BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică „Gheorghe Asachi” din Iaşi
Volumul 69 (73), Numărul 2, 2023
Secţia
ELECTROTEHNICĂ. ENERGETICĂ. ELECTRONICĂ
DOI:10.2478/bipie-2023-0008

ENHANCING CYBERSECURITY READINESS THROUGH THE RED AND BLUE TEAM COMPETITION

BY

CRISTIAN CHINDRUŞ[*] and CONSTANTIN-FLORIN CĂRUNTU

“Gheorghe Asachi” Technical University of Iași, Romania,
Faculty of Automatic Control and Computer Engineering

Received: June 29, 2023
Accepted for publication: September 1, 2023

Abstract. Cybersecurity threats are evolving rapidly, necessitating effective strategies to combat them. Red and Blue team training is a valuable approach to address this challenge. It simulates real-world attack scenarios, with the Red team acting as attackers and the Blue team as defenders. This training helps organizations identify vulnerabilities and trains employees to respond effectively to security incidents. Introducing competition further enhances this training by motivating participants to excel and stay updated with evolving threats. This paper proposes a combined Red and Blue team approach to improve communication and understanding between teams. The findings indicate that this approach enhances capabilities in reacting to real attacks. By fostering better team understanding, participants effectively identify and mitigate vulnerabilities. These results highlight the potential value of a combined Red and Blue team approach for enhancing cybersecurity readiness. Further research is needed to fully explore its benefits and limitations.

Keywords: Cybersecurity, Red and Blue Team, training, attack scenarios, competition, mitigation.

[*]Corresponding author; *e-mail*: cristian.chindrus@student.tuiasi.ro

1. Introduction

The rapidly evolving digital landscape of the modern era has introduced numerous cybersecurity challenges for organizations across the globe. Cybercriminals adapt and employ sophisticated methods as technology advances, necessitating robust strategies to ensure effective cybersecurity readiness. Thus, the Red and Blue team competition has emerged as a promising approach to fortify organizations' cybersecurity defenses by simulating real-world attack scenarios in response to these escalating threats. This scientific paper aims to explore the potential of Red and Blue team competition in enhancing cybersecurity readiness and equipping organizations with the necessary tools to detect, respond to, and mitigate cyber threats effectively. By fostering collaboration, skill development, and a culture of continuous improvement, the Red and Blue team competition provides a dynamic and realistic training environment that empowers organizations to bolster their cybersecurity posture.

The primary objective of this paper is to explore the benefits and practical implications of Red and Blue team competition in strengthening cybersecurity readiness (Cheung *et al.*, 2012). Through an in-depth analysis of existing literature and case studies, this study aims to shed light on the significance of Red and Blue team competition in the ever-changing landscape of digital security. By examining the outcomes and lessons learned from implementing this training approach, organizations can gain valuable insights into its efficacy and potential to enhance cybersecurity readiness.

The Red and Blue team competition brings together two essential roles in cybersecurity: the Red team, which represents the attackers, and the Blue team, which represents the defenders. This collaborative approach enables organizations to simulate realistic attack scenarios, challenging the Blue team to detect and respond effectively while the Red team attempts to breach their defenses. By actively engaging in these simulations, organizations can identify vulnerabilities, test incident response procedures, and refine their cybersecurity strategies (DeCusatis *et al.*, 2021).

In a comparative analysis, the Red versus Blue competition manifests a distinct structure where two clearly defined teams engage in contrasting roles: one team undertakes the role of attackers, while the other assumes the position of defenders. This dynamic unfolds within a network architecture similar to that of a corporate setup. The competition's core essence lies in the strategic interplay between these two teams, emulating the adversarial landscape of cybersecurity. The attacking team seeks vulnerabilities and exploits to breach the system, while the defending team focuses on fortifying the network against these incursions. This format mirrors real-world scenarios where organizations confront the perpetual challenge of safeguarding their digital assets from malicious intent. This approach accentuates the competitive aspect of cybersecurity training, prompting teams to showcase their skills, adaptability, and ingenuity in either exploiting or thwarting vulnerabilities. The Red versus Blue competition thus encapsulates the dualistic nature of cybersecurity, where the relentless pursuit of vulnerabilities and the relentless defense against them converge in a high-stakes challenge.

The Red and Blue competition model involves collaborative training between two teams. This approach mirrors real-world scenarios, encouraging communication, mutual understanding, and cooperation between offensive and defensive roles. The emphasis on teamwork fosters a holistic view of cybersecurity, allowing participants to develop strategies that encompass both attack and defense perspectives. By identifying vulnerabilities together and improving responses, Red and Blue competitions enhance readiness to confront dynamic threats. On the other hand, the "Red versus Blue" competition format places the Red Team in direct opposition to the Blue Team. This adversarial setting intensifies the competitive aspect, pushing each team to outsmart the other. While this model fosters strategic thinking and quick decision-making under pressure, it may limit opportunities for collaboration and shared learning. The focus on competition could inadvertently detract from a comprehensive understanding of holistic cybersecurity practices.

Furthermore, the Red and Blue team competition facilitates skill development among cybersecurity professionals. Participants are exposed to a dynamic and ever-evolving threat landscape, requiring them to continuously enhance their knowledge and expertise. The collaboration between the Red and Blue teams encourages the exchange of insights and best practices, fostering a culture of continuous improvement within organizations (Pusey *et al.*, 2016).

By exploring the success of this training approach, organizations can gain valuable insights into how they can better detect, respond to, and mitigate cyber threats. The subsequent sections of this paper will delve into the multifaceted advantages offered by Red and Blue team competition, providing a comprehensive understanding of its significance in strengthening organizations' cybersecurity posture in an ever-evolving digital landscape.

2. Understanding the Red and Blue Team Competition

The use of Red and Blue team competition as a training methodology in the cybersecurity domain has garnered considerable interest. This section seeks to offer an extensive elucidation of the concept and intricacies surrounding the Red and Blue team competition, emphasizing its fundamental constituents and goals.

The Red and Blue team competition is a simulated exercise in which a group of attackers (the Red team) and a group of defenders (the Blue team) engage in strategic battles within a cybersecurity context. The Red team assumes the role of adversaries, employing offensive tactics to breach the security measures implemented by the Blue team, who act as the protectors of the system or network. The primary objective of the Red and Blue team competition is to enhance the overall cybersecurity posture of organizations by evaluating the effectiveness of defensive strategies and identifying potential vulnerabilities (Veerasamy, 2009).

In this context, Red team members employ their expertise to identify and exploit weaknesses in the system, simulating real-world attack scenarios. Conversely, the Blue team strives to detect and respond to the Red team's actions, applying their defensive skills to safeguard the system. Through this interactive and dynamic process, participants gain practical experience in both offensive and defensive cybersecurity tactics.

The goals of the Red and Blue team competition encompass several crucial aspects. Firstly, it enables organizations to assess the resilience of their security measures by subjecting them to simulated attacks (Zhang *et al.*, 2018). This evaluation provides valuable insights into the strengths and weaknesses of existing cybersecurity strategies and facilitates targeted improvements. Additionally, the Red and Blue team competition serves as a platform for enhancing the technical skills of cybersecurity professionals, fostering a proactive mindset, and promoting collaboration and effective communication among team members.

The intricate nature of the Red and Blue team competition demands a multidimensional approach. It involves meticulously designing realistic scenarios, incorporating advanced threat intelligence, and adopting robust evaluation methodologies (Thomas *et al.*, 2019). Moreover, effective coordination and cooperation between the Red and Blue teams are essential for extracting optimal benefits from the competition.

2.1. Red Team

In the realm of cybersecurity competitions, the Red team assumes the critical role of the offensive force. Their primary responsibility revolves around simulating real-world cyber attacks and striving to breach the cybersecurity defenses deployed by organizations. Comprising proficient cybersecurity professionals, the Red team leverages its expertise to meticulously identify vulnerabilities, exploit weaknesses, and illicitly infiltrate the organization's systems. The overarching objective of the Red team centers on rigorously challenging and scrutinizing the efficacy of the Blue team's defense mechanisms.

As skilled adversaries, the Red team employs a range of sophisticated techniques, tools, and strategies to emulate the tactics employed by actual cyber attackers. Their comprehensive knowledge and expertise enable them to emulate realistic threat scenarios, uncover potential vulnerabilities, and assess the overall resilience of an organization's security infrastructure (Bock *et al.*, 2018). By adopting the perspective of malicious actors, the Red team provides invaluable insights into the strengths and weaknesses of the defensive measures implemented by the Blue team.

Throughout the competition, the Red team efforts to push the limits of the Blue team's capabilities and expose any weaknesses in their defense strategy. This dynamic interaction between the Red and Blue teams fosters a constant cycle of learning, improvement, and innovation. By conducting realistic and simulated cyber-attacks, the Red team effectively challenges the Blue team's ability to detect, respond to, and mitigate potential threats.

The Red team's contribution to the competition extends beyond mere testing and assessment. Their works significantly contribute to the overall enhancement of an organization's cybersecurity posture. By meticulously scrutinizing the effectiveness of the Blue team's defense mechanisms, the Red team assists in identifying areas for improvement, facilitating the implementation of targeted security measures, and bolstering the organization's overall resilience against cyber threats.

The Red team plays a pivotal role as the offensive force in cybersecurity competitions. Their expertise, ingenuity, and simulated cyber-attacks enable organizations to fortify their defensive capabilities by exposing vulnerabilities and weaknesses. Through this rigorous assessment, organizations can refine their cybersecurity strategies, enhance their incident response capabilities, and foster a proactive security culture (Haney and Paul, 2018). The collaborative interaction between the Red and Blue teams within the competition framework contributes to the continuous advancement of cybersecurity practices and ultimately helps organizations stay one step ahead in the ever-evolving landscape of cyber threats.

2.2. Blue Team

In the realm of cybersecurity competitions, the Blue team assumes the critical role of the defensive force. Comprising cybersecurity professionals entrusted with safeguarding the organization's digital assets, the Blue team is primarily responsible for detecting, responding to, and mitigating the attacks orchestrated by the Red team. With a comprehensive understanding of cybersecurity principles and technologies, the Blue team employs a diverse array of defensive measures to fortify the organization's infrastructure and protect sensitive data from unauthorized access.

The Blue team's core objective centers on preserving the integrity, confidentiality, and availability of the organization's digital resources. To achieve this, they employ a multifaceted approach that includes continuous monitoring of systems, implementing robust security controls, and executing well-defined incident response procedures (Kokkonen and Puuska, 2018). Through proactive threat hunting, vulnerability assessments, and security assessments, the Blue team strives to identify and neutralize potential threats before they can exploit vulnerabilities within the organization's infrastructure.

During the competition, the Blue team demonstrates their expertise by deploying various defensive techniques and technologies. They leverage intrusion detection and prevention systems, firewalls, and advanced malware analysis tools to detect and block malicious activities. Additionally, the Blue team employs security information and event management (SIEM) solutions to monitor network traffic, identify anomalous behavior, and initiate timely incident response actions.

The Blue team's commitment extends beyond incident detection and response. They continually refine their defensive strategies, update security configurations, and enhance incident response plans based on the insights gained from the Red team's simulated attacks. By analyzing attack vectors, tactics, and techniques employed by the Red team, the Blue team gains valuable intelligence that enables them to reinforce their defensive measures, close security gaps, and strengthen the organization's overall cybersecurity posture.

The Blue team's resilience, expertise, and proactive defense contribute significantly to the success of the competition and the organization's overall cybersecurity readiness. Their unwavering dedication to protecting the organization's digital assets, detecting emerging threats, and responding effectively to security incidents underscores their pivotal role in safeguarding sensitive data and maintaining operational continuity.

The Blue team's role as the defensive force in cybersecurity competitions is of paramount importance. Their proficiency, resourcefulness, and utilization of advanced defensive measures help organizations protect their digital assets from malicious activities (Haney and Paul, 2018). Through continuous monitoring, incident response preparedness, and proactive defense strategies, the Blue team strengthens the organization's resilience against cyber threats and minimizes the potential impact of attacks. The collaborative interaction between the Blue and Red teams within the competition framework fosters a holistic approach to cybersecurity, driving continuous improvement, innovation, and a proactive security culture.

2.3. Objectives of Red and Blue Team Competition

The primary aim of the Red and Blue team competition is to bolster cybersecurity preparedness through the establishment of a simulated environment that closely replicates real-world cyber-attack scenarios. This approach enables organizations to proactively evaluate their defensive capabilities, identify vulnerabilities, and refine their incident response strategies.

The simulated environment of Red and Blue team competitions allows organizations to gain valuable insights into their cybersecurity strengths and weaknesses. It highlights areas that require improvement, such as vulnerability management, incident response processes, and security controls. By analyzing the Red team's attack vectors and the Blue team's response effectiveness, organizations can identify gaps in their cybersecurity defenses and develop targeted strategies to enhance their overall resilience (Attiah *et al.*, 2018).

Moreover, Red and Blue team competitions foster a collaborative and cooperative atmosphere among cybersecurity professionals. The exchange of knowledge, skills, and best practices between the Red and Blue teams facilitates continuous learning and improvement. It encourages innovation in defensive strategies, encourages the adoption of proactive security measures, and cultivates a culture of resilience within the organization.

To maximize the benefits of Red and Blue team competitions, organizations should incorporate lessons learned from these exercises into their cybersecurity practices. This includes strengthening security protocols, enhancing threat intelligence capabilities, and providing ongoing training to personnel. Additionally, organizations should continually update their defenses based on emerging threats and industry best practices to ensure their cybersecurity readiness remains robust and adaptive.

The competition aims to achieve the following primary goals (Katsantonis *et al.*, 2021):

- **Identify Vulnerabilities**: Red and Blue team competition provides organizations with an unique opportunity to uncover vulnerabilities in their cybersecurity defenses. The Red team's simulated attacks expose weaknesses that may otherwise go unnoticed. By identifying vulnerabilities, organizations can proactively address and mitigate potential threats.
- **Test Incident Response**: Red and Blue team competition allows organizations to evaluate the effectiveness of their incident response procedures. The Blue team's ability to detect and respond to the Red team's attacks is assessed, enabling organizations to refine their incident response plans and optimize their cyber-defense capabilities.
- **Skill Development**: Red and Blue team competition offers valuable skill development opportunities for cybersecurity professionals. Participating in the competition enhances their technical expertise, critical thinking abilities, and problem-solving skills. The intense and dynamic nature of the competition fosters professional growth and equips participants with the necessary skills to combat real-world cyber threats.

- **Collaboration and Knowledge Exchange**: Red and Blue team competition promotes collaboration between the Red and Blue teams. The competition provides a platform for cybersecurity professionals to share insights, exchange knowledge, and learn from each other's experiences. This collaboration fosters a cooperative environment, where best practices are shared, and innovative approaches to cybersecurity are developed.

3. Benefits of Red and Blue Team Competition

Red and Blue team competition has emerged as a valuable methodology in cybersecurity training, offering numerous benefits that enhance an organization's cybersecurity readiness. By simulating real-world attack scenarios, this training approach enables organizations to proactively identify vulnerabilities, improve defensive capabilities, and refine incident response strategies.

One of the key advantages of the Red and Blue team competition is its ability to provide a realistic and immersive training environment. By mimicking actual cyber attacks, participants gain practical experience in defending against sophisticated adversaries (Yamin *et al.*, 2020). The competition fosters critical thinking, problem-solving skills, and the ability to make quick decisions under pressure, all of which are essential in real-world cybersecurity incidents.

Moreover, the Red and Blue team competition promotes collaboration and teamwork among participants. The dynamic interplay between the Red and Blue teams encourages information sharing, communication, and joint efforts to identify and mitigate threats. This collaborative approach enhances the overall success of cybersecurity operations and cultivates a culture of cooperation and knowledge exchange within the organization.

Another benefit of Red and Blue team competition is its role in uncovering vulnerabilities in an organization's systems and infrastructure (Brilingaitė *et al.*, 2020). The attacks launched by the Red team serve as a comprehensive test of the organization's defenses, revealing potential weaknesses that may have gone unnoticed. This insight allows organizations to proactively address vulnerabilities, strengthen security controls, and improve the overall resilience of their digital assets.

Furthermore, the Red and Blue team competition provides a platform for continuous learning and skill development. Participants have the opportunity to stay updated on the latest attack techniques, defense strategies, and industry best practices. This ongoing learning process enables cybersecurity professionals to adapt to evolving threats and apply their knowledge to real-world scenarios, thereby increasing their effectiveness in defending against cyber-attacks (Shen *et al.*, 2021).

3.1. Realistic Simulation of Attacks

Red and Blue team competition in cybersecurity training offers a significant advantage in the form of a realistic simulation of cyber-attacks. This methodology accurately emulates the tactics, techniques, and procedures (TTPs) employed by actual threat actors, providing organizations with valuable insights into their vulnerabilities and weaknesses. Unlike traditional training approaches, this simulation approach actively uncovers potential security gaps that may have gone undetected.

The realistic nature of Red and Blue team competition enables organizations to experience first-hand the challenges associated with defending against sophisticated adversaries. By replicating real-world attack scenarios, participants are exposed to a wide range of attack vectors and strategies. This exposure allows them to identify areas where their defenses may be inadequate or where improvements can be made (Yang *et al.*, 2021).

The simulation aspect of the Red and Blue team competition provides a controlled environment for testing and evaluating an organization's cybersecurity measures. It allows organizations to assess the strength of their security controls, incident response procedures, and overall cybersecurity posture. Through this process, organizations can gain a better understanding of their strengths and weaknesses, enabling them to refine their defense strategies and allocate resources effectively.

Additionally, the simulation-based approach of the Red and Blue team competition offers a valuable learning opportunity. Participants can acquire practical experience in responding to cyber-attacks, honing their skills in incident detection, analysis, and mitigation (Andreolini *et al.*, 2020). The hands-on nature of the competition promotes critical thinking, problem solving, and decision-making under pressure, which are essential skills in the rapidly evolving landscape of cybersecurity.

3.2. Enhanced Detection and Response Capabilities

Red and Blue team competition plays a role in cultivating robust detection and response capabilities within organizations. The dynamic nature of these competitions allows the Blue team, responsible for defending against simulated attacks, to refine their skills in effectively detecting and responding to emerging threats (Khan *et al.*, 2022). Through continuous testing and evaluation of their defensive strategies, organizations can enhance their incident response procedures and Reduce response times, thereby mitigating the potential impact of cyber-attacks.

During Red and Blue team competitions, the Blue team gains valuable experience in recognizing and mitigating various attack vectors. They become adept at identifying anomalies, suspicious activities, and indicators of compromise within their network environment. This hands-on experience provides them with insights into the evolving TTPs employed by threat actors, enabling them to better anticipate and respond to real-world threats.

The iterative nature of Red and Blue team competitions allows organizations to identify gaps and weaknesses in their defense strategies. The Blue team's experiences and lessons learned from these competitions provide valuable feedback for refining their incident response plans, strengthening their defensive measures, and optimizing their detection capabilities. This continuous improvement process helps organizations stay ahead of emerging threats and adapt their security posture accordingly (Karjalainen and Kokkonen, 2020).

3.3. Skill Development and Knowledge Sharing

Red and Blue team competition plays a pivotal role in facilitating skill development and knowledge sharing among cybersecurity professionals. This unique platform creates a competitive environment that motivates participants to elevate their technical expertise, enhance critical thinking skills, and sharpen their problem-solving abilities. By engaging in simulated attack and defense scenarios, professionals are challenged to think analytically, strategize effectively, and demonstrate their proficiency in cybersecurity.

One of the significant advantages of Red and Blue team competition is the opportunity for collaboration between the two teams. This collaboration allows for the exchange of best practices, innovative techniques, and lessons learned, fostering a culture of continuous learning and improvement within the cybersecurity community. Participating in these competitions enables professionals to expand their technical knowledge by encountering diverse attack vectors and scenarios (Katsantonis *et al.*, 2017).

Red and Blue team competitions promote critical thinking and problem-solving skills. Participants are challenged to analyze complex situations, make quick decisions, and adapt their strategies in real time. The pressure and competitive nature of these competitions simulate the dynamic environment of actual cybersecurity incidents, fostering the ability to handle high-stress situations with composure and agility.

The knowledge-sharing aspect of Red and Blue team competitions is equally valuable. Professionals have the opportunity to learn from their peers, gain insights into different perspectives and approaches, and discover innovative solutions to cybersecurity challenges (Vigna, 2003). This collaborative environment encourages participants to continuously refine their skills, stay updated with the latest industry trends, and remain at the forefront of cybersecurity practices.

3.4. Identification and Mitigation of Vulnerabilities

The Red and Blue Teams competition helps organizations proactively identify and mitigate vulnerabilities in their cybersecurity defenses. These competitions simulate real-world attack scenarios, putting organizations' systems and networks to the test. By emulating the tactics and techniques of actual threat actors, Red teams expose potential weak points in the organization's defenses, allowing for targeted vulnerability assessments.

The simulated attacks conducted during the competitions serve as valuable opportunities to identify and analyze vulnerabilities that may have otherwise gone unnoticed (Seker and Ozbenli, 2018). Through these exercises, organizations gain insights into the effectiveness of their security measures, detection capabilities, and incident response procedures. By identifying weaknesses in their defenses, organizations can take proactive measures to address these vulnerabilities and strengthen their systems and networks.

Addressing vulnerabilities identified during Red and Blue team competitions is vital for enhancing an organization's overall security posture. It allows organizations to prioritize remediation efforts, allocate resources effectively, and implement necessary security controls to mitigate the identified risks. By taking proactive steps to close security gaps and strengthen their defenses, organizations can significantly Reduce the likelihood of successful cyber attacks.

3.5. Development of Cybersecurity Mindset

Engaging in the Red and Blue team competition has a profound impact on cultivating a cybersecurity mindset among participants. These competitions encourage a proactive approach to security, emphasizing the importance of continuous monitoring, threat hunting, and risk assessment. By immersing participants in realistic attack scenarios, Red and Blue team competitions instill a sense of urgency and vigilance, fostering a mindset that prioritizes proactive defense measures (Thomas *et al*., 2019).

The competitive nature of these exercises challenges participants to think critically and strategically about potential vulnerabilities and attack vectors. It promotes an active exploration of the organization's digital infrastructure, encouraging participants to identify and address potential weaknesses before they can be exploited. This mindset shift is instrumental in building a security-conscious culture within organizations.

By engaging in this kind of competition, participants develop a heightened awareness of the evolving threat landscape and the need for constant adaptation. This mindset extends beyond the competition itself and becomes ingrained in daily operations and decision-making processes. Participants become more attuned to potential risks, actively seeking out indicators of compromise and taking proactive steps to mitigate them.

4. Implementing Red and Blue Team Competition

The Red and Blue competition incorporates an infrastructure comprising a router, a core system, and multiple network segments (subnets) corresponding to the participating teams (Fig. 1). The network architecture employed in this type of competition is designed to create a realistic environment simulating cyber-attack scenarios. Each subnet contains vulnerable systems that require protection, and participants must identify and address these vulnerabilities while also launching attacks on other teams to uncover designated flags.

The primary objective of this architecture is to evaluate the participants' incident response capabilities, promoting teamwork and collaboration among teams. However, configuring the router rules can pose challenges as it involves managing a large number of rules that restrict access to specific phases of the competition. Direct access to opposing teams' virtual machines (VMs) is strictly prohibited. Additionally, each team is only granted access to the VM corresponding to their assigned mission. Network Address Translation (NAT) is applied to mask the actual IPs of both opposing teams and the core system. This NAT functionality ensures the concealment of IP addresses, maintaining anonymity and preventing unauthorized access.

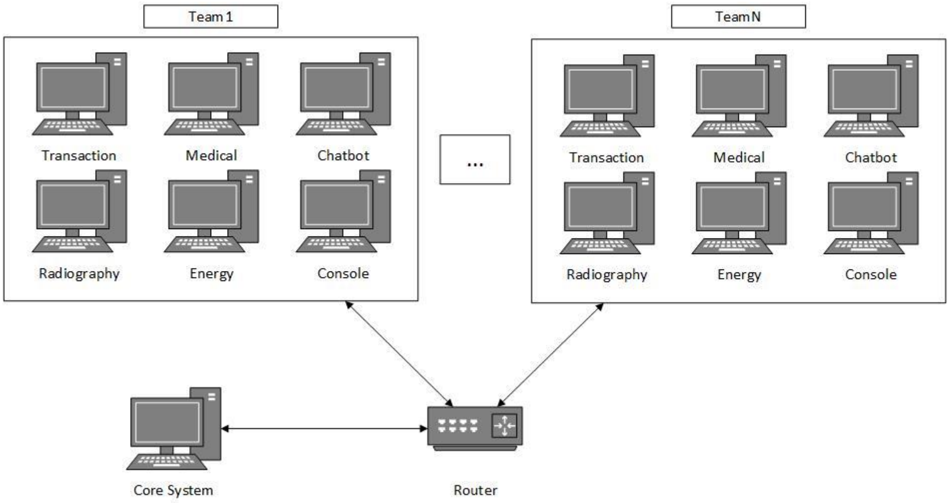

Fig. 1 – Red and Blue team competition network.

4.1. Network Architecture and Vulnerable Machines

The network architecture in a cybersecurity competition scenario is crucial for testing participants' incident response abilities and fostering communication and teamwork. It typically comprises a router, core system, and multiple subnets corresponding to the participating teams. Each subnet houses vulnerable systems used by teams to launch attacks and identify flags.

The architecture encompasses six VMs with distinct vulnerabilities, necessitating the implementation of rules to ensure fair competition. One set of rules prohibits direct access to opposing teams' VMs, restricting access to the specific subnet of the current team. With three phases, each consisting of two available VMs, additional rule sets are essential to control access to the phase-specific VMs.

During each phase's grace period, teams become familiar with their own machines but are restricted from accessing opposing teams' VMs. In the connection between any two teams, three new rules are enforced for each period, obscuring detection by using a single IP as the default gateway within each subnet. NAT is employed to mask IPs between subnets.

Teams can only access the VM corresponding to their assigned mission. For instance, a team connected to VM1 can only exploit vulnerabilities on the opposing team's VM1. This requires six rules for each connection between two teams, one for each available mission. With the number of participating teams, the management of these rules becomes significant. Hence, the network architecture in a cybersecurity competition scenario plays a pivotal role in creating a real-world-like environment, testing participants' technical expertise, teamwork, and understanding of attacker tactics and strategies.

The cybersecurity competition comprises six virtual machines, each featuring unique vulnerabilities to evaluate participants' incident response capabilities. The initial VM, named ‘Transaction’, emulates cryptocurrency wallet operations, and involves vulnerabilities related to wallet functionality. The second VM, ‘Medical’, represents a medical clinic website with vulnerabilities such as Local File Inclusion (LFI), Remote Code Execution (RCE), SQL Injection, and JSON Web Token (JWT) attacks.

In the second phase, two additional VMs are introduced. The first, ‘Chatbot’, simulates a chat service with predetermined questions and vulnerabilities like SQL Injection, Command Injection, and Directory Traversal. The second VM, ‘Radiography’, replicates the web page of an X-ray clinic, featuring vulnerabilities such as XML External Entity (XXE) and LFI.

The final stage introduces two industrial-focused VMs. The first, ‘Energy’, simulates a Supervisory Control and Data Acquisition (SCADA) communication protocol among multiple power stations, emphasizing the protection of critical information like nuclear fuel. The second VM, ‘Console’, resembles an administration console for an industrial power plant, highlighting vulnerabilities resulting from control software manufacturer oversights that could be exploited by attackers.

Each virtual machine (VM) within the system is meticulously crafted with a customized design, tailored to align with the unique characteristics of the respective machine. In tandem with this, vulnerabilities have been deliberately engineered to correspond precisely with the attributes of each VM. This strategic approach ensures that the vulnerabilities integrated into the system are intrinsically aligned with the individual nuances of each machine, thus enhancing the realism and relevance of the training environment. By adapting the vulnerabilities to the specific attributes of each VM, this methodology facilitates a more authentic and practical learning experience for participants.

VMs are configured and deployed using ansible scripts that can specify hardware requirements and other necessary parameters. Recommended hardware specifications for VM are 2 CPU, 4 GB of RAM and 40 GB hard disk. For Core System a minimum of 16 CPU, 64 GB of RAM and 100 GB of hard disk is required. No special hardware equipment is required, only servers that can meet all hardware requirements.

The network architecture and VMs employed in this competition create a challenging and realistic scenario for participants to assess their skills in identifying and mitigating cybersecurity threats. By incorporating diverse vulnerability types and scenarios, the competition offers a comprehensive approach to testing participants' abilities and ensuring their readiness to tackle real-world cybersecurity challenges.

4.2. Core System Architecture

The core system serves as the central component in the proposed scenario, functioning as the "brain" of the training exercise. It comprises three distinct modules: GenerateThings (GT), ServicesMonitor (SM), and ValidateFlags (VF). Although these modules operate independently, they share certain resources. A configuration file plays a crucial role in defining the start and end dates and times of the exercise, which can span multiple days.

Within the core system, various aspects can be identified, including the determination of days, team names, mission names, team IP addresses, and the duration of an epoch, which represents the period when the flags will change. Additionally, the core system encompasses additional functionalities and features to support the effective execution of the cybersecurity training exercise.

The GenerateThings (GT) module plays a central role in the generation of unique flags and other mission-specific information, including usernames, login passwords, and decryption keys. These generated items are random strings created based on Python functions specific to each mission and unique for each team, and their creation is scheduled based on the epoch period. GT stores all generated data in local folders, organized in a clear and easily navigable structure. To facilitate the activities of the ValidateFlags (VF) module, the flags are also saved in a separate file.

The folder structure has been designed to be straightforward and user-friendly, ensuring that all generated information from each epoch is readily accessible. This layout proves valuable in cases where debugging becomes necessary, as it allows for easy access to the required information.

Furthermore, the GT component is responsible for updating the flags and mission-related data at regular intervals determined by the epoch period. These files are transferred via a generic user account present on each virtual machine (VM). This user account is utilized for establishing Secure Shell (SSH) connections, through which the files are placed in the designated locations for each mission. The appropriate permissions are granted to ensure that the applications on the VMs can utilize these files effectively.

Additionally, the GT module performs the important task of verifying the successful submission of flags. If a submission is unsuccessful, the transmission process is automatically restarted every minute, with a maximum of three attempts made to ensure the flags are successfully received.

The ServicesMonitor (SM) component is responsible for monitoring the availability of mission-specific services. It performs four types of availability checks: FailWrite (FW), FailConnect (FC), FailRead (FR), and FailFunctional (FF). FW indicates a failure to establish an SSH connection with the corresponding machine, which may be caused by issues with the SSH service, connection permissions, or VM shutdown. FC signifies the inability to establish a connection between the monitoring system and the port on which the application is running. If the SM fails to retrieve the mission-specific information (the flag) using legitimate methods, it is marked as FR. The most comprehensive test performed by SM is the FailFunctional (FF), which examines the various functionalities the service should possess. This test can involve actions like registration or login on an application or the availability of specific web pages. If any of these tests fail, it is considered an FF.

All the information collected by SM is stored in a database, along with the duration of service unavailability. The length of unavailability serves as a negative scoring factor for teams. To track this information accurately, separate databases are maintained for each team and mission. This is necessary to ensure the precise calculation of final availability, which is derived exponentially from the total exercise duration and expressed as a percentage.

The ValidateFlags module is the final component of the core system, responsible for verifying the flags submitted by each team. Its primary task is to check the consistency between the transmitted flag and the corresponding value stored in the internal database, which is saved in the specified location mentioned earlier. Additionally, it ensures that the submitted information differs from the value generated by the validating team and that it has not expired due to the epoch change.

For every correctly entered flag, the player is awarded points based on the difference in ranking between their team and the attacked team. If the attacked team has a higher position in the ranking, the player receives points equal to the difference. Conversely, if the attacked team is ranked lower, the player receives one point. Furthermore, the ValidateFlags module can be utilized to create a graphical interface for real-time monitoring of scores, service availability, and the status of the last six epochs. A more detailed presentation of the Core System architecture can be found in another paper by the same authors (Chindruș and Căruntu, 2022).

4.3. Results

The Red and Blue team competition was conducted with a total of 20 teams, each comprising 6 individuals, resulting in a diverse pool of participants. The competition spanned over a period of 2 days, incorporating three distinct phases that unlocked new challenges as the competition progressed. The outcomes of the competition surpassed initial expectations, particularly due to the participants' receptive attitude towards the novel approach implemented in the competition.

An analysis of the statistical data collected revealed that all participants demonstrated a noteworthy improvement in their knowledge and incident response skills throughout the competition. This observation underscores the strength of the Red and Blue team competition in fostering learning and skill development among the participants.

The participants' openness to embracing the new competition format contributed significantly to the positive outcomes. This receptiveness allowed them to engage actively with the challenges presented, enabling them to enhance their understanding of cybersecurity concepts and refine their incident response capabilities. The competition format provided a dynamic and stimulating environment that facilitated the acquisition of practical skills and the application of theoretical knowledge in real-world scenarios.

Table 1 presents a detailed breakdown of the vulnerabilities identified by different organizations, in a top five relevant results, participating in the Red and Blue team competition. The table categorizes vulnerabilities into four distinct areas: web application, network infrastructure, software patching, and social engineering.

Table 1
Identified Vulnerabilities by Organization

Organization	**Web Application**	**Network Infrastructure**	**Software Patching**	**Social Engineering**	**Total**
A	*5*	*3*	*4*	*2*	***14***
B	*3*	*4*	*3*	*0*	***10***
C	*1*	*1*	*0*	*0*	***2***
D	*4*	*5*	*2*	*1*	***12***
E	*3*	*1*	*1*	*0*	***5***

Upon analysis, it is evident that organizations A and D identified the highest number of vulnerabilities across multiple categories, indicating potential weaknesses in their web applications and network infrastructure. Organization B demonstrated a relatively balanced distribution of vulnerabilities across the various categories, with particular emphasis on network infrastructure and software patching. In contrast, organizations C and E exhibited a lower overall number of vulnerabilities, suggesting that their cybersecurity defenses were relatively stronger in the assessed areas.

The table underscores the importance of conducting a comprehensive assessment of vulnerabilities across multiple dimensions to gain a holistic understanding of an organization's cybersecurity posture. It enables organizations to prioritize areas for improvement based on the identified vulnerabilities, allowing them to allocate resources effectively and implement targeted mitigation strategies. By leveraging these insights, organizations can enhance their cybersecurity readiness and strengthen their defenses against potential threats.

Table 2 highlights the skill development ratings of participants in the Red and Blue team competition. The ratings range from 1 to 5, with higher values indicating greater skill enhancement.

Table 2
Skill Development Rating

Organization	Pre-Competition Skill Level	Post-Competition Skill Level
A	*3*	*4*
B	*2*	*4*
C	*1*	*3*
D	*4*	*5*
E	*2*	*3*

Upon analysis, it can be observed that the participants from different organizations experienced varying degrees of skill improvement throughout the competition. Organization D's participants demonstrated the highest pre-competition skill level and showed significant growth, achieving the maximum rating of 5 post-competition. Organizations A, B, and E had moderate skill levels initially, which were further enhanced through the competition, resulting in commendable post-competition ratings. Organization C started with a relatively lower pre-competition skill level but exhibited notable improvement, reaching a post-competition rating of 3.

The data in Table 2 highlights the performance of the Red and Blue team competition in promoting skill development among participants. The competition provided a dynamic and challenging environment that stimulated the growth of technical expertise, critical thinking abilities, and problem-solving skills. The increase in skill levels indicates the participants' improved ability to detect and respond to cyber threats, ultimately enhancing their overall cybersecurity readiness.

The outcomes of the competition underwent meticulous analysis, relying extensively on the data extracted from the logs. This comprehensive assessment encompassed a multifaceted approach, beginning with a pre-competition questionnaire that participants completed prior to the commencement of the event. This initial questionnaire served as a benchmark, capturing participants perceptions of their preparedness, expectations, and anticipated outcomes. Through this systematic process of evaluation, valuable insights were garnered into the evolution of participants' skill sets, problem-solving abilities, and overall cybersecurity readiness. The comparison between pre-competition perceptions and in-competition behaviors provided a holistic perspective on the efficacy of the training approach. This data-driven analysis not only validated the training methodology but also offered a platform for continuous improvement by identifying areas of success and potential areas for enhancement.

These findings underscore the significance of Red and Blue team competitions as a valuable training approach for nurturing and enhancing cybersecurity skills. By providing a collaborative and realistic setting, the competition encourages continuous learning, knowledge sharing, and the cultivation of a proactive cybersecurity mindset among participants. Such skill development is essential for organizations to stay ahead of evolving threats and effectively safeguard their digital assets in today's rapidly changing cyber landscape.

The analysis of the aforementioned tables reveals the successful achievement of several key objectives. The tables provide valuable insights into the vulnerabilities identified during the Red and Blue team competition. By categorizing vulnerabilities across different areas such as web applications, network infrastructure, software patching, and social engineering, organizations gained a comprehensive understanding of their weaknesses and areas in need of improvement.

Secondly, the skill development ratings presented in the tables demonstrate the effectiveness of the Red and Blue team competition in enhancing participants' cybersecurity expertise. The participants exhibited notable growth in their technical skills, critical thinking abilities, and problem-solving capabilities. This indicates that the competition served as an effective platform for skill enhancement and knowledge acquisition in the field of cybersecurity.

Moreover, the statistics showcased in the tables highlight the overall improvement in participants' incident response capabilities. By participating in the Red and Blue team competition, individuals sharpened their ability to detect, respond to, and mitigate cyber threats effectively. This outcome signifies an enhanced level of cybersecurity readiness among the participants.

Additionally, the tables serve as evidence of the positive impact of the competition on organizational cybersecurity readiness. The identification and mitigation of vulnerabilities, combined with the skill development of participants, contribute to a stronger cybersecurity posture. The competition's dynamic and realistic environment fosters a proactive cybersecurity mindset and encourages continuous improvement within organizations.

Overall, the results indicate the success of the Red and Blue team competition in fostering knowledge growth and skill enhancement among the participants. The competition's design, encompassing multiple phases and challenges, contributed to the participants' continuous learning and engagement. These findings highlight the value of incorporating such innovative training approaches to enhance cybersecurity readiness and empower individuals to respond to evolving cyber threats.

5. Conclusion

In today's rapidly evolving digital landscape, enhancing cybersecurity readiness is of paramount importance for organizations. Red and Blue team competition has emerged as a compelling approach to fortify cybersecurity defenses and prepare organizations to effectively mitigate cyber threats. This paper has explored the concept, dynamics, and benefits of Red and Blue team competition, shedding light on its potential to enhance cybersecurity readiness.

Through realistic simulations of attacks, Red and Blue team competition provides organizations with invaluable insights into their vulnerabilities and weaknesses. It enables the development of robust detection and response capabilities, empowering organizations to swiftly identify and mitigate cyber threats. Furthermore, the collaborative nature of the Red and Blue team competition fosters skill development, knowledge sharing, and the cultivation of a proactive cybersecurity mindset.

By actively engaging in Red and Blue team competition, organizations can proactively identify and address vulnerabilities in their cybersecurity defenses, reducing the risk of successful attacks. This training methodology instills a culture of continuous learning and improvement, ensuring that cybersecurity strategies remain up to date in the face of evolving threats.

Red and Blue team competition offers a dynamic and effective approach to enhancing cybersecurity readiness. By leveraging the benefits of realistic simulations, skill development, and collaborative learning, organizations can strengthen their defenses, respond more effectively to cyber incidents, and reduce their overall risk exposure. As the cybersecurity landscape continues to evolve, embracing Red and Blue team competition becomes increasingly critical in maintaining a resilient and secure digital environment. Implementing this training methodology empowers organizations to stay one step ahead of cyber threats and safeguard their valuable assets and information.

Acknowledgments. Part of this research was supported by the project "**Collaborative environment for developing OpenStack-based cloud architectures with applications in RTI**" SMIS 124998 from The European Regional Development Fund through the Competitiveness Operational Program 2014–2020, priority axis 1: Research, technological development and innovation (RTI) — the POC/398/1/1 program.

REFERENCES

Andreolini M., Colacino V.G., Colajanni M., Marchetti M., *A framework for the evaluation of trainee performance in cyber range exercises*, Mobile Networks and Applications, vol. 25, pp. 236–247, 2020.

Attiah A., Chatterjee M., Zou C.C., *A game theoretic approach to model cyber attack and defense strategies*, in International Conference on Communications, Kansas City, MO, USA, 2018, pp. 1–7.

Bock K., Hughey G., Levin D., *King of the hill: A novel cybersecurity competition for teaching penetration testing*, in USENIX Workshop on Advances in Security Education, Baltimore, MD, 2018.

Brilingaitė A., Bukauskas L., Juozapavičius A., *A framework for competence development and assessment in hybrid cybersecurity exercises*, Computers Security, vol. 88, p. 101607, 2020.

Chindruș C., Căruntu C.F., *Development and Testing of a Core System for Red and Blue Scenario in Cyber Security Incidents*, 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 2022, pp. 1-7.

Cheung R.S., Cohen J.P., Lo H.Z., Elia F., Carrillo-Marquez V., *Effectiveness of cybersecurity competitions*, in International Conference on Security and Management. Las Vegas, USA: The Steering Committee of The World Congress in Computer Science, 2012, p. 1.

DeCusatis C., Bavaro J., Cannistraci T., Griffin B., Jenkins J., Ronan M., *Red-Blue team exercises for cybersecurity training during a pandemic*, in IEEE 11th Annual Computing and Communication Workshop and Conference, NV, USA, 2021, pp. 1055–1060.

Haney J.M., Paul C.L., *Toward integrated tactical operations for Red/Blue cyber defense teams*, in Workshop on Security Information Workers at Symposium on Usable Privacy and Security, Baltimore, MD, USA, 2018.

Karjalainen M., Kokkonen T., *Comprehensive cyber arena; the next generation cyber range*, in IEEE European Symposium on Security and Privacy Workshops, Genoa, Italy, 2020, pp. 11–16.

Katsantonis M.N., Fouliras P., Mavridis I., *Conceptual analysis of cyber security education based on live competitions*, in IEEE Global Engineering Education Conference, Athens, Greece, 2017, pp. 771–779.

Katsantonis M.N., Mavridis I., Gritzalis D., *Design and evaluation of cofelet-based approaches for cyber security learning and training*, Computers & Security, vol. 105, p. 102263, 2021.

Khan M.A., Merabet A., Alkaabi S., Sayed H.E., *Game-based learning platform to enhance cybersecurity education*, Education and Information Technologies, pp. 1–25, 2022.

Kokkonen T., Puuska S., *Blue team communication and reporting for enhancing situational awareness from white team perspective in cyber security exercises*, in Internet of things, smart spaces, and next generation networks and systems. Cham: Springer, 2018, pp. 277–288.

Pusey P., Gondree M., Peterson Z., *The outcomes of cybersecurity competitions and implications for underrepresented populations*, IEEE Security & Privacy, vol. 14, no. 6, pp. 90–95, 2016.

Seker E., Ozbenli H.H., *The concept of cyber defence exercises (cdx): Planning, execution, evaluation*, in International Conference on Cyber Security and Protection of Digital Services. Glasgow, UK: IEEE, 2018, pp. 1–9.

Shen C.C., Chiou Y.-M., Mouza C., Rutherford T., *Work-inprogress-design and evaluation of mixed reality programs for cybersecurity education*, in 7th International Conference of the Immersive Learning Research Network. Eureka, CA, USA: IEEE, 2021, pp. 1–3.

Thomas L.J., Balders M., Countney Z., Zhong C., Yao J., Xu C., *Cybersecurity education: From beginners to advanced players in cybersecurity competitions*, in International Conference on Intelligence and Security Informatics. Shenzhen, China: IEEE, 2019, pp. 149–151.

Veerasamy N., *High-level methodology for carrying out combined Red and Blue teams*, in 2nd International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 2009, pp. 416–420.

Vigna G., *Teaching network security through live exercises*, in Security Education and Critical Infrastructures, C. Irvine and H. Armstrong, Eds. New York, NY: Springer US, 2003, pp. 3–18.

Yamin M.M., Katt B., Gkioulos V., *Cyber ranges and security testbeds: Scenarios, functions, tools and architecture*, Computers Security, vol. 88, p. 101636, 2020.

Yang P., Gao F., Zhang H., *Multi-player evolutionary game of network attack and defense based on system dynamics*, Mathematics, vol. 9, no. 23, p. 3014, 2021.

Zhang H., Jiang L., Huang S., Wang J., Zhang Y., *Attack-defense differential game model for network defense strategy selection*, IEEE Access, vol. 7, pp. 50 618–50 629, 2018

ÎMBUNĂTĂȚIREA PREGĂTIRII ÎN DOMENIUL SECURITĂȚII CIBERNETICE PRIN COMPETIȚIA PE ECHIPE RED AND BLUE

(Rezumat)

Amenințările la adresa securității cibernetice evoluează rapid, ceea ce necesită strategii eficiente pentru a le combate. Formarea echipelor Red și Blue este o abordare valoroasă pentru a răspunde acestei provocări. Aceasta simulează scenarii de atac din lumea reală, în care echipa Red acționează ca atacatori, iar echipa Blue ca apărători. Această instruire ajută organizațiile să identifice vulnerabilitățile și îi pregătește pe angajați să răspundă eficient la incidentele de securitate. Introducerea competiției îmbunătățește și mai mult această formare, motivând participanții să exceleze și să rămână la curent cu evoluția amenințărilor informaționale. Această lucrare propune o abordare combinată a echipelor Red și Blue pentru a îmbunătăți comunicarea și înțelegerea între echipe. Constatările indică faptul că această abordare îmbunătățește capacitățile de reacție la atacuri reale. Prin încurajarea unei mai bune înțelegeri în echipă, participanții identifică și atenuează eficient vulnerabilitățile. Aceste rezultate evidențiază valoarea potențială a unei abordări combinate a echipelor Red și Blue pentru îmbunătățirea pregătirii în domeniul securității cibernetice. Sunt necesare cercetări suplimentare pentru a explora pe deplin beneficiile și limitările sale.