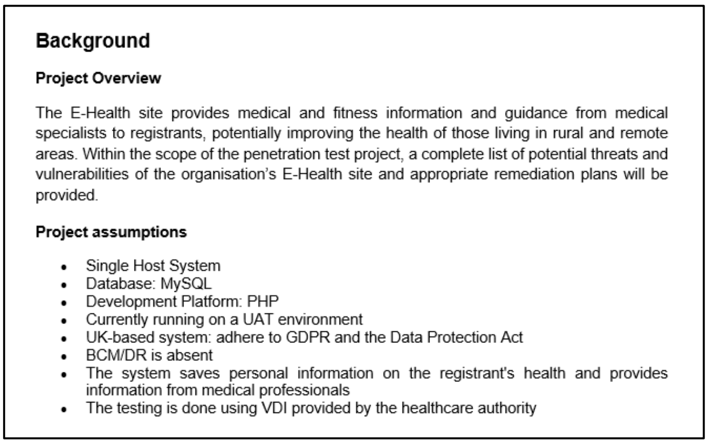
Individual Reflection

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 1* and *Figure 2* shows my contribution to the Design Document.



Background

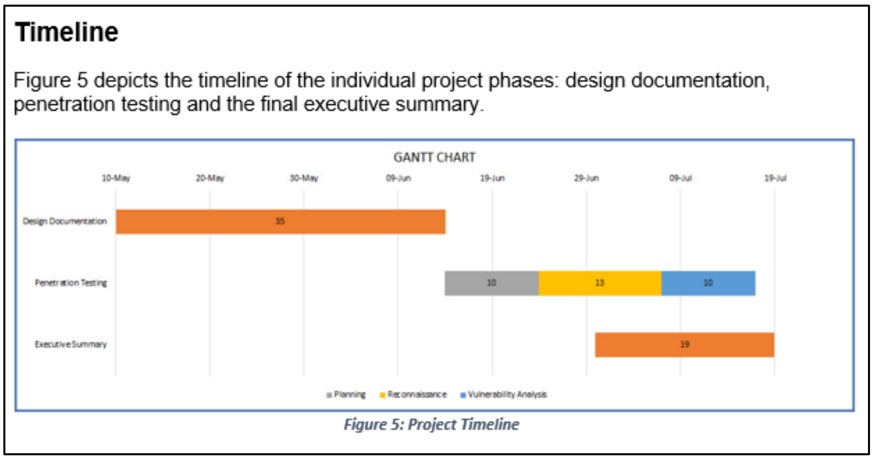
Project Overview

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 1 - Individual Contribution for Design Document – Background



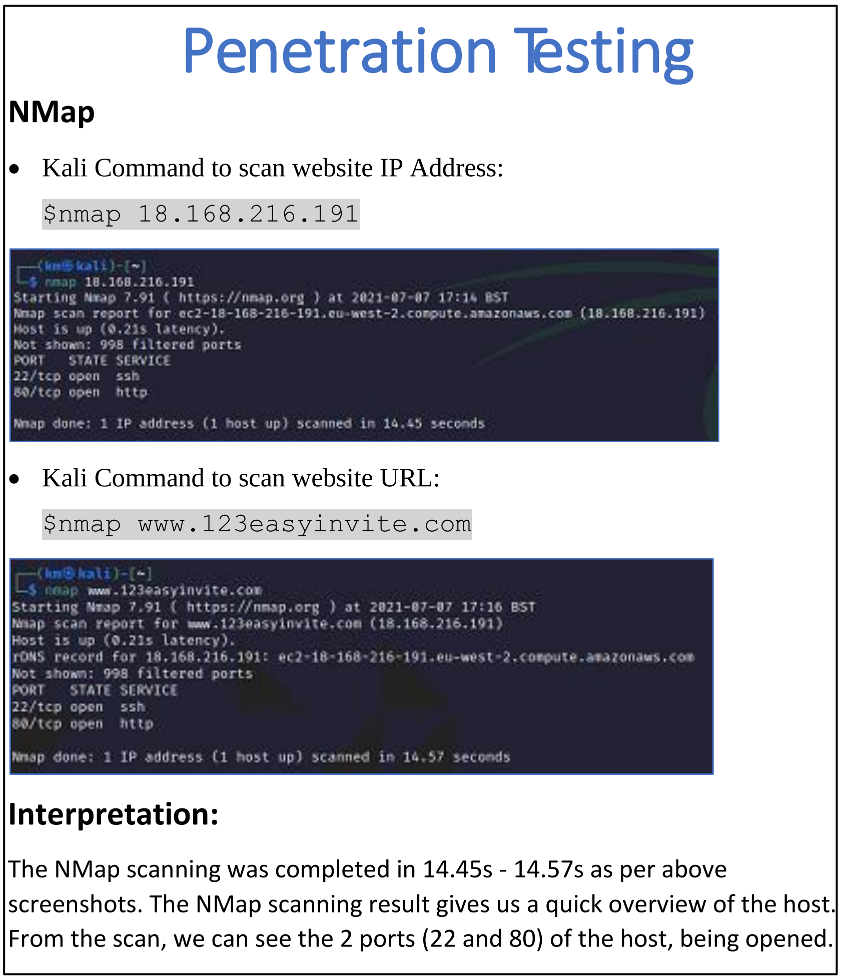
Timeline

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

Figure 5: Project Timeline

Figure 2 - 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 3*.



Penetration Testing

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
```

- Kali Command to scan website URL:

```
$nmap www.123easyinvite.com
```

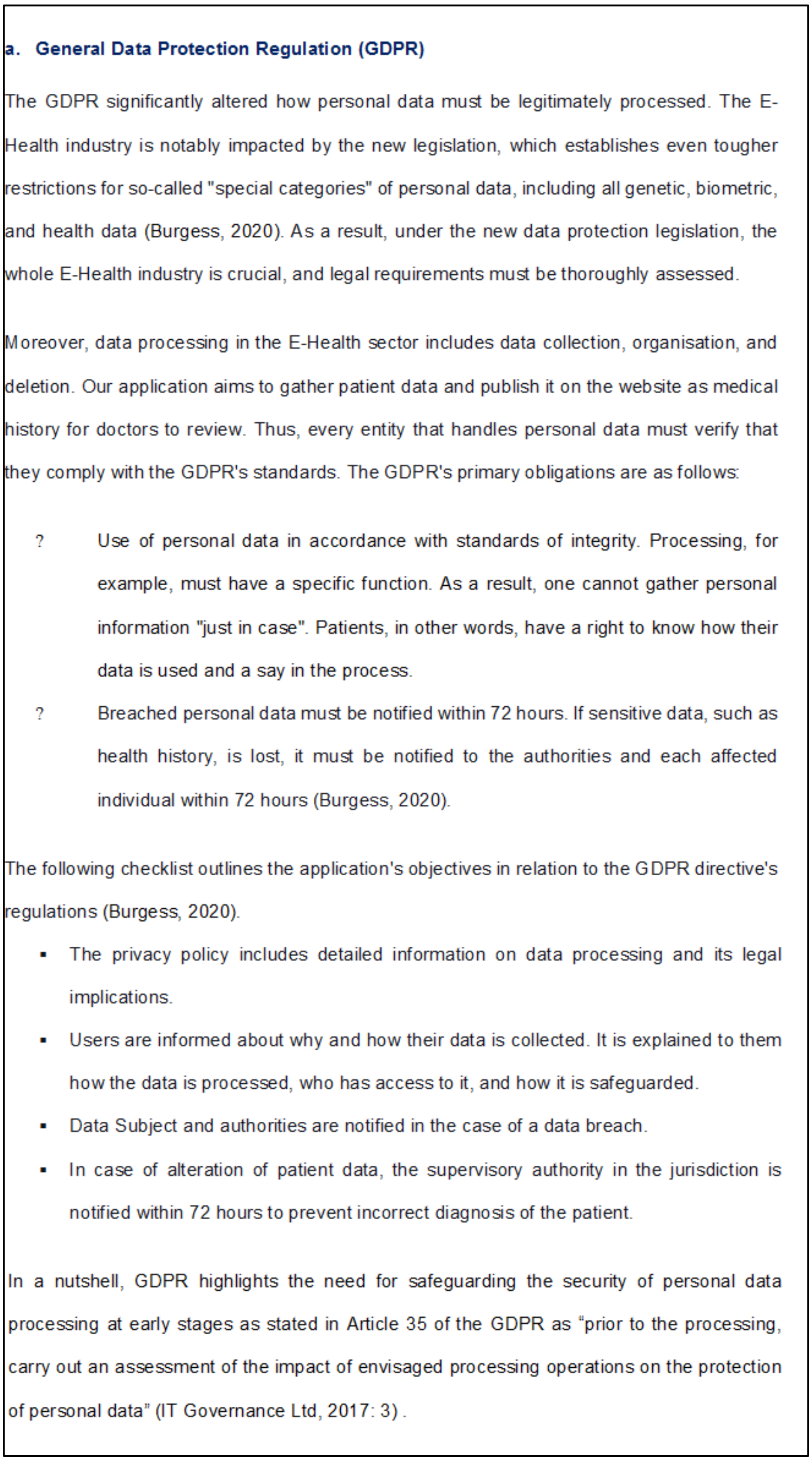
```
┌──(km㉿kali)-[~]
└─$ nmap www.123easyinvite.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-07 17:16 BST
Nmap scan report for www.123easyinvite.com (18.168.216.191)
Host is up (0.21s latency).
rDNS record for 18.168.216.191: ec2-18-168-216-191.eu-west-2.compute.amazonaws.com
Not shown: 998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

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.

Figure 3 - 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 4* and *Figure 5*.



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.

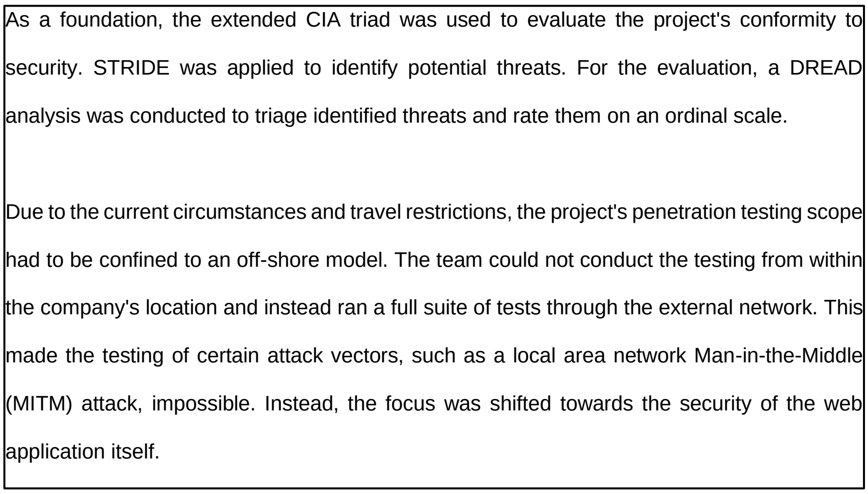
? Breached personal data must be notified within 72 hours. If sensitive data, such as health history, is lost, it must be notified to the authorities and each affected individual within 72 hours (Burgess, 2020).

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 4 - 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 5 - 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.

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].