International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),
Vol.13, No.5, October 2023

BLOCK-AD: BLOCKCHAIN ATTACK-DEFENSE CTF COMPETITION FOR NEXT-WEB3 SECURITY

Inas Hasnaoui, Maria Zrikem and Rajaa Elassali

Smart Systems and Applications (SSA) National School of Applied Sciences (ENSA)
Marrakech, Morocco

ABSTRACT

The rapid growth of blockchain technology has introduced new security challenges in decentralized systems.In this paper, we present Block-AD, a Blockchain Attack-Defense Capture The Flag (CTF) competition aimed at improving smart contract security skills and addressing evolving security threats in Next-Web3 environments.

Unlike traditional CTF competitions, participants engage in attack and defense actions to exploit vulnerabilities and protect their smart contract services. This game-based approach concludes with rewards distributed from the competition's vault and the allocation of non-fungible tokens (NFTs) as proof of participation. This approach aims to provide a fun and engaging way to improve the security skills of all participants, as well as to identify and fix vulnerabilities in smart contracts.

By combining blockchain technology, CTF methodology, and Next-Web3 security, Block-AD provides a unique and innovative approach for enhancing cybersecurity skills in decentralized systems and smart contracts.

KEYWORDS

Security, Blockchain, Smart Contracts, Capture The Flag (CTF), Competition, Attack and defense, Vulnerabilities

1. INTRODUCTION

Capture the Flag (CTF) competitions have gained significant popularity in the cybersecurity community as an effective means to test and enhance participants' skills across various security domains[5, 8, 16]. Withthe rapid adoption of blockchain technology and the increasing reliance on smart contracts, it is crucial to address the vulnerabilities and security risks associated with decentralized systems[8, 9, 11].

This paper proposes the implementation of an Attack/Defense CTF competition specifically tailored to the blockchain context, aimed at improving smart contract security skills among blockchain technical staff. The game-based approach presented in this paper allows teams to engage in a competitive environment, with each team tasked with protecting their own vulnerable smart contract while simultaneously attempting to attack others' contracts. The competition incorporates additional challenges and achievements, providing a comprehensive and immersive experience for skill enhancement and vulnerability discovery in smart contracts[3, 4, 12].

Through the implementation of the Blockchain Attack/Defense CTF competition, this paper aims to foster a community of skilled blockchain professionals equipped with robust smart contract

Dhinaharan Nagamalai (Eds): CGASP, VCOI, BLKCA -2023
pp. 29-37, 2023. IJCI – 2023 DOI : 10.5121/ijcseit.2023.13503

security skills. By combining the competitive nature of CTF competitions with the unique challenges of blockchain environ- ments, this approach offers an engaging platform for participants to enhance their expertise and contribute to the advancement of secure blockchain systems. Additionally, the proposed competition serves as a valu- able training ground for blockchain technical staff, preparing them to address the evolving challenges in Next-Web3 security.

The subsequent sections of this paper delve into various aspects related to the Blockchain Attack/Defense CTF competition. Section 2 explores the synergy between CTF competitions and blockchain security, em- phasizing the importance of adapting CTF competitions to the specific challenges of decentralized systems. Section 3 introduces the Blockchain-Based Attack/Defense CTF Competition, providing in-depth techni- cal details on attack and defense actions and presenting the proposed architecture for its implementation. Section 4 comprehensively covers the evaluation process, score calculation, and reward aspects. Finally, Section 5 concludes the paper, summarizing the key findings and discussing potential avenues for future research[9, 14, 15].

In conclusion, the Blockchain Attack/Defense CTF competition represents a significant step forward in improving smart contract security skills and addressing the security challenges of Next-Web3 environments. By combining the elements of CTF competitions, blockchain technology, and game-based learning, this innovative approach offers a practical and engaging platform for training and preparing technical staff tosafeguard decentralized systems. It is anticipated that this competition will contribute to the development of a more secure and resilient blockchain ecosystem.

2. CTF COMPETITIONS AND BLOCKCHAIN SECURITY

In this section, we explore the dynamic world of Capture the Flag (CTF) competitions and their relevance to blockchain security. CTF competitions have gained significant popularity in the cybersecurity community as a means to test and enhance participants' skills in various security domains.

2.1. Overview of CTF Competitions

Capture the Flag (CTF) competitions are dynamic and engaging events[1] that serve as training groundsfor honing cybersecurity skills. These competitions simulate real-world security scenarios and challenge participants to solve a variety of puzzles and tasks related to different areas of cybersecurity.[13, 14]

CTF competitions are designed to test and improve participants' skills in areas such as reverse engineering, cryptography, web security, and more. They create a competitive environment where individuals or teams compete against each other to solve complex problems and capture flags[6, 11], which are digital tokens or codes representing successful completion of a challenge.
The following are the common types of CTF competitions:

i. **Jeopardy:** Jeopardy-style competitions involve solving a series of independent challenges across dif- ferent categories. Participants earn points for successfully completing each challenge, and the team with the highest score at the end wins. Categories may include cryptography, reverse engineering, web security, binary exploitation, forensics, and more.

ii. **Attack/Defense:** In Attack/Defense competitions, teams are tasked with defending their own vulner-able systems while simultaneously attacking opponents' systems. Teams must

secure their infras- tructure, while exploiting vulnerabilities in their opponents' systems to gain points[4]. It requires abalance between defensive and offensive strategies.

iii. **King of the Hill:** King of the Hill competitions revolve around capturing and defending a centralized target. Teams strive to maintain control of the target while defending against other teams' attemptsto dethrone them. The team that successfully captures and holds the target for the longest duration emerges as the winner.

2.2. Blockchain Security: Importance of Training

Blockchain technology has emerged as a revolutionary concept that ensures the integrity, transparency, and security of digital transactions. It utilizes cryptographic techniques and a decentralized network to provide trust and immutability. However, the security of blockchain systems, particularly smart contracts, is of utmost importance due to the potential risks and vulnerabilities they face.

Smart contracts, being self-executing agreements with predefined rules and conditions, are an integral part of blockchain systems. They enable the execution of complex transactions without the need for intermedi- aries, revolutionizing various industries[2]. However, their programmable nature makes them susceptibleto coding errors, bugs, and malicious attacks.

Training in blockchain security plays a vital role in equipping blockchain professionals, including develop- ers, auditors, and researchers, with the necessary skills to identify, prevent, and mitigate potential security risks. It helps them understand the intricacies of smart contract development, conduct comprehensive se- curity audits, and implement robust security measures to safeguard blockchain applications.

Furthermore, we will discuss notable cases of blockchain hacks and vulnerabilities that have occurred in the past. These incidents highlight the importance of proactive security practices and the need for continuous improvement in blockchain security.

By gaining a comprehensive understanding of blockchain security and undergoing appropriate training[3], individuals can contribute to the development of secure and reliable blockchain applications. In the subse- quent sections, we will explore a novel approach, the Blockchain Attack/Defense Capture the Flag (CTF) competition, which combines gaming and training to enhance smart contract security skills.

3. BLOCKCHAIN- BASED ATTACK/DEFENSE CTF COMPETITION

This section explores the technical components of the Blockchain-Based Attack/Defense Capture the Flag(CTF) Competition. It delves into the architecture, implementation, and key features of the competition, emphasizing its effectiveness in bolstering smart contract security. With a focus on critical elements like authentication, competition creation, team provisioning, and attack and defense actions.

3.1. Authentication Process: Wallet Integration

The authentication process in the Blockchain-Based Attack/Defense Capture the Flag (CTF) Competition involves users being identified by their username and wallet address. Participants connect to the com- petition platform through a compatible wallet, such as Metamask, which enables a secure connection to the blockchain. By integrating wallet functionality, users can

seamlessly interact with the competition and utilize their native blockchain currency, allowing them to participate in the competition. Furthermore, participants are required to join a specific team by entering a team code provided by the competition orga-nizers. This team-based approach promotes collaboration and strategic coordination among participants throughout the competition.

3.2. Creating and Hosting a New Competition

The process of creating and hosting a new competition in the Attack/Defense Capture the Flag (CTF) framework involves the interaction with the CompetitionFactory smart contract. As shown in Figure 1,the competition creator initiates the process by providing essential information, including the competition ID, start date, end date, maximum number of teams, and the vault amount. This information is then used by the CompetitionFactory contract to create a new competition.

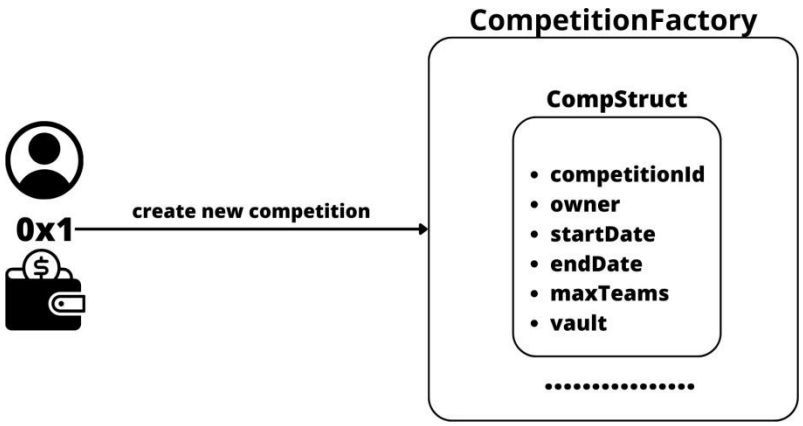

Figure 1. Creating New Competition

To initiate the competition, the creator is required to make a payment for hosting the event. The hostingprice is calculated based on the formula:

$$P = \frac{C \cdot (E - S)}{3600}$$

Where: P is the total price. C is the fixed price per hour. E is the end date in seconds. S is the start datein seconds.

Furthermore, the specified vault amount is deposited into the contract as a dedicated fund for the competi-tion.

3.2.1. Steps to Join a Competition: An Outline

In order to participate in the Blockchain-Based Attack/Defense CTF Competition, users need to follow aspecific process detailed in “Algo. 1” to join a competition and register their team.

Algorithm 1 Join Competition

```
1:  function JOINCOMPETITION(compId, teamId, merkleProof)
2:      require validateMerkleProof(merkleProof, teamId, msg.sender)
3:      if isExist(teamId, compId) then
4:          return "already exist"
5:      else
6:          require msg.value == joinPrice
7:          comp.vault + = msg.value
8:          compTeams[compId].add(teamId)
9:      end if
10: end function
```

The Merkle proof validation process is a crucial step to ensure the integrity of the team's identity. The algorithm begins by calling the validateMerkleProof function, which verifies the authenticity of the Merkle proof provided by the user. This validation process involves checking the validity of the Merkle proof against the team's ID and the sender's address (msg.sender). By leveraging the Merkle root stored within the competition contract, the algorithm confirms that the provided Merkle proof is valid andcorresponds to the team attempting to join the competition.

A Merkle tree, also known as a hash tree, is a cryptographic data structure that allows efficient verification of the integrity and membership of data within a large dataset. In our context, a Merkle tree is used to store the team members' addresses.Figure 2 illustrates an example of a Merkle tree for a specific team thatcontains four members. The root of the Merkle tree, represented by the topmost node, is stored as a mapping with each team ID within the competition contract. This mapping enables easy verification to prove that amember is part of a specific team.

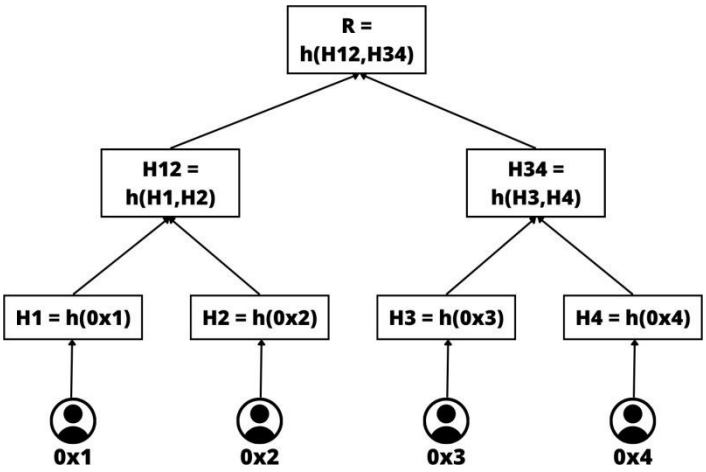

Figure 2. Team Members Merkle Tree

If the Merkle proof validation is successful, the algorithm proceeds with the next steps to join the competition. Otherwise, if the Merkle proof is invalid or does not match the expected team identity, the algorithm halts and returns an error message. This robust validation process ensures the integrity and security of team registrations within the Blockchain-Based Attack/Defense CTF Competition.

3.3. Master Contract and Service Instances

The Blockchain-Based Attack/Defense Capture the Flag (CTF) Competition introduces a unique and en- gaging approach to the gameplay, where teams compete in attacking and defending services deployed on the blockchain.

The foundation of the attack and defense mechanism lies in the concept of the Master Contract. Each team member is responsible for deploying their team's Master Contract, which acts as the central hub formanaging the team's services. The Master Contract maintains a mapping of service IDs to their respectiveinstance addresses. Upon deployment, the Master Contract creates instances of the specified services, ensuring that all teams have identical service contracts.

The Figure 3 provides a summary of the architectural differences between a traditional approach anda blockchain-based approach in terms of the services that users need to attack and defend during the competition.

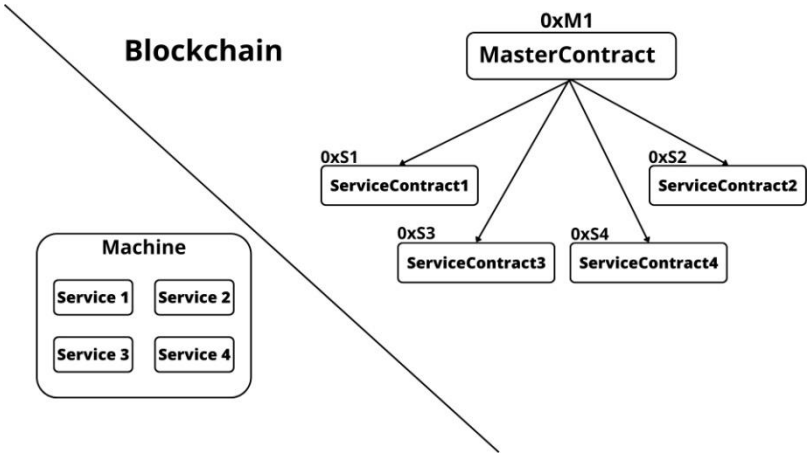

Figure 3. Team Contracts Architecture

3.4. Attack and Defense Actions

Attack and defense actions are orchestrated through the Master Contract, which relies on the specific instance addresses of each service. The Master Contract provides functionality to reset a particular service (reset(serviceID)), allowing teams to obtain a clean instance with initial states. However, team members are required to pay a fee to reset the service, incentivizing strategic decision-making.

In the backend logic, the system periodically checks the status of each team's service instances. If a service is found to be down or compromised, points are awarded to the attacking team responsible for the breach. To recover their service and prevent further attacks, the defending team must reset their service to restore itto a functional state. This prompts them to identify and fix any vulnerabilities or issues within their services.

3.5. Verification and Fixing

Each service contract includes a verification function (verify()) that checks whether it has been attacked and returns the ID of the attacking team if applicable. It also maintains a state variable

(e.g., "down" or "up") indicating the current status of the service. The backend logic continuously monitors changes in thestate of the team's service instances.

Teams must write and deploy fix contracts to defend their services against vulnerabilities. However, the blockchain's immutability prevents modifications to the original service contracts. Instead, teams write thefix contract, deploy it, and submit the new instance to the CTF platform. The backend logic validates the bytecode of the submitted fixed contract against the correctFix contract. If the bytecode matches, the team is granted access to the FixService(serviceID) function to update their service instance with the fixed version.

Figure 4 illustrates a scenario with three teams in an attack-defense competition. Each team deploys their own master contract instance and associated services. The master contract and services are cloned for each team.

In the illustration, Team 1's Service Contract 2 is attacked by Team 2, compromising its state. Team 3 defends their services, fixes vulnerabilities in Service 2, and replaces the vulnerable instance with the fixedService. As a result, Team 2 cannot attack Service 2 of Team 3.

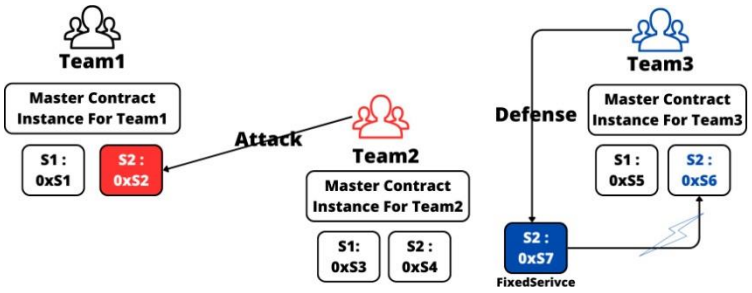

Figure 4. Simulation of Attack-Defense Actions

In the Blockchain-Based Attack/Defense CTF Competition, teams can strategically target and exploit vul- nerabilities in other team's service instances. By discovering and exploiting weaknesses, attackers can gain an advantage and accumulate points. However, to successfully solve each service, teams must meet the conditions defined in the verification function specific to that service, which returns a boolean value and the ID of the last attacking team.

By implementing this attack and defense logic, the Blockchain-Based Attack/Defense CTF Competition provides an immersive and educational experience for participants, enabling them to gain practical insights into the intricacies of blockchain security.

4. Evaluation and Score Calculation Mechanisms

The evaluation of the proposed proof of concept architecture is performed through a comparative analysis between the traditional Attack and Defense Competition and the Blockchain-Based Attack and Defense Competition. Table 1 provides a comprehensive comparison of key aspects in both approaches, It showcases the advantages of the blockchain-based approach in terms of enhanced user identification, streamlined competition creation and team joining processes, centralized management through the master contract, consistent categories and challenge types, dynamic fee calculation, shared services logic, and the use of attack contracts for submissions. These improvements contribute to a more secure and efficient competition environment, empowering participants to hone their skills in smart contract security.

Table 1. Comparison between Normal and Blockchain Attack/Defense Competitions

Categories	Normal Competition	Blockchain Competition
User Identification	usernames/passwords	wallet addresses
Competition Creation	Centralized platform	Smart contract interaction
Validating Members	Based on centralized database	Merkle OnChain Verification
Machines	Machines running services	Master contract managing services
Services Logic	Flag-based challenges	Vulnerable Service Contracts
Fee Calculation	Fixed fee structure	Native-currency
Submitting Attacks	Flag submission mechanism	Verify function for service instance
Challenges Categories	Web2 security	Web3 security

4.1. Score & Rewards

In the proposed architecture, the score calculation mechanism in the Blockchain-Based Attack and DefenseCompetition differs from the traditional competition approach. Instead of relying on tick-based point cal-culation and flag modification, the scoring is based on the verification of service instance states and the outcome of the verify function. When a team submits a service, the system verifies the validity of the verify function and checks if it returns true, indicating a successful attack. If the verification is successful and theteam ID matches the attacker team, the team's score is incremented.

At the end of the competition, a percentage of the competition's vault is awarded to the winner. Addition- ally, a percentage of the competition creation fee is allocated. Users who participated in the competition receive a non-fungible token (NFT) as proof of their participation. The NFT follows the ERC1155 stan- dard, and each participant receives a unique token bound to their account. The winner of the competition is also awarded an NFT minted specifically for them, acknowledging their victory. After the competition concludes, all users have the opportunity to claim their respective NFTs as rewards and as a testament totheir participation in the competition.

5. CONCLUSION

In conclusion, this paper introduced the Blockchain-Based Attack/Defense Capture the Flag (CTF) compe-tition as a means to enhance smart contract security skills. The key findings indicate that combining CTF principles with blockchain technology offers a realistic and engaging platform for participants to develop their expertise in protecting blockchain systems against vulnerabilities. The proposed architecture, focusingon service instance states and attack verification, provides an effective scoring and rewarding mechanism.

For future work, the implementation of the proposed architecture in a real-world setting would offer valu- able practical insights. In conclusion, the Blockchain-Based Attack/Defense CTF competition holds signifi-cant promise in enhancing smart contract security skills and equipping technical staff to tackle the evolving challenges of decentralized systems. Its gamified approach not only promotes a fun and engaging learn- ing environment but also fosters a deeper understanding of blockchain vulnerabilities and effective defense strategies. This competition serves as a valuable training tool for blockchain researchers, auditors, and technical staff, ultimately contributing to the overall improvement of blockchain security practices.

REFERENCES

[1] CTFtime, 2020. URL https:// ctftime.org/.

[2] Maher Alharby and Aad van Moorsel. Blockchain-based Smart Contracts: A Systematic Mapping Study. Fourth International Conference on Computer Science and Information Technology (CSIT-2017), 2017. doi: 10.5121/ csit.2017.71011. URL https:// doi.org/ 10.48550/ arXiv.1710.06372.

[3] Sridhar Adepu Martín Ochoa Nils Ole Tippenhauer Daniele Antonioli. Gamifying Education and Research on ICS Security: Design, Implementation and Results of S3. arXiv preprint arXiv:1702.03067, 2017.

[4] Cliff Changchun Zou Afraa Attiah. A Game Theoretic Approach to Model Cyber Attack and Defense Strategies. 2018 IEEE International Conference on Communications (ICC), 2018. URL 10.1109/ICC.2018.8422719.

[5] Ibrahim (Abe) Baggili Tyler Balon. Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. Education and Information Technologies, 2023. URL 10.1007/ s10639-022-11451-4.

[6] S. González M. Beltran. Experiences using capture the flag competitions to introduce gamification in undergraduate computer security labs. 2018 International Conference on Computational Science and Computational Intelligence (CSCI), pages 574–579, 2018. URL 10.1109/ CSCI46756.2018.00101.

[7] Chris Novakovic Tom Chothia. An Offline Capture The Flag-Style Virtual Machine and an Assessmentof its Value for Cybersecurity Education. Computer Science, 2015.

[8] J. Cohen K. Chung. Learning obstacles in the capture the flag model. {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.

[9] Hanan Hibshi Nicolas Christin Alejandro Cuevas. Observations From an Online Security Competition and Its Implications on Crowdsourced Security. arXiv preprint arXiv:2204.12601, 2022.

[10] Emmanouil Magkos Stylianos Karagiannis. An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools. IFIP Advances in Information and Communication Technology, 579, 2020. URL 10.1007/ 978-3-030-59291-2_5.

[11] Maria Leitner Stela Kucek. An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments. Journal of Network and Computer Applications, 151:102470–102470, 2020. URL 10.1016/ j.jnca.2019.102470.

[12] S. J. Petrilli Jr K. Leune. Using capture-the-flag to enhance the effectiveness of cybersecurity education. Proceedings of the 18th Annual Conference on Information Technology Education, pages 47–52, 2017. URL 10.1145/ 3133041.3133082.

[13] B. Hay L. McDaniel. Capture the flag as cyber security introduction. 2016 49th Hawaii International Conference on System Sciences (HICSS), pages 5479–5486, 2016.

[14] Paul A. H. Peterson Jelena Mirkovic. Class Capture-the-Flag Exercises. 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), pages 1–8, 2014.

[15] Eng Lieh Ouh Kee Hock Tan. Lessons Learnt Conducting Capture the Flag CyberSecurity Competition during COVID-19. Institutional Knowledge at Singapore Management University, 2022.

[16] Jan Vykopal Silvia Brišáková Valdemar Švábenský. Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges. arXiv preprint arXiv:2101.01421, 2021.