DIEM - University of salerno
Master's degree in Computer Engineering
Situation Awareness

Report
Project 3: E-learning

Lecturers:
Giuseppe D'Aniello,
Matteo Gaeta

Group 6 Members:

Surname	**Name**	**Number**	**E-mail**
Galasso	Gianluca	622702000	g.galasso33@studenti.unisa.it
Iovaro	Damiana	622702017	d.iovaro@studenti.unisa.it
Murati	Camilla	622702126	c.murati@studenti.unisa.it
Sellitto	Marco	622702105	m.sellitto13@studenti.unisa.it

2023/2024

Contents

Chapter 1

Introduction

The objective of this project is to implement a comprehensive e-learning system designed to assist users in tailoring their learning pathways and enhancing their skill sets. Developed with a strong emphasis on situational awareness, this project is structured into two primary components: the first involves *Goal-Driven Task Analysis* (GDTA), and the second focuses on the implementation of an integrated dashboard.

This system is meticulously crafted with a **User-Centric Approach**, ensuring that users can effectively monitor their competencies and track their learning progress. In developing the GDTA, we delineated operational concepts through detailed personas and scenario analysis, ensuring that the system is attuned to the diverse needs and contexts of its users. To fulfill the goals described inside the GDTA, we implemented two dashboards: the first dashboard is focused on the user's global learning progress, while the second dashboard is focused on the user's progression in a specific course.

For the dashboard implementation, we leveraged *ElasticSearch* as the underlying database and *Kibana* as the visualization tool. The data presented on the dashboard were specifically curated for this project and are stored in multiple .csv files.

Initially, our goal was to conduct a comprehensive data analysis using an extensive dataset found online. However, we faced significant challenges in locating suitable data that aligned perfectly with our needs. Consequently, we chose to create our own .csv files containing the essential data required to populate our dashboard.

This decision granted us full control over the data, enabling precise customization according to the specific requirements of our project. By curating our own dataset, we ensured the accuracy and relevance of the information presented, thereby facilitating a more insightful and effective implementation of our e-learning system. The data are shown on a time slice of twenty days, from May 1st to May 20th. The reason for this time interval is to illustrate the user's learning situation on the platform before the end of the courses, which is set for the last day of May.

Chapter 2

Data Description

The dataset used to create the mockup of the dashboards has been handcrafted by the authors. It consists of different CSV files, each one representing a table. These files describe the courses within an e-learning platform, the interactions between a user and courses, the interactions between users, the resources used by the user on the platform, and the user's results in the courses.

The dataset is composed of the following tables:

- **Completed Course:** This table indicates whether the user has completed something each day or not for the different courses;
- **User Hours Sessions:** This table represents the hours spent by the user on the platform each day and the average hours spent by other users;
- **Resources:** This table represents the hours of use of the different resources that are available on the platform for each day;
- **Forum:** This table represents the interactions between users on the forum, showing the number of questions asked, the number of answers given, and the number of answers received;
- **Completed Modules Votes:** This table shows the votes obtained by the user for each completed module, categorized by type (theory or exercise).

The files produced are tailored on the specific dashboard where used. Some of the previously described files are duplicated and adapted to the particular needs of the dashboard. For example, the **Forum** table describes the interactions for each course or the interactions for each module inside a specific course. The same applies to the **Resources** table, where the resources are divided by course or represent the resources used for a particular course.

Chapter 3

Operational Concept

We questioned which requirement could be critical for a Situational Awareness System. This phase involved identifying and understanding the essential needs that the system must fulfill to be effective and user-friendly.

To achieve this, we conducted a detailed analysis of the *Operational Concept*, which involved the development of detailed personas and scenario analysis.

The Operational Concept is a critical phase in the design of complex systems, translating system requirements into actionable plans. It provides a comprehensive understanding of the system's operational environment, including the roles and responsibilities of the users, the tasks they perform, and the context in which they operate.

Since we are developing an e-learning dashboard intended for users who may access it from various locations, we have not defined specific environmental constriants. The flexibility of online learning environments means that users could be utilizing the system in diverse settings, such as homes, offices, or public spaces, each with varying levels of connectivity and hardware capabilities. Additionally, given the global reach of e-learning platforms, environmental conditions can differ widely among users, making it impractical to impose rigid environmental constraints.

3.1 Scenario

The company requires all employees to pursue upskilling or reskilling opportunities based on their previous studies and work experiences. Marta and Matteo are two employees whose skills and knowledge will be monitored to ensure they can effectively contribute to projects in the Offensive Cybersecurity field. The company's e-learning platform provides courses that enable employees to obtain the *OSCP* (Offensive Security Certified Professional) certification.

The platform is accessible both on-site at the company and remotely, offering flexible learning options that accommodate diverse schedules. Each employee receives a personalized dashboard where they can track their progress and access a wide range of educational resources, including video courses (concept pills), slide decks, and practical exercises. At the end of each module, employees can take assessments to reinforce their understanding and ensure they meet the learning objectives.

Additionally, the platform includes analytics and trend reports that help employees understand their learning journey, estimate the time required for course completion, and measure their engagement levels. The course design features a tailored approach, continuously monitoring each employee's performance and adapting to their specific learning needs. This customization

enhances the overall learning experience, ensuring employees are well-prepared for the OSCP certification.

3.2 Supported Figure: Matteo

Matteo is a student from the University of Salerno, with a bachelor's degree in Computer Engineering. His passion for cybersecurity has led him to specialize in this field, acquiring basic skills ranging from understanding the fundamentals of cybersecurity to networking and network protocols, from vulnerability analysis to familiarity with essential security tools. Now, Matteo faces a new challenge: a project in collaboration with Marta concerning Offensive Cybersecurity. However, to best address this task, Matteo needs to broaden his skills and knowledge.

Characteristic	**Description**
Age Range	20-25
Gender	Male
Culture	Italian
Education	Bachelor's degree in Computer Engineering
Language	Italian, English (proficient for technical literature)
Frequency of Use	Several times a week
Experience	Familiar with basic cybersecurity tools and platforms, intermediate programming skills
Personality	Curious, analytical, detail-oriented, enjoys problem-solving, goal-oriented, collaborative
Acquired Skills	Fundamentals of cybersecurity, networking, vulnerability analysis, basic scripting/programming, offensive cybersecurity
Learning Style	Visual and hands-on learner

3.3 Supported Figure: Marta

Marta is a student from the University of Naples Federico II. She completed a bachelor's degree in Computer Engineering and has now specialized in machine learning, acquiring basic skills in the field of artificial intelligence, including the structure and applications of neural networks and deep neural networks, their applications in robotics, and autonomous driving. Marta wants to collaborate with Matteo on a new project in the field of Offensive Cybersecurity. Since Marta has followed a different academic path from Matteo's, which does not involve cybersecurity, she needs to upskill her competencies.

Characteristic	**Description**
Age Range	20-25
Gender	Female
Culture	Italian
Education	Bachelor's degree in Computer Engineering, specializing in Machine Learning
Language	Italian, English (proficient for technical literature)
Frequency of Use	A few times a week
Experience	Skilled in AI and Machine Learning platforms, novice in cybersecurity
Personality	Innovative, inquisitive, enjoys learning new skills, collaborative, adaptable
Acquired Skills	Basics of AI, neural networks, deep learning, robotics, autonomous driving, basic programming, willingness to learn cybersecurity
Learning Style	Visual and auditory learner, prefers structured guidance

Chapter 4

Goal-Directed Task Analysis

We applied the *Cognitive Task Analysis* (CTA) methodology to explore individuals' knowledge and thought processes. Among the various CTA methodologies available, we selected *Goal-Directed Task Analysis* (GDTA), specifically focusing on Situation Awareness (SA) and the goals inherent in SA processes.

GDTA is tailored to identify user goals, the decisions they make, and the critical information needed to achieve these goals. This methodology not only maps out user objectives but also provides insights into their decision-making strategies and information requirements.

By employing GDTA, our aim is to deepen our understanding of how users perceive and interact with information. This understanding informs our design process, ensuring that our solutions align closely with user needs and preferences. Ultimately, this approach enhances the usability and effectiveness of our project outcomes by prioritizing User-Centric design principles.

4.1 Initial GDTA Goal Tree

The initial GDTA Goal Tree, shown in Figure 4.1, identified three Major-Goals. However, after an in-depth review and analysis, we concluded that the Major-Goal 1 **"Identify prior knowledge in the field of Cybersecurity"** can be integrated into the Major-Goal 2 **"Define and evaluate the knowledge required for Offensive Cybersecurity by monitoring students' progress"**. This conclusion was drawn from a comprehensive analysis of the sub-goals associated with Major-Goal 1.

Upon examining the sub-goals of Major-Goal 1, it became evident that both the sub-goals and the Major-Goal itself address topics that students need to master throughout their learning journey in cybersecurity. Given that Major-Goal 2 aims to delineate the specific topics and skills students must acquire, we decided to incorporate Major-Goal 1 as a sub-goal within Major-Goal 2. This integration ensures a more cohesive framework for evaluating and defining the necessary knowledge for Offensive Cybersecurity.

Furthermore, the sub-goals of Major-Goal 1 have been reclassified as Level 2 elements, signifying their importance in the comprehension phase of the learning process.

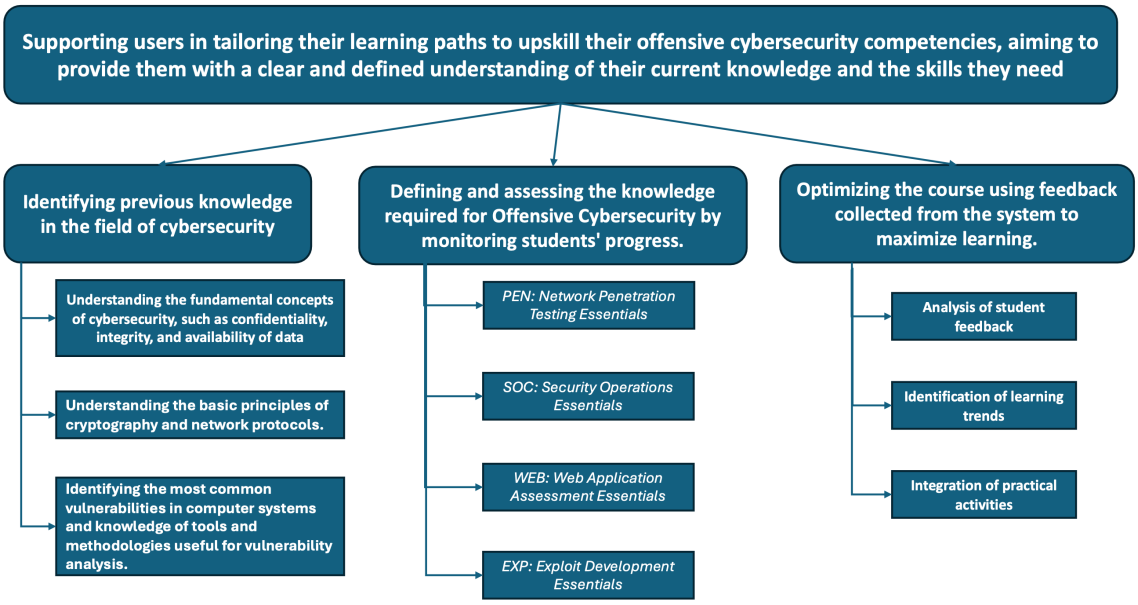

Figure 4.1: Initial GDTA Goal Tree

4.2 Final GDTA Goal Tree

In Figure 4.2, we present our Final GDTA Goal Tree, which outlines the primary goals of the system and the sub-goals that contribute to their achievement. In particular, our GDTA Goal Tree supports users in adapting their learning paths to enhance their expertise in Offensive Cybersecurity. The *Overall Operator Goal* is broken down into two primary *Major-Goals* as shown in the picture below. Each Major-Goal is further divided into *Sub-Goals* that are essential for achieving the Major-Goals.

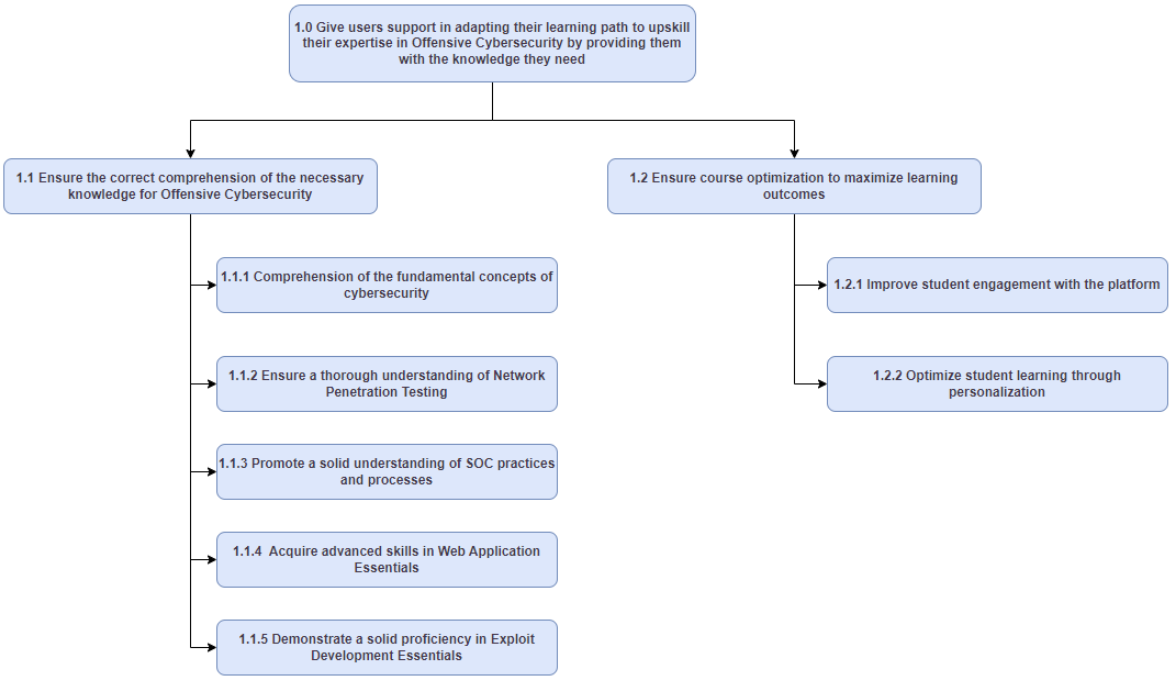

Figure 4.2: Final GDTA Goal Tree

The following sections will delve into the details of each sub-goal, providing a comprehensive understanding of the cognitive processes involved in achieving these objectives, rather than focusing on the methods or actions needed. Achieving these goals necessitates more complex cognitive processes than simply searching for a single piece of information.

Subsequently, we defined the *Informational Requirements* for each goal, which are crucial for users to make informed decisions and achieve their objectives. While these requirements might be mistakenly viewed as lower-level goals within the hierarchy, they actually serve as supportive elements that facilitate the achievement of primary goals.

In order to fulfill a goal, a decision must be made based on the available information. We are not interested in trivial yes-or-no questions: instead, we are focusing on decisions that enable the fulfillment of high-level goals. Moreover, these decisions require complex cognitive processes and a deep understanding of the situation.

4.3 Major-Goal 1.1: Ensure the correct comprehension of the necessary knowledge for Offensive Cybersecurity

In this section, we describe Major Goal 1.1 and its sub-goals. The main aim of this goal, along with its sub-goals, is to outline the modules that users need to study to enhance their skills. Essentially, this major goal represents how the course is structured in terms of modules that every student on the platform must learn.

We've taken a different approach compared to the typical GDTA (Goal Directed Task Analysis) process. The specific problem we're addressing (e-learning) isn't well-suited to the GDTA techniques typically taught in class. Therefore, we explain how we've proposed sub-goals and levels of perception, comprehension, and projection for these sub-goals.

The objective of this major goal is to enable all platform users to acquire Offensive Cybersecurity knowledge. Although the sub-goals may initially seem like tasks, they are intended as individual objectives that each student must achieve to solidify their understanding of the field.

There are no time constraints for achieving these individual objectives, allowing students to start studying whichever module they prefer and proceed at their own pace. This approach enables users to create a personalized learning path: they can skip modules they already know and only take end-of-module tests, or revisit topics where they feel they need more practice based on platform recommendations.

Regarding *Perception Level*, we've included the fundamental concepts of each course that students perceive, focusing on concise micro-learning. For instance, topics such as firewall, PHP, and SHA256 are covered in concept pills.

At the *Comprehension Level*, we've incorporated broader concepts that connect one or more micro-learning modules. The goal is to help students understand concepts that emerge after assimilating micro-learning, such as data integrity through understanding algorithms like MAC combined with SHA256.

Finally, at the *Projection Level*, we've identified the advanced competencies that students acquire through comprehension and perception, such as the ability to apply learned methodologies in future scenarios.

4.3.1 Sub-Goal 1.1.1: Comprehension of the fundamental concepts of cybersecurity

The objective of comprehending the fundamental concepts of cybersecurity is to provide individuals with a robust understanding of essential security principles and practices. Key areas of focus include ensuring confidentiality through mechanisms like OTP and MAC, maintaining data integrity with tools such as SHA256, and guaranteeing availability via digital signatures. Additionally, an understanding of blockchain technology and threat models is crucial, along with proficiency in cybersecurity algorithms and protocols like TLS. This foundational knowledge enables individuals to critically evaluate emerging technologies in relation to IT security and stay informed about current laws and regulations. The decision associated with subgoal 1.1.1 and its SA requirements are shown in the following figures.

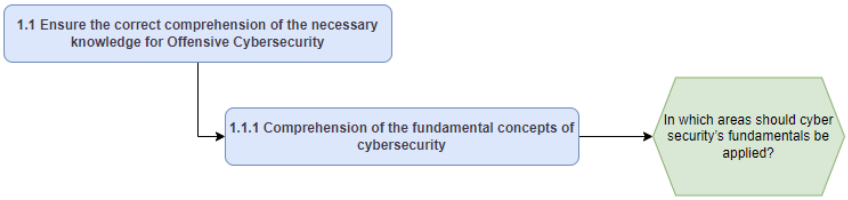

Figure 4.3: Sub-Goal 1.1.1

Level 1 SA requirements	**Level 2 SA requirements**	**Level 3 SA requirements**
OTP	Confidentiality	Capability to critically evaluate emerging technologies in relation to IT security, current laws and regulations
SHA256	Integrity	
MAC	Confidentiality	
Digital Signature	Availability	
Blockchain	Threat Models	
TLS Protocol	Algorithms for Cybersecurity	

Table 4.1: SA requirements for subgoal 1.1.1

4.3.2 Sub-Goal 1.1.2: Ensure a thorough understanding of Network Penetration Testing

The objective of ensuring a thorough understanding of network penetration testing is to equip individuals with the necessary skills and knowledge to effectively identify and mitigate security vulnerabilities within network infrastructures. This includes mastering fundamental programming concepts such as Python operators, syntax, and Powershell scripting, as well as understanding key network protocols like the Internet Protocol (IP) and Domain Name System (DNS). Advanced competencies involve applying cryptography techniques and hashing, acquiring in-depth Windows networking knowledge, and efficiently using variables, loops, and functions in Python and Powershell. Ultimately, this comprehensive understanding enables individuals to select the most appropriate penetration testing strategies for various scenarios, ensuring robust network security. The decision associated with subgoal 1.1.2 and its SA requirements are shown in the following figures.

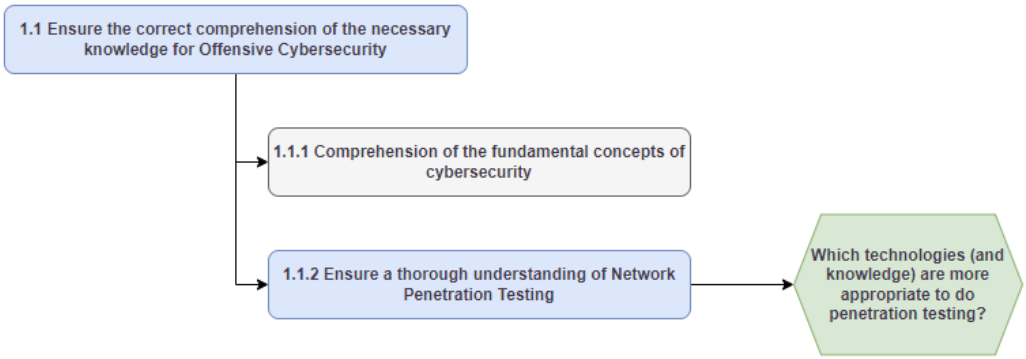

Figure 4.4: Sub-Goal 1.1.2

Level 1 SA requirements	Level 2 SA requirements	Level 3 SA requirements
Python operators	Cryptography techniques and hashing	Capability to choose the best penetration testing strategies based on the situation
Python syntax	Windows networking knowledge	
Powershell Scripting	Usage of variables	
Internet Protocol	Loops and functions in Python and Powershell	
Domain Name System		

Table 4.2: SA requirements for subgoal 1.1.2

4.3.3 Sub-Goal 1.1.3: Promote a solid understanding of SOC pratices and processes

The objective of promoting a solid understanding of Security Operations Center (SOC) practices and processes is to provide individuals with the knowledge and skills necessary to effectively manage and respond to cybersecurity incidents. This includes foundational knowledge of network protocols such as the Internet Protocol (IP) and Domain Name System (DNS), as well as scripting skills with Powershell. Advanced competencies involve data conversion in Python between decimal, binary, and hexadecimal formats, understanding operational security and security management, and familiarity with practices such as the Cyber Kill Chain and logging. Ultimately, this comprehensive understanding enables individuals to proficiently detect and respond to cyber threats, ensuring robust security operations. The decision associated with subgoal 1.1.3 and its SA requirements are shown in the following figures.

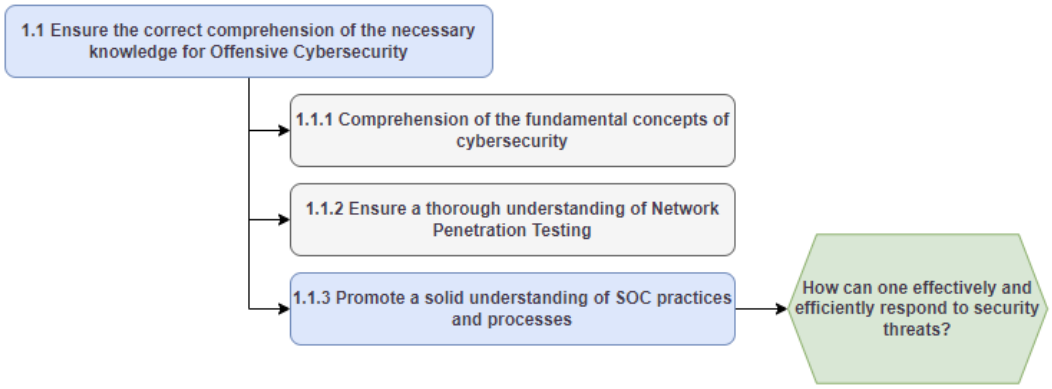

Figure 4.5: Sub-Goal 1.1.3

Level 1 SA requirements	Level 2 SA requirements	Level 3 SA requirements
Internet Protocol	Data conversion in Python between decimal, binary, and hexadecimal	Knowing how to detect and respond to cyber threats
Powershell Scripting	knowledge of operational security and security management	
Domain Name System	practices of Cyber Kill Chain and Logging	
Firewall		

Table 4.3: SA requirements for subgoal 1.1.3

4.3.4 Sub-Goal 1.1.4: Acquire advanced skills in Web Application Essentials

The objective of acquiring advanced skills in web application essentials is to enable individuals to develop and maintain secure web applications. This encompasses foundational knowledge of web development technologies such as HTML, CSS, PHP, and JavaScript, along with proficiency in security tools like ZAP, AFL, SonarQube, and Flawfinder. Advanced skills include managing secure sessions, handling authentication, authorization, passwords, and cookies, and ensuring the security of REST, SOAP, and GraphQL services, as well as security practices in GIT. Ultimately, this comprehensive understanding equips individuals to recognize and mitigate vulnerabilities such as Server Side and Client Side XSS, Cross-Site Request Forgery, Clickjacking, and Content Sniffing, thereby ensuring robust web application security. The decision associated with subgoal 1.1.4 and its SA requirements are shown in the following figures.

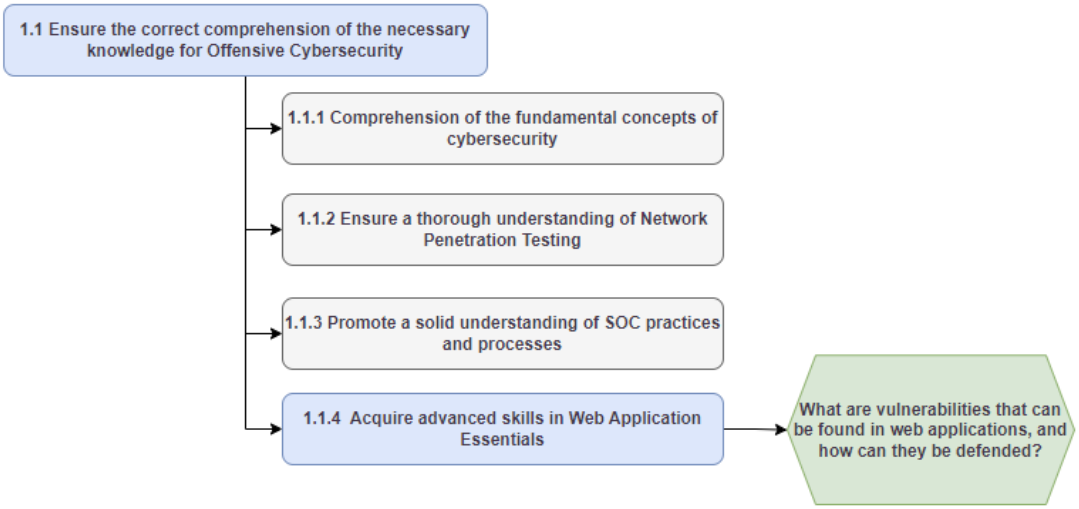

Figure 4.6: Sub-Goal 1.1.4

Level 1 SA requirements	Level 2 SA requirements	Level 3 SA requirements
HTML, CSS, PHP, Javascript	Managing secure sessions, including authentication, authorization, passwords, and cookies, REST, SOAP and GraphQL services, security in GIT	Understanding how to make a secure web application
ZAP		Recognizing Server Side & Client Side XSS, Cross-Site Request Forgery, Clickjacking, Content Sniffing
AFL		
SonarQube, Flawfinder		

Table 4.4: SA requirements for subgoal 1.1.4

4.3.5 Sub-Goal 1.1.5: Demonstrate a solid proficiency in Exploit Development Essentials

The objective of demonstrating solid proficiency in exploit development essentials is to enable individuals to effectively identify and develop exploits for various security vulnerabilities. This includes foundational knowledge of network protocols, VPNs, and firewalls. Advanced competencies involve understanding ARM-32 and ARM-64 assembly, manipulating registers, stacks, and functions, and analyzing binary files. Ultimately, this comprehensive skill set allows individuals to understand how malicious scripts affect applications, identify flaws in security measures, and leverage exploit frameworks to enhance cybersecurity defenses. The decision associated with subgoal 1.1.5 and its SA requirements are shown in the following figures.

Level 1 SA requirements	**Level 2 SA requirements**	**Level 3 SA requirements**
Network Protocols	Assembly for ARM-32 and ARM-64	Understanding how a malicious script affects an application
VPN	Registers, stacks and functions	Ability to identify flaws in security measures
Firewalls	Analysis of binary files	Knowledge of exploits frameworks

Table 4.5: SA requirements for subgoal 1.1.5

4.4 Major Goal 2.1: Ensure course optimization to maximize learning outcomes

This Major-Goal aims to make the platform more engaging and effective for users. It focuses on two main things: boosting how users interact with the platform and making studying more personalized based on how each user learns.

To achieve this, the platform will track how users use it—what they're interested in, what skills they have, and where they might need help. With this info, the platform can suggest topics for users to review and adjust how it works to match each user's progress and preferences. This will make learning easier and more effective, helping users reach their goals faster.

4.4.1 Sub-Goal 2.1.1: Improve student engagement with the platform

The objective of improving student engagement with the platform focuses on increasing and enhancing student interactions. Key metrics include the frequency of logins, session length, click-through rates on content, return visits, retention rates, and forum activity (questions and answers). Comparative analyses involve user login frequencies versus average rates, material usage percentages, and forum activity levels. Ultimately, the goal is to prevent student dropout by understanding and addressing engagement factors. The decision associated with subgoal 2.1.1 and its SA requirements are shown in the following figures.

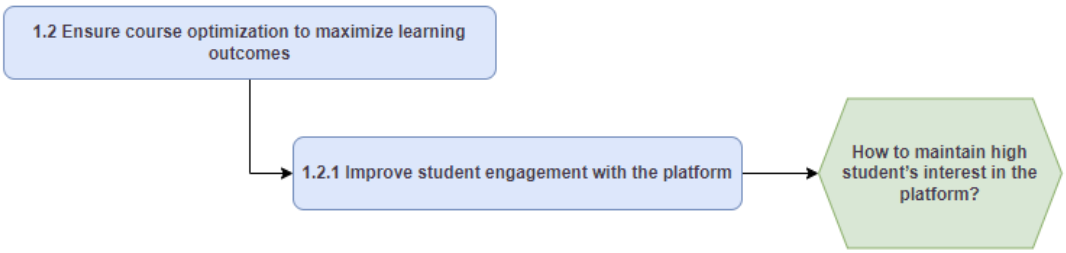

Figure 4.7: Sub-Goal 2.1.1

Level 1 SA requirements	**Level 2 SA requirements**	**Level 3 SA requirements**
The frequency of logins	Comparison between user logins onto the platform and the average login rate of other users	Preventing student dropout
Session length	Percentage of usage of the different kind of materials provided to the students	
Click-through Rate (CTR) on Content	Comparison of activity on the forum between users	
Return Visits and Retention Rates		
Number of answers on the forum		
Number of questions on the forum		

Table 4.6: SA requirements for subgoal 2.1.1

4.4.2 Sub-Goal 2.1.2: Optimize student learning through personalization

The objective of optimizing student learning through personalization is to enhance educational effectiveness by tailoring the learning experience to individual student needs and preferences. This involves assessing student performance through end-of-module assessments and tracking course completion rates to understand overall engagement. Additionally, it requires analyzing trends in student performance over time to identify areas for improvement. Furthermore, the initiative aims to optimize learning by monitoring resource reuse, identifying areas of difficulty and preferred learning styles, and evaluating the acquisition of specific skills. By leveraging these insights, the goal is to create a more personalized educational environment that supports and enhances student learning outcomes effectively.

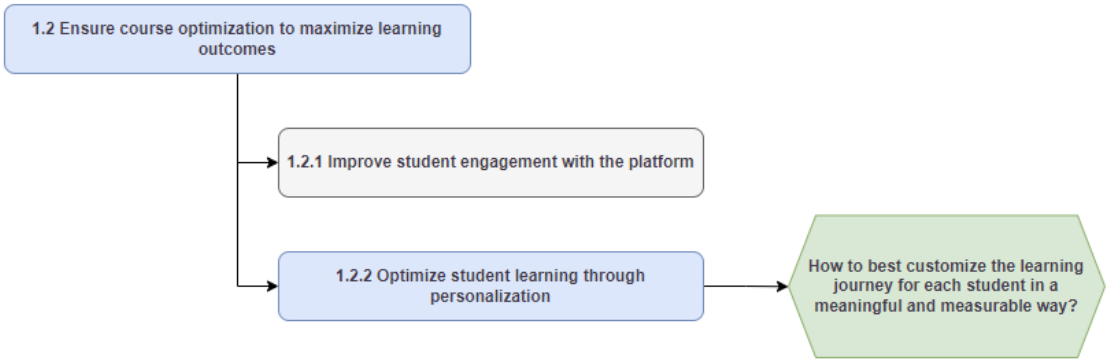

Figure 4.8: Sub-Goal 2.1.2

Level 1 SA requirements	**Level 2 SA requirements**	**Level 3 SA requirements**
End-of-module assessments for each student	Percentage of completed course	Trends in student performance over time
Number of reuses of a resource	Skill types and areas of difficulty	
Modules visited	Problem-Solving vs Memory Performance	
Used material	Student Preferences	
Skills acquired		

Table 4.7: SA requirements for subgoal 2.1.2

Chapter 5

Context Space Theory

Chapter 6

Dashboard

Chapter 7

Conclusions

List of Figures

List of Tables