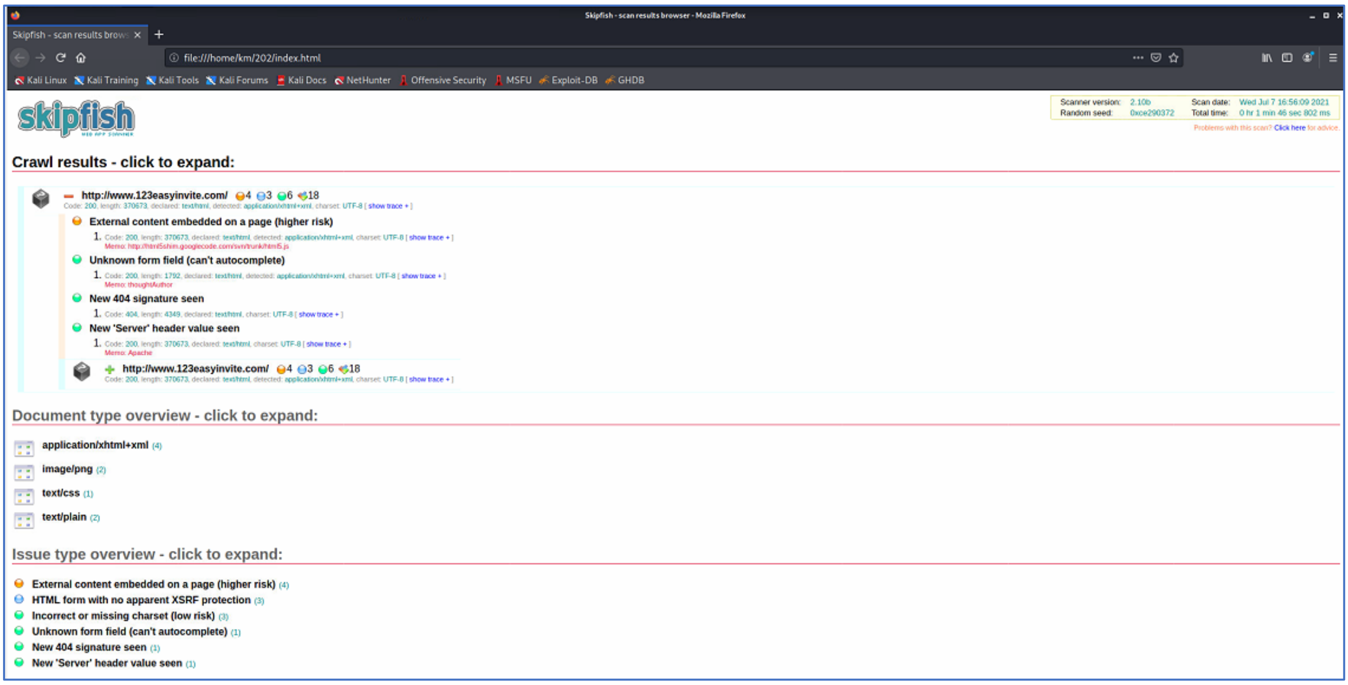
$skipfish -o 202 http://www.123easyinvite.com

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



```
skipfish version 2.10b by lcamtuf@google.com

  - www.123easyinvite.com -

Scan statistics:

      Scan time : 0:01:46.701
  HTTP requests : 3385 (31.7/s), 15692 kB in, 802 kB out (154.6 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 58 total (58.4 req/conn)
     TCP faults : 0 failures, 0 timeouts, 7 purged
 External links : 1541 skipped
   Reqs pending : 0

Database statistics:

         Pivots : 21 total, 21 done (100.00%)
    In progress : 0 pending, 0 init, 0 attacks, 0 dict
  Missing nodes : 11 spotted
     Node types : 1 serv, 8 dir, 7 file, 0 pinfo, 2 unkn, 3 par, 0 val
   Issues found : 6 info, 0 warn, 3 low, 4 medium, 0 high impact
      Dict size : 23 words (23 new), 2 extensions, 256 candidates
     Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 21
[+] Looking for duplicate entries: 21
[+] Counting unique nodes: 20
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 21
[+] Generating summary views...
[+] Report saved to '202/index.html' [0xce290372].
[+] This was a great day for science!
```

*Figure 9 - Skipfish outcome 1*



Skipfish - scan results browser - Mozilla Firefox
Skipfish - scan results brows
file:///home/km/202/index.html
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
skipfish

Scanner version: 2.10b  Scan date: Wed Jul 7 16:56:09 2021
Random seed: 0xce290372  Total time: 0 hr 1 min 46 sec 802 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

- http://www.123easyinvite.com/ 4 3 6 18
  Code: 200, length: 370673, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [ show trace + ]
  - External content embedded on a page (higher risk)
    1. Code: 200, length: 370673, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [ show trace + ]
       Memo: http://html5shim.googlecode.com/svn/trunk/html5.js
  - Unknown form field (can't autocomplete)
    1. Code: 200, length: 1792, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [ show trace + ]
       Memo: thoughtAuthor
  - New 404 signature seen
    1. Code: 404, length: 4349, declared: text/html, charset: UTF-8 [ show trace + ]
  - New 'Server' header value seen
    1. Code: 200, length: 370673, declared: text/html, charset: UTF-8 [ show trace + ]
       Memo: Apache
  - http://www.123easyinvite.com/ 4 3 6 18
    Code: 200, length: 370673, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [ show trace + ]

Document type overview - click to expand:

- application/xhtml+xml (4)
- image/png (2)
- text/css (1)
- text/plain (2)

Issue type overview - click to expand:

- External content embedded on a page (higher risk) (4)
- HTML form with no apparent XSRF protection (3)
- Incorrect or missing charset (low risk) (3)
- Unknown form field (can't autocomplete) (1)
- New 404 signature seen (1)
- New 'Server' header value seen (1)

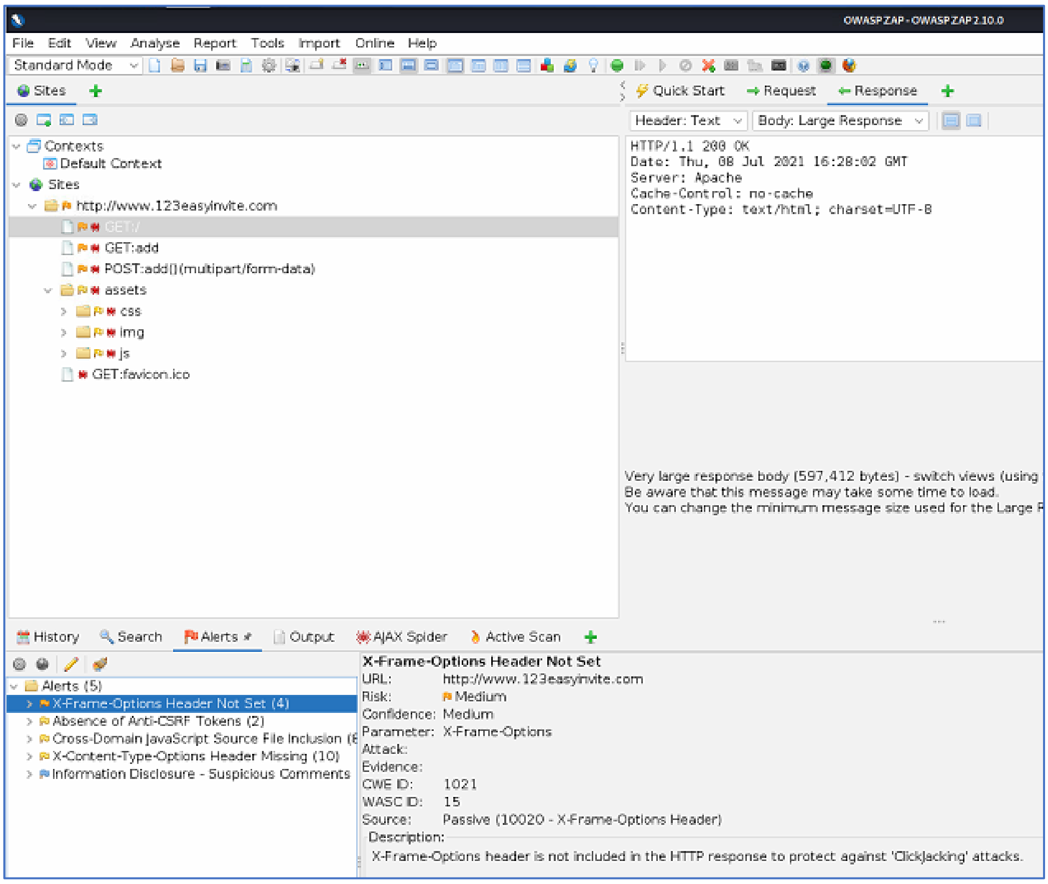
*Figure 10 - Skipfish outcome 2*

**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



```
HTTP/1.1 200 OK
Date: Thu, 08 Jul 2021 16:28:02 GMT
Server: Apache
Cache-Control: no-cache
Content-Type: text/html; charset=UTF-8
```

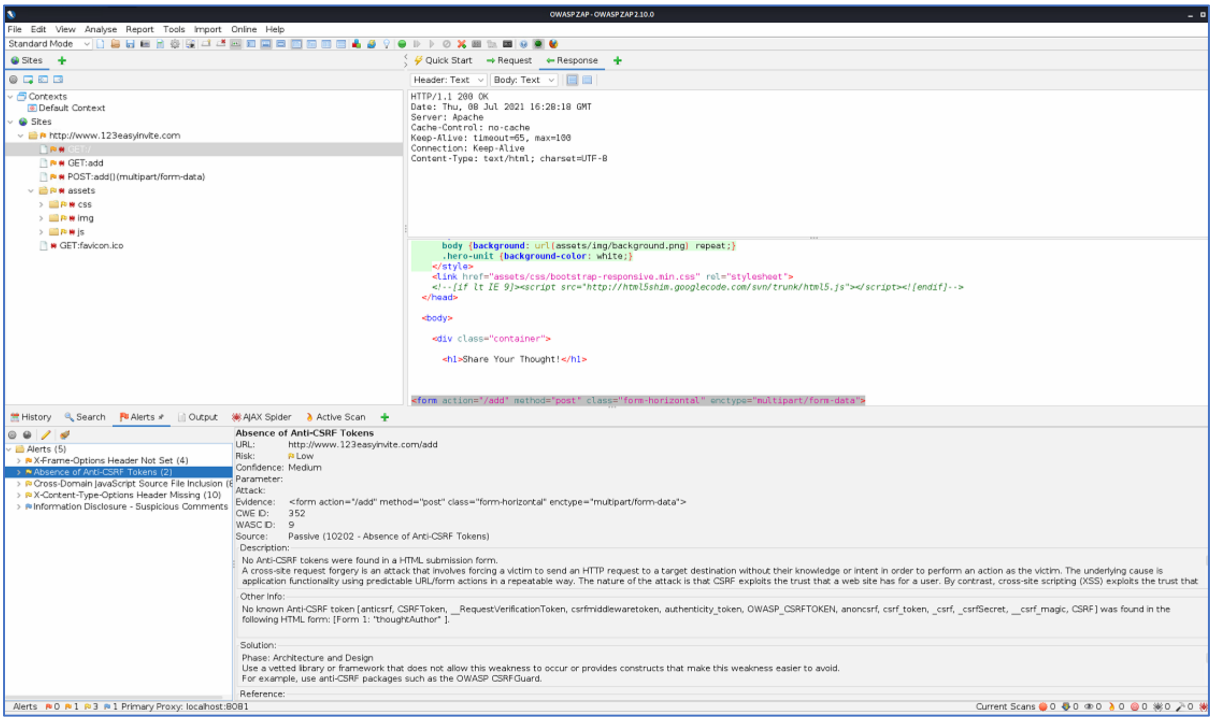
Very large response body (597,412 bytes) - switch views (using
Be aware that this message may take some time to load.
You can change the minimum message size used for the Large R

Alerts (5)
- X-Frame-Options Header Not Set (4)
- Absence of Anti-CSRF Tokens (2)
- Cross-Domain JavaScript Source File Inclusion (6
- X-Content-Type-Options Header Missing (10)
- Information Disclosure - Suspicious Comments

**X-Frame-Options Header Not Set**

URL: http://www.123easyinvite.com
Risk: Medium
Confidence: Medium
Parameter: X-Frame-Options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - X-Frame-Options Header)
Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

*Figure 11 - ZAP outcome 1*



Contexts
Default Context
Sites
http://www.123easyinvite.com
GET:/
GET:add
POST:add()(multipart/form-data)
assets
css
img
js
GET:favicon.ico

```
HTTP/1.1 200 OK
Date: Thu, 08 Jul 2021 16:28:18 GMT
Server: Apache
Cache-Control: no-cache
Keep-Alive: timeout=65, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

```
      body {background: url(assets/img/background.png) repeat;}
      .hero-unit {background-color: white;}
    </style>
    <link href="assets/css/bootstrap-responsive.min.css" rel="stylesheet">
    <!--[if lt IE 9]><script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script><![endif]-->
  </head>

  <body>

    <div class="container">

      <h1>Share Your Thought!</h1>


<form action="/add" method="post" class="form-horizontal" enctype="multipart/form-data">
```

Alerts (5)
X-Frame-Options Header Not Set (4)
Absence of Anti-CSRF Tokens (2)
Cross-Domain JavaScript Source File Inclusion (6
X-Content-Type-Options Header Missing (10)
Information Disclosure - Suspicious Comments

Absence of Anti-CSRF Tokens
URL: http://www.123easyinvite.com/add
Risk: Low
Confidence: Medium
Parameter:
Attack:
Evidence: <form action="/add" method="post" class="form-horizontal" enctype="multipart/form-data">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)

Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that

Other Info:
No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF] was found in the following HTML form: [Form 1: "thoughtAuthor" ].

Solution:
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Reference:

Alerts 0 1 3 1 Primary Proxy: localhost:8081

*Figure 12 - ZAP outcome 2*

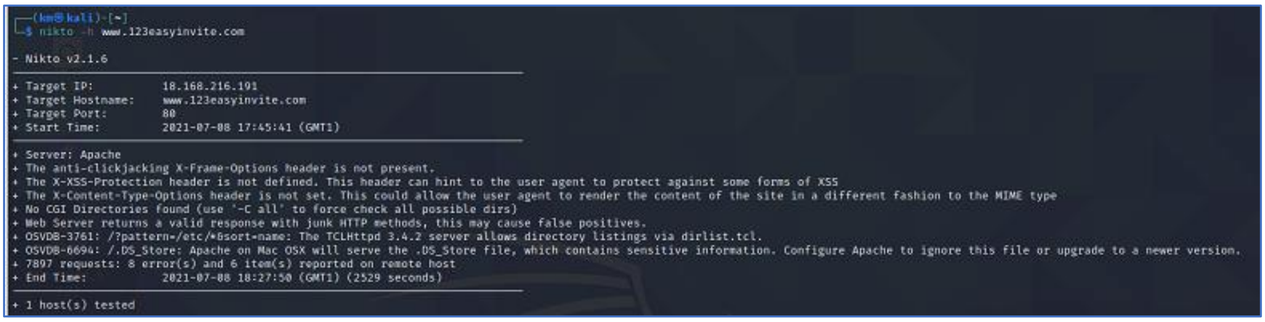
**Interpretation:**

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



```
┌──(km㉿kali)-[~]
└─$ nikto -h www.123easyinvite.com

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          18.168.216.191
+ Target Hostname:    www.123easyinvite.com
+ Target Port:        80
+ Start Time:         2021-07-08 17:45:41 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3761: /?pattern=/etc/*&sort=name: The TCLHttpd 3.4.2 server allows directory listings via dirlist.tcl.
+ OSVDB-6694: /.DS_Store: Apache on Mac OSX will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version.
+ 7897 requests: 8 error(s) and 6 item(s) reported on remote host
+ End Time:           2021-07-08 18:27:50 (GMT1) (2529 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

*Figure 13 - Nikto outcome*

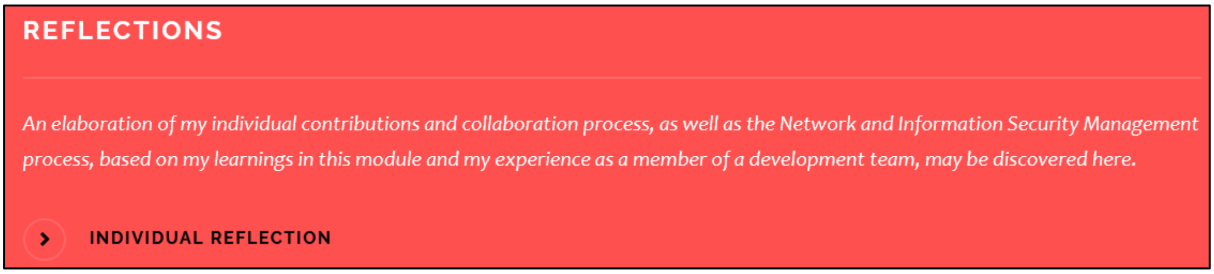
**Interpretation:**

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 14* shows how the reflective essay is shown in the e-portfolio.



REFLECTIONS

*An elaboration of my individual contributions and collaboration process, as well as the Network and Information Security Management process, based on my learnings in this module and my experience as a member of a development team, may be discovered here.*

*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 analyse 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 usual because we had already worked together. Since Shoumik is in a different time zone, we planned to maintain the meetings at a specific time so that we could be on the same page and review the project's tasks and progress on a regular base. We shared our knowledge and technological talents with Shoumik to become friends, and we concluded the contract agreement at our first Google Meet meeting.*

*Further to our introductory meeting, all team participant was given an assigned tasks to examine the various suggested websites as from project, as well as their related business objective. 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. Accordingly, I considered it relevant to engage in the first collaborative conversation, which was focused on “Compromising a Medical Mannequin,” in order to discover more about the project background for our chosen eHealth website. So, I initiated a post about the challenges faced by the Food and Drug Administration in identifying medical device failures from deliberate or malicious activities in order to get my peers’ perceptions. his has definitely helped me write the project background for the Design Document. The e-Portfolio contains a summary of the collaborative discussion (Kalina Mohonee e-Portfolio, 2021a).*

*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. My contributions to the Design Document may be accessed on the e-Portfolio (Kalina Mohonee e-Portfolio, 2021b).*

*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 carried out on each of the above-mentioned tools, as well as their interpretations may be accessed on the e-Portfolio (Kalina Mohonee e-Portfolio, 2021c).*

*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 document may be accessed on the e-Portfolio (Kalina Mohonee e-Portfolio, 2021d).*

*Consequently, 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 have 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:*

- *Finding and assessing security risks and vulnerabilities in IT network systems and considering the best approaches, tools, and strategies for managing and resolving them.*
- *Creating solutions to assist manage, audit risk and security concerns by designing and critically evaluating computer programs and systems.*
- *Obtaining and combining data from a variety of sources to help in the methodical study of security breaches and problems.*
- *Defining the legal, social, ethical, and professional problems that information security practitioners must deal with.*

*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 me and the other members to keep a better eye on the project's development. This module 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.*

*References*

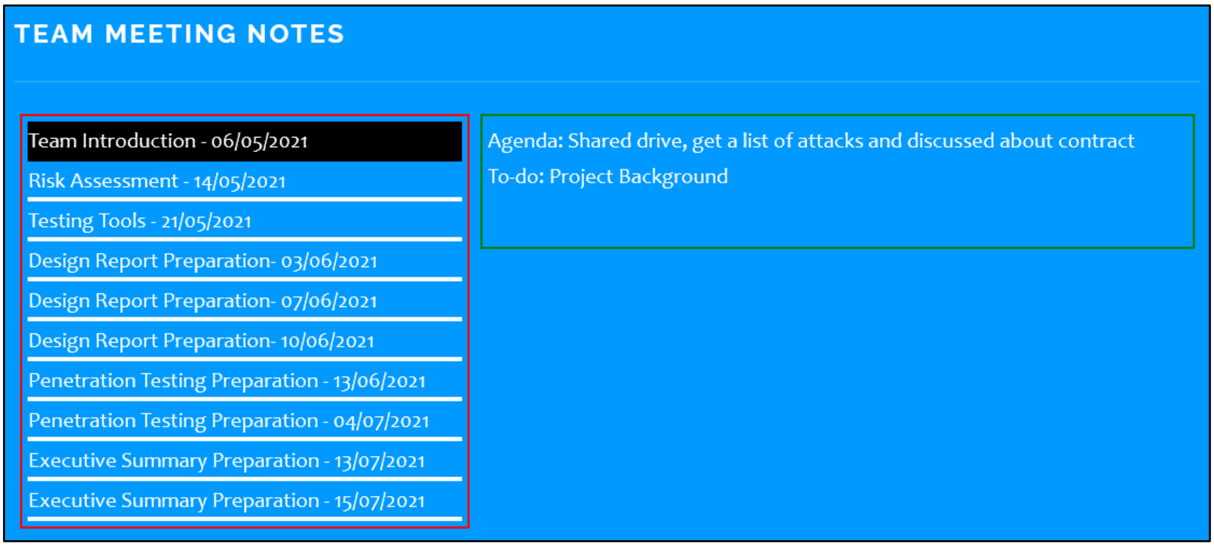
*UKEssays.com. 2021. Example Reflective Essay using Rolfe Reflective Model. [online] Available at: <https://www.ukessays.com/essays/nursing/rolfe-reflective-model.php>.*

*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].*

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

**-------------------------------------------------Reflection ends-----------------------------------------**

## Section 5 - Team Meeting Notes



TEAM MEETING NOTES

- Team Introduction - 06/05/2021
- Risk Assessment - 14/05/2021
- Testing Tools - 21/05/2021
- Design Report Preparation- 03/06/2021
- Design Report Preparation- 07/06/2021
- Design Report Preparation- 10/06/2021
- Penetration Testing Preparation - 13/06/2021
- Penetration Testing Preparation - 04/07/2021
- Executive Summary Preparation - 13/07/2021
- Executive Summary Preparation - 15/07/2021

Agenda: Shared drive, get a list of attacks and discussed about contract

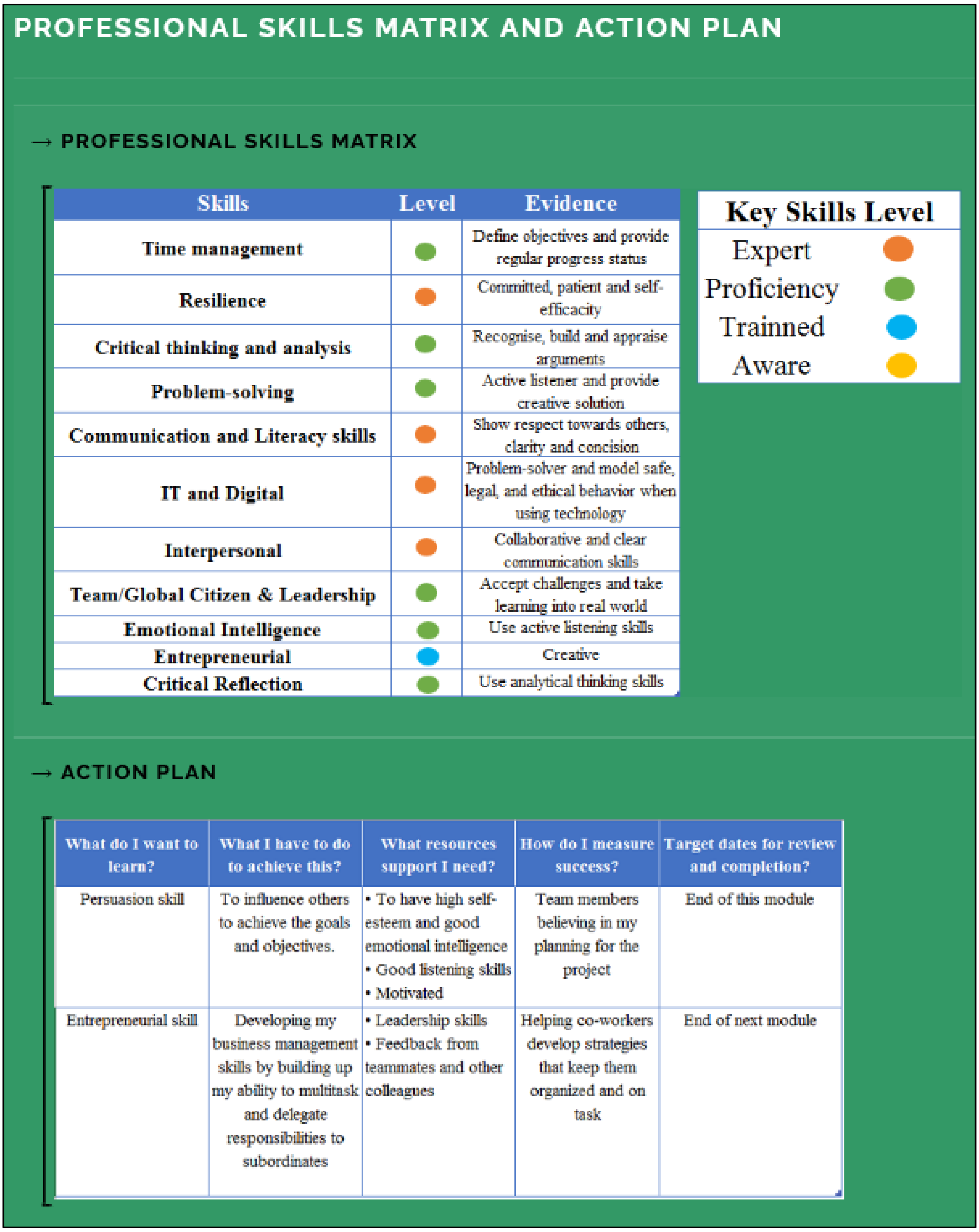
To-do: Project Background

*Figure 15 - 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 15* shows that after each meeting, each member was assigned a task to ensure that everyone participated equally in the group assignment.

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

## 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<br>• Good listening skills<br>• 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<br>• Feedback from teammates and other colleagues | Helping co-workers develop strategies that keep them organized and on task | End of next module |

*Figure 16 - 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 16*, 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 subsequently use in the workplace. 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].