Cyber range platform for Industry 4.0 training on Cyber Security

by

Emmanouil Vasilakis

A THESIS

submitted in partial fulfillment of the requirements for the degree

Master of SCIENCE

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

SCHOOL OF ENGINEERING

HELLENIC MEDITERRANEAN UNIVERSITY

2023

Approved by:

Spyros Panagiotakis

Associate Professor

Abstract

Industry 4.0, also known as the fourth industrial revolution, is characterized by the integration of advanced technologies such as IoT, big data, and artificial intelligence into industrial processes. However, with the increasing reliance on technology, industries are becoming more vulnerable to cyber-attacks. The increasing use of connected devices and the integration of complex systems in industrial environments can create new vulnerabilities and expose sensitive information. These attacks can have severe consequences, including financial losses, data breaches, reputational damage, and destructive attacks on systems. To mitigate these risks, it is necessary students, engineers, workers and experts of Industry 4.0 to have hands-on training on various realistic cyber security scenarios.

But the successful education and training in the field of Industry 4.0 cybersecurity is a considerable problem since the traditional methods of training frequently do not match the complexity of modern cybersecurity technologies or the realistic scenarios they try to simulate. These methods frequently prioritize the acquisition of theoretical knowledge and learning that takes place within the confines of a classroom setting. In most cases, traditional methods are unable to accurately represent or simulate the challenges and difficulties that practitioners and students may run into when experiencing real cybersecurity incidents.

Cyber-range platforms can provide a solution towards this direction by creating real-world scenarios and allowing users to practice their skills in a controlled environment. Cyber range systems are virtual training environments that simulate real-world cybersecurity scenarios and provide hands-on training and evaluation opportunities for cybersecurity users. These systems are designed to mimic the complex and evolving nature of cyber threats and help security teams develop and enhance their skills in a controlled and safe manner. Cyber ranges can range from simple environments that allow users to experiment with new technologies to highly complex systems that recreate the behavior of real-world cyber-attacks. Such systems can be used to train a wide range of cybersecurity skills, including incident response, network security, threat intelligence, and digital forensics.

On the other hand, the gamification concept of Capture-The-Flag (CTF) events has recently attracted the attention of the cybersecurity community. In CTF events, which mimic treasure

hunting, the trainee can test his competences, follow his score, compete with other trainees, and be motivated to improve his cybersecurity skills, while trying to be the first who will raise the flag.

This thesis aims to implement and evaluate, based on available open-source tools, an integrated cyber-range platform which exploits the concept of Capture-The-Flag challenges to create realistic cybersecurity scenarios and propose an interactive solution towards industrial training. CTFd is a powerful open-source solution for organizing CTF challenges supporting a plethora of integrated plugins, such as Naumachia. The latter provides and orchestrates a secure, lightweight and containerized infrastructure for creating at will isolate virtual machines. Based on Naumachia and CTFd, an open-source cyber range infrastructure has been developed, which is easily expandable, and the training is organized in the logic of gamification through a series of challenges that aim to train in cyber-security issues. The challenges provoke the trainee to test defenses and attacks in a safe manner. The cybersecurity scenarios we have developed in our prototype cyber-range system are SQL injection, Snort Ruling, forensic analysis, and man-in-the-middle spoofing.

With our study we aim to investigate the following research questions:

- Development of a cyber range system based on open-source technologies.
- Development of a secure and extendable environment for cybersecurity training, based on virtual machines and containers which will be refreshed after the end of each training session.
- Development of cybersecurity training according to the gamification rules, following the CTF paradigm.

Finally, an anonymous survey, based on pre- and post- questionnaires, has been organized in the evaluation process to assess a) acquired knowledge, b) training and organization of the platform, c) provided educational material, and d) the challenges. The results provide information on how well the platform bridges the knowledge gap between theory and practice.

Table of Contents

Table of Contents 4
List of Figures 6
List of Tables 8
Table of Abbreviations 9
Chapter 1 - Introduction 11
1.1 Motivation 11
1.2 Problem Statement 13
1.3 Objectives of the Study 13
1.4 Scope and Limitations 14
1.5 Thesis Organization 14
Chapter 2 - State of the Art 16
2.1. Theoretical background 16
2.1.1 Industry 4.0 16
2.1.2 Cyber Physical Systems 19
2.1.3 Artificial Intelligence 20
2.1.4 Cybersecurity challenges in Industry 4.0 20
2.1.5 Virtual Machines Vs Containers 21
2.1.6 Docker Container Networking 22
2.1.7 The Role of Gamification via Capture The Flag Challenges in Cybersecurity 27
2.2 Systematic Literature Review on Industry 4.0 and cybersecurity 29
2.2.1 Methodology 29
2.2.2 Research Questions 29
2.2.3 Eligibility criteria 30
2.2.3 Database Selection 31
2.2.4 Keywords Selection 31
2.2.5 Screening - Results 32
2.2.6 General Review 38
2.3 Related works 39
2.3.1 Effectiveness of Cyber Range Platforms 39
2.3.2 Role of educational guides 42
2.3.3 Interactive, Scenario-based Training 44

Chapter 3 - System Design 48
3.1 Infrastructure Organization 48
3.1.1 Virtual Machine Networking Services 49
3.2 System Entities 52
3.3 Tools and Technologies 54
Chapter 4 - Implementation 56
4.1 (CTFd)platform implementation with dockers 56
4.1.1 (CTFd) docker networking diagram 61
4.1.2 Communication across machines (Docker container to container, or Docker container to a remote host machine) 64
4.2 Naumachia framework implementation with docker 66
4.2.1 Key features and importance of Naumachia 66
4.2.2 Naumachia docker networking 67
4.3 Development of Challenges 71
4.3.1 SQL Injection 71
4.3.2 Snort 74
4.3.3 Forensics 75
4.3.4 Man in the middle 78
4.3.5 Challenges and learning guides 81
4.3.6 Conclusion 84
Chapter 5 - Evaluation and Findings 85
5.1 Overall evaluation of the participants' experience and the training platform 85
5.2 Evaluation of challenges and guides 87
Chapter 6 - Conclusions and future work 90
Bibliography 91
APPENDIX A –Evaluation Questionnaires 101

List of Figures

Figure 2.1 Essential Architecture on Industry 4.0 source 17
Figure 2.2 Components on Industry 4.0source 18
Figure 2.3 Virtual Machine Vs Docker Container source 22
Figure 2.4 Docker Diagram source 23
Figure 2.5 Overview of Docker architecture source 24
Figure 2.6 Container network model 25
Figure 2.7 Docker0 default bridge network 25
Figure 2.8 Keywords representation in Clusters. 32
Figure 2.9 Overview of the systematic review procedure according to PRISMA flow diagram. 34
Figure 2.10 RQ1, RQ2, RQ3 categorization in percentage. 35
Figure 2.11 Number of publications per year. 35
Figure 2.12 General Review - number of papers according to keyword searching. 39

Figure 3.1 Network Architecture 49
Figure 3.2 Network architecture analysis 50
Figure 3.3 Virtual machine in isolated network 52
Figure 3.4 System Entities 54
Figure 3.5 Overview of tools used. 55

Figure 4.1 CTFd deployment 56
Figure 4.2 Connection types between administrators and users in CTFd 57
Figure 4.3 Challenge setup 58
Figure 4.4 Total of challenges and categories 59
Figure 4.5 Challenge setup 60
Figure 4.6 CTFd Welcome page 60
Figure 4.7 User statistics 61
Figure 4.8 CTFd networking diagram 62
Figure 4.9 Ping between containers in different docker bridge networks 65
Figure 4.10 Naumachia key features 66
Figure 4.11 Deployed naumachia with all the challenges 67
Figure 4.12 Naumachia networking 68

Figure 4.13 Naumachia network flow 69
Figure 4.14 VPN connection process 70
Figure 4.15Docker challenge structure 72
Figure 4.16 SQL injection web app interaction 73
Figure 4.17 SQL injection process 73
Figure 4.18 Web app snort checker 75
Figure 4.19 FTP log-in attempt 75
Figure 4.20 SSH bruteforce 76
Figure 4.21 Telnet connected user 77
Figure 4.22 Forensics process 78
Figure 4.23 The logged-in user can execute specific commands 78
Figure 4.24 Poisoning the network 80
Figure 4.25 Capture the packets to find the flag 81
Figure 4.26 Challenges categories and descriptions 82
Figure 4.27 Learning guides 83

Figure 5.1 Years of experience in cybersecurity 86
Figure 5.2 Statistics for those who participated in cybersecurity training or capture the flag 86
Figure 5.3 The usage of the training platform was useful and convenient 87
Figure 5.4 Satisfaction with the overall experience of participation 87
Figure 5. 5 How challenging did you find the SQL injection challenge? 88
Figure 5.6 Ability to craft your own rules for the Snort intrusion detection 88
Figure 5.7 Effectiveness of the forensic challenge 88
Figure 5.8 Did you enhance your knowledge on how MITM attack works? 89
Figure 5.9 How explanatory did you find the learning guides 89

List of Tables

Table 1 All papers included in the systematic literature review..... 36
Table 2 Summarization table 50
Table 3 Summary of challenges and learning goals..... 82

Table of Abbreviations

Abbreviation	Definition
CR	Cyber Range
CTF	Capture the flag
CTFd	Capture the flag framework
ICT	Information and communication technologies
Man in the middle	Mitm
IoT	Internet of Things
CPS	Cyber Physical Systems
HMI	Human machine interfaces
AI	Artificial Intelligent
ACL	Access control list
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RQ	Research question
DDOS	Distributed Denial Of Service
CVE	Common Vulnerabilities and Exposures
ARP	Address Resolution Protocol
Veth	Virtual ethernet interface
BR	Bridge network
SNAT	Source Based Network Address Translation
DNAT	Destination based Network Address Translation

MAC	Media Access Control
VM	Virtual Machine
VPN	Virtual Private Network
SSH	Secure Shell

Chapter 1 - Introduction

1.1 Motivation

A key component of Industry 4.0 is the integration of Information Technology (IT) and Operational Technology (OT), which provides widespread connectivity between systems and devices, improving performance and flexibility. Nonetheless, it also brings with it security flaws, opening these systems up to hackers.

The growing concern about how Industry 4.0 relates to cyberattacks is affecting the industrial sector as cyber security concerns grow alongside digital transformation and automation [1]. Cybercriminals are constantly adapting their attack methods to various systems and applications connected by networks for profit purposes or illegal activities.In order to address this issue, it is necessary to implement effective learning and training programs in order to educate, since they teach professionals and students alike about the creation of secure systems and raise awareness of the risks posed by cyber-attacks when managing cyber range systems [2].

Therefore, the growing importance of cyber education is crucial to the training of personnel in organizations, specifically those that are responsible for operating critical infrastructure.Pedagogical practices and modeling cybersecurity in educational ways dynamically support education processes. Training programs are tailored to the needs of trainees, providing continuous training and improvement in employee performance [3,4].

Recently, Cyber ranges platforms are becoming more and more well-liked as professional training tools to counteract cyber threats and attacks. The idea of a cyber range platform is to provide cyber security training in a realistic, isolated environment within an organization's network. It highlights how crucial it is to create vulnerable virtual machines within a cyber range platform, which can be a difficult and time-consuming task [5].

Hackathons and cyber security challenges are good ways to spread knowledge about information and communication technologies (ICT) security. During these trainings, participants can enhance their programming and security skills through the process of creating and developing challenges as if they were real threats [6].

The concept of a capture the flag (CTF) platform has been developed. The CTFd platform [7], serves as a practical implementation of realistic concepts about the challenges in cyber security, providing in participants' specialized knowledge acquisition as the system has a record of each user's performance on the challenges they solve and anoverall performance score, thus making it more competitive [8].

Developing virtual lab environments is a key component of countering cyber-attacks, providing interactive, hands-on training as well as a secure environment to simulate and counteract cyber-attackswith principles for designing cybersecurity exercises that maximize the success while minimizing the cyber security risk [9].

A modern cybersecurity training system should create a realistic environment for the trainee to test defenses and attacks in a safe manner. The virtual machines provide a safe environment for testing, and the containers used are a lightweight infrastructure to do something like this. The strategy to create virtual terminals from within other virtual terminals in isolated environments is very secure, having the possibility that once the user disconnects, all resources will be freed up. Based on Naumachia and CTFd, an open-source cyber range infrastructure has been developed and is easily expandable, and the training is organized in the logic of gamification through a series of challenges that aim to train in cyber security issues.

The training experience is more authentic, and the transition from theory to practice is smoother since the scenarios include a wide range of cybersecurity challenges. The indicative use cases and the educational materialhave been developed are SQL injection [10], Snort detection [11], forensic analysis [12], and Man-in-the-Middle (MITM) attacks [13], through the integration of the CTFD platform with the Naumachia framework [14], individuals are immersed in industry-specific cyber-defense scenarios that closely resemble the issues encountered by contemporary enterprises within the Industry 4.0 environment.Moreover, the training guides that accompany these challenges provide participants with a comprehension of the underlying principles and strategies necessary to address each given scenario. The guides not only function as important resources but also underscore the significance of knowledge transmission within the wider scope of cybersecurity education.This research contributes to the development of a comprehensive training approach by utilizing both the CTFd cyber range platform and educational guides [15]. The aim is to enhance cybersecurity awareness and competence, which

are crucial in the context of Industry 4.0. The evaluation of the CTF as a cybersecurity learning approach and the identification of areas that need improvement for subsequent editions were made feasible by examining the participants' performance on the challenges and their feedback.

In summary, this research aims at investigating the comprehensive relationship between training in cybersecurity and Industry 4.0. The present research endeavor explores the techniques used by individuals to adjust and develop creative methods in the context of the digital age. It involves the utilization of educational guides, hands-on interactive scenarios, and open-source technologies. The aim is to provide participants with the necessary skills to effectively handle the complex challenges caused by the digital revolution in manufacturing. The objective of the research is to provide scientific and practical views on the prospective development of cybersecurity training in the context of Industry 4.0**.**

1.2 Problem Statement

The successful education and training of students, engineers, and experts in the field of Industry 4.0 cybersecurity is a considerable problem. Even when they have their uses, traditional methods frequently do not match the complexity of modern cybersecurity technologies or the realistic scenarios they try to simulate. The existence of a gap between theoretical knowledge and practical skills[6]in cybersecurityhighlights the necessity for creative approaches in the realm of cybersecurity education.These methods frequently prioritize the acquisition of theoretical knowledge and learning that takes place within the confines of a classroom setting.Inmost cases, traditional methods are unable to accurately represent or virtualize the challenges and difficulties, creating real-world scenarios that practitioners and students may run into when practicing cybersecurity.

1.3 Objectives of the Study

Enhancing cybersecurity skills and knowledge in the context of Industry 4.0 is the primary objective of this thesis. Realistic scenario-based and interactive challenges will be developed and implemented in order to do this. Providing hands-on experience in managing and recognizing cybersecurity threats and weaknesses in Industry 4.0 is the aim of this project.

The study aims to achieve the following specific objectives:

1. Developing a cyber range system based on open source technologies.
2. Developing a secure and extendable environment for cybersecurity training, based on virtual machines and containers which will be refreshed after the end of each training session.
3. Developing cybersecurity training according to the gamification rules, following the CTF paradigm.

1.4 Scope and Limitations

The main objective of this study is to focus on the development and implementation of four interactive scenario-based challenges. These challenges are designed to target significant aspects of cybersecurity in Industry 4.0. The issues presented in this context are primarily focused on the topics of SQL injection, snort intrusion detection, forensic analysis, and man-in-the-middle (MitM) attacks. The research admits some limitations, such as the narrow focus on selected difficulties for examination and potential restrictions in participant recruitment. Furthermore, in the context of exploratory research, it is crucial to acknowledge the inherent limitations pertaining to the ability to generalize findings beyond the specific context and characteristics of this study.

1.5 Thesis Organization

The remainder of this thesis is organized as follows:

Chapter 2 provides a comprehensive systematic literature review covering Industry 4.0, cybersecurity, interactive scenario-based training, and cybersecurity challenges according to research questions and theoretical background in key domains.

Chapter 3 aims to clarify the system design and organizational structure of the cybersecurity training system. The entities in the system and the tools and technologies that have been used are the main topics of this chapter.

Chapter 4 presents the implementation phase and involves the development of interactive cybersecurity scenarios for Industry 4.0. The frameworks include the CTFd and Naumachia, addressing challenges such as SQL injection, snort, Man-in-the-middle, and forensics, characterized by this chapter.

Chapter 5 is divided into three stages evaluation of the final system by its users using pre- and post-survey questionnaires. The first stage evaluates participants' previous experiences and provides an overall evaluation of the training platform. The second stage focuses on questions about the challenges, and the third stage focuses on how effective the learning guides are.

Chapter 6 is the conclusion chapter which summarizes this thesis and discusses some issues for future development and further improvement of the system.

Chapter 2 - State of the Art

2.1 Theoretical background

2.1.1 Industry 4.0

Industry 4.0, or the 4th Industrial revolution, is a significant change in the industrial and information technology sectors [16]. In order to develop smarter, more connected, and efficient systems, this paradigm introduces the use of various interconnected digital technologies into the industrial landscape[17].

Fundamentally, it includes the following, as shown in figure 2.1:

- **Cloud** is a service that provides on-demand access to a shared pool of computer hardware and software [18]. To manage the massive amount of data produced by Industry 4.0, they offer the analytics features, storage, and processing that are necessary.
- **Internet of Things (IoT)** consistsof a huge network of intelligent sensors and network devicesthat makes up the backbone of the fourth industrial revolution, often known as Industry 4.0 [19].
- **Cyber Physical Systems (CPS)** refer to the integration of physical and digital domains. The entities encompass machinery, robotics, and automation systems that are interconnected with software and networks [20]. The CPS functions independently while maintaining connectivity to central control systems.
- **Communication networks**, such as high-speed and dependable networks like 5G, play a crucial role in facilitating uninterrupted data transmission across various devices and systems. The utilization of these networks is crucial in attaining prompt responsiveness in real-time scenarios.

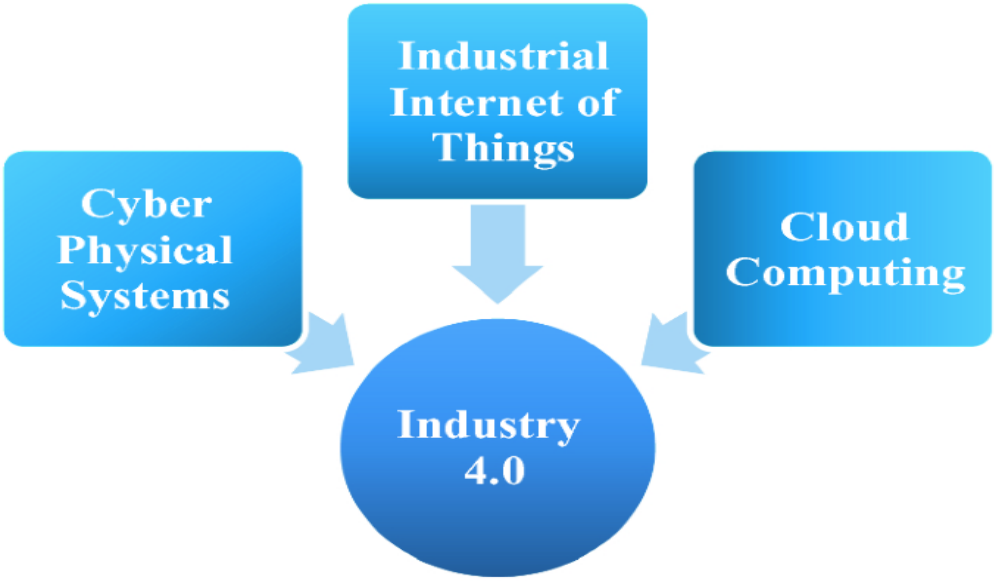


Figure 2.1 Essential Architecture on Industry 4.0 source

Components:

The fundamental components, as show in figure 2.2 of Industry 4.0 include the following:

- **Sensors [21]**are devices that are utilized for the purpose of monitoring physical processes and subsequently initiating actions based on collected data. These actions may involve making changes to machinery settings, among other possibilities.
- **Smart Factories:**Intelligent manufacturing facilities, or "smart factories," are transforming from conventional ones into advanced production centers by incorporating robotics, automation, and the Internet of Things[22].
- **Advanced Analytics**: Quality control, predictive maintenance, and process optimization are achieved using artificial intelligence and machine learning [23].
- **Digital twins** refer to virtual representations of real assets or systems. Simulation, testing, and optimization of real-world processes are facilitated by their assistance [24].
- **Human machine interfaces** (HMIs) facilitate the interaction between human operators and intelligent systems [25], enabling the exchange of information and providing immediate access to data analysis and system management.

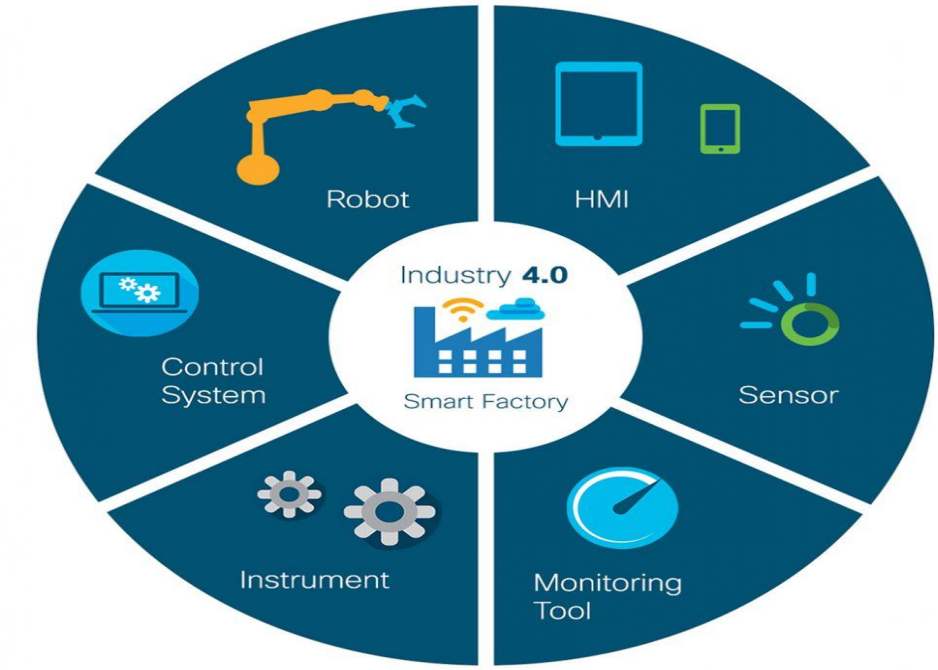


Figure 2.2 Components on Industry 4.0source

Briefly description of how Industry 4.0 works

The way Industry 4.0 works is by making data-driven, intelligent decisions. IoT devices are always collecting data from products, systems, and equipment. Platforms that run on the cloud or in physical systems within the company collect these data. Big data analytics tools are used there to process and analyze it. This analysis provides valuable insights into the various manufacturing processes, enabling the identification of anomalies and the prediction of maintenance requirements.

These insights enable companies to increase manufacturing efficiency, decrease idle time, improve product quality, and provide personalized options. The process encompasses the continuous monitoring of operations in real-time, the implementation of predictive maintenance strategies, and the ability to dynamically adjust production as needed.

In summary, Industry 4.0 harnesses sophisticated information technology to establish interconnected industrial ecosystems that are driven by data, resulting in heightened levels of efficiency, quality, and adaptability that have not been witnessed before.

*2.1.2 Cyber*Physical Systems

The advent of Industry 4.0 brings out a new era of digitally interconnected manufacturing, with Cyber Physical Systems (CPS) occupying a central position within this paradigm. These systems integrate the tangible aspects of machinery and production processes with the intangible aspects of information technology, resulting in a harmonious collaboration between the two domains. In Industry 4.0, CPS includes a broad range of technologies [30], such as robots, IoT devices, smart sensors, and autonomous systems that can connect with central control systems and with each other. These systems provide extraordinary levels of automation, real-time monitoring, and decision-making capabilities, thereby leading to improved efficiency and production in the manufacturing sector. Nevertheless, integration at this level also gives rise to many vulnerabilities.The reliance on interconnected networks and the large amount of data transmission creates an open door to cyber threats, which have the capacity to hinder operational activities, compromise sensitive information, and pose risks to public safety.Due to the dependence on networks and the massive volume of data exchanged, there is a potential for cyberattacks that could impede operations, jeopardize confidential information, or even endanger the safety of the public. Though predictive maintenance and optimization benefit from the integration of AI and machine learning, hostile AI assaults are a danger associated with this approach.

The scope of CPS within the context of Industry 4.0 is extensive, covering a wide range of industries suchas automobile manufacturing, pharmaceuticals, and so on. These systems find use in several domains such as production processes, supply chain logistics, and the innovation of new products. The integration of physical and digital components presents intricate issues within the realm of vulnerabilities [31]. One example is the potential exploitation of sensors and controllers that are integrated inside machinery used in industries, which can occur if appropriate security measures are not implemented. The establishment of communication among devices via networks or cloud-based services presents vulnerabilities [32], that can be exploited by malicious actors. Furthermore, the difficulty of finding and dealing with vulnerabilities is increased by the complex structure of CPS networks, which include several layers of hardware and software. CPS, being the central component of Industry 4.0, provides substantial prospects for enhanced

efficiency and innovation [33]. Nevertheless, companies also bear a substantial need for improving the security of these systems in order to mitigate potential cyber-attacks.

2.1.3 Artificial Intelligence

The concept of Industry 4.0 is radically changing the production scene with artificial intelligence (AI), which offers unprecedented levels of automation, efficiency, and decision-making power. Massive volumes of data produced in real-time by linked devices and sensors are processed using artificial intelligence (AI) technologies, including machine learning [34] Intelligent systems possess the capability to enhance manufacturing processes, identify anomalies, forecast equipment failures, and enable autonomous decision-making. Artificial intelligence (AI) has a multitude of advantages within the context of Industry 4.0; nevertheless, it also adds novel facets of cybersecurity challenges.Cyberattacks using artificial intelligence are a growing security risk in the age of Industry 4.0, [35]. There is an increasing desire among attackers to exploit the capabilities of artificial intelligence (AI) in order to develop and carry out assaults that are more advanced and specifically targeted. Adversarial machine learning, in which AI models are deceived to exploit security systems, and attack automation, which makes exploitation quicker and more scalable, are two examples of AI-driven attacks. In the context of Industry 4.0, potential ramifications encompass AI-driven cyber threats targeting smart factories, interruptions in supply chains, and breaches of data security.It is critical to identify AI systems' vulnerabilities, such as their vulnerability to adversarial assaults and data poisoning, in order to protect against these constantly arising dangers. To effectively minimize these vulnerabilities and take advantage of AI's inherent capabilities for proactive cyber defense in the Industry 4.0 environment, security professionals need to create sophisticated AI-based threat detection and response systems [36].

*2.1.4*Cybersecurity challenges in Industry 4.0

Industry 4.0 is bringing with it a plethora of cyber security challenges as it continues to change manufacturing and industrial processes. The increasing dependence on automation systems, sensors, and smart devices expands the attack surface [26] that malevolent actors can target. The defense of these networked systems from cyberattacks is one of the main issues. In order to prevent unauthorized access, information breaches, and disruption of critical operations,

it is imperative that the integrity and security of such devices and networks be secured.Robust, encryption of information, restrictions on access control list (ACL), and monitoring are essential for organizations to protect confidential data and comply with legal requirements.

An additional challenge relates to the vulnerabilities associated with cyber-attacks [27]. The perpetrators have demonstrated an increasing level of sophistication, employing methodologies such as machine learning and artificial intelligence to execute more advanced targeted assaults. Consequently, it is imperative for enterprises to consistently enhance their defense systems in order to align with the nature of these threats. In addition, a lot of Industry 4.0's vulnerabilities are in industrial control systems and legacy systems, which can have weaknesses in security because they were not developed to deal withcurrent cyberattacks.

Maintaining the operating effectiveness of these older systems while protecting and patching them can be a challenging task. In addition, Industry 4.0 promotes the use of cutting-edge technologies such as the (Iot), which present new security risks that enterprises need to manage in order tomaintaina secure operating environment.The use of modern security technology, the provision of staff training, and the implementation of cyber risk assessments are all important aspects of a robust plan aimed at protecting Industry 4.0 assets in context with these potential risks [28,29].

2.1.5 Virtual Machines Vs Containers

These two technologies are different ways of achieving virtualization. Virtual machines are what is called hardware virtualization because it happens at the hardware level. The hardware is at the bottom, and on top of the hardware is a hypervisor. A hypervisor is responsible for creating these virtualized instances of each of the components, such as processors, RAM, storage, and network cards. All these components are being virtualized by the hypervisor that is running on the host machine. On the other hand, with containers, there is hardware at the bottom, and on top of the hardware is a kernel, which helps the software and hardware talk to each other. On top of the kernel is our operating system, called Host OS, because it is going to be what is hosting all of our containers. Then, on top of the operating system, there are the running containers. That's why it is called operating system-level virtualization because it happens at the

operating level, whereas the virtual machine architecture works at the hardware level [73]. A schema of these two technologies is shown in Figure 2.3.

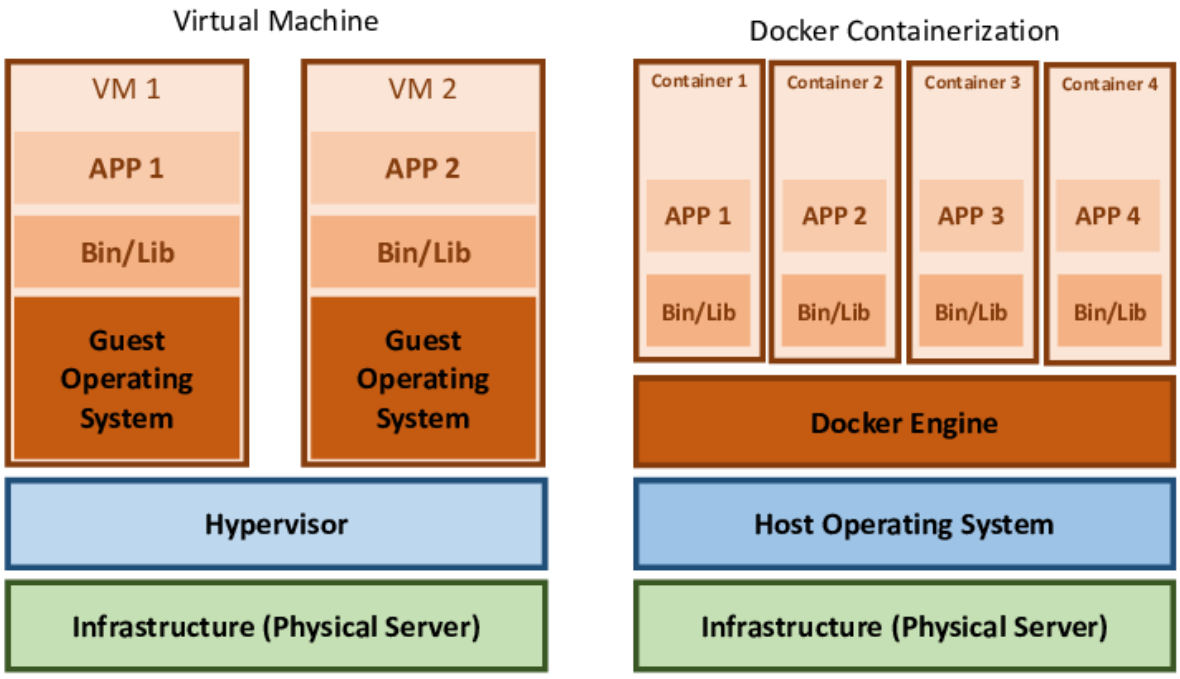


Figure 2.3 Virtual Machine Vs Docker Container**source**

2.1.6 Docker Container Networking

Docker Engine is an open-source containerization technology for building and containerizing applications. Docker facilitates the automated deployment of the developing application into containers. Virtualization adds an application deployment engine to the container execution environment. An environment that is lightweight and quick is what the docker engine aims to deliver, enabling developers to run their programs and quickly and easily transfer them from their notebooks to testing environmentsand then to the live environment [70].

2.1.6.1 Docker Daemon

Figure 2.4Docker operates on a client-server architecture. Docker daemon manages heavy and complex actions like running, building, and publishing docker containers. Docker client communicates with the daemon for communication. The docker daemon and client are

capable of running on the same machine. The utilization of the docker client can also facilitate the establishment of a connection with a remote docker daemon. Connecting using a socket or Restful API allows the docker client and daemon to communicate [71] . docker client can be communicate with docker deamon as acts as communication client between them as shown in Figure 2.3.

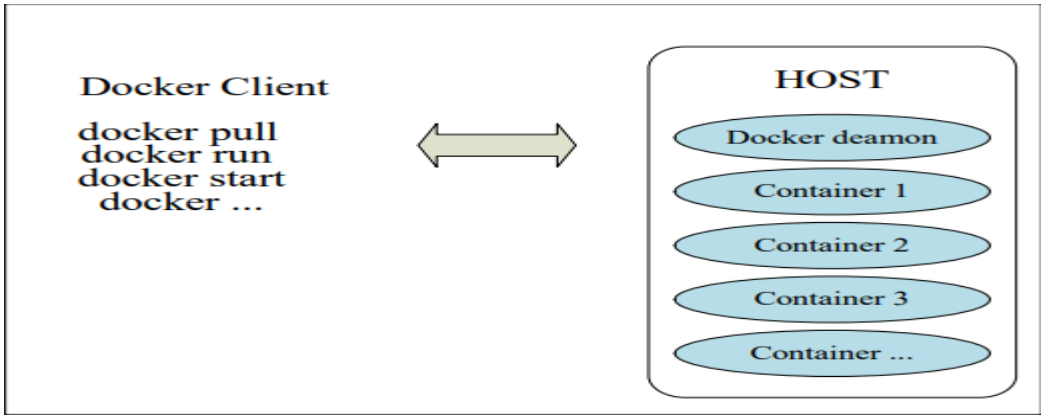


Figure 2.4 Docker Diagram**source**

2.1.6.2 Docker Registries

Assume a user wishes to share his own images that he has developed with other users. The Docker registry is the point at which the idea of Docker is introduced. Docker registries offer a storage platform for images created with Docker. Anybody can pull or push images from Docker hub and Docker cloud, two public registries by default. Docker is made to search for images on Docker Hub. A lot of companies use internal private registries to store their proprietary images. Using the docker run or pull commands, you can retrieve any image. To push an image to your registry, perform the docker push command [72]. An overview of the previous paragraphs shown in Figure 2.5.

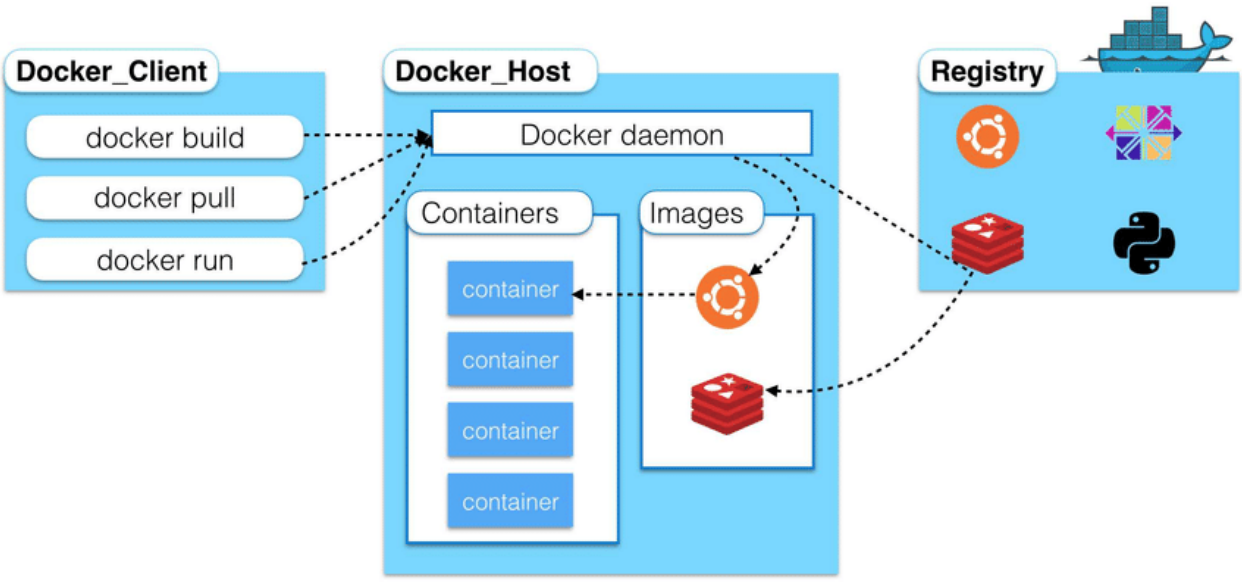


Figure 2.5 Overview of Docker architecture**source**

The Docker architecture is very useful in transferring our application from server to server and from development environment to development environment. What docker does is have all the configurations needed in code in a so-called dockerfile. The dockerfile is a code structure that defines how the servers are to be; for example, if the dockerfile has ubuntu, nginx, and PHP, then running this docker file creates the so-called images, which are the services declared in the dockerfile, and can use them and run them. When the images are running, the so-called running services become containers. To make the implementation better, docker Compose is used to define the services it wants to run without running separate docker files for each of them.

2.1.6.3 Docker Container Communication

The design of docker networking is intended to be reasonably straightforward. There are five main models that are supported: the default bridge, user-defined bridge, host networking, Media Access Control Virtual Local Area Network (MACVLAN), and none. Figure 2.6 presents the initial four models, while the fifth model is an independent container devoid of any network link. If no other network parameters are given, the default bridge network model is utilized throughout container runtime and is configured during Docker installation.

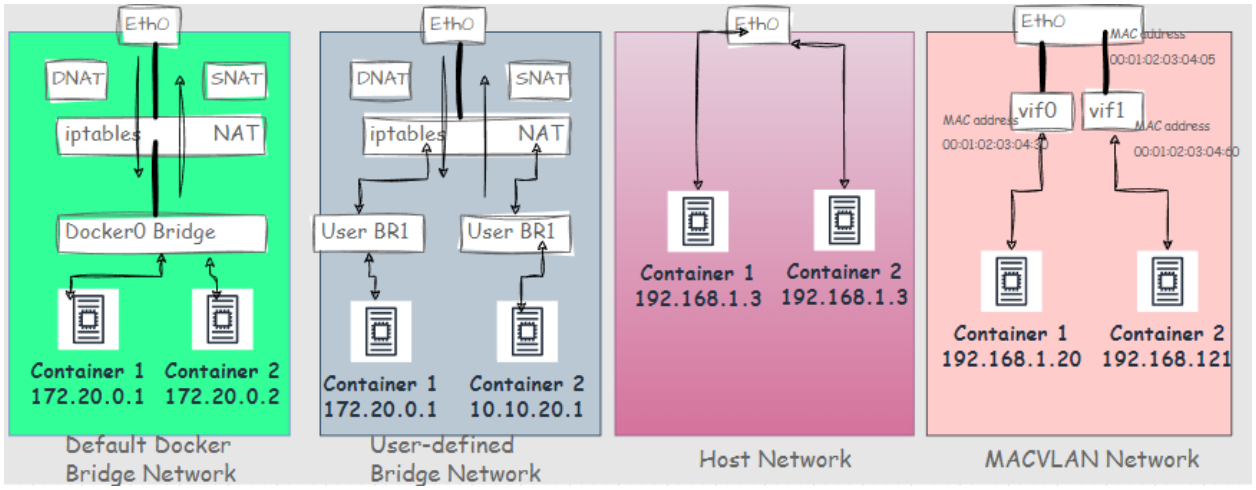


Figure 2.6 Container network model

2.1.6.3.1 Default Docker Bridge

In the default Docker bridge network, when the containers have been deployed, in our case (Container 1 and Container 2), docker automatically creates two Virtual Ethernet Interfaces (Veth) and connects them to it or links them to the Docker0 (the default network created by docker) bridge network as shown in Figure 2.7.



Figure 2.7 Docker0 default bridge network

This kind of acts as a switch, which means the containers can communicate to each other and there is a virtual ethernet interface for each of those containers. The default bridge network not only creates virtual ethernet interfaces, but also allocates IP address which means running Dynamic Host Configuration Protocol (DHCP) and each container have their own IP address.

Suppose Container 1 has a web server running. How does this web server reach out to the internet? For external communication, a protocol called Source Based Network Address Translation (SNAT) is responsible for this function. This process includes the use of a shared host IP address, analogous to the way a router allocates a single public IP address among all the services linked to the network. On the other side, to access any of the services the docker containers might offer, such as a web server, the host machine cannot be reached that services. The protocol called Destination based Network Address Translation (DNAT) is responsible for exposing those ports to the local network and allowing access to the services running on containers. It is common as a port forward or mapping on a home router. SNAT and DNAT in the host-based firewall, commonly referred to as iptables on the Linux system by default, is responsible for managing the connectivity of containers in the wider network [74].

2.1.6.3.2 User-defined bridge Network

The user defined bridge network shown in the gray box in Figure 3.1, the definition has the name of you created it you made it. The key keyword is isolation. The networks are isolated and protected from other networks such as the default network. These two networks cannot communicate with each other, and this is very important for specific purposes. User-defined bridge networks allow users to have more control over network configuration by specifying subnet parameters and bridge interface names. These networks function similarly to standard bridges using DNAT and SNAT but isolate containers on one bridge from another [75].

2.1.6.3.3 Host Network

Docker host networking, shown in the gray box in Figure 3.1, allows containers to share the host's default network namespace, physical network interfaces, and configurations. This model allows administrators to run pre-configured containers without configuring theenvironment, allowing web servers to have the same IP and port 80 by default [76]. However,

this model has some problems. Suppose a nginx container is running and uses the port TCP 4343. Then the same port is consumed on the host machine, and the user can access it using the host IP and the port TCP 4343. In the case of attempting to run another container on the same host with the same services, port and networking mode will fail because port TCP 4343 is already used on the host. Host networking is great in the case of running lots of different containers on a host, which use different ports. The problem starts when running multiple at the same container.

2.1.6.3.4 MACVLAN Network

MACVLAN network shown in the last box in Figure 3.1, that network connects the containers directly to our physical network. The ethernet interfaces directly connected to the switch and get their own Media Access Control (MAC) addresses and the own IP address. Docker uses the kernel's built-in MACVLAN driver for networking, assigning a unique IP address to each container. This is similar to host networking but separates containers from the host's IP or MAC address. MACVLAN interfaces are useful for applications requiring direct network connectivity but requiring isolation from the container. Service providers often support this method for container-based services.

2.1.7 The Role of Gamification via Capture The Flag Challenges in Cybersecurity

Gamified learning platforms have become increasingly popular in the last years, for introducing cyber security education and training.The application of gamification in the field of cyber security through capture the flag is not only a form of gaming, but also an effective means of training and educational practice for cyber security, enabling the cultivation of skills and understanding of the real threats they face and how to face them [77].

The advent of Capture The Flag (CTF) challenges has revolutionized cybersecurity training and skill development by offering a unique, gamified approach to learning and addressing security concerns.Capture The Flag is a type of competition where participantsin these competitions can develop cybersecurity techniques and skills while expanding their knowledge of real-world security scenarios. During the race, participants explore vulnerable resources, discover, and exploit vulnerabilities in a security environment, usually in virtual or

real networks, to solve security problems and earn points, usually by retrieving flags that represent the successful resolution of a problem, familiarizing themselves with security tools, and identifying flags for the final submission of the flag [78].

Cybersecurity Capture The Flag (CTF) is a practice that combines competition and education into one game to train students and professionals in dealing with cybersecurity threats. It is a popular educational tool that allows practice in identifying system vulnerabilities and resolving them by working with real or virtual networks. In recent years the role of gamification as capture the flag has been transferred to both undergraduate and postgraduate levels. The implementation of gamification in computer security labs through online Capture The Flag competitions aims to enhance students' skills. The application reveals that students find the new labs more interactive, collaborative, useful, and motivating, while minimizing administrative, financial, and technical costs through the open-source platforms [79,80].

CTFd is a popular open-source CTF framework used in CTF games. It has several features, some of which are:

Challenge value: Students are aware of the fixed-point value assigned to each problem (question). This value typically indicates the difficulty of the challenge.

Flag submission: Players can check if a flag (answer) sent to the CTF portal is correct. Additionally, they won't be penalized for submitting false flags.

Scoreboard: Displays the overall result of all participating users, which is accessible to all those engaged in the game. The nicknames of the users were anonymized in order to safeguard their privacy.

Hints: Several challenges include one or more hints.Every hint has a fixed cost of points. Once the player sees the hint, the points are subtracted from their existing score. Free hints can also be offered at no cost (0 points).

Some of these are the core features on a large set of platforms focused on Capture the Flag competitions [81].

2.2 Systematic Literature Review on Industry 4.0 and cybersecurity

2.2.1 Methodology

This systematic review methodology aims to thoroughly assess the effectiveness of Cyber Range platforms as an essential part of cybersecurity training for Industry 4.0. By doing this, the review objective is to analyze the purpose of educational guides and investigate the impact of interactive, scenario-based training in preparing students, professionals, and engineers for the complex problems that come with Industry 4.0. The objective of the systematic review is to provide a comprehensive understanding of how these elements collectively contribute to the improvement of participants' skills with learning guides and hands-on practice, cyber security awareness and preparedness to deal with real threats in cyberspace.The Framework that was used in research for systematic review was the (Preferred Reporting Items for Systematic Reviews and Meta-Analyses)**PRISMA** [82]. It helps structure the search strategy for a comprehensive review of existing literature.

2.2.2 Research Questions

The research questions (RQ)is guided by the following questions:

- **RQ1**: How effective are the Cyber Range platforms in providing hands-on training and realistic scenarios in cybersecurity?
- **RQ2**:What is the relationship between the provision of educational guides and the success of participants in solving hands-on cybersecurity challenges?
- **RQ3**: How can interactive, scenario-based training enhance awareness and skills in Industry 4.0 cybersecurity among participants.

The research questions outlined in this systematic review serve as guiding principles, shedding light on critical areas of research in the field of cyber education in the context of Industry 4.0. Each research question is carefully designed to explore key aspects of cyber security education.Through answering these questions, this systematic review objective is to provide significant knowledge to the field of cybersecurity training and education, enhancing our

understanding of the most effective ways to prepare professionals for Industry 4.0's challenges. Research questions can be separated into the following categories:

- **Effectiveness of Cyber Range Platforms (RQ1)**

This category focuses on papers and studies that assess the overall effectiveness of Cyber Range platforms in delivering hands-on training. Discuss the impact of such platforms on participants' skills and preparedness to tackle real-world cyber threats within the context of Industry 4.0.

- **Role of educational guides (RQ2)**

This category centers on educational guides' role and impact. Identified papers that discuss the influence of educational guides on hands-on cybersecurity challenges. Analyze the role of these guides in enhancing learning outcomes.

- **Interactive, Scenario-based Training (RQ3)**

This topic delves into the concept of interactive, scenario-based training. Providing papers that explore the utilization of realistic scenarios and interactive techniques with hands-on experience, in the field of cybersecurity education. Discussing why this way enhances participants' awareness and practical skills in Industry 4.0 cybersecurity.

2.2.3 Eligibility criteria

The PRISMA framework, which is frequently used for systematic includes screening criteria that determine the appropriateness of studies for incorporation into the review. Depending on the study question and subject matter, the exact screening criteria may change, although the following general standards are frequently used.

The **InclusionCriteria** are as follows:

- Articles that are directly relevant to Cyber Range platforms for Industry 4.0 cybersecurity training are included in the selection of papers for this systematic review.

- Studies that are included in the research must be in accordance with the research objectives that are set within each of the three separate categories of research questionsas described before. These topics include papers on the relevance of educationalguides, the efficacy of cyber range platforms, and the effects of interactive, scenario-based training.English language publications are taken into consideration, and the publication date must fall within a given window of time to guarantee currency. Most of the selected papers are between the years 2020-2023. With4 articles selected by honorable mention.

Exclusion Criteria

- Exclusion criteria includeBook and Chapter, Editorials, duplicate studies, Early access, Proceedings papers, posters, not published in English.
- Papers that do not address the specified study fields.
- Papers from other scientific fields except computer science

The initial set of 2573 papers were whittled down to 75 papers that underwent additional analysis following the filtering procedure in Figure 2.8

2.2.3 Database Selection

Common databases used in cybersecurity and Industry 4.0 research are selected, including IEEE Xplore, Google Scholar, Scopus, and mdpi. In Figure 2.9 depicts a representation of the systematic review process based on these digital libraries.

2.2.4 Keywords Selection

In this review, multi-search queries were used, which are listed below. Some search queries are merged without meaning they were used as is and some others used as single query. The queries were tailored to meet the specific query writing requirements for each of the digital libraries and search engines used.

"Capture the flag" AND "Cyber Security"

"Cybersecurity skills development" OR "security training"

"Cybersecurity skills development" OR "security training" OR "capture the flag" OR "docker security" OR "Cyber range"

"SQL injection" OR "forensic analysis" OR "man-in-the-middle attacks" OR "Snort detection"

"cybersecurity" and "challenges"

Figure 2.8shows how the seven groups of keywords discovered mirror each other. Keyword usage from publications was analyzed for representativeness. Authors define keywords with general or specific research-related terminology in order to pique readers' interest. The largest circle denotes the representativeness of a group of terms. The most representative cluster is Cluster 1 (red), Cluster 3 (green) and Cluster 2 (blue) follow, and then the rest.

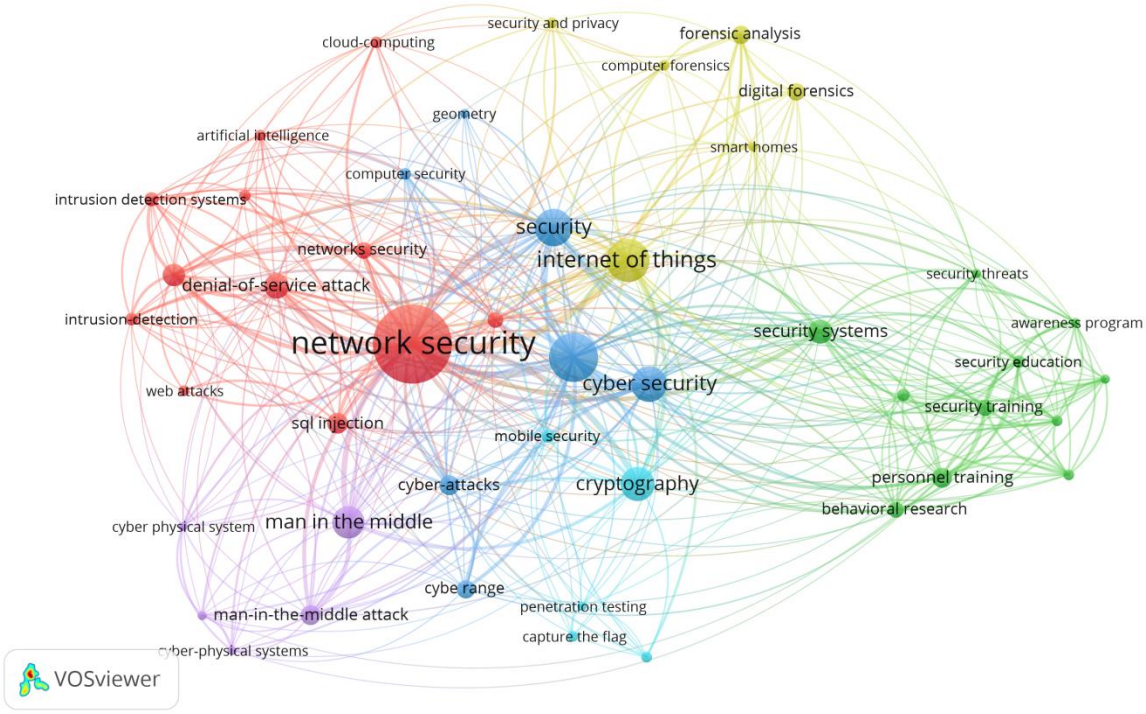


Figure 2.8 Keywords representation in Clusters.

2.2.5 Screening - Results

Total papers through the keyword searches were 2573. The screening of the abstracts was done for those papers that were included; they got 1, for those that were rejected, they got 0, and for those that were both yes and no, they got 2.Out of the total selected papers 44, in total were selected by the research process in Figure2.9. All papers were categorized into three categories according to the research questions. Figure 2.10presents the percentages for each category. 36%

of (16) publications refer to the effectiveness of Cyber Range platforms, 32% of the results (14)on educational guides' role and impact to solve cybersecurity challenges and 32%, (14) presented the utilization of realistic scenarios and interactive techniques with hands-on, in the cybersecurity field. In Figure 2.11 presents the papers according to the year they were published. Most papers are presented between the years 2021 and 2023 (37) in total, with some honorable exceptions in the (5) remaining papers. Thus, this means that the analysis is recent in terms of cybersecuritytechnologies and findings.All of the papers that were part of this systematic review are shown in Table 1, along with the enumeration number, title, year of publication, associated category (RQ), and reference.

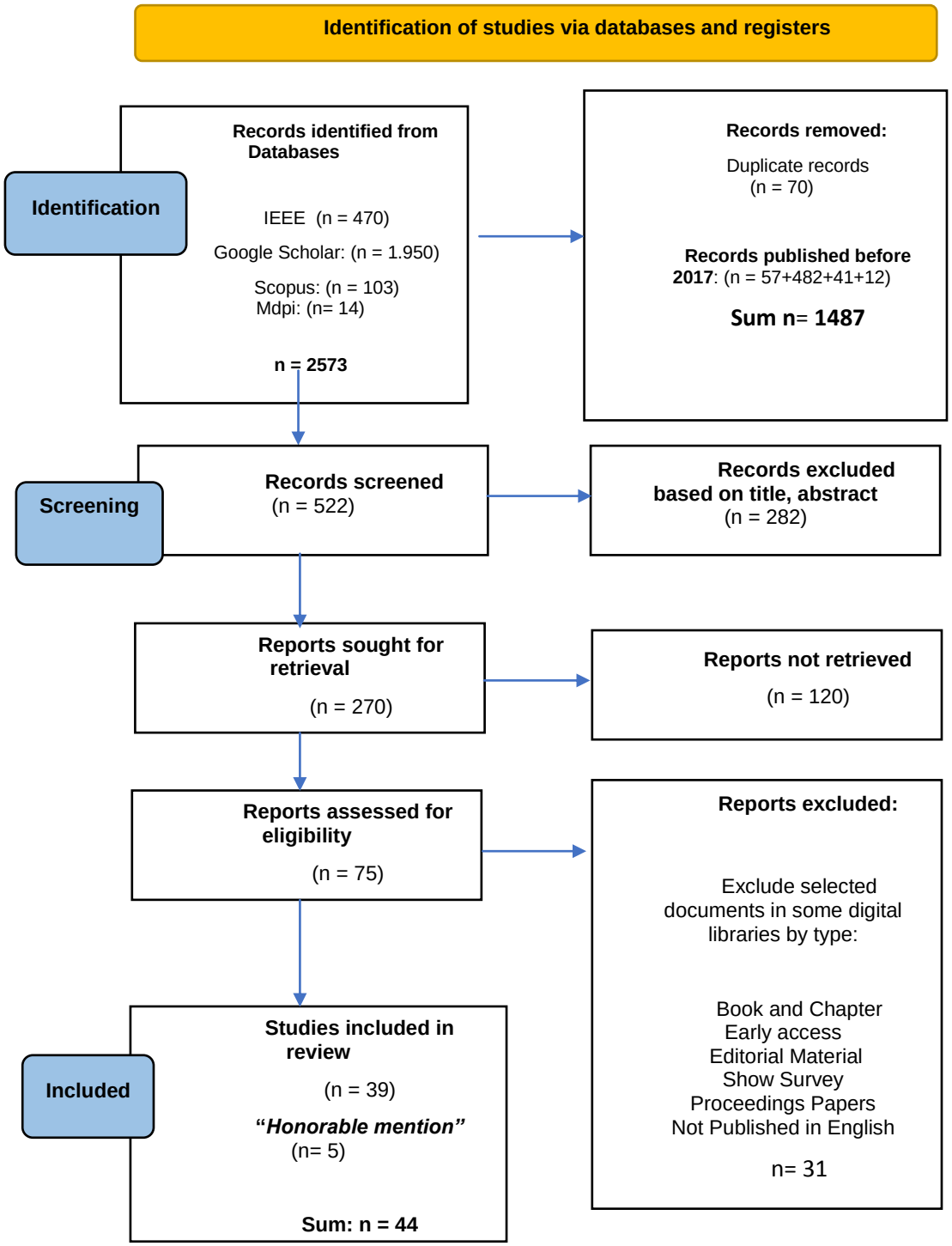


Figure 2.9 Overview of the systematic review procedure according to PRISMA flow diagram.

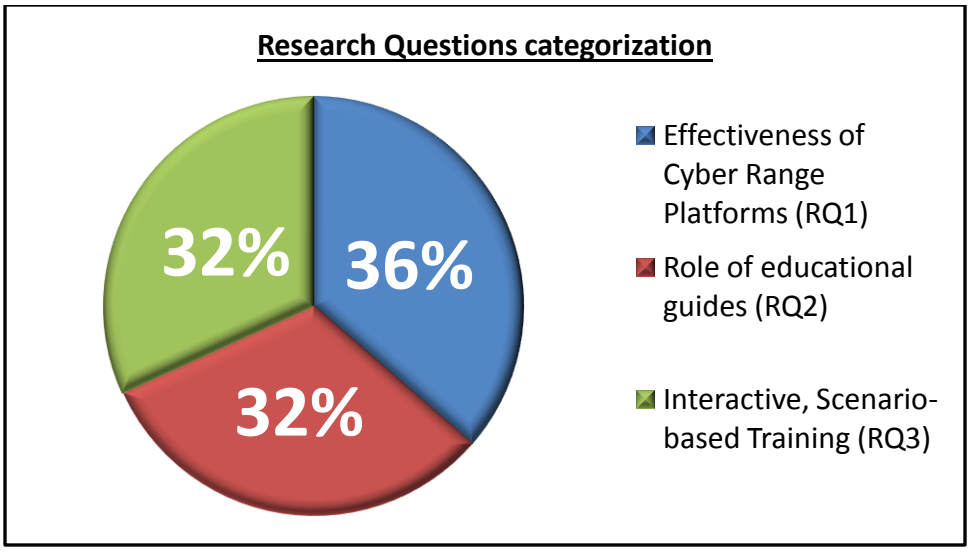


Figure 2.10 RQ1, RQ2, RQ3 categorization in percentage.

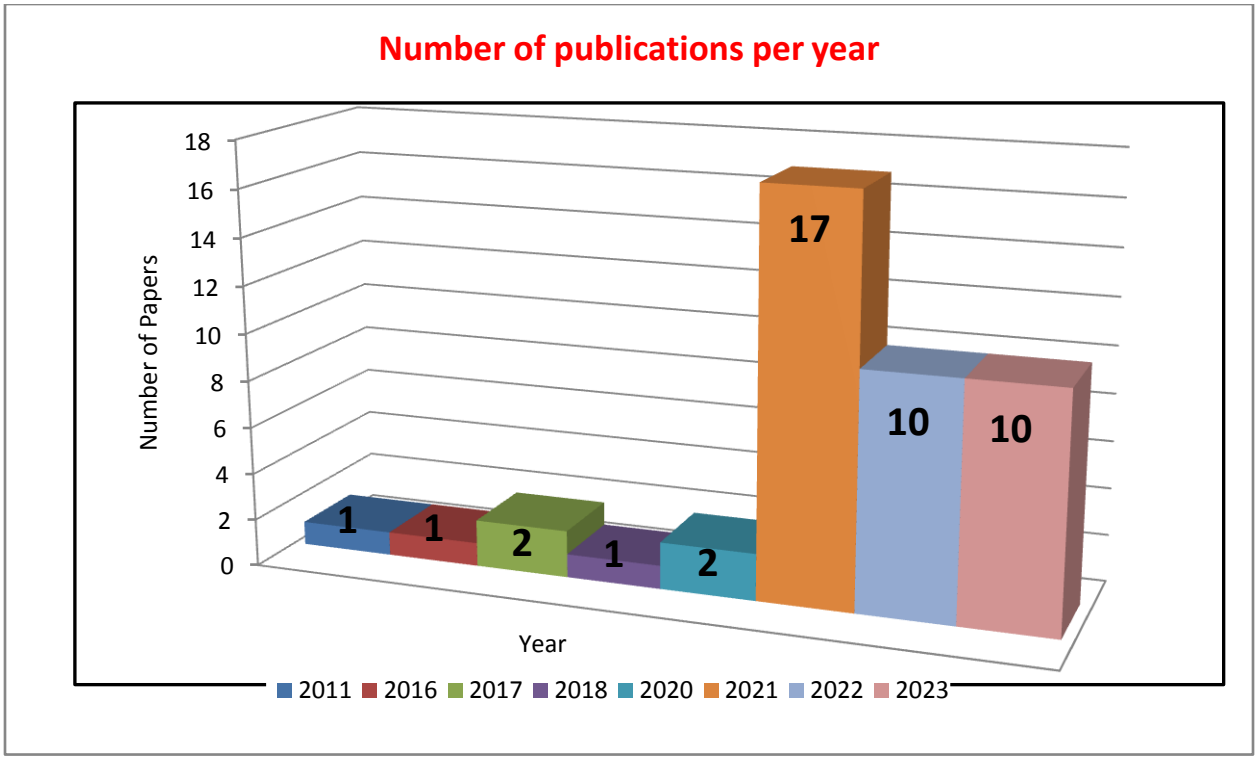


Figure 2.11 Number of publications per year.

Table 1 All papers included in the systematic literature review.

No.	Publication Year	Publication Title	Category	Reference
1	2017	Enabling practical experimentation in cyber-security training	Role of educational guides (RQ2)	[8]
2	2023	A Decade of Studies on Cyber Security Training in Organizations using Social Network Analysis: A Systematic Literature Review Through Keyword co-Occurrence Network	Role of educational guides (RQ2)	[37]
3	2023	Role of Artificial Intelligence based Chat Generative Pre-trained Transformer (ChatGPT) in Cyber Security	Role of educational guides (RQ2)	[38]
4	2023	Real World Autonomous IoT Based Data Privacy Protection Using Machine Learning	Interactive, Scenario-based Training (RQ3)	[39]
5	2023	A Comparative Study of Cyber Security Awareness, Competence and Behavior	Role of educational guides (RQ2)	[40]
6	2022	Gamification of Cyber Security Training - EnsureSecure	Effectiveness of Cyber Range Platforms (RQ1)	[41]
7	2022	ExploitWP2Docker: a Platform for Automating the Generation of Vulnerable WordPress Environments for Cyber Ranges	Effectiveness of Cyber Range Platforms (RQ1)	[5]
8	2022	Research and Design of Network Information Security Attack and Defense Practical Training Platform based on ThinkPHP Framework	Effectiveness of Cyber Range Platforms (RQ1)	[42]
9	2022	Security Scenarios Automation and Deployment in Virtual Environment using Ansible	Interactive, Scenario-based Training (RQ3)	[43]
10	2022	Ethical Hacking and Web Security: Approach Interpretation	Role of educational guides (RQ2)	[44]
11	2021	A Review on Gamification for Information Security Training	Interactive, Scenario-based Training (RQ3)	[45]
12	2021	Unveiling the user requirements of a cyber range for 5G security testing and training	Effectiveness of Cyber Range Platforms (RQ1)	[46]
13	2021	Privilege Escalation Focused Offensive Security Training Platform	Effectiveness of Cyber Range Platforms (RQ1)	[47]
14	2021	The THREAT-ARREST Cyber Range Platform	Effectiveness of Cyber Range Platforms (RQ1)	[48]
15	2021	Frankenstack: Real-time Cyberattack Detection and Feedback System for Technical Cyber Exercises	Effectiveness of Cyber Range Platforms (RQ1)	[49]
16	2021	Cyber-Security Training Evaluation	Role of educational	[50]

		Metrics	guides (RQ2)	
17	2021	Wireless Cybersecurity Education: A Focus on Curriculum	Interactive, Scenario-based Training (RQ3)	[51]
18	2022	Learning Cybersecurity in IoT-based Applications through a Capture the Flag Competition	Interactive, Scenario-based Training (RQ3)	[2]
19	2021	Software Security (Capture the Flag)	Interactive, Scenario-based Training (RQ3)	[52]
20	2021	Hacking an IoT Home: New opportunities for cyber security education combining remote learning with cyber-physical systems	Role of educational guides (RQ2)	[53]
21	2020	Eliciting Requirements for a Student-focussed Capture The Flag	Role of educational guides (RQ2)	[54]
22	2021	An Implementation of Capture the Flag (CTF) Tool	Interactive, Scenario-based Training (RQ3)	[55]
23	2022	Strengthening Database Security with Capture the Flag Exercises	Interactive, Scenario-based Training (RQ3)	[10]
24	2021	Open Source and Commercial Capture The Flag Cyber Security Learning Platforms - A Case Study	Effectiveness of Cyber Range Platforms (RQ1)	[56]
25	2021	Bridging the Gap: Adapting a Security Education Platform to a New Audience	Effectiveness of Cyber Range Platforms (RQ1)	[57]
26	2023	Experimental Analysis of Security Attacks for Docker Container Communications	Interactive, Scenario-based Training (RQ3)	[58]
27	2021	Metapod: Accessible Hardening of Docker Containers for Enhanced Security	Interactive, Scenario-based Training (RQ3)	[59]
28	2022	On-demand deployment and orchestration of Cyber Ranges in the Cloud	Effectiveness of Cyber Range Platforms (RQ1)	[60]
29	2023	Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey	Effectiveness of Cyber Range Platforms (RQ1)	[1]
30	2021	A next-generation platform for Cyber Range-as-a-Service	Effectiveness of Cyber Range Platforms (RQ1)	[61]
31	2021	Cybersecurity knowledge and skills taught in capture the flag challenges	Role of educational guides (RQ2)	[62]
32	2023	Addressing Cybersecurity Challenges in Education	Role of educational guides (RQ2)	[63]
33	2018	Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience	Role of educational guides (RQ2)	[9]
34	2023	Cyber range design framework for cyber security education and training	Effectiveness of Cyber Range Platforms (RQ1)	[15]
35	2021	A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead	Interactive, Scenario-based Training (RQ3)	[83]

36	2017	Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool	Role of educational guides (RQ2)	[14]
37	2022	Effectiveness Analysis of Public Rule Sets Used in Snort Intrusion Detection System	Interactive, Scenario-based Training (RQ3)	[11]
38	2016	Developing and evaluating a hands-on lab for teaching local area network vulnerabilities	Interactive, Scenario-based Training (RQ3)	[13]
39	2021	Network Forensics: An approach towards detecting Cyber Crime	Interactive, Scenario-based Training (RQ3)	[12]
40	2022	Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework MDPI	Effectiveness of Cyber Range Platforms (RQ1)	[64]
41	2023	A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience	Effectiveness of Cyber Range Platforms (RQ1)	[65]
42	2020	A Review of Cyber-Ranges and Test-Beds: Current and Future Trends	Effectiveness of Cyber Range Platforms (RQ1)	[66]
43	2023	A personalized learning theory-based cyber-security training exercise	Role of educational guides (RQ2)	[67]
44	2011	Experiences In Cyber Security Education: The MIT Lincoln Laboratory Capture-the-Flag Exercise	Role of educational guides (RQ2)	[68]

2.2.6 General Review

This section presents the results of the general review of some of the search queries used. This research provides an overview of the evolution and the number of research papers over the past 5 years under the keywords. The database used was google scholar.

- capture the flag AND Cybersecurity
- Industry 4.0 cybersecurity and cybersecurity training
- cybersecurity and gamification

Figure 2.12 presents the number of papers per year, according to keywords. Based on the information that has been gathered, it is feasible to confirm that:

- The publications of the last five years have increased in every keyword between the 3 combinations.

- In the keyword Industry 4.0 cybersecurity and cybersecurity training, the papers that were published in 2018 were 15.600 and in 2020 were 20.800, indicated that there is an impact in the research community.
- The rising linear lines of each year on each chosen keyword can also show this.
- Calculating, the median factor between the years 2018 - 2022, the result is 1.088. This indicates that, on average, there was an increase in the number of papers published from one year to the next.

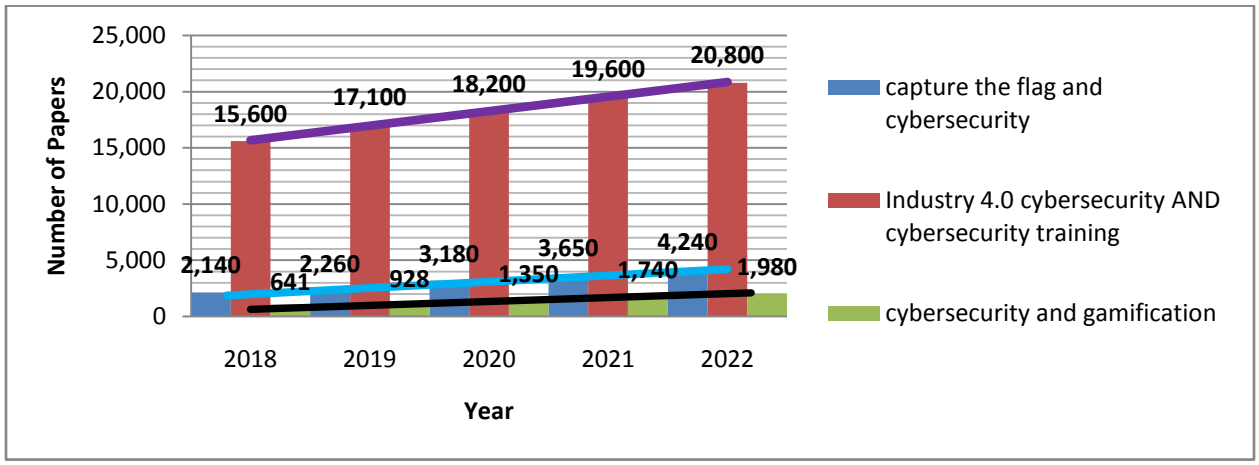


Figure 2.12 General Review - number of papers according to keyword searching.

2.3 Related works

This section discusses,according to Table 1, the categoriesof the selected papers,considering the overall effectiveness of Cyber Range platforms in delivering hands-on training, the role, impact, and influence of educational guides to prepare the participants' background knowledge,and the role of interactive, scenario-based training.

2.3.1 Effectiveness of Cyber Range Platforms

The authors of [41]discussed the growing concern about cyberattacks in the modern workplace and the importance of effective workplace training. It criticizes conventional training methods for their lack of engagement, hindering information retention, especially for non-experienced participants. The study proposes a conceptual physical card game as an e-learning resource to enhance cybersecurity knowledge retention. The paper outlines the preliminary

research, design phases, and evaluation process of this innovative approach to improving cybersecurity training. A method [5], which uses container-based virtualization and extracts data from exploit databases, enhances the realism and effectiveness of cyber range training by automating the generation of vulnerable environments. The work presented in [42] presents a practical cyber range training framework called ThinkPHPfor network information security attack and defenseto address the information security expert shortage and provide a communication hub for information security enthusiasts and students, incorporating support vector machine algorithms for personalized services.In [46], it discusses the need for 5G security training in cyber ranges, highlighting the effectiveness of the EU-funded SPIDER project's Cyber Range as a Service (CRaaS) platform for 5G cybersecurity testing and training. The evaluation framework used was gathered through questionnaires distributed to telecom industry stakeholders, providing insights for developing 5G training capabilities within a cyber range. The paper [47] aims to address this by designing a training system platform that improves privilege escalation skills among security personnel using containerization and virtualization technologies.

Emerging technologies like IoT and 5G communications are driving digital transformation, but they also present complex attack surfaces. Cyber security training is becoming mandatory, and the authors of [48] presented the THREAT-ARREST platform, which offers modern training features like emulation, simulation, serious games, and fabricated data. The platform has been evaluated in smart energy, intelligent transportation, and healthcare domains.M.Pihelgas et al. [49] introduces Frankenstack, a situation awareness framework designed to enhance cybersecurity expertise by providing real-time feedback during exercises and verifying monitoring tools' performance. Redeveloped to improve data collection and detection capabilities, it serves as a reference for other monitoring frameworks, bridging the gap between theoretical research and practical implementation.Gamified learning platforms, as described by Authors in [56],are increasingly used for cyber security education, training, and awareness. The paper compares related work and contemporary literature to identify the best platforms for gamified cyber security learning. It develops a metric for comparing these platforms and applies it to the most popular ones.The authors in [57] report that the current shortage of specialized cyber security professionals is insufficient for digitization. To address this, higher education students need to be introduced to cyber security. Haaukins, a cyber rangetraining platform, was developed to support this need. Design principles were adapted to

cater to different target audiences, including dynamic tooling, centralized access, and scalability. Implementation has shown its viability in various institutions. The paper [60] introduces a framework for dynamically deploying, configuring, and orchestrating cyber ranges in a cloud-based environment, using a distributed architecture for environment isolation, remote access management, procedure automation, secure operation, and accountability, and implementing it using Amazon Web Services.The rise of cyberattacks in the industrial sector, driven by digitization and Industry 4.0 technologies, poses risks to organizations. Artificial intelligence-based cyberattacks, which can be combined with conventional technologies, can cause exponential damage. This paper presents systematic literature research to identify and analyze AI-based cyberattacks, aiming to provide insights for developing defenses against future threats and guide the analysis of cyberattacks supported by AI, as presented in [1]. The authors of [61] present that the Cyber Ranges have become popular for training to respond to cyber threats, with cloud computing playing a crucial role. However, setup and management can be expensive. Next-generation platforms offer features like virtual cloning, automated monitoring, and behavior emulation, reducing setup and management costs.Also, the authors of [15] agree that the Cyber Ranges (CRs) are essential for effective training in critical infrastructures and corporations. However, there is a lack of standards and methodologies for their development and effectiveness. To strengthen cyber security education and research, the Cyber Range Design Framework (CRDF) is proposed. CRDF builds on the Conceptual Framework for eLearning and Training (COFELET) and the Exercise Life Cycle, aiming to optimize CRs' impact, mitigate weaknesses, and minimize preparation and running costs.P. Rajesh et al. [64] discuss the importance of cyber intelligence in protecting information and analyzes current frameworks like Diamond Model, Cyberkill Chain, and MitreAtt&ck. It concludes that MitreAtt&ck is the most suitable due to its flexibility, permanent updates, and powerful database. The paper also discusses how MitreAtt&ck can be integrated with artificial intelligence research for detecting cyberattack patterns.Another framework from the authors of [65] for implementing cyber threat intelligence (CTI) in organizations includes a knowledge base, detection models and visualization dashboards. The framework includes behavior-based, signature-based, and anomaly-based detection, and provides insights for future studies on adjusting approaches to meet organizational needs and resources. The authors in [66] mention Cyber-situational awareness is crucial for understanding threats and vulnerabilities within organizations. The rapid

increase in the automation of cyberattacks reduces the gap between information and operational technologies. Reviewing current robustness against sophisticated cyber-attacks, trends, technologies, and mitigation countermeasures is essential. CRs' and Test-Beds (TBs) platforms help in understanding attack evolution and deploying countermeasures.

In conclusion, the effectiveness of CRs' platforms highlights the growing concern about cyberattacks and the need for effective cybersecurity training. Proposed various innovative approaches, such as physical card games, container-based virtualization, and gamified learning platforms, to enhance knowledge retention and improve training outcomes. The papers also emphasize the importance of cyber ranges as training platforms, with features like emulation, simulation, and behavior emulation. Additionally, the papers address the shortage of cybersecurity professionals and the need to introduce cybersecurity education in higher education. They also discuss frameworks and methodologies for developing and implementing cyber ranges, as well as the integration of artificial intelligence and cyber threat intelligence in cybersecurity defense. Overall, these papers contribute to the advancement of cybersecurity training and defense strategies in the face of evolving cyber threats.

2.3.2 Role of educational guides

In [8]the authors discuss the importance of practical skills in cybersecurity education, highlighting the development of infrastructures and curricula to promote experimentation and enhance students' understanding of theoretical knowledge.The authors of [37] explored the importance of cyber security training for organizations to stay compliant and competitive. Uses clustering and social network analysis to map the state of cyber security training research. The findings reveal core topics in training, including immersive technologies for better understanding employees' cyber behavior. This quantitative approach fills a critical gap in cyber security training reviews, providing valuable insights for organizations. The paper [38] examines the potential of Artificial Intelligence-based Chat Generative Pre-Trained Transformer (ChatGPT) in assisting Chief Information Security Officers (CISOs) in their role of threat prevention and management in the evolving field of Cyber Security. It explores if ChatGPT can effectively aid CISOs in their tasks and contribute to a cyber-resilient organization.The work presented in [40]investigates the relationship between human awareness, knowledge, and behavior in relation to security tools. It found that, despite understanding cyber threats, internet users only take a few

simple precautions. The study also found a connection between greater cyber experience and understanding and the threshold of cyber awareness, beyond differences in participant countries or gender. K. Yadav et al. [44] highlights that cyber security training emphasizes the ethics of hacking and web safety, as identifying flaws in computer technology is crucial for effective web security. Growth hacking is a popular marketing strategy, but failure can lead to cybervandalism or disappointment. Ethical hackers help consumers understand security requirements, while web security protects information and computers from threats.The [50]reviews trainee performance assessment metrics in cyber-security training, aiming to assist designers in identifying the most prominent means for their training programs and identify additional research directions involving evaluation metrics. The goal is to help cybersecurity professionals acquire the necessary knowledge and skills to combat increasing cyberattacks.

A new approach is proposed in [53] to inspire a new generation of learners to teach cyber security. Traditional capture the flag (CTF) exercises are combined with interactive sessions via video conferencing platforms and home IoT devices. This interactive and engaging experience benefits from remote working, inspiring the notion of hacking an IoT home.Another capture the flag approach presented in [54] aimed to identify the requirements of a student-focused capture the flag (CTF) exercise, which may help promote student engagement and learning in the field. In the same concept, the authors of [62] present the capture the flag challenges as a popular platformfor cybersecurity education that involves students solving hands-on tasks in an informal setting. However, the skills practiced by these challenges may not align with formal cybersecurity curricula. The analysis reveals that technical knowledge is predominant. Future challenges should include non-technical aspects to address advanced cyber threats. Will Triplette et al. [63] explorecybersecurity challenges in education, particularly in the conceptof online learning. A systematic review of ten studies found that game-based strategies effectively increase students' awareness and interest in cybersecurity.In [9],thedemand for cybersecurity graduates is increasing, prompting universities to develop new courses. However, creating safe, secure, and reusable cybersecurity exercises is challenging due to legal, operational, and pedagogical challenges. This article provides course designers with principles to maximize student success while minimizing organizational risk, based on a Midwestern university's experience. The findings of the [14] a large-scale survey of 588 cybersecurity competition participants revealed that those with higher self-efficacy, rational decision-making style, and investigative interests

were more likely to pursue a cybersecurity career after the competition.The study also examined individual differences between self-proclaimed hackers and non-hackers, males and females, and cybersecurity employees versus students.The authors in [67] present that the development of cyber-security training programs has been criticized for being inadequate or ineffective. A personalized learning theory-based model was developed to address this issue. The model was tested on 12 students from the Norwegian Institute of Science and Technology Information Security master's degree program, resulting in increased engagement and motivation. The work presented in [68] discusses the design and organization of an education-focused Cybersecurity Capture the Flag (CTF) at MIT/LL, aiming to make the event accessible to a wider community, despite the limited educational opportunities.

In conclusion, the related works discussed in this collection highlight the importance of practical skills in cybersecurity education, the need for cyber security training in organizations, the potential of Artificial Intelligence in the cybersecurity field, the relationship between human awareness and behavior in relation to security tools, the ethics of the hacking concept, trainee performance assessment metrics in cyber-security training, new approaches to inspire learners in teaching cyber security, the use of capture the flag exercises in cybersecurity education are very important, the challenges in cybersecurity education and the development of effective training programs. These papers provide valuable insights and recommendations for improving cybersecurity education and training programs.

2.3.3 Interactive, Scenario-based Training

D. Jagadeesan et al. [39] discuss the importance of practical skills in cybersecurity education, the role of immersive technologies in training, and the potential of artificial intelligence-based chat generative pre-trained transformers in assisting cybersecurity students and professionals in threat prevention and management. It also highlights the need for trainee performance assessment metrics in training programs. The methodology also proposes a new approach to teaching cybersecurity, combining traditional exercises with interactive sessions via video conferencing and IoT devices. It also discusses the challenges in creating safe, secure, and reusable cybersecurity exercises and the development of personalized learning theory-based models.The paper [43] highlights the need for cybersecurity learning environments and introduces a cyber range platform for virtual security training. It uses cloud technology and

automation with Ansible to create virtual environments for effective training. The platform's effectiveness in training cybersecurity is demonstrated, in future research suggests exploring cybersecurity challenges in virtual reality platforms.The authors of [45] discuss the effectiveness of information security training programs in reducing user attacks. It highlights the need for efficient use of prevention techniques and gamification as a tool to counter existing weaknesses in training. The paper also explores the selection of effective training methods and their gaps.In the work presented in [51], higher education is urged to improve cyber education, including hands-on experiential training. Despite the availability of tools and techniques, traditional cybersecurity training primarily focuses on wireless. This research aims to identify nascent cyber training emphasizing a broader spectrum of wireless security and encourage curricular development that includes critical experiential training.In [2], the IoT, a key component of Industry 4.0, enhances performance and responsiveness but also poses security risks. To address these challenges, a Capture the Flag competition on IoT cybersecurity is proposed. This hands-on competition aims to educate students and professionals on designing secure systems and managing cyber threats.The authors of [52] aim to guide the capture of the flag process, different cyberattack phases, and defense from intrusion attempts. It focuses on developing and hardening system file permission, such as setting up scanners for setUID/sGUID permissions.

Cybersecurity competitions presented in [55] are gaining popularity for computer security education. This task analyzed 3600 issues from 150 competitions over two years, identifying safety issues relevant to industry and academia. It provided safety tools and techniques for players, offering exercises for newcomers to practice system security threats identification and prevention.Database security is crucial for protecting websites and IT services. Analyzed by the authors in [10], capture the flag attacks simulation to map existing weaknesses and vulnerabilities into CTF style problems. It identifies databases vulnerabilities not covered by CTF challenges and discusses adding these fields to offensive security exercises. In [58] the Docker, an open-source platform for running applications as containers, is popular for cloud services due to its portability and lightweight nature. However, recent cyberattacks, such as DDoS and cryptocurrency mining, have exploited its vulnerabilities. This paper investigates these attacks, analyzing network traffic, CPU consumption, and malicious reverse shell execution. The findings aim to detect and prevent lateral movement attacks between Docker containers. The authors also describe in [59] that the containers are popular for building scalable

applications, but they also come with security vulnerabilities. Existing hardening methods require prior knowledge of concepts and application procedures. The work of the authors aims to create an easy-to-use application that simplifies incorporating recommended security practices in Docker containers, allowing developers to manage security controls intuitively, giving them more time to focus on application development.The work presented in [83] presentsa systematic review of attacks, vulnerabilities, and defense strategies in Industry 4.0, focusing on network layer attacks, particularly dos-related and mitm attacks. Vulnerabilities include security flaws in services and source code, and incorrect validations in authentication procedures. Blockchain is a relevant defense technology used in various solutions, like intrusion detection systems and preventing Distributed Dos attacks. However, most defense strategies are seen as after-attack solutions rather than mitigation strategies. The paper in [11] tests the effectiveness of public rule sets for snort intrusion detection against various attack traffic types. Experiments were conducted with different rule sets, including CVE-referenced vulnerability exploitation attacks, web application attacks, and malware traffic. The most effective rule set was the Talos rule set when used alone, while the highest efficiency was achieved when all rule sets were used together.In [12], presented two types of systems are used to analyze network traffic: batch-based and sequential-based. Packet analyzers are open-source tools that can efficiently study packet behavior and help identify suspicious packets, providing secure networks and conducting network forensics in various aspects like port filtering, packet follow-up, raw data collection, and tracing of network threats. The authors in Verizon's [13] data breach investigation report highlightreport highlights LAN access as a top vector for insider threats. Address Resolution Protocol (ARP) vulnerabilities are common in Ethernet. Students should learn these vulnerabilities and countermeasures. A hands-on lab is introduced to help students create ARP spoofing packets, allowing them to understand the attack mechanisms deeper. Tests and surveys show the lab's effectiveness in helping students understand LAN vulnerabilities and motivate them to learn more about cyber security.

From the papers analyzed, it can be concluded that practical skills are crucial in cybersecurity education.The use of cloud technology and automation can create effective virtual environments for security training. Gamification and personalized learning theory-based models can enhance information security training programs. There is a need for broader spectrum training that includes wireless security and more offensive techniques and challenges. Capture

the flag competitions and cybersecurity competitions are effective in educating students and professionals on designing secure systems and managing cyber threats. Database security and Docker container security are some examples of important areas of focus. Industry 4.0 vulnerabilities, network layer attacks, and defense strategies are also significant topics. Intrusion detection systems and packet analyzers are valuable tools for network security analysis. LAN access and ARP vulnerabilities are common vectors for insider threats, and hands-on labs can help students understand these vulnerabilities. Overall, these papers emphasize the importance of practical training, the use of innovative technologies, and the need for comprehensive cybersecurity hands-on training with interactivity and realistic scenarios.

Chapter 3 - System Design

Chapter 3, entitled "System Design," aims to clarify the architectural and organizational structure of our cybersecurity training system. The entities in the system andthe tools and technologies used are the main topics of this chapter. Also, we demonstrate how docker container networking is designed in the context of our cyber-range platform.

3.1 Infrastructure Organization

The structural components related to the organization of the system infrastructure described in this sub-chapter, such as the virtual machine (VM) as the main implementation core system that hosts the cybersecurity platform. The ubuntu 22.0.4 VM contains the containers deployed for each necessary system component, describes the services running in the virtual machine (VM), provides the IP addresses assigned to each component that is part of the network, and assigns the overall IP address that it has assigned.

Figure 3.1 represents a basic system networkarchitecture. When the user visits the index web page, in our case the welcome page of the CTFd platform, the traffic passes through the cloud firewall. If the traffic passes, the central cloudVM,which is responsible for all the implementation of the docker networks andto create the appropriate containers for the cftd and naumachia, where the userwith the mapping port 8080, the docker host forwards the request from the index page and the docker container translates it to port 8080 to be accessible to visit the web page. Also includes a VPN tunnel where the user can access the challenges througha Virtual Private Network(VPN).

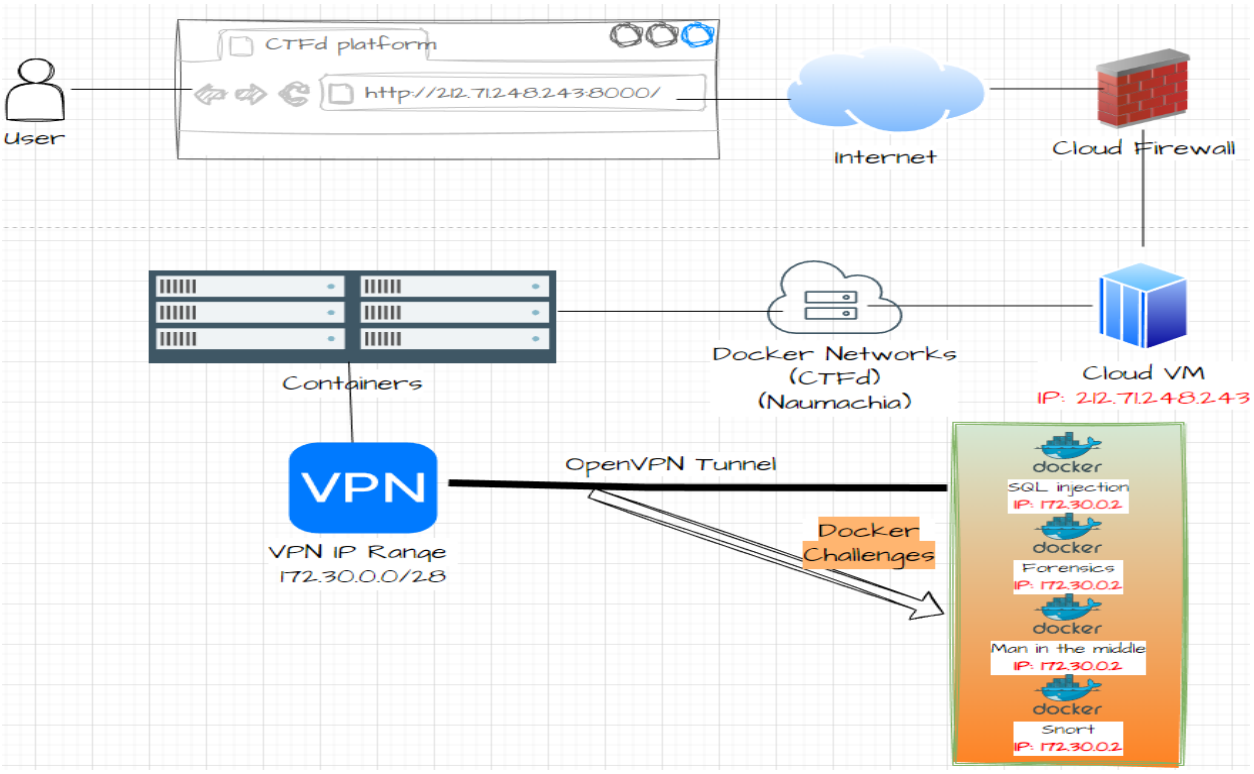


Figure 3.1 Network Architecture

3.1.1Virtual Machine Networking Services

The representation in Figure 3.2 shows several services running to implement the cyber range system. The two main ones that run inside the cloud virtual machine are ssh and docker, where docker runs various containers such as ctfd and Naumachia, where they also run other services for the results.The diagram should also represent the network architecture, illustrating how services within the VM communicate and interact with the internal networks.

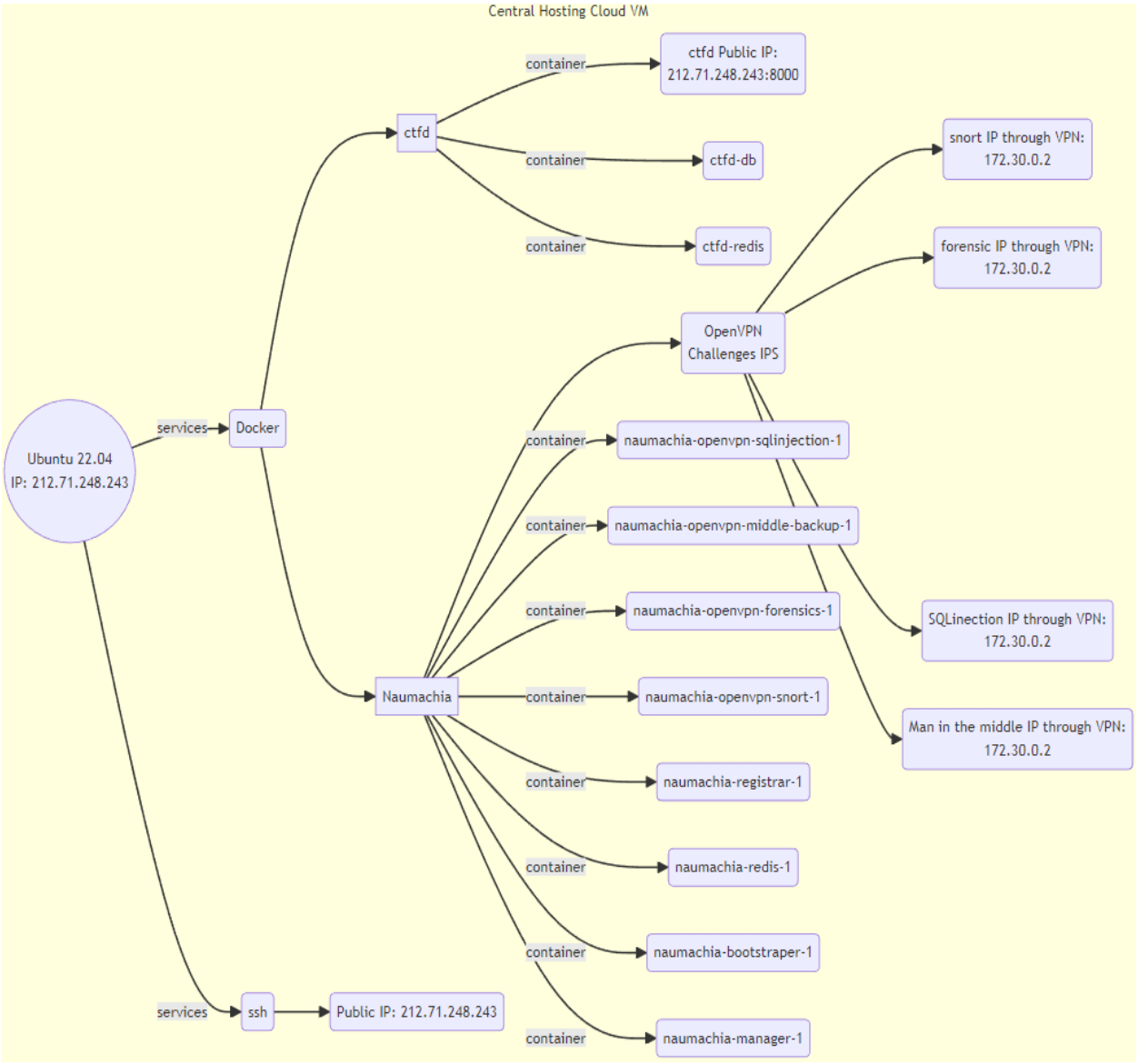


Figure 3.2 Network architecture analysis

A summary of the IPs, containers and networks used by the previous image is summarized in Table 2, where the CTFd elements are illustrated in blue, and Naumachia'sin Green.

Table 2 Summarization table

Containers	Local IPs	Network Bridges
Ctfd	172.20.0.4/16 172.21.0.2/16	Internal Default
ctfd-db	172.20.0.2/16	Internal

ctfd-Redis	172.20.0.3/16	Internal
Naumachia-Registrar	172.18.0.3/16 172.19.0.2/16	InternalDefault
Naumachia-sqlinjection	172.18.05/16 172.19.0.3/16	Internal Default
Naumachia-Snort	172.18.0.6/16 172.19.0.4/16	Internal, Default
Naumachia-middle(mitm)	172.18.0.7/16 172.19.0.5/16	Internal Default
Naumachia-Forensics	172.18.0.8/16 172.19.0.6/16	Internal Default
Naumachia-manager	172.18.0.4/16	Internal
Naumachia-redis	172.18.0.2/16	Internal

Figure 3.3 shows another infrastructure in an isolated network (176.16.11.0/24), with access to it via a VPN connection and the tools were used. Some services were implemented to demonstrate and testthe functionality of the challenges. Some of them that were installed areWordPress for the forensics challenge and using the Hydra tool to bruteforce the SSH credentials by logging the packets with wireshark.Then,Apache2 and MySQL database were installed for the SQLinjection challenge and the SQLmap tool was used to test the challenge automatically. A restricted shell that a usercan access the VM, where the user can execute specific commands for investigating two different log files, is another implementation for the forensics challenge and lastly the snort was installed using the tool Hping to flood the IP to trigger some record alerts in the specific rules and generate the log files.

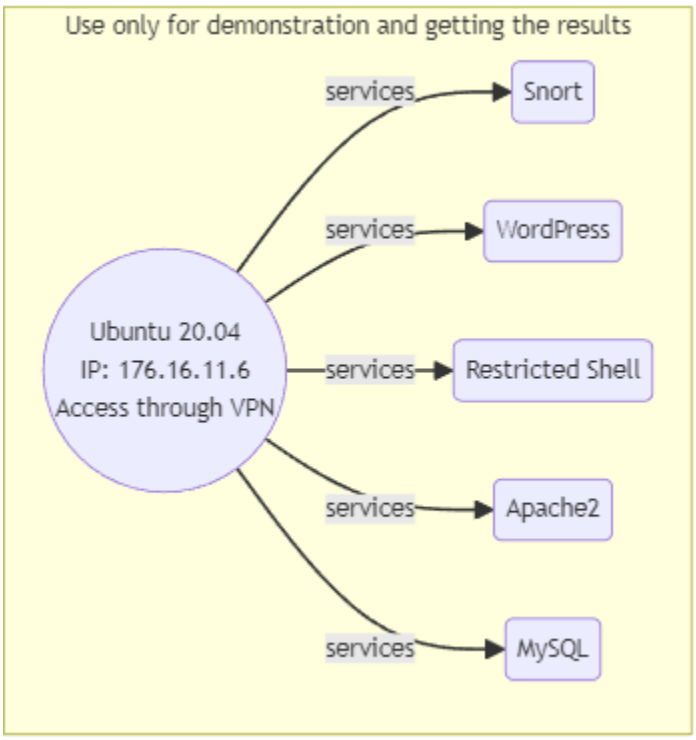


Figure 3.3 Virtual machine in isolated network

3.2 System Entities

The system entities play a crucial role in the cybersecurity training system. The followinglisting depicts all the interactions and relationships that users and administratorsare engaged inside the system.

Users: This group comprises those who interact with the cyber range platform, such as participants or trainees. Users will be able to use the platform to take part in practical tasks and cybersecurity challenges.

The **system administrator** takes responsibility for the management and supervision of the platform and the services. The responsibility of developing and configuring challenges, tracking user progress, and maintaining the overall functionality of each infrastructure is assigned to him.

Welcome Page: Theindex page is displayed to users every time they visit the server. The web site provides extensive information about the challenges, as well as detailed guides to solving them and instructions on how to connect via a Virtual Private Network (VPN).

Virtual Machine: The cloud virtual machine hosts all Docker containers, showing it as the parent environment.Other VMs in other infrastructure to demonstrate and display results when running.

Learning Guides:The development of training guides for the challenges addressed within the CTFd serves as an effective means of facilitating participants' understanding of the basic principles and successful completion of the challenges. Each guide includes an explanation of the topic, relevant details regarding the chosen topic, instructions with examples, and hints where necessary to overcome difficulties.

Challenges: This section represents the challenges in every category these exists.

- **SQL Injection challenge**: A web page serves for the challenge. The user can test SQL injection parameters in the vulnerable web application to exploit it and answer the challenge questions.
- **Snort challenge**: The user should craft his own rules according to the challenges through a web application which the user interacts to solve the challenge questions.
- **Forensics challenge**: This challenge enables users to perform analysis using digital forensics. The components of this challenge encompass the provision of two log files which participants through telnet can investigate the challenge questions.
- **Man in the middle challenge**: The user should intercept the communication between two hosts.

These entities engage in interactions within the system to provide an interesting and realistic training experience for the participants. Figure 3.4 represents a skeleton of the entities for the readers, facilitating their comprehension of the linkages and operations of each entity inside the cyber range training system.



Figure 3.4 System Entities

3.3 Tools and Technologies

An overview of the tools used is shown in Figure 3.5

1. **CTFd**: A Capture The Flag (CTFd) platform for creating challenges and oftenused for hosting CTF competitions and providing realistic scenarios for participants.
2. **Naumachia**: A multi-tenant isolated network for developed cybersecurity challenges.

3. **Snort**: An open-source intrusion prevention system for traffic analysis and packet logging.
4. **WordPress**: A widely used open-source content management system (CMS)
5. **Hydra**: A popular password-cracking tool.
6. **SSH (Secure Shell)**: A protocol for secure remote login.
7. **Nmap**: A network scanner tool used for discovering hosts and services on a network.
8. **Hping3**: A network tool to send TCP/IP packets.
9. **SQLmap**: An open-source tool for detecting and exploiting SQL injection flaws in web applications.

These tools in Figure 3.5 cover a wide array of functionalities, from simulating real-time challenges, analyzing network traffic, hosting challenges, detecting security threats to executing attacks and security assessments.

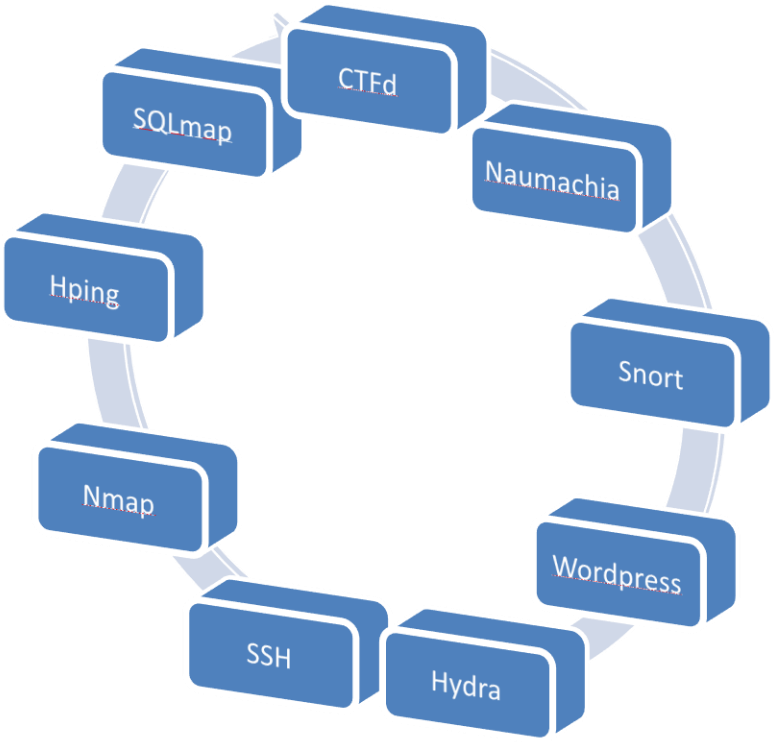


Figure 3.5 Overview of tools used.

Chapter 4 - Implementation

The implementation phase of this process involves the development of interactive scenarios that are specifically tailored to actively involve participants in realistic cybersecurity challenges. The scenarios have been carefully designed to correspond with fundamental areas of cybersecurity in the context of Industry 4.0. After the implementation phase, participants can engage in hands-on learning as the entire infrastructure has been implemented for the cybersecurity scenarios.The actual development and application include two main components: the CTFd framework [7], and the Naumachia framework [14], with challenges that associated with SQL injection, snort, Man-in-the-middle (Mitm) and forensics characterized by this phase.

4.1 (CTFd)platform implementation with dockers

CTFd (Capture The Flag Platform) is an open-source web application designed for creating and managing Capture the Flag (CTF) competitions and is one of the most popular open source platform all over the world. CTFs are cybersecurity competitions or projects where users compete to solve challenges that test their knowledge of computer security concepts.

The deployment of CTFd using Docker entails utilizing containerization to encapsulate the entirety of the CTFd platform, hence enhancing the portability, scalability, and manageabilityfor the administrator in a user-friendly environment.

CTFd deployed using a docker compose file,which includes in one file all the necessary images needed to run the CTFd according to our preferences.Each container is responsible for delivering a service or component within the CTFd application. A network that Docker creates allows these containers to communicate to one another. Figure 4.1 shows the creation of the containers and the networks for the CTFd platform. This platform acts as the gateway for the training in cybersecurity practical experiences.

```
022f59f42ef3   ctfd/ctfd          "/opt/CTFd/docker-en…"   3 weeks ago   Up 3 weeks   0.0.0.0:8000->8000/tcp, :::8000->8000/tcp   ctfd
8bee51a90621   redis:4            "docker-entrypoint.s…"   3 weeks ago   Up 3 weeks                                               ctfd-redis
b3f85df2783b   mariadb:10.4.28    "docker-entrypoint.s…"   3 weeks ago   Up 3 weeks                                               ctfd-db
```

Figure 4.1 CTFd deployment

- **(ctfd) container:** Runs the CTFd (Capture The Flag platform) application

- **(ctfd-db)mariadbdatabase container:** Hosts the MariaDB database for the CTFd application.
- **(ctfd-redis) cache container:** Provides a Redis cache for the CTFd application.

The system administrator has used the secure shell (SSH) protocol to configure Docker containers, including one specifically for the Capture The Flag (CTFd) platform, on the server. These containers are subsequently made available for user access.

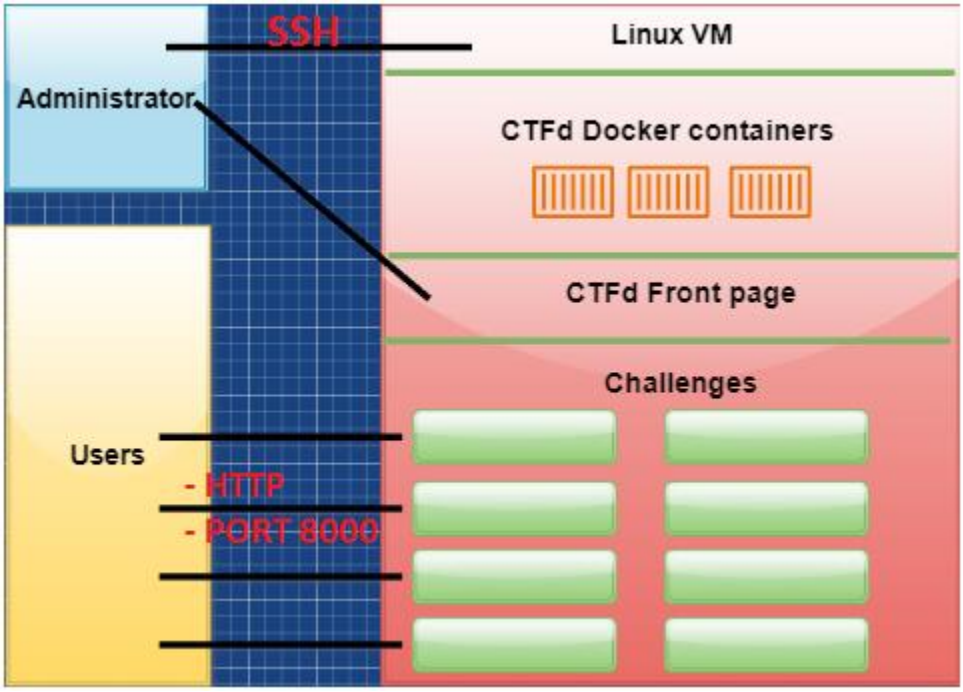


Figure 4.2 Connection types between administrators and usersinCTFd

The configuration of CTFd is performed using a web interface,where the administrator sets it up first and then adds challenges with options such as description, flag, points and other options that are consideredappropriate for the challenges, as shown in Figure 4.3, or the general setup of the CTFd platform.The whole process involing the users and the administrators shown in Figure 4.2.

The challenges implemented on the CTFd platform for each category and the total challenges for each category are shown in Figure 4.4. The user can open any challenge to solve as shown in Figure 4.5, which contains the description of the challenge, the number of users that have solved the challenge and, an input textbox to put the flag for submission. When a challenge is anwered correctly it is highlighted in green.

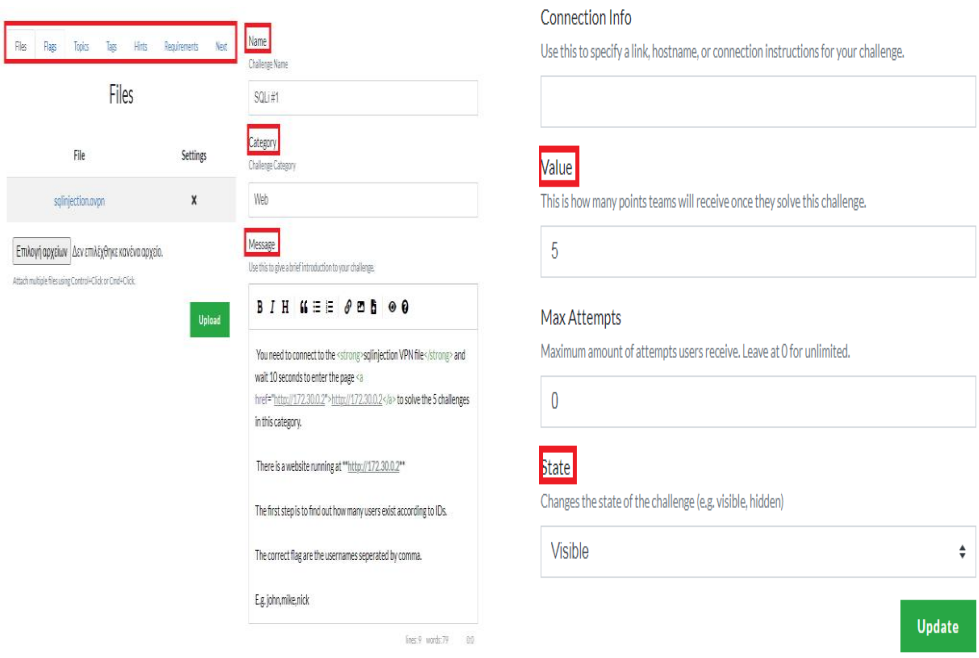


Figure 4.3 Challenge setup



Figure 4.4 Total of challenges and categories

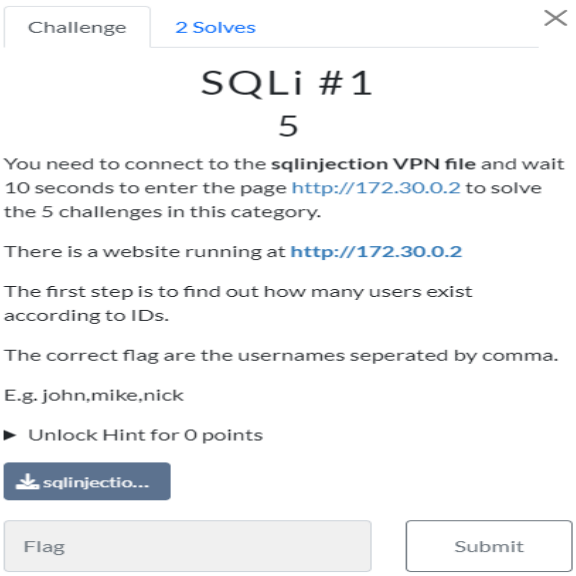


Figure 4.5 Challenge setup

Users can through the CTFd webpage, http://212.71.248.243:8000/ enter and create their own accounts to take part in the challenges. Figure 4.6 shows the welcome page.

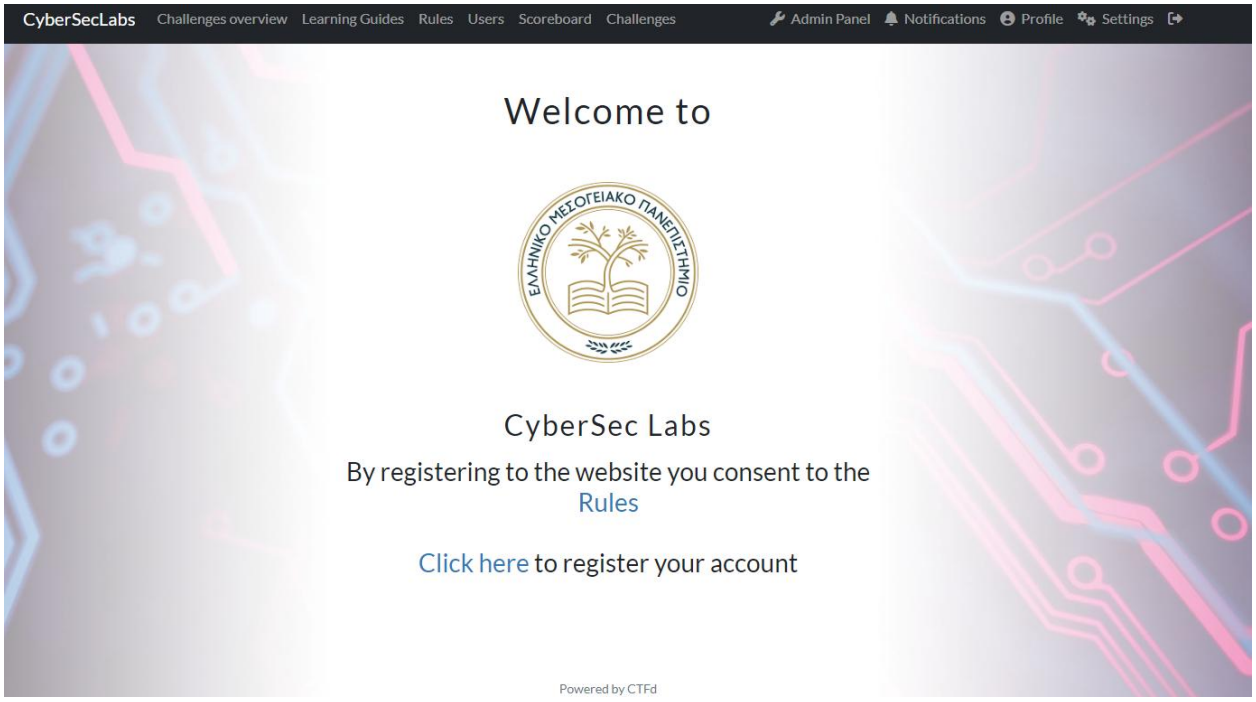


Figure 4.6CTFd Welcome page

The CTFd platform provides several statistics.

Score refers to the numerical representation of the points accumulated by an individual user or team during a competitive event.

Rank refers to the position occupied by a person or team on the scoreboard, indicating their relative standing in comparison to other participants.

Solved challenges refer to the quantification of the challenges that have been effectively resolved by a user or a team.

Challenge details of the challenges include their respective names, descriptions, categories, and point values.

Submission History: An account of a user's submissions for individual challenges, encompassing the timestamp of submission, the accuracy of the submission, and any feedback furnished by the platform.

An example of a user to see his own scoreboard and other statistics according to the challenges that has been tried in Figure 4.7.

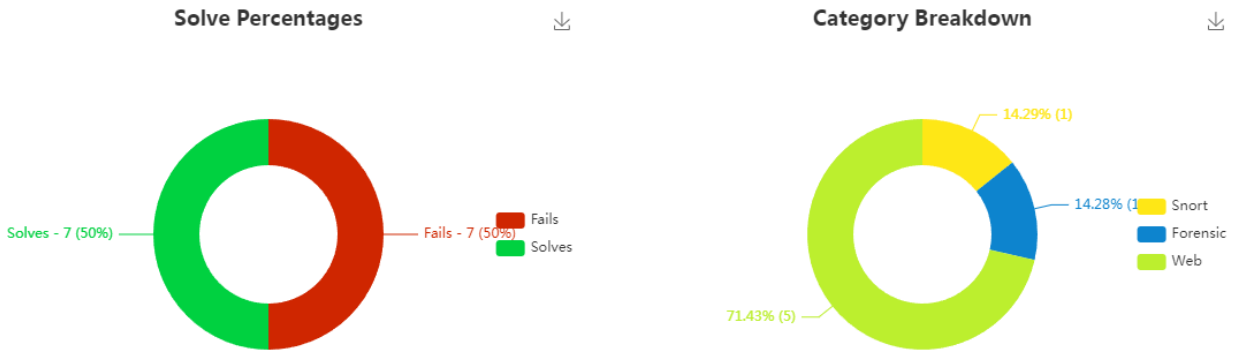


Figure 4.7 User statistics

4.1.1 (CTFd) docker networking diagram

The representation in Figure 4.8 shows how the network is created after deployed the CTFd via docker composed, how the bridge networks (default and internal) connect

containersthrough Virtual Ethernet Interfaces (Veth) pairs and how those containersare connected to the host machine (eth0) interface and to the external network.

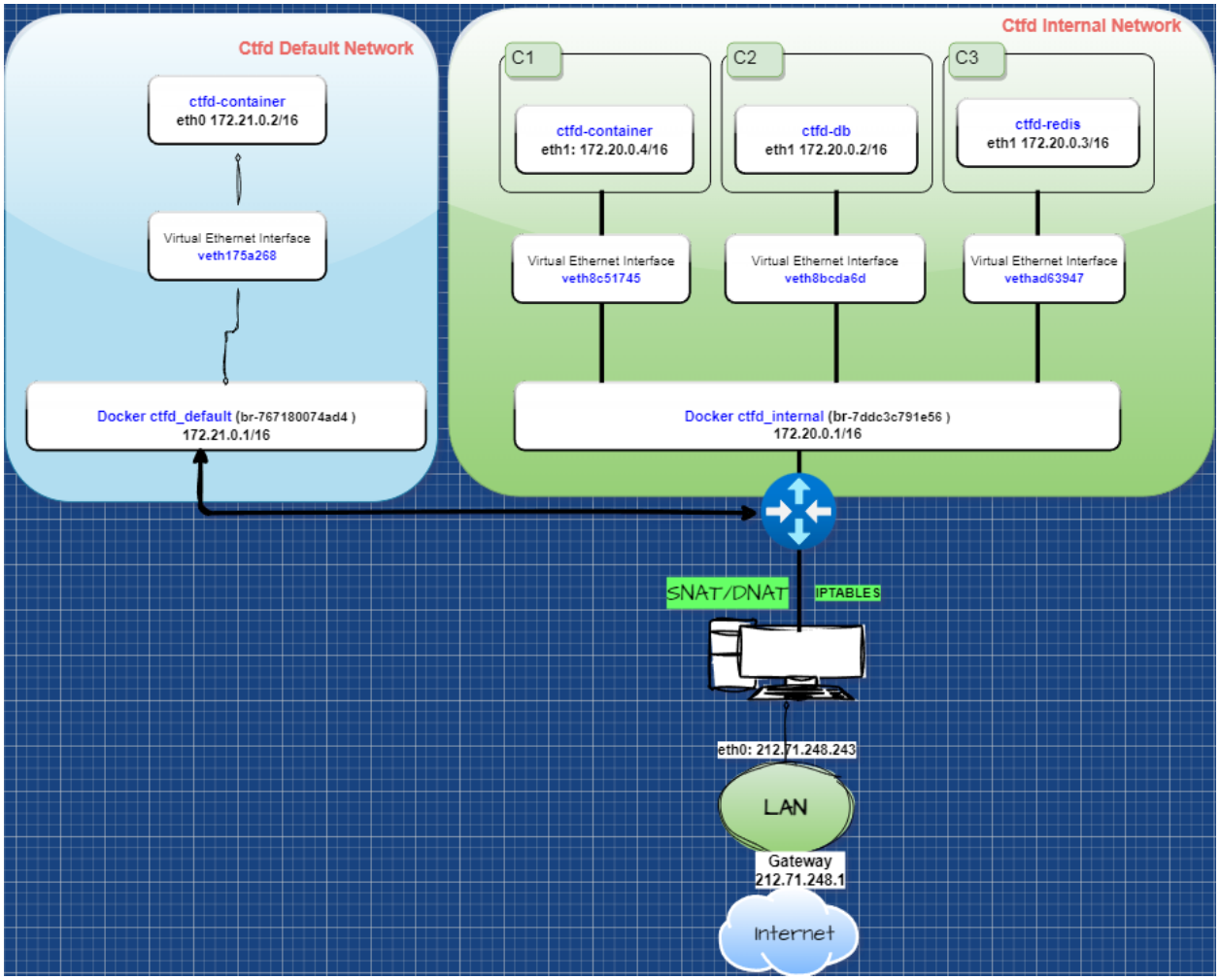


Figure 4.8 CTFd networking diagram

More in-depth analysis:

- The **eth0** interface refers to the Ethernet interface of the host machine. The host interfacerefers to the network interface card (NIC) that is integrated into the host operating system.
- **Docker bridge networks (default, internal)**: Docker creates the establishment of the bridge networks, which are custom networks created via code in the docker compose fileto interconnect containers, ensuring the isolation of each bridge

network from others. Containers that are connected to the exact same bridge network can establish communication with one another. In the case of Figure 4.6, where there are two bridged networks, with the host machine communicating with each other.Within Docker, this is a standard method for handling container networking.

- Docker provides a pair of **virtual Ethernet interfaces**, also known as veth pairs, for each container which represents the challenges connected to a bridge network. Each container is assigned a unique IP. The containers are connected to one end of the pair, while the bridge network is connected to the other end. Between the bridge network and the containers, these virtual interfaces provide network connectivity.

The reason why CTFd is on both networks in the Docker Compose file can be attributed to the intention of achieving balance among network isolation and external accessibility for the CTFd application. By mapping port **8000:8000,** the CTFd is accessible to the host machine through port 8000 port and for external users through port 8000 accordingly.

The reason CTFd is present on both networks is explained as follows:

By using both networks, allows the CTFdcontainer to be isolated from the internal network for security reasons while still being externally available for management and participant access. Disconnecting CTFd from the default network and attaching it solely to the internal network provides maximal network isolation without external access to the CTFdweb application only with VPN.

ctfd container is connected to both **default** and **internal** networks, which allows it to have external accessibility (via the **default** network) and internal isolation (via the **internal** network).

ctfd-db container is connected only to the **internal** network, ensuring isolation and not being externally accessible.

ctfd-redis container is connected to the **internal** network for internal use and isolation.

The network architecture balances network isolation and external access for the CTFd application, ensuring secure internal network containers and flexibility for specific on-premises requirements.

4.1.2 Communication across machines (Docker container to container, or Docker container to a remote host machine)

Packet Transfer Process

When the container in this case, the ctfd container from the default network (172.21.0.2) sends a packet to thectfd-db container (172.20.0.2) in the internal network, as shown in Figure 4.9. Docker manages this packet internally.

Internal network process

The Docker bridge network routes the packet coming from ctfd_container (IP 172.21.0.4) in accordance with the internal configuration of the bridge.Docker guarantees packets are sent to the correct receiver based on the IP address, in this case, that recipient is ctfd-db (IP 172.20.0.2).

ctfd-db container processing

When this container's application or service reaches ctfd-db, it starts listening for data that arrives on the specified port and IP address.Then, a ctfd-db response may resemble the path that the source container took.

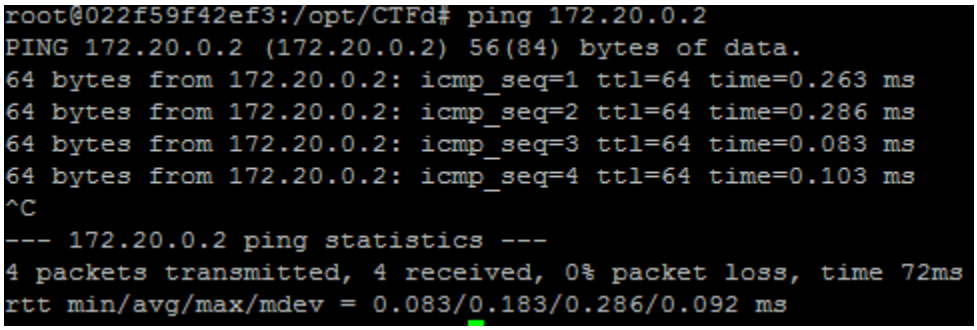


Figure 4.9 Ping between containers in different docker bridge networks

On the other hand, when an external user attempts to access the public IP address (213.15.11.55:8080), which is the CTFd web application platform corresponding to a service that is operating within a Docker container such as ctfd_container, several steps occur to ensure effective communication.

External access is achieved by users accessing the IP address of the host, denoted as host_IP, through port 8080.

Port forwarding involves the redirection of incoming requests on port 8080 to the Docker host machine by the router.

The **process of Docker** port mapping involves the Docker host redirecting incoming requests on port 8080 to the ctfdcontainer service operating within the Docker environment, thereby translating it to port 8000.

Ctfd_container Service: A service running within the container responds to requests received on port 80 by processing them and sending the appropriate information back to the user who accessed host_IP:8080.

It is essential to verify that the service within the container is operational on port 8000, as indicated in the port mapping, in order to effectively manage the incoming requests.

4.2 Naumachia framework implementation with docker

Naumachia is a multi-tenant network. The primary objective of Naumachia is to facilitate the implementation of interactive challenges in an isolated, secure environment where users can connect through VPNs, involving multi-host connections, to practice with security challenges. The term multi-tenancy means that the aim of technologies such as containerization, virtualization, and others that enable various workloads to share hardware resources is to maximize system utilization and allocate resources as effectively as possible.The workloads operating in such an environment, however, frequently fail to make the most of the hardware's potential power and often leave a large portion of the resources inactive.

4.2.1 Key features and importance of Naumachia

The characteristics of the Naumachiaare shown in Figure 4.10 and described below.

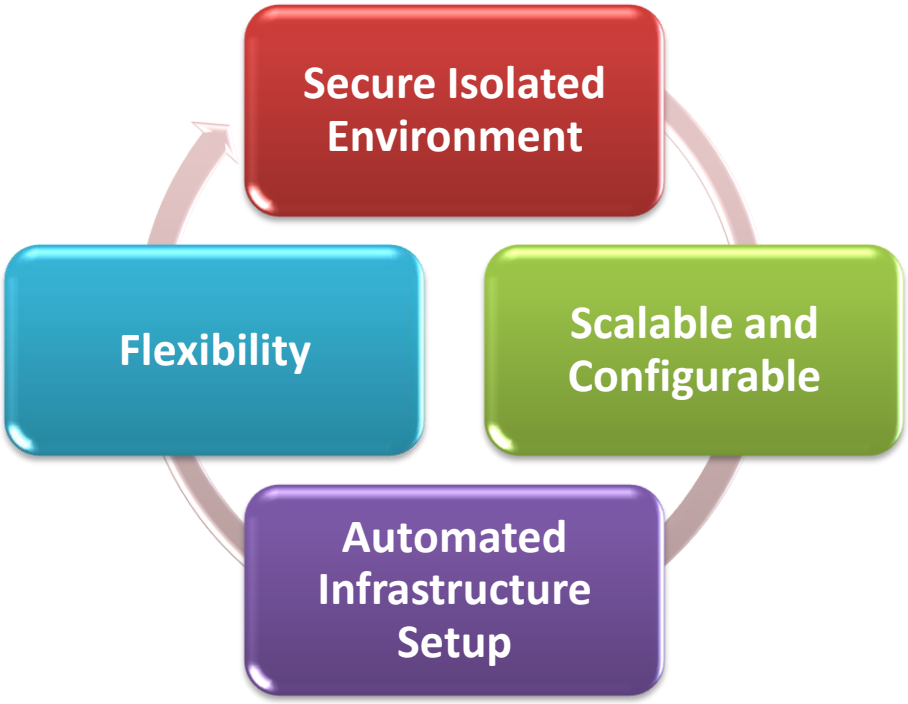


Figure 4.10 Naumachia key features

1. **Secure isolated environment**: Naumachia creates and maintains secure environments that are isolated and secure for participants to learn about a range of cybersecurity challenges.
2. **Scalable and Configurable:** Naumachia is both extremely adaptable and scalable, making it easy to accommodate multiple participants at once and adapt to different training needs.
3. **Automated Infrastructure Setup:** Provides an automated and easily installed environment to create and manage different challenges in the fields of cybersecurity, pen-testing and red-blue teams. Can be easily torn down for the following session after the challenges have been finished to free the resources for the next season.

Naumachia is a useful open-source framework providing a high degree of flexibility in the field of cybersecurity for a wide range of applications because it offers an organized, secure, and efficient environment for training,skill development, and the advancement of a deeper comprehension of cybersecurity threats, issues, and defense tactics.

4.2.2 Naumachia docker networking

Once the necessary configurations are made for the Naumachia. Including all the implemented challenges integrated on the naumachia, Docker creates the necessary networks and spins up all the necessary containers to run, as shown in Figure 4.11.

```
diamond@localhost:~/Naumachia/challenges/web$ docker ps
CONTAINER ID   IMAGE                COMMAND                  CREATED        STATUS        PORTS                                          NAMES
48a7645b6027   naumachia/openvpn    "/scripts/naumachia-…"   19 hours ago   Up 19 hours   0.0.0.0:9297->1194/udp, :::9297->1194/udp      naumachia-openvpn-middle-backup-1
4c1efd702b67   naumachia/openvpn    "/scripts/naumachia-…"   19 hours ago   Up 19 hours   0.0.0.0:9296->1194/udp, :::9296->1194/udp      naumachia-openvpn-forensics-1
7143b1ce5d03   naumachia/openvpn    "/scripts/naumachia-…"   19 hours ago   Up 19 hours   0.0.0.0:9295->1194/udp, :::9295->1194/udp      naumachia-openvpn-snort-1
81d44f1113c1   naumachia/manager    "python -m app"          19 hours ago   Up 19 hours                                                  naumachia-manager-1
f398afc1e539   naumachia/openvpn    "/scripts/naumachia-…"   19 hours ago   Up 19 hours   0.0.0.0:9294->1194/udp, :::9294->1194/udp      naumachia-openvpn-sqlinjection-1
9169ab233b5f   naumachia/registrar  "gunicorn -c python:…"   19 hours ago   Up 19 hours   0.0.0.0:3960->3960/tcp, :::3960->3960/tcp      naumachia-registrar-1
062b0ca9ee6d   redis:alpine         "docker-entrypoint.s…"   19 hours ago   Up 19 hours                                                  naumachia-redis-1
aea1dddc5036   naumachia/mitm.alice "python ./alice.py"      2 weeks ago    Up 2 weeks                                                   usertest_middle-backup_alice_1
0dbcbb8ce9dc   naumachia/mitm.bob   "python ./bob.py"        2 weeks ago    Up 2 weeks                                                   usertest_middle-backup_bob_1
```

Figure 4.11 Deployed naumachia with all the challenges

A secured and isolated architecture, as represented in Figure 4.12, allows the participants to interact with the challenges without interfering with each other's work or damaging the host system. Naumachia handles the management of the Docker environments, allowing participants to concentrate on challenging solutions.

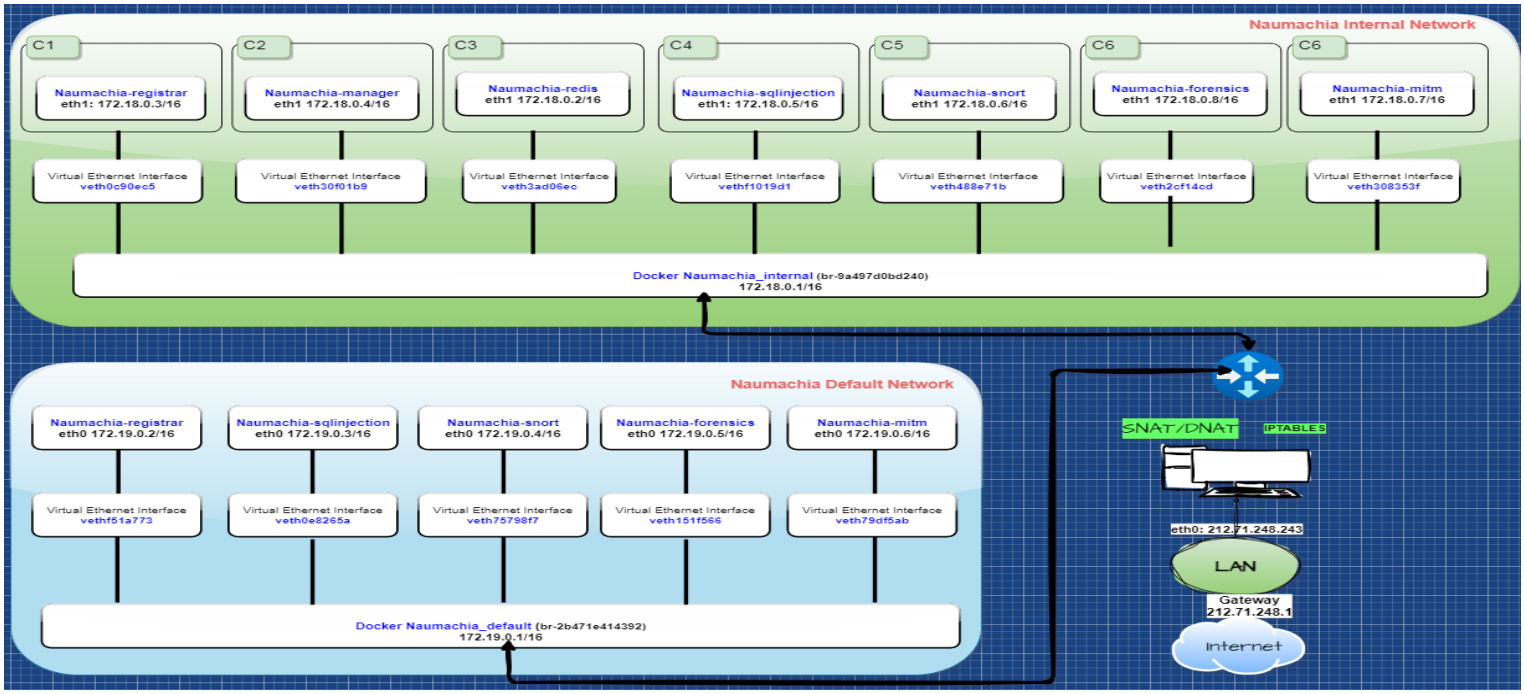


Figure 4.12 Naumachia networking

Key aspects of naumachia network

1. Naumachia creates a Docker network with the purpose of isolating the challenges from both the system that hosts them and each other.
2. Every challenge has its own isolated environment and is deployed as a distinct Docker container. These containers might be built using customized Docker images made for that kind of challenge.
3. Usingthe Docker network, CTF users access the challenges and try to solve them, to find the flags, within an isolated Docker environment.

There are several services running on Naumachia. Each service has its own purpose. Figure 4.13 explains the containers and the network structure that have been designed.

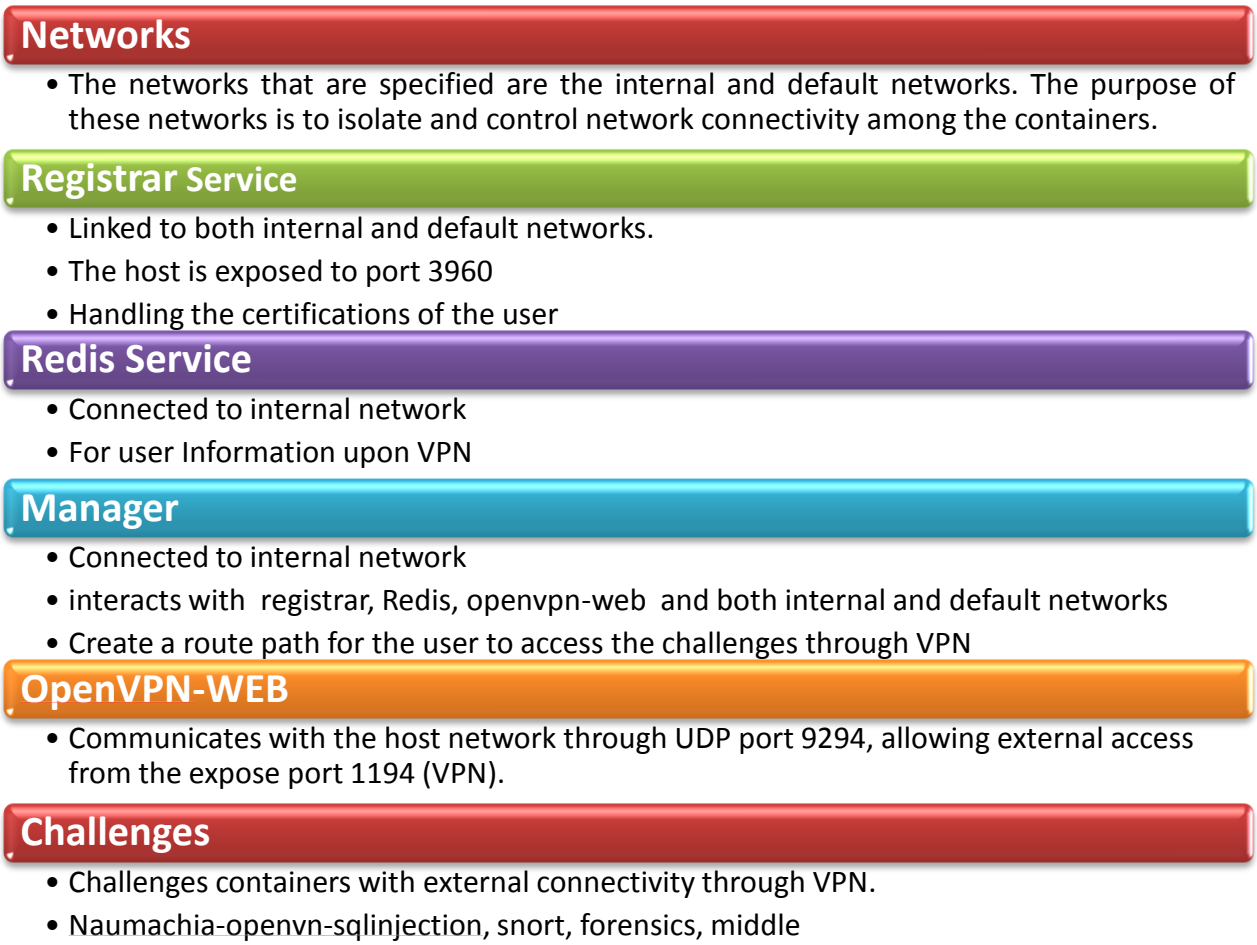


Figure 4.13 Naumachia network flow

Network flow is structured to provide balance between services that need private, isolated communication (via the internal network) and those that require external network access (by the default network). For these network configurations, the host network namespace is prepared via the bootstrapper service.

Challenges access through VPN

With the creation of each challenge on Naumachia, the appropriate VPN file must also be created for each challenge, which allows the user to connect via VPN to the specific namespace of the challenge. The user's certificate is created by the registrar server, this means that when the user establishes a connection via VPN, a check is made to see if the user is certified, and the information is passed to a Redis database. Subsequently, the manager will establish a network

route for the user to access the challenge, allowing the user to start participating.Figure 4.14 describes the previous process.The purpose of this VPN is to ensure secure access to the challenges through Naumachia. Participants can connect securely using the .ovpn files that are given, protecting their personal information and the privacy of their interactions with the cybersecurity challenges. Through the CTFd, which integrated with the Naumachia framework to create secure and isolated namespaces for solving challenges, participants have access to challenges.

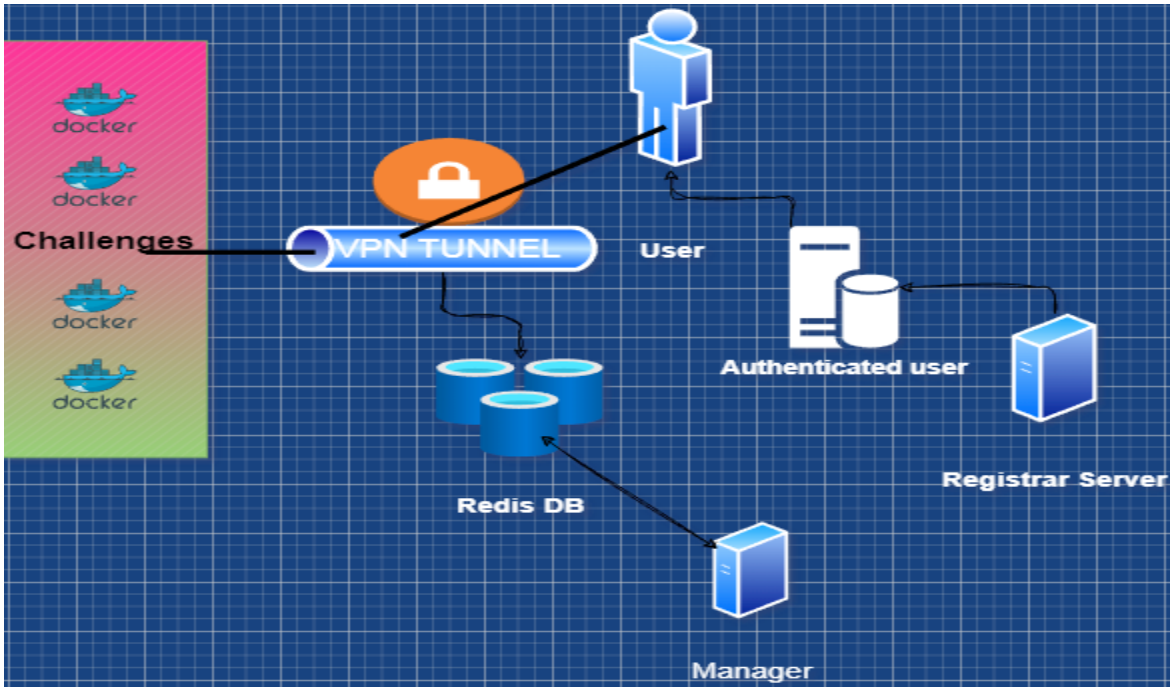


Figure 4.14 VPN connection process

4.3 Developmentof Challenges

4.3.1 SQL Injection

4.3.1.2 Explanation of SQL

Programming languages like MySQL, MSs (Microsoft SQL Server), PostgreSQL, and IBM are typically used to manage databases. SQL stands for Structured Query Language. The SQL Injection technique, often known as SQLi, involves the injection of malicious code into an existing "query" with the ultimate objective of manipulating the set of instructions prior to its execution within the database.

4.3.1.3 How SQL injection works

SQL injection is a type of security vulnerability that happens when an attacker intentionally inserts malicious SQL code into the input fields of a web application, therefore abusing the application's vulnerability to execute SQL commands.Attackers can modify the database's data by injecting malicious SQL queries when a web application does not properly use input validation and sanitization [84].

4.3.1.4 SQL injection Types

Union-based SQL injection: This specific type of injection enables an attacker to extract data from numerous tables inside a database by consolidating the results of multiple SELECT statements into a unified query [85].

Error-based SQL injection: This particular type of injection exploits the database and generates error messages as a means to get information about the structure and characteristics of the database where the data is stored [85].

Boolean-based SQL injection: This particular type of injection exploits the response of a website when a query is evaluated against a true or false statement [85].

Blind SQL injection: When an attacker can't see the results of their injection but still determines whether it was successful based on alterations in the website's behavior, they utilize this kind of injection [85].

4.3.1.5 SQL injection scenario implementation

The following scenario has been implemented with docker, inside the naumachia framework. The main services running on docker are a MySQLdatabase, a web server (nginx) to serve the content, the PHP and the necessarycode files (html, PHP) needed to implement the scenario. The structure of the files is shown in Figure 4.15 and it is the same with the rest of the challenges.

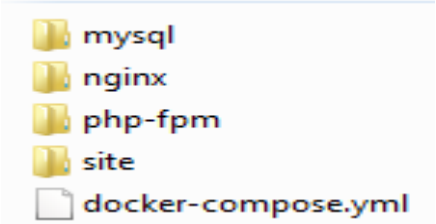


Figure 4.15 Docker challenge structure

This scenario presents asimulated web-based application that is vulnerable to the use of SQL injection attacks. That means the user input (textbox) does not have any validation and passes to a SQL query without validation. The purpose of the challenge is to create an interaction between a user and a vulnerable web application in which the userexecutes SQL injection techniques in a textbox, Figure 4.16to retrieve the data from the database as an unauthorized user. The complete process is shown in Figure 4.17.

Users have the flexibility to choose which methods to use to solve the challenges, manually or with an automated tool called SQLmap, which is an automatic injection database tool, as well as how to put them into practice, which allows them to try new things while making mistakes along the way. There are five challenges in this category, and each challenge has a different degree of difficulty. In order to effectively complete the challenge, participants must carefully carry out the necessary actions to take advantage of the application vulnerability.



Figure 4.16 SQL injection web app interaction

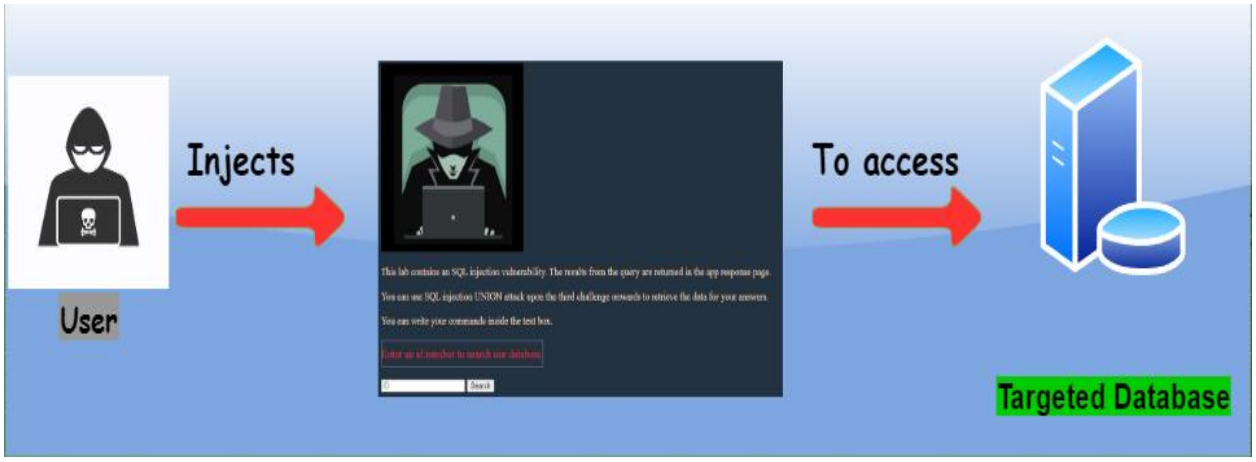


Figure 4.17 SQL injection process

In the same web application, a secure version was also implemented to protect against SQL injection attacks [86]. Therefore, when the user executes the commands for injection in the text box, the web app is properly secured and does not allow the execution of such commands.

4.3.2 Snort

4.3.2.1 Explanation of snort

Snort, developed by Cisco, is a network intrusion prevention system (IPS) that operates on an open-source framework. The system has the ability toperform real-time analysis of traffic and log packets on IP networks. The configuration process of Snort is straightforward. Based on the rules that a system administrator has specified, snort can analyze protocols, information within packets, capture packets in real time, and identify a variety of intrusions. There exists a community that oversees a vast collection of snort rules, which may be customized according to individual preferences [87].

4.3.2.2 Basic types of snort rules

Alert rules: When suspicious or malicious activities are detected, alerts are generated. In addition to logging data and sending notifications to administrators.

Log rules: These maintain a record of data about noticed network activity without sounding an alert. Log rules are helpful for recording network events that might be interesting for study but aren't immediately recognized as malicious.

4.3.2.3 Snort scenario implementation

In this scenario, a web application is running via docker, where the user visits the web page and has to write the correct rules according to the challenges in this category as show in Figure 4.18. The challenges are about creating snort rules for different services to identify the network from malicious traffic. The purpose of this challenge is to learn to create basic rules in the most common services: The Web server (port 80), the FPT server (port 21), and the SMTP server (port 25). The user has an interaction with the web application. When the rule is correct, return the flag with a small description of the challenge solved and the final flag to put it in the appropriate challenge. When the rule is wrong, you must try again to find the correct snort rule. There are 3 different task for this category.

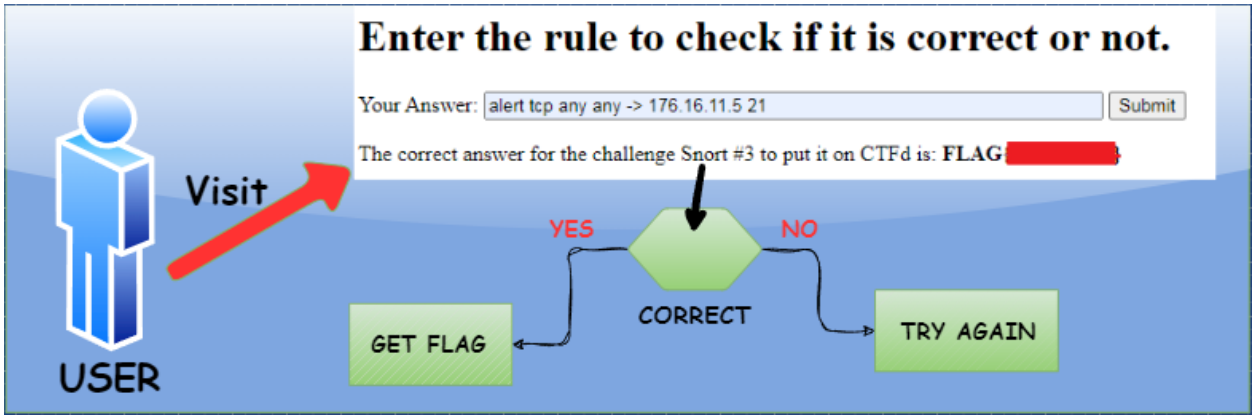


Figure 4.18 Web app snort checker

The validation of the snort rules for the creation of these was implemented on two local machines, with the snort installed on one machine and the other created the traffic into the snort to detect the suspicious traffic from an FTP in this example (Figure 4.19).

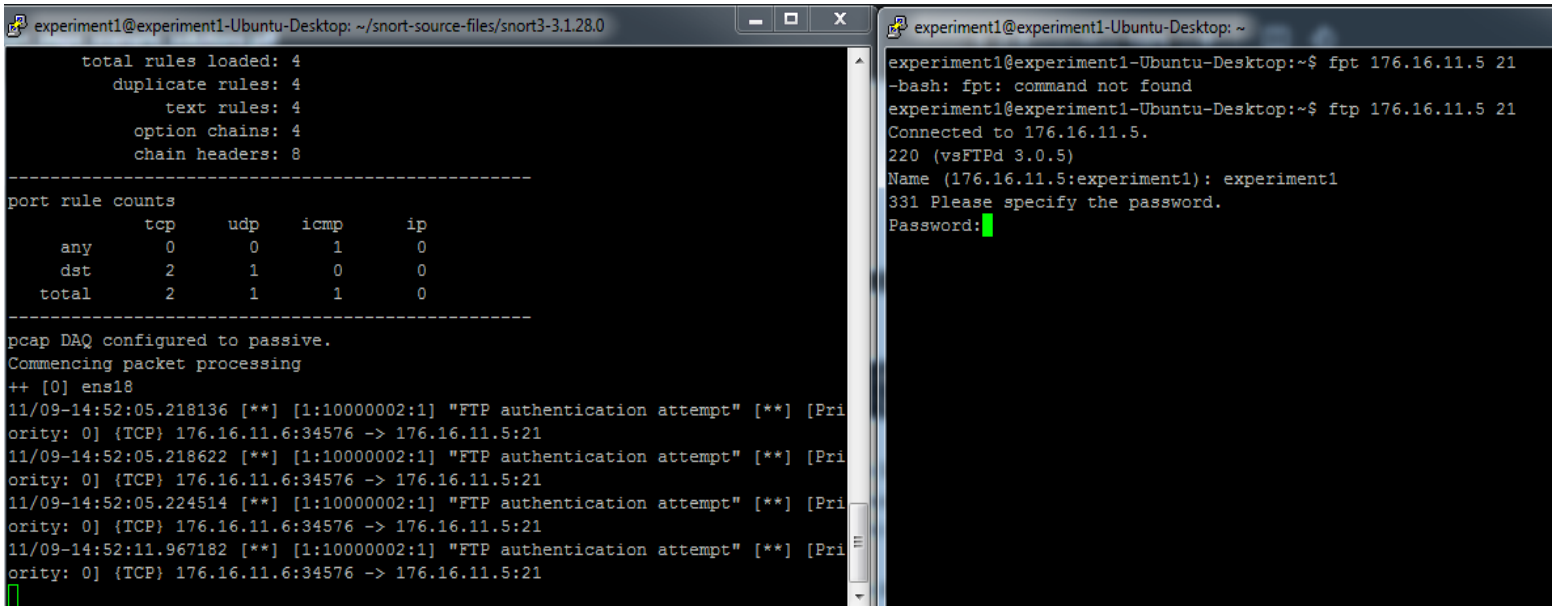


Figure 4.19 FTP log-in attempt

4.3.3 Forensics

4.3.3.1 Explanation of Forensics

A crucial step in identifying the parties that are responsible for an incident and its root cause is forensic analysis. Forensic analysis pertains to web servers and systems and entails

obtaining information that might assist investigators in determining how the computer system was accessed, what steps were taken, and potential data loss [88].

4.3.3.2 Forensics scenario implementation

This scenario consists of several steps and all deployed using docker. First of all, the files to be used for analysis must be created. There are two main files: an access.log file and an auth.log file.

- The **access.log** file consistsof 33 requests from a wordpress CMS deployed with docker, where the user gains unauthorized access.
- The **auth.log** file consistsof SSH login attempts where the attackerused brute force as shown in Figure 4.20, with the hydra[1] tool togain access to the VM and created another user to keep access to the system. Both files contain logs generated by capturing the packets during the process with Wireshark[2,] a packet network analyzer tool.

1https://www.hydradongle.com/

2https://www.wireshark.org/

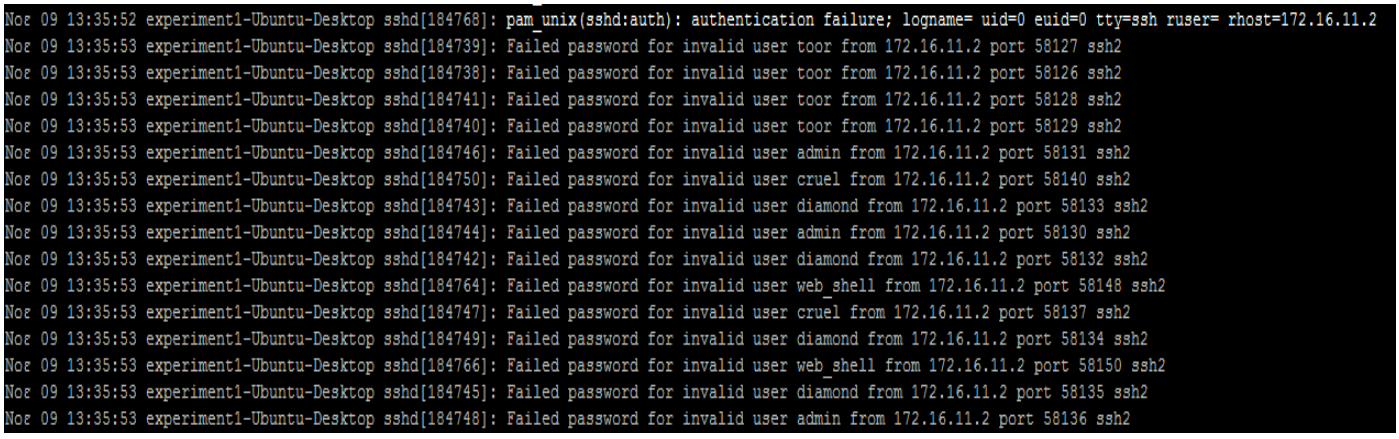


Figure 4.20SSH bruteforce

Interactivity

The user connects via telnet (172.30.0.2) and port 23 with the username and password given in the challenge description. Once connected, the initial folder contains the two files for analysis. There are 7 tasks in this category, which include: the server that the attacker compromised, when an event occurred with timestamps, how many times he logged in with the cracked username or with others and a sequence of actions taken. Users can choose which data to pay attention to as well as how to analyze it, which allows them to experiment while gaining knowledge from their mistakes.The main command to solve the challenges is the grep command. A sample from the process is shown in Figures 4.21, 4.22.

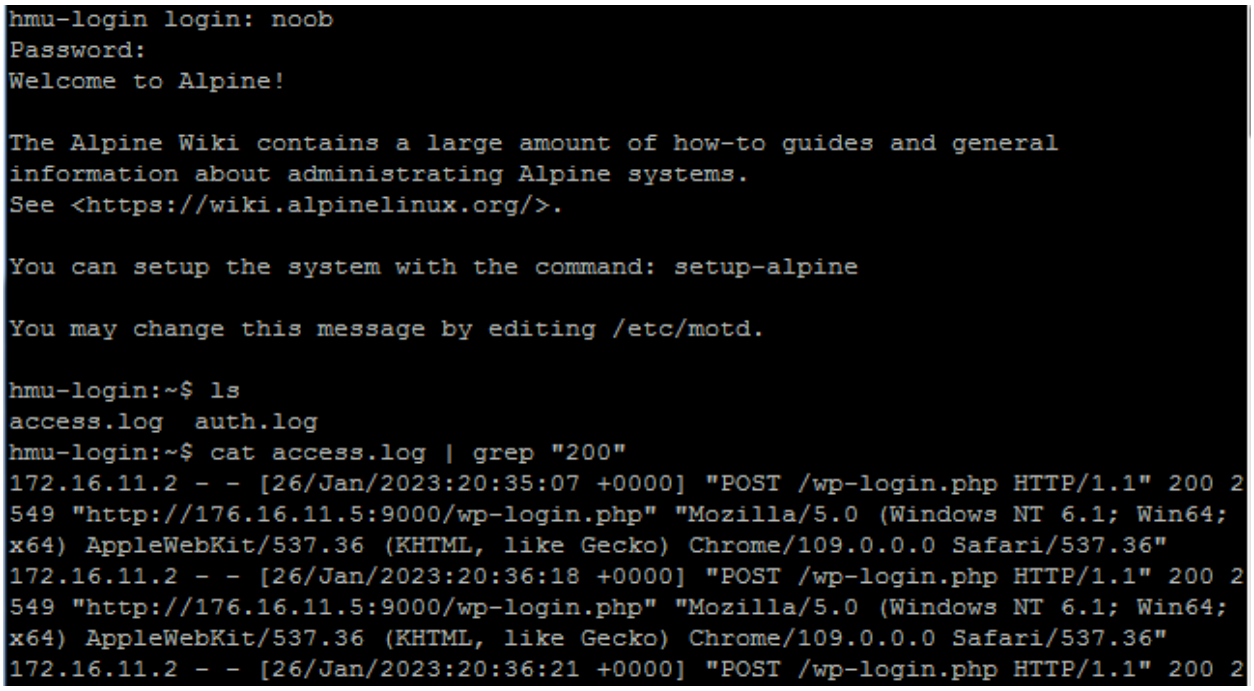


Figure 4.21 Telnet connected user

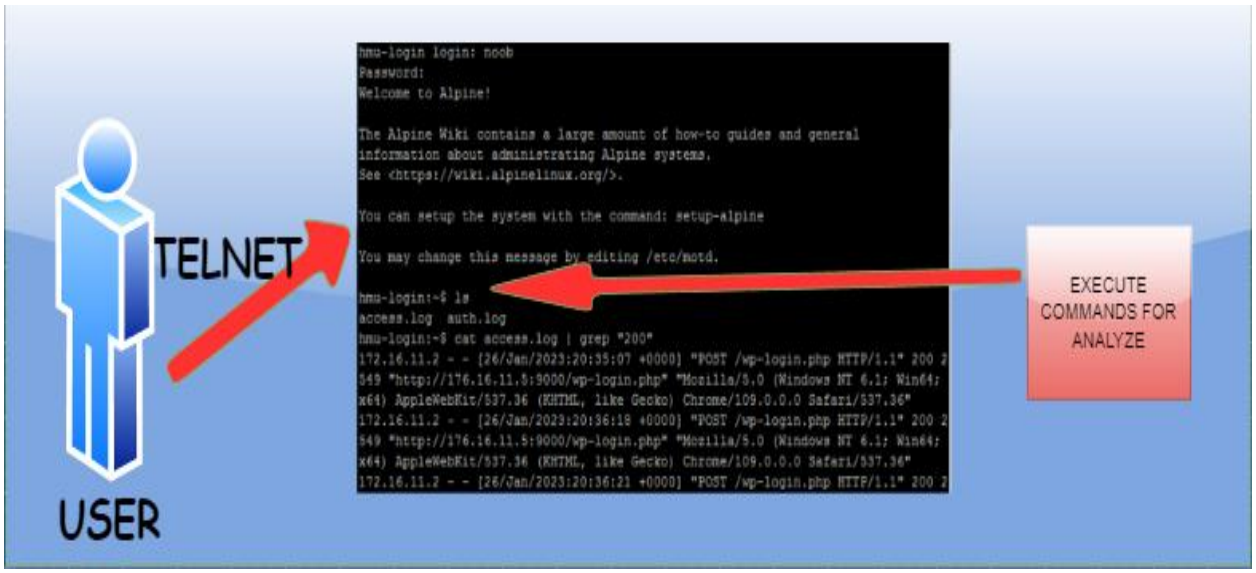


Figure 4.22 Forensics process

Also, another implementation was implemented for this category. Which is called "Restricted Shell". This means that the user connects to the VM in a restricted area and can only execute certain commands without being able to do illegal activities on the whole system. The allowed commandsare: grep, ls, and cat, as shown in Figure 4.23.

```
demouser@experiment1-Ubuntu-Desktop:~$ uname -r
-rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command na
mes
demouser@experiment1-Ubuntu-Desktop:~$ whoami
-rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command na
mes
demouser@experiment1-Ubuntu-Desktop:~$ ls
access.log  auth.log  bin
demouser@experiment1-Ubuntu-Desktop:~$ head -n 4 access.log
-rbash: /usr/lib/command-not-found: restricted: cannot specify `/' in command na
mes
demouser@experiment1-Ubuntu-Desktop:~$
```

Figure 4.23 The logged-in user can execute specific commands

4.3.4 Man in the middle

4.3.4.1 Explanation of Man-in-the-middle

Man-in-the-middle (Mitm) attack is a cyberattack, in which an attacker captures and exchanges packets between two parties. The perpetrator secretly intercepts and perhaps modifies the communications or information being transmitted between the two entities [89].

4.3.4.2 Challenge analysis

In this challenge deployed using dockers, there are two containers (Alice and Bob).

Alice

Objective: Alice wants to communicate the first half of a secret flag with Bob by simulating a communication being sent to him.

Process:

- For communication purposes, Alice specifies a UDP socket connection for Bob.
- In Alice's python script, there is a variable CTF_FLAG which kept the flag to share.
- The flag is divided into two equal halves, referred to as the first half and the second half.
- Every three seconds, Alice creates a message and transmits it to Bob that contains the first half of the flag.

Bob

Objective: Bob's python script waits for Alice to send messages, reads the first half of the flag, and reacts appropriately.

Process:

- Bob specifies a UDP socket connection for Alice's communication.
- Bob listens for communications from Alice.
- Bob examines messages to check if they include the first half of the flag.
- Bob reacts by giving the other half of the flag.

4.3.4.3 Overview of Interaction

- Bob receives communications from Alice frequently that contain the first half of the flag.
- After listening for messages, Bob looks for the first half of any messages he receives and, if it is located, responds with the second half.
- The challenge is for an external attacker to eavesdrop on Alice and Bob's conversation, intercept the first half that Alice sends, then acquire the second half from Bob's answer in order to piece together the entire flag.

The practical process is to use ettercap and scan the network to find the hosts to add as targets to poison the network, as shown in Figure 4.24, and at the same time capture the packets in the specific VPN interface, depending on your connection, to find the constructed flag, as shown in Figure 4.25.

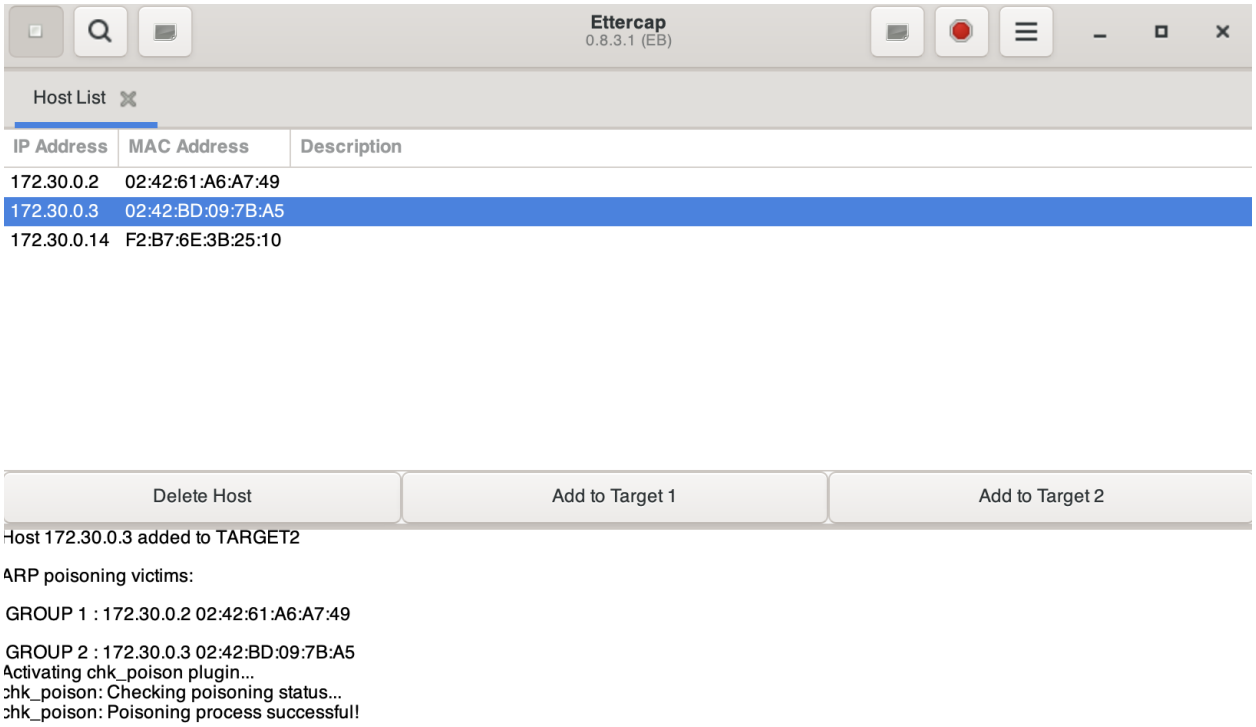


Figure 4.24 Poisoning the network

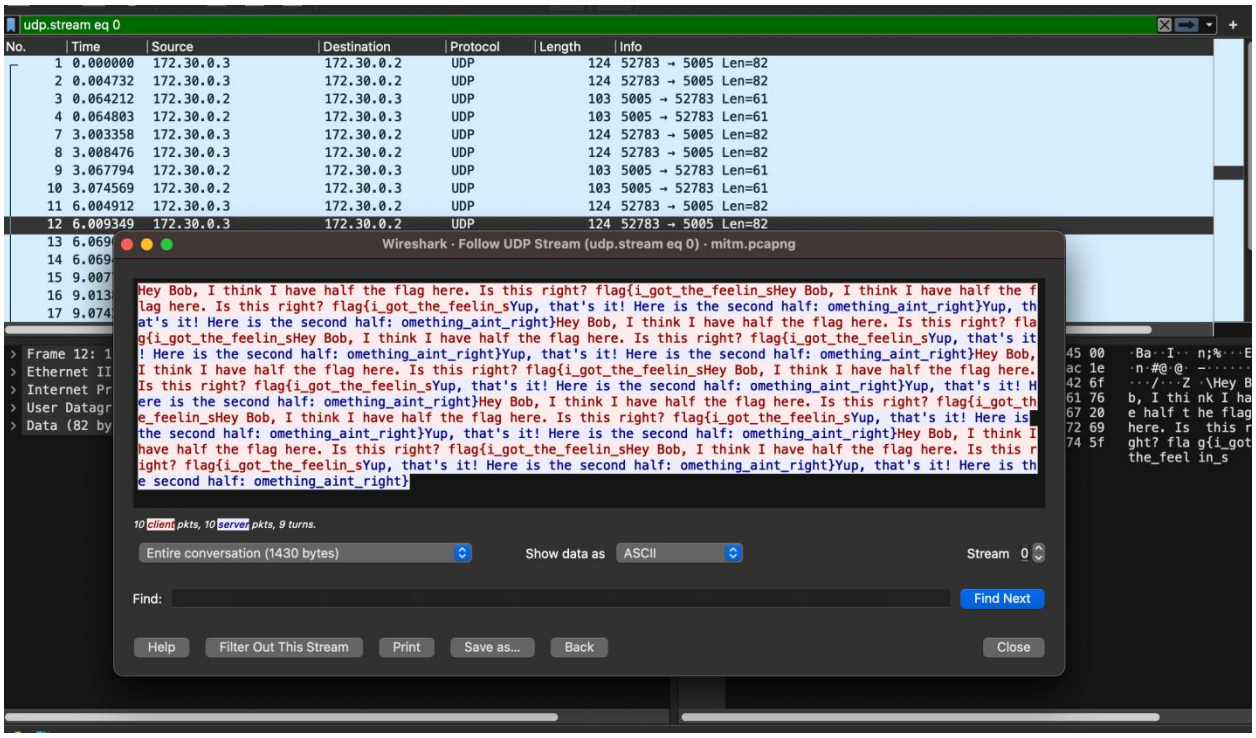


Figure 4.25 Capture the packets to find the flag

4.3.5 Challengesand learning guides

All the implemented challenges are represented in Figure 4.26. Providing the category, the number of challenges, and the descriptions for each challenge. In Table 3, there is a brief explanation of the challenges and the learning goals.Containerization technology is used to implement all the challenges and scenarios, with Docker containers being used.By using this approach, participants are guaranteed that they will work in secure, controlled environments that mirror realistic Industry 4.0 scenarios.Participants can interact with the challengesin safe, isolated areas without endangering any external systems.

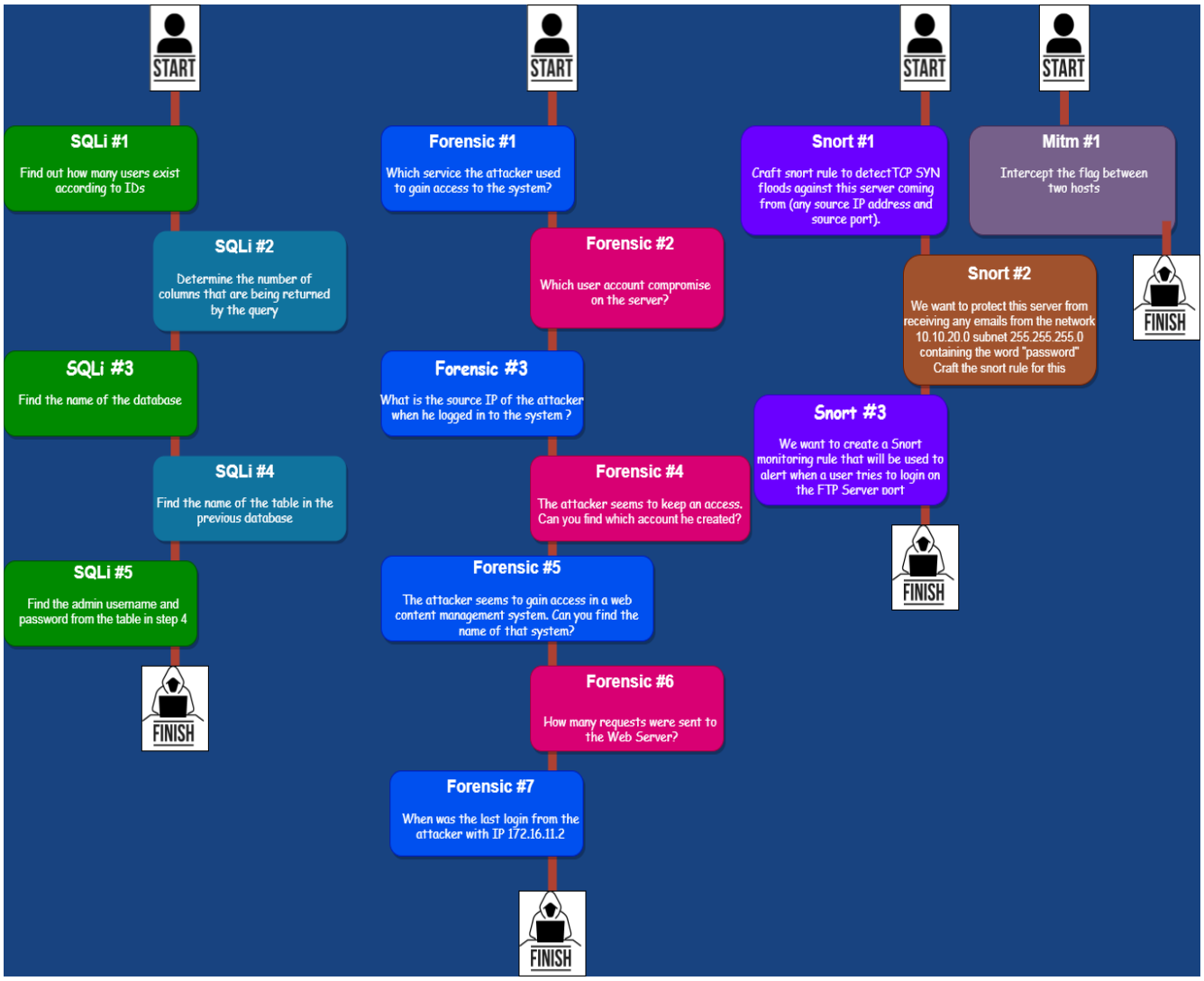


Figure 4.26 Challenges categories and descriptions

Table 3 Summary of challenges and learning goals

#	Category	Learning goals
SQL Challenges	Web	Gain hands-on experience in identifying and exploiting SQL injection vulnerabilities.
Snort Challenges	Snort, Linux	Practicing creating basic snort rules in common services.
Forensics	Forensics	Develop skills in analyzing log files, recognizing threats, and extracting relevant information.
Man in the middle	Networking	Understanding and practicing how an attacker can intercept the traffic between two hosts.

Four learning guides were created for the requirements of the challenges as shown in Figure 4.111. The learning guides are a very important element, offering help to the participants with the challenges they have to face.

The structure of each training guide includes a general theory of what each technology is and how it works according to the four categories of challenges and important instructions with examples to direct participants in the right direction to solve the challenges. Providing the basic guidelines for the participants, where, when needed, more details are able to search based on the guidance given below for more details.

It is necessary for each participant to read the learning guides before starting to solve the problems. Because the difficulty of not reading them is huge. Guidance is very important, according to the analysis made in Chapter 2, to improve the gap between theory and practice and for better self-improvement and the addition of knowledge for each of us.

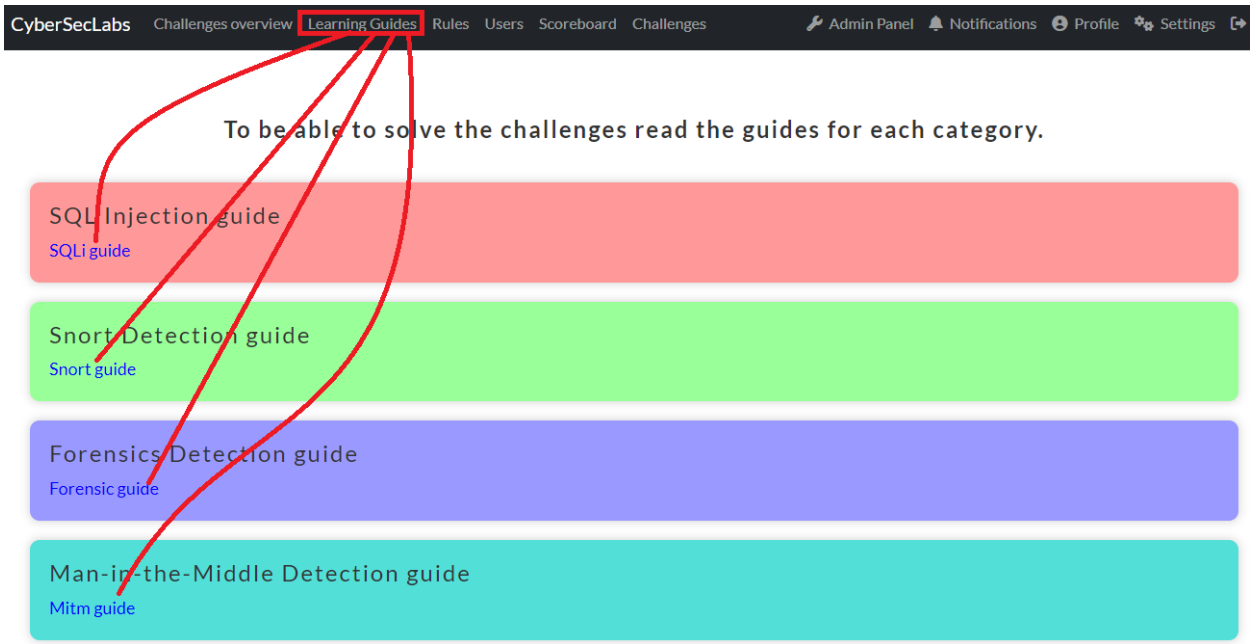


Figure 4.27 Learning guides

4.3.6 Conclusion

This section on practical implementation highlights the CTFd platform integrated with the Naumachia framework and the effective use of the Naumachia framework. Also, it highlights how important it is to provide secure access via VPN challenges and how important it is for learning guides to provide a theoretical background before participants move into the practical parts. Additionally, it places emphasis on the useful security and safety features integrated into the setup to establish a controlled and practical learning environment and the purposes of eachscenario of SQL injection, forensics, Snort IDS, and man-in-the-middle (MitM) attack.

Chapter 5 - Evaluation and Findings

5.1 Overall evaluation of the participants' experience and the training platform

The effectiveness of cybersecurity training is determined by its ability to narrow the gap between theory and practice and to provide participants with practical skills. The objective of this assessment is to evaluate the overall experience of the participants and the training platform. The evaluation of the challenges included four general questions for each challenge and how effective the learning guides were.

In total, there were 25 participants in a time period of 1 month who read the learning guides and practiced with the challenges. 15 people were postgraduate students, and the remaining 10 graduated in computer science and IT fields.

The CTFd is an important component to track the patrician's performance, where it tracks the overall progress of each participant or individually for each channel, including percentages for correct and failed submissions and percentages for each category that has been solved.

The evaluation approach incorporates the pre-survey, which must be completed before starting to participate and the post-survey, which is completed after the training access time is completed (30 days).

Pre-Survey: Participants will first complete a pre-survey to determine their baseline cybersecurity knowledge before engaging in with the challenges and the learning guides.This initial pre-survey is crucial for analyzing the educational experience across different participants.

Post-Survey: The purpose of this post-survey is to evaluate the usefulness of the cyber range platform and how the platform affected the knowledge, skills, and confidence of the participants when handling the challenges. Provides evaluation on the effectiveness of each challenge and, in addition, evaluation on the effectiveness and clarity of the training guides.

The anonymous surveys provide valuable information about participants' levels of satisfaction, knowledge, and the overall impact of the cybersecurity training.

After analyzing the answers provided by the participants, the most interesting results emerge as follows:

There is alack of cybersecurity knowledge. In Figure 5.1,out of 25 participants, only 5 (20%) have experience from 3-5 years and only 10 (40%) have experience from 1-3 years.Also, Figure 5.2 shows that only 6 (24%) participants have previously participated in cybersecurity training or competitionsuch as Capture the Flag.

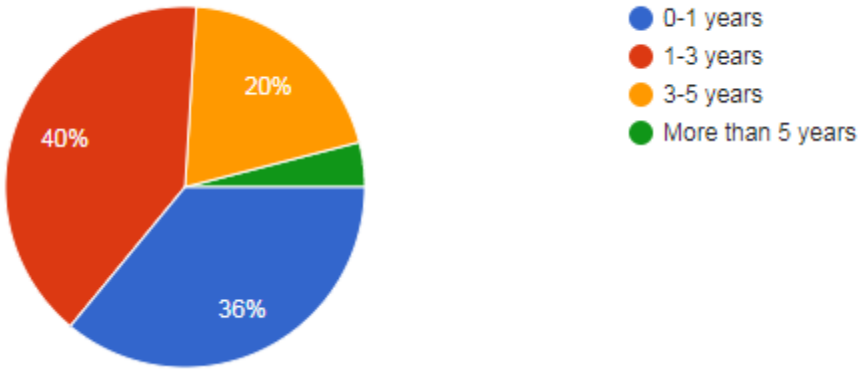


Figure 5.1 Years of experience in cybersecurity

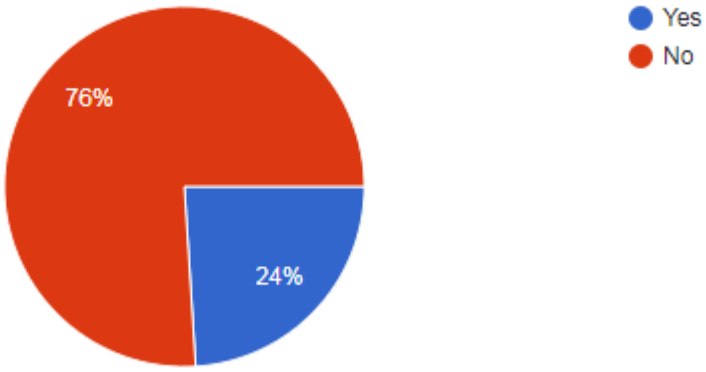


Figure 5.2 Statistics for those who participated in cybersecurity training or capture the flag

The statistics below show that the organization of the training was useful and convenient,and the challenges were well organized. Figure 5.3 shows that participants were satisfied with the general image of the usage of the training. Most answers are in climates 4 and 5 where they are quite high. Figure 5.4 shows that a large quota of participants 60% were quite satisfied and 30% satisfied with their participation in the cyber range platform and challenges.

This means that the content and the implementation were presented in a clear and understandable manner.

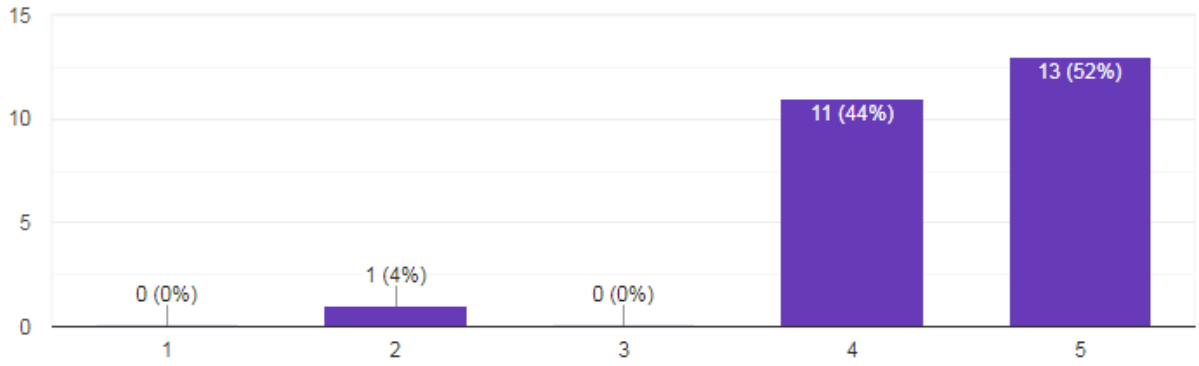


Figure 5.3 The usage of the training platform was useful and convenient

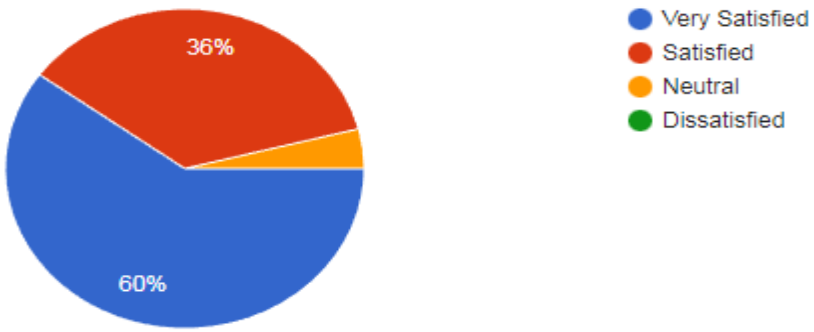


Figure 5.4 Satisfaction with the overall experience of participation

5.2 Evaluation of challenges and guides

The most important part was in the evaluation of the challenges and training guides. Summarizing below the 4 challenges the participants found them quite effective as seen from the following feedback in Figures 5.5, 5.6, 5.7, 5.8.

For the SQL challenge 64% find it very challenging.

- 44% stated that they can create their own rules in snort.
- 65% of the forensic challenge wasanswered, which is very effective.

- 56% of the mitm challenge participants said they understood how mitm works and how to identify it.

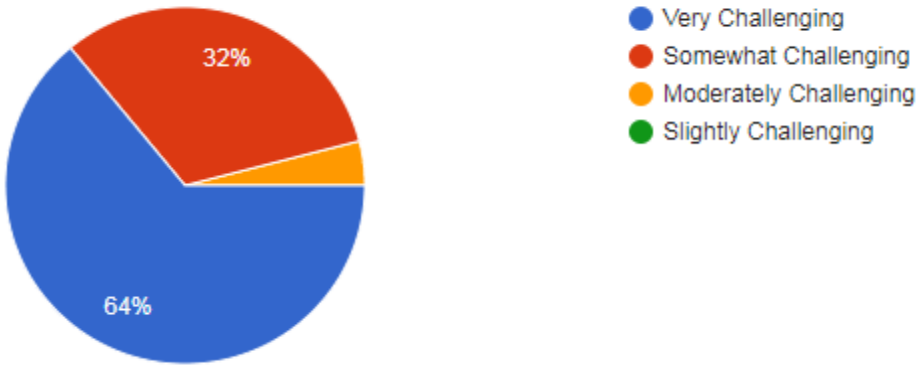


Figure 5. 5 How challenging did you find the SQL injection challenge?

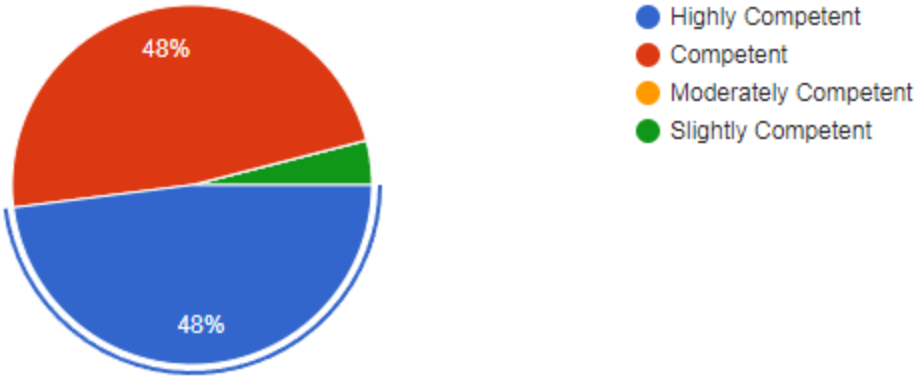


Figure 5.6 Ability to craft your own rules for the Snort intrusion detection

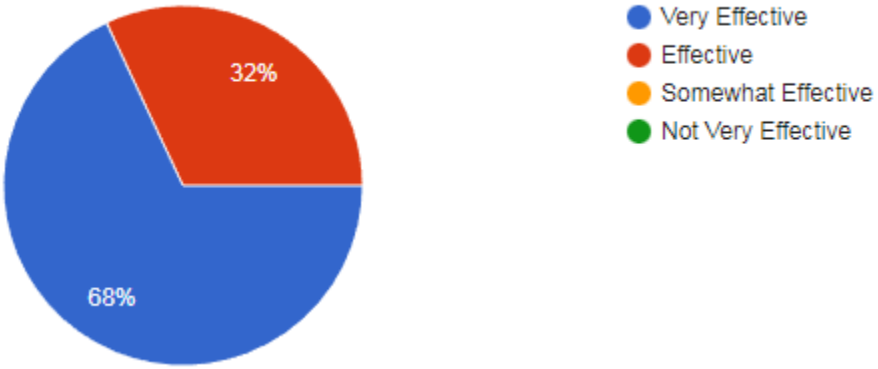


Figure 5.7 Effectiveness of the forensic challenge

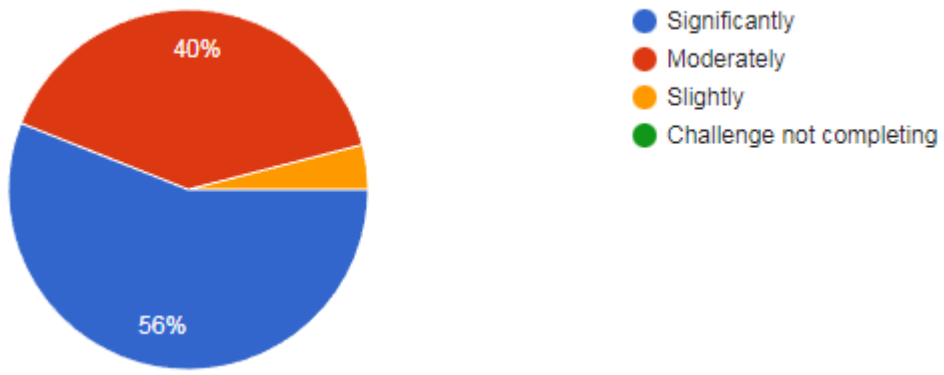


Figure 5.8 Did you enhance your knowledge on how MITM attack works?

On the other hand, about the evaluation of the training guides. The participants were very positive in favor of these guides because they helped them a lot to understand the topic they would face and the challenges they would face. In Figure 5.9 shows that 96% agree with the existence of these guides.

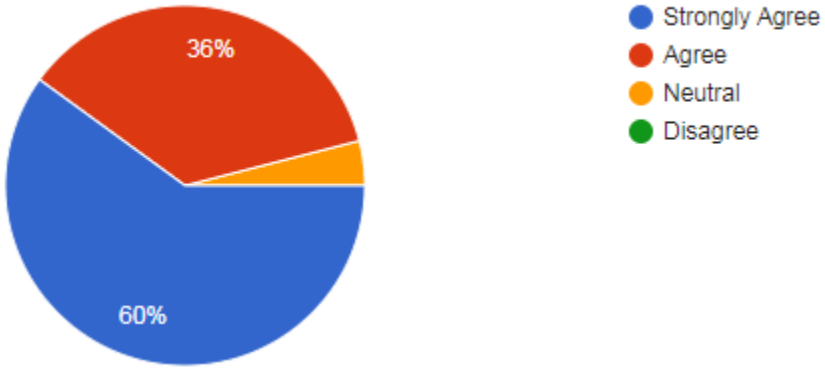


Figure 5.9 How explanatory did you find the learning guides

Chapter 6 - Conclusions and future work

This thesis introduced a comprehensive Cyber Range Platform that integrates open-source frameworks and provides a range of challenges to enhance cybersecurity education. The platform includes tasks such as SQL Injection, Snort Detection, Forensics Analysis, and Man-in-the-Middle, targeting specific cybersecurity skill sets. Docker containerization is used to provide a scalable and secure environment, and the platform is deployed on a cloud-based virtual machine for enhanced accessibility. The evaluation process includes pre- and post-surveys to gauge participants' knowledge and the effectiveness of the platform. Overall, this training paradigm aims to bridge the knowledge gap between theory and practice and produce cybersecurity professionals capable of navigating realistic scenarios in the Industry 4.0 era.

Future work in this field may entail adding more complex topics to the training cyber range platform, including incident response planning, penetration testing and security analysis. Furthermore, there can be chances to incorporate other tools and technologies, such as artificial intelligence and machine learning, into the training to ensure that participants have a deeper comprehension of the most recent advancements in the subject of cybersecurity. In addition, one key avenue for future work involves extending the participants pool for a more diverse evaluation with more participants.

Bibliography

[1] de Azambuja AJG, Plesker C, Schützer K, Anderl R, Schleich B, Almeida VR. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*. 2023; 12(8):1920. https://doi.org/10.3390/electronics12081920

[2] A. O. Junior et al., "Learning Cybersecurity in IoT-based Applications through a Capture the Flag Competition," 2022 IEEE 20th International Conference on Industrial Informatics (INDIN), Perth, Australia, 2022, pp. 560-565, doi: 10.1109/INDIN51773.2022.9976079

[3] Hatzivasilis G, Ioannidis S, Smyrlis M, Spanoudakis G, Frati F, Goeke L, Hildebrandt T, Tsakirakis G, Oikonomou F, Leftheriotis G, et al. Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Applied Sciences. 2020; 10(16):5702. https://doi.org/10.3390/app10165702

[4] Kweon, E., Lee, H., Chai, S. et al. The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. Inf Syst Front 23, 361–373 (2021). https://doi.org/10.1007/s10796-019-09977-z

[5] F. Caturano, N. d'Ambrosio, G. Perrone, L. Previdente and S. P. Romano, "ExploitWP2Docker: a Platform for Automating the Generation of Vulnerable WordPress Environments for Cyber Ranges," 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), Prague, Czech Republic, 2022, pp. 1-7, doi: 10.1109/ICECET55527.2022.9872859

[6] M. Bashir, C. Wee, N. Memon, and B. Guo, "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool," Computers & Security, vol. 65, pp. 153–165, 2017.

[7] "CTFd: Capture the Flag Platform." [Online]. Available: https://ctfd.io/. [Accessed: 9-10-2023]

[8] J. Mao, Z. L. Chua and Z. Liang, "Enabling practical experimentation in cyber-security training," *2017 IEEE Conference on Dependable and Secure Computing*, Taipei, Taiwan, 2017, pp. 516-517, doi: 10.1109/DESEC.2017.8073870.

[9] Jim Marquardson, David L. Gomillion, Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience, Information Systems Education Journal (ISEDJ), October 2018, https://files.eric.ed.gov/fulltext/EJ1193469.pdf

[10] R. Hubert, A. Bánáti, L. Erdődi and R. Fleiner, "Strengthening Database Security with Capture the Flag Exercises," 2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES), Georgioupolis Chania, Greece, 2022, pp. 000137-000142, doi: 10.1109/INES56734.2022.9922636

[11] İ. Gündoüdu, A. A. Selçuk and S. özarslan, "Effectiveness Analysis of Public Rule Sets Used in Snort Intrusion Detection System," 2021 29th Signal Processing and Communications Applications Conference (SIU), Istanbul, Turkey, 2021, pp. 1-4, doi: 10.1109/SIU53274.2021.9477698

[12] A. Mishra, C. Singh, A. Dwivedi, D. Singh and A. K. Biswal, "Network Forensics: An approach towards detecting Cyber Crime," 2021 International Conference in Advances in Power, Signal, andInformation Technology (APSIT), Bhubaneswar, India, 2021, pp. 1-6, doi: 10.1109/APSIT52773.2021.9641399

[13] J. Xu, X. Yuan, A. Yu, Jung Hee Kim, Taehee Kim and Jinghua Zhang, "Developing and evaluating a hands-on lab for teaching local area network vulnerabilities," 2016 IEEE Frontiers in Education Conference (FIE), Erie, PA, USA, 2016, pp. 1-4, doi: 10.1109/FIE.2016.7757364

[14] "Github - nategraf/Naumachia: A multi-tenant network sandbox for security challenges." [online]. Available: https://github.com/nategraf/Naumachia, [Accessed]: 20-10-2023].

[15] Katsantonis, M.N., Manikas, A., Mavridis, I. *et al*. Cyber range design framework for cyber security education and training. *Int. J. Inf. Secur*. **22**, 1005–1027 (2023). https://doi.org/10.1007/s10207-023-00680-4

[16] Ting Zheng, Marco Ardolino, Andrea Bacchetti & Marco Perona (2021) The applications of Industry 4.0 technologies in manufacturing context: a systematic literature review, International Journal of Production Research, 59:6, 1922-1954, DOI: 10.1080/00207543.2020.1824085

[17] Jamwal A, Agrawal R, Sharma M, Giallanza A. Industry 4.0 Technologies for Manufacturing Sustainability: A Systematic Review and Future Research Directions. *Applied Sciences*. 2021; 11(12):5725. https://doi.org/10.3390/app11125725

[18] Dmitry Ivanov, Alexandre Dolgui, Boris Sokolov,Cloud supply chain: Integrating Industry 4.0 and digital platforms in the "Supply Chain-as-a-Service", Transportation Research Part E: Logistics and Transportation Review, Volume 160, 2022, 102676, ISSN 1366 5545,https://doi.org/10.1016/j.tre.2022.102676

[19] Kumar R, Rani S, Awadh MA. Exploring the Application Sphere of the Internet of Things in Industry 4.0: A Review, Bibliometric and Content Analysis. *Sensors*. 2022; 22(11):4276. https://doi.org/10.3390/s22114276

[20] Diego G.S. Pivoto, Luiz F.F. de Almeida, Rodrigo da Rosa Righi, Joel J.P.C. Rodrigues, Alexandre Baratella Lugli, Antonio M. Alberti, Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review, Journal of Manufacturing Systems, Volume 58, Part A,2021,Pages 176-192, ISSN 0278-6125,https://doi.org/10.1016/j.jmsy.2020.11.017

[21] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shanay Rab, Rajiv Suman, Significance of sensors for industry 4.0: Roles, capabilities, and applications,Sensors International, Volume 2, 2021, 100110, ISSN 2666-3511, https://doi.org/10.1016/j.sintl.2021.100110

[21] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Shanay Rab, Rajiv Suman, Significance of sensors for industry 4.0: Roles, capabilities, and applications,Sensors International, Volume 2, 2021, 100110, ISSN 2666-3511, https://doi.org/10.1016/j.sintl.2021.100110

[22] Mohsen Soori, Behrooz Arezoo, Roza Dastres, Internet of things for smart factories in industry 4.0, a review, Internet of Things and Cyber-Physical Systems,Volume 3, 2023, Pages 192-204, ISSN 2667-3452, https://doi.org/10.1016/j.iotcps.2023.04.006

[23] Rahul Rai, Manoj Kumar Tiwari, Dmitry Ivanov & Alexandre Dolgui (2021) Machine learning in manufacturing and industry 4.0 applications, International Journal of Production Research, 59:16, 4773-4778, DOI: 10.1080/00207543.2021.1956675

[24] Singh M, Fuenmayor E, Hinchy EP, Qiao Y, Murray N, Devine D. Digital Twin: Origin to Future. *Applied System Innovation*. 2021; 4(2):36. https://doi.org/10.3390/asi4020036

[25] Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849-3886

[26] K. FERENCZ, J. DOMOKOS and L. KOVÁCS, "Review of Industry 4.0 Security Challenges," 2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2021, pp. 245-248, doi: 10.1109/SACI51354.2021.9465613

[27] A. Corallo, M. Lazoi, M. Lezzi and P. Pontrandolfo, "Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level," in IEEE Transactions on Engineering Management, vol. 70, no. 11, pp. 3745-3765, Nov. 2023, doi: 10.1109/TEM.2021.3084687

[28] V. Mullet, P. Sondi and E. Ramat, "A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0," in IEEE Access, vol. 9, pp. 23235-23263, 2021, doi: 10.1109/ACCESS.2021.3056650.

[29] Naanani, A. (2021). Security in Industry 4.0: Cyber-attacks and countermeasures. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 6504-6512.

[30] Radanliev, P., De Roure, D., Nicolescu, R. *et al.* Digital twins: artificial intelligence and the IoT cyber-physical systems in Industry 4.0. *Int J Intell Robot Appl* **6**, 171–185 (2022). https://doi.org/10.1007/s41315-021-00180-5

[31] Hisham A. Kholidy, Autonomous mitigation of cyber risks in the Cyber–Physical Systems, Future Generation Computer Systems, Volume 115, 2021, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.09.002.

[32] Azfar Khalid, Zeashan Hameed Khan, Muhammad Idrees, Pierre Kirisci, ZiedGhrairi, Klaus-Dieter Thoben & Jürgen Pannek (2022) Understanding vulnerabilities in cyber physical production systems, International Journal of Computer Integrated Manufacturing, 35:6, 569-582, DOI: 10.1080/0951192X.2021.1992656

[33] S. Paul, F. Ding, K. Utkarsh, W. Liu, M. J. O'Malley and J. Barnett, "On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review," in IEEE Systems Journal, vol. 16, no. 2, pp. 2367-2378, June 2022, doi: 10.1109/JSYST.2021.3123904.

[34] Radanliev, P., De Roure, D., Van Kleek, M. *et al.* Artificial intelligence in cyber physical systems. *AI & Soc* **36**, 783–796 (2021). https://doi.org/10.1007/s00146-020-01049-0

[35] Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz & Vera Pospelova (2022) The Emerging Threat of Ai-driven Cyber Attacks: A Review, Applied Artificial Intelligence, 36:1, DOI: 10.1080/08839514.2022.2037254

[36] J. Zhang, L. Pan, Q. -L. Han, C. Chen, S. Wen and Y. Xiang, "Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Survey," in IEEE/CAA Journal of AutomaticaSinica, vol. 9, no. 3, pp. 377-391, March 2022, doi: 10.1109/JAS.2021.1004261

[37] S. Vasudevan, A. Piazza and M. Carr, "A Decade of Studies on Cyber Security Training in Organizations using Social Network Analysis: A Systematic Literature Review Through Keyword co-Occurrence Network," *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, Dubai, United Arab Emirates, 2023, pp. 1-6, doi: 10.1109/ICBATS57792.2023.10111127

[38] S. G. Prasad, V. C. Sharmila and M. K. Badrinarayanan, "Role of Artificial Intelligence based Chat Generative Pre-trained Transformer (ChatGPT) in Cyber Security," *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India, 2023, pp. 107-114, doi: 10.1109/ICAAIC56838.2023.10141395

[39] D. Jagadeesan, S. R, S. S, T. S and A. B, "Real World Autonomous IoT Based Data Privacy Protection Using Machine Learning," *2023 Eighth International Conference on Science Technology*

Engineering and Mathematics (ICONSTEM), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICONSTEM56934.2023.10142934

[40] S. S. Shukla, M. Tiwari, A. C. Lokhande, T. Tiwari, R. Singh and A. Beri, "A Comparative Study of Cyber Security Awareness, Competence and Behavior," *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, Uttar Pradesh, India, 2022, pp. 1704-1709, doi: 10.1109/IC3I56241.2022.10072880

[41] C. Brady and A. M'manga, "Gamification of Cyber Security Training - EnsureSecure," 2022 IEEE International Conference on e-Business Engineering (ICEBE), Bournemouth, United Kingdom, 2022, pp. 7-12, doi: 10.1109/ICEBE55470.2022.00010

[42] S. Ma, "Research and Design of Network Information Security Attack and Defense Practical Training Platform based on ThinkPHP Framework," 2022 2nd Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS), Shenyang, China, 2022, pp. 27-31, doi: 10.1109/ACCTCS53867.2022.00014

[43] R. Acheampong, T. C. Bălan, D. -M. Popovici and A. Rekeraho, "Security Scenarios Automation and Deployment in Virtual Environment using Ansible," 2022 14th International Conference on Communications (COMM), Bucharest, Romania, 2022, pp. 1-7, doi: 10.1109/COMM54429.2022.9817150

[44] K. Yadav and R. Agrawal, "Ethical Hacking and Web Security: Approach Interpretation," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, 2022, pp. 1382-1384, doi: 10.1109/ICAIS53314.2022.9742736

[45] K. H. Sharif and S. Y. Ameen, "A Review on Gamification for Information Security Training," 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI), Sana'a, Yemen, 2021, pp. 1-8, doi: 10.1109/MTICTI53925.2021.9664771

[46] A. Angelogianni, I. Politis, P. L. Polvanesi, A. Pastor and C. Xenakis, "Unveiling the user requirements of a cyber range for 5G security testing and training," 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Porto, Portugal, 2021, pp. 1-6, doi: 10.1109/CAMAD52502.2021.9617776

[47] S. H. Said Abdelaziz Abdelrazek, H. B. Kutty Mammi and M. M. Din, "Privilege Escalation Focused Offensive Security Training Platform," 2021 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 2021, pp. 169-174, doi: 10.1109/ICoDSA53588.2021.9617497

[48] G. Hatzivasilis et al., "The THREAT-ARREST Cyber Range Platform," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 422-427, doi: 10.1109/CSR51186.2021.9527963

[49] M. Pihelgas and M. Kont, "Frankenstack: Real-time Cyberattack Detection and Feedback System for Technical Cyber Exercises," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 396-402, doi: 10.1109/CSR51186.2021.9527923

[50] N. Koutsouris, C. Vassilakis and N. Kolokotronis, "Cyber-Security Training Evaluation Metrics," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 192-197, doi: 10.1109/CSR51186.2021.9527946

[51] E. J. Glantz, M. R. Bartolacci, M. Nasereddin, D. J. Fusco, J. C. Peca and D. Kachmar, "Wireless Cybersecurity Education: A Focus on Curriculum," *2021 Wireless Telecommunications Symposium (WTS)*, CA, USA, 2021, pp. 1-5, doi: 10.1109/WTS51064.2021.9433709

[52] R. Singh, "Software Security (Capture the Flag)," 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2021, pp. 165-168, doi: 10.1109/CCICT53244.2021.00041

[53] P. Legg, T. Higgs, P. Spruhan, J. White and I. Johnson, "“Hacking an IoT Home”: New opportunities for cyber security education combining remote learning with cyber-physical systems," 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2021, pp. 1-4, doi: 10.1109/CyberSA52016.2021.9478251

[54] D. Szedlak and A. M'manga, "Eliciting Requirements for a Student-focussed Capture The Flag," 2020 7th International Conference on Behavioural and Social Computing (BESC), Bournemouth, United Kingdom, 2020, pp. 1-4, doi: 10.1109/BESC51023.2020.9348329

[55] M. N. Uddin, S. Mishra, A. Das, T. Rastogi, A. Verma and P. Kothari, "An Implementation of Capture the Flag (CTF) Tool," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 388-393, doi: 10.1109/ICTAI53825.2021.9673160

[56] M. Swann, J. Rose, G. Bendiab, S. Shiaeles and F. Li, "Open Source and Commercial Capture The Flag Cyber Security Learning Platforms - A Case Study," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 198-205, doi: 10.1109/CSR51186.2021.9527941

[57] G. M. Mennecozzi, K. Hageman, T. K. Panum, A. Türkmen, R. -V. Mahmoud and J. M. Pedersen, "Bridging the Gap: Adapting a Security Education Platform to a New Audience," 2021 IEEE Global Engineering Education Conference (EDUCON), Vienna, Austria, 2021, pp. 153-159, doi: 10.1109/EDUCON46332.2021.9453985

[58] Lee H, Kwon S, Lee J-H. Experimental Analysis of Security Attacks for Docker Container Communications. Electronics. 2023; 12(4):940. https://doi.org/10.3390/electronics12040940

[59] R. Sengupta, R. S. Sai Prashanth, Y. Pradhan, V. Rajashekar and P. B. Honnavalli, "Metapod: Accessible Hardening of Docker Containers for Enhanced Security," 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2021, pp. 01-06, doi: 10.1109/CONECCT52877.2021.9622572

[60] Luise, Alessandro & Perrone, Gaetano & Perrotta, Claudio & Romano, Simon Pietro. (2022). On-demand deployment and orchestration of Cyber Ranges in the Cloud

[61] Vittorio Orbinato DIETI, university, degli Studi di Napoli Federico II, Italy, 2021, https://doi.org/10.48550/arXiv.2112.11233

[62] Švábenský, V., Čeleda, P., Vykopal, J., &Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security, 102, 102154. doi:10.1016/j.cose.2020.102154

[63] Will Triplette, Addressing Cybersecurity Challenges in Education, International Journal of STEM Education for Sustainability, Vol.3, No.1, 2023, pp. 47-67

[64] P. Rajesh, M. Alam, M. Tahernezhadi, A. Monika and G. Chanakya, "Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework," 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA), San Antonio, TX, USA, 2022, pp. 4-12, doi: 10.1109/IDSTA55301.2022.9923170

[65] Saeed S, Suayyid SA, Al-Ghamdi MS, Al-Muhaisen H, Almuhaideb AM. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. Sensors. 2023; 23(16):7273. https://doi.org/10.3390/s23167273

[66] Ukwandu E, Farah MAB, Hindy H, Brosset D, Kavallieros D, Atkinson R, Tachtatzis C, Bures M, Andonovic I, Bellekens X. A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. Sensors. 2020; 20(24):7148. https://doi.org/10.3390/s20247148

[67] Chowdhury, N., Gkioulos, V. A personalized learning theory-based cyber-security training exercise. Int. J. Inf. Secur. 22, 1531–1546 (2023). https://doi.org/10.1007/s10207-023-00704-z

[68] Werther, J., Zhivich, M., Leek, T., &Zeldovich, N. (2011). Experiences in Cyber Security Education: The {MIT} Lincoln Laboratory {Capture-the-Flag} Exercise. In 4th Workshop on Cyber Security Experimentation and Test (CSET 11)

[69] M. Bashir, C. Wee, N. Memon, and B. Guo, "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool," Computers & Security, vol. 65, pp. 153–165, 2017.

[70] J. Wenhao and L. Zheng, "Vulnerability Analysis and Security Research of Docker Container," 2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, 2020, pp. 354-357, doi: 10.1109/ICISCAE51034.2020.9236837

[71] Rad, B. B., Bhatti, H. J., & Ahmadi, M. (2017). An introduction to docker and analysis of its performance. *International Journal of Computer Science and Network Security (IJCSNS)*, *17*(3), 228.

[72] Bhatia, G., Choudhary, A., & Gupta, V. (2017). The road to docker: a survey. *International Journal of Advanced Research in Computer Science*, *8*(8), 83-87.

[73] Ebrahimi Mehr, Iman & Minetto, Alex & Dovis, Fabio & Pica, Emanuele &Cesaroni, Claudio & Romano, Vincenzo. (2023). An Open Architecture for Signal Monitoring and Recording Based on SDR and Docker Containers: A GNSS Use Case. 10.36227/techrxiv.22212142.v1

[74] Bryan Scarbrough, Container-Based Networks: Lowering the TCO of the Modern Cyber Range, 2019, GIAC (GCIH) Gold Certification and ISE 5501

[75] K. Suo, Y. Zhao, W. Chen and J. Rao, "An Analysis and Empirical Study of Container Networks," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, Honolulu, HI, USA, 2018, pp. 189-197, doi: 10.1109/INFOCOM.2018.8485865.

[76] U. Abbasi, E. H. Bourhim, M. Dieye and H. Elbiaze, "A Performance Comparison of Container Networking Alternatives," in IEEE Network, vol. 33, no. 4, pp. 178-185, July/August 2019, doi: 10.1109/MNET.2019.1800141.

[77] M. Swann, J. Rose, G. Bendiab, S. Shiaeles and F. Li, "Open Source and Commercial Capture The Flag Cyber Security Learning Platforms - A Case Study," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 2021, pp. 198-205, doi: 10.1109/CSR51186.2021.9527941

[78] L. McDaniel, E. Talvi and B. Hay, "Capture the Flag as Cyber Security Introduction," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 2016, pp. 5479-5486, doi: 10.1109/HICSS.2016.677.

[79] M. Beltrán, M. Calvo and S. González, "Experiences Using Capture The Flag Competitions to Introduce Gamification in Undergraduate Computer Security Labs," 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2018, pp. 574-579, doi: 10.1109/CSCI46756.2018.00116

[80] Zack Kaplan, Ning Zhang, and Stephen V. Cole. 2022. A Capture The Flag (CTF) Platform and Exercises for an Intro to Computer Security Class. In Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 2 (ITiCSE '22). Association for Computing Machinery, New York, NY, USA, 597–598. https://doi.org/10.1145/3502717.3532153

[81] Jan Vykopal, Valdemar Švábenský, and Ee-Chien Chang. 2020. Benefits and Pitfalls of Using Capture the Flag Games in University Courses. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). Association for Computing Machinery, New York, NY, USA, 752–758. https://doi.org/10.1145/3328778.3366893

[82] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, 2021, doi: 10.1136/bmj.n71

[83] Pedreira V, Barros D, Pinto P. A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. *Sensors*. 2021; 21(15):5189. https://doi.org/10.3390/s21155189

[84] Rai, A., Miraz, M. M. I., Das, D., & Kaur, H. (2021, April). SQL Injection: Classification and Prevention. In *2021 2nd International conference on Intelligent Engineering and Management (ICIEM)* (pp. 367-372). IEEE.

[85] Z. C. S. S. Hlaing and M. Khaing, "A Detection and Prevention Technique on SQL Injection Attacks," 2020 IEEE Conference on Computer Applications(ICCA), Yangon, Myanmar, 2020, pp. 1-6, doi: 10.1109/ICCA49400.2020.9022833.

[86] I. Tasevski and K. Jakimoski, "Overview of SQL Injection Defense Mechanisms," 2020 28th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2020, pp. 1-4, doi: 10.1109/TELFOR51502.2020.9306676.

[87] N. Khamphakdee, N. Benjamas and S. Saiyod, "Improving Intrusion Detection System based on Snort rules for network probe attack detection," 2014 2nd International Conference on Information and Communication Technology (ICoICT), Bandung, Indonesia, 2014, pp. 69-74, doi: 10.1109/ICoICT.2014.6914042.

[88] Jan Svacina, Jackson Raffety, Connor Woodahl, Brooklynn Stone, Tomas Cerny, Miroslav Bures, Dongwan Shin, Karel Frajtak, and Pavel Tisnovsky. 2020. On Vulnerability and Security Log analysis: A Systematic Literature Review on Recent Trends. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems (RACS '20). Association for Computing Machinery, New York, NY, USA, 175–180. https://doi.org/10.1145/3400286.3418261

[89] Javeed, D., MohammedBadamasi, U., Ndubuisi, C. O., Soomro, F., & Asif, M. (2020). Man in the middle attacks: Analysis, motivation and prevention. *International Journal of Computer Networks and Communications Security*, *8*(7), 52-58.

APPENDIX A –Evaluation Questionnaires

Pre-Survey Questions

Please rate your level of cybersecurity knowledge on a scale from 1 to 5 (1 = Very Low, 5 = Very High).

1	2	3	4	5
○	○	○	○	○

How many years of experience do you have in the field of cybersecurity? *

- ○ 0-1 years
- ○ 1-3 years
- ○ 3-5 years
- ○ More than 5 years

Have you previously participated in cybersecurity training or capture the flag (CTF) challenges?

- ○ Yes
- ○ No

Post-Survey Questions

Please rate: The usage of the training was useful and convenient on a scale from 1 to 5 (1 = Very Low, 5 = Very High)

1	2	3	4	5
○	○	○	○	○

Please indicate whether you believe your knowledge and skills in cybersecurity have improved after completing the challenges.

- ○ Significantly Improved
- ○ Improved
- ○ Remained the Same
- ○ Don't Know

How satisfied are you with the overall experience of participating in the cybersecurity challenges?

- ○ Very Satisfied
- ○ Satisfied
- ○ Neutral
- ○ Dissatisfied

How would you rate the relevance of the **bacis** training scenarios to real-world Industry 4.0 cybersecurity challenges?

- ○ Highly Relevant
- ○ Moderately Relevant
- ○ Somewhat Relevant
- ○ Not Very Relevant

How challenging did you find the SQL injection challenge? *

- ◯ Very Challenging
- ◯ Somewhat Challenging
- ◯ Moderately Challenging
- ◯ Slightly Challenging

How would you rate your ability to craft your own rules for the Snort intrusion detection after completing this challenge in the most common services (FTP,SMTP,HTTP/HTTPS? *

- ◯ Highly Competent
- ◯ Competent
- ◯ Moderately Competent
- ◯ Slightly Competent

How effective was the forensic analysis challenge in enhancing your understanding the basics of digital forensics? *

- ◯ Very Effective
- ◯ Effective
- ◯ Somewhat Effective
- ◯ Not Very Effective

Did participating in the MITM challenge enhance your knowledge of how MITM attack works? *

- ◯ Significantly
- ◯ Moderately
- ◯ Slightly
- ◯ Challenge not completing

Did the provided learning guides effectively explain the concepts and techniques related to the challenges you encountered?

- ◯ Strongly Agree
- ◯ Agree
- ◯ Neutral
- ◯ Disagree