Оглавление

[1 CTF как вид соревнования 2](#_Toc141481634)

[1.1 История CTF 2](#_Toc141481635)

[1.2 Виды CTF 3](#_Toc141481636)

[1.2.1 Jeopardy 3](#_Toc141481637)

[1.2.2 Attack-defense 4](#_Toc141481638)

[1.3 Платформы мониторинга CTF соревнований 6](#_Toc141481639)

[2 Основные виды заданий 11](#_Toc141481640)

[2.1 WEB 11](#_Toc141481641)

[2.2 Криптография 12](#_Toc141481642)

[2.3 Реверс-инжиниринг 13](#_Toc141481643)

[2.4 Форензика 14](#_Toc141481644)

[2.5 Стеганография 16](#_Toc141481645)

[3 Nimda CTF 18](#_Toc141481646)

[3.1 История 18](#_Toc141481647)

[3.2 Проведение в 2023 году 18](#_Toc141481648)

[3.2.1 Контингент 18](#_Toc141481649)

[3.2.2 Планируемые задания 18](#_Toc141481650)

[3.2.3 Планируемые этапы 19](#_Toc141481651)

[3.2.4 Планируемые даты проведения 19](#_Toc141481652)

[3.2.5 Планируемое количество участников в отборочном этапе 19](#_Toc141481653)

[3.2.6 Планируемое количество участников в финальном этапе 19](#_Toc141481654)

[3.2.7 Потенциальные партнерства 19](#_Toc141481655)

[3.2.8 Планируемая платформа проведения очного этапа 20](#_Toc141481656)

[3.2.9 Планируемая платформа проведения финального этапа 20](#_Toc141481657)

1. CTF как вид соревнования
   1. История CTF

История “CTF” (“Capture The Flag”) начинается в компьютерной безопасности и киберспорте. “CTF” — это формат соревнований, в которых участники пытаются найти и "захватить флаги" (файлы или строки) на компьютерных системах с различными уязвимостями. Победитель - тот, кто сможет найти наибольшее количество флагов или первым захватит особо ценный флаг.

История “CTF” связана с ранними днями хакерской культуры и развитием компьютерной безопасности в 1990-х годах. Коллективы хакеров начали устраивать свои собственные соревнования и участия в них. В то время “CTF”-игры были простыми, часто состояли из уязвимых программ и сетей, в которых участники пытались обнаружить слабые места и эксплуатировать их.

С течением времени “CTF” стал популярной формой тестирования навыков и знаний в области информационной безопасности. Организации, университеты и компании стали устраивать “CTF”-соревнования для обучения и проверки своих сотрудников, студентов и команд по безопасности.

Со временем формат “CTF” расширился и стал разнообразным, включая различные категории задач, такие как:

Криптография: разгадывание шифров, взлом шифрованных сообщений и т.д.

Веб-безопасность: поиск уязвимостей в веб-приложениях, эксплуатация кода на сервере и т.д.

Реверс-инжиниринг: анализ исполняемых файлов и декомпиляция программ.

Стеганография: обнаружение скрытой информации в изображениях, звуке и т.д.

Форензика: анализ криминалистических данных и поиск следов.

Соревнования “CTF” стали широкораспространёнными событиями на многих конференциях по безопасности и киберспорту. Они стали важной частью образования в области компьютерной безопасности, помогая участникам развивать навыки в обнаружении уязвимостей, решении сложных задач и командной работе.

Кроме того, “CTF”-игры стали привлекательными событиями для рекрутинга в области кибербезопасности, где компании и правительственные организации могут привлечь талантливых специалистов соревнованиями и предложить им работу.

Сегодня “CTF” продолжает развиваться, и у него появляются новые форматы и категории задач, а также международные соревнования, привлекающие участников со всего мира. Это важный инструмент для повышения уровня компьютерной безопасности и развития специалистов в этой области.

* 1. Виды CTF
     1. Jeopardy

“Jeopardy CTF” (или “task-based”) - это один из наиболее распространенных форматов соревнований в области компьютерной безопасности. Он получил свое название от американской телевизионной игры "Jeopardy!", в которой участники отвечают на вопросы в различных категориях.

В формате “Jeopardy CTF”, участники сталкиваются с серией заданий (флагами) разного уровня сложности, которые относятся к различным категориям, таким как криптография, веб-безопасность, реверс-инжиниринг, стеганография, форензика и другие. Каждое задание имеет свой уникальный флаг — это строка текста или файл, который участник должен обнаружить или извлечь.

Чтобы заработать очки, участники решают задания, найденные вовремя   
“CTF”-соревнования, и предоставляют организаторам флаги, найденные ими. За каждый правильно найденный флаг команда получает определенное количество очков. Чем сложнее задание, тем больше очков оно приносит. Команды соревнуются друг с другом, пытаясь набрать наибольшее количество очков за ограниченное время соревнования.

Организаторы “CTF”-соревнований предоставляют участникам доступ к соревновательному серверу, на котором размещены задания и их окружение для решения. Обычно участникам также предоставляются некоторые инструменты, такие как различные скрипты, программы или виртуальные машины, которые помогают решить задания.

Jeopardy “CTF” отличается от других форматов, таких как “Attack-Defense CTF”, где команды также имеют возможность атаковать друг друга и защищаться от атак. В “Jeopardy CTF” соревнованиях, участники фокусируются исключительно на решении заданий, что делает этот формат более доступным и подходящим для участия более широкой аудитории, включая студентов, начинающих специалистов и опытных профессионалов.

“Jeopardy CTF”-соревнования широко популярны на конференциях по компьютерной безопасности, вузах и организациях, посвященных кибербезопасности. Они предоставляют участникам отличную возможность проверить и улучшить свои знания и навыки в области информационной безопасности, а также научиться работать в команде и решать сложные задачи.

* + 1. Attack-defense

“Attack-Defense CTF” — это формат соревнований в области компьютерной безопасности, в которых команды соревнуются, пытаясь одновременно атаковать компьютерные системы друг друга и защищать свои собственные системы от атак. Этот формат CTF требует от участников не только навыков поиска уязвимостей, но и способности защищать свои ресурсы.

Принцип “Attack-Defense CTF” следующий:

Командам предоставляется доступ к идентичным (или похожим) копиям виртуальных машин или серверов, называемых "заданиями" или "контейнерами". Каждое задание содержит уязвимости или "флаги", которые участники должны найти и захватить, чтобы заработать очки.

Команды начинают соревноваться одновременно и имеют доступ к сети, где они могут обнаруживать и атаковать системы друг друга, пытаясь найти и эксплуатировать уязвимости в их заданиях. Найденные флаги сразу же отправляются на сервер организаторов, чтобы заработать очки.

Одновременно с атаками команды также должны защищать свои собственные системы от атак других участников. Они должны активно мониторить свои системы на предмет взлома, устранять обнаруженные уязвимости и предпринимать меры по обеспечению безопасности.

В течение определенного времени соревнования, которое может быть несколько часов или дней, команды продолжают атаковать и защищать, набирая очки за каждый успешный захват флага или защиту своих систем от атак.

Соревнования “Attack-Defense CTF” предоставляют участникам возможность не только продемонстрировать свои навыки в поиске уязвимостей и атаках, но и научиться обеспечивать безопасность своих собственных систем. Этот формат CTF также подчеркивает важность реактивной и проактивной защиты, а также способность команды работать в условиях реальных кибератак и обеспечивать надежность своих ресурсов.

Соревнования “Attack-Defense CTF” обычно проводятся на конференциях, в образовательных учреждениях и специализированных событиях, привлекая опытных профессионалов и начинающих специалистов в области компьютерной безопасности. Это отличная возможность для участников попрактиковать свои навыки в безопасности, сотрудничать в команде и научиться эффективно справляться с киберугрозами.

* 1. Платформы мониторинга CTF соревнований

Самой известной платформой мониторинга “CTF” соревнований является “CtfTime”. Визуальное отображение платформы (сайта) показано на рисунке 1.3.1.

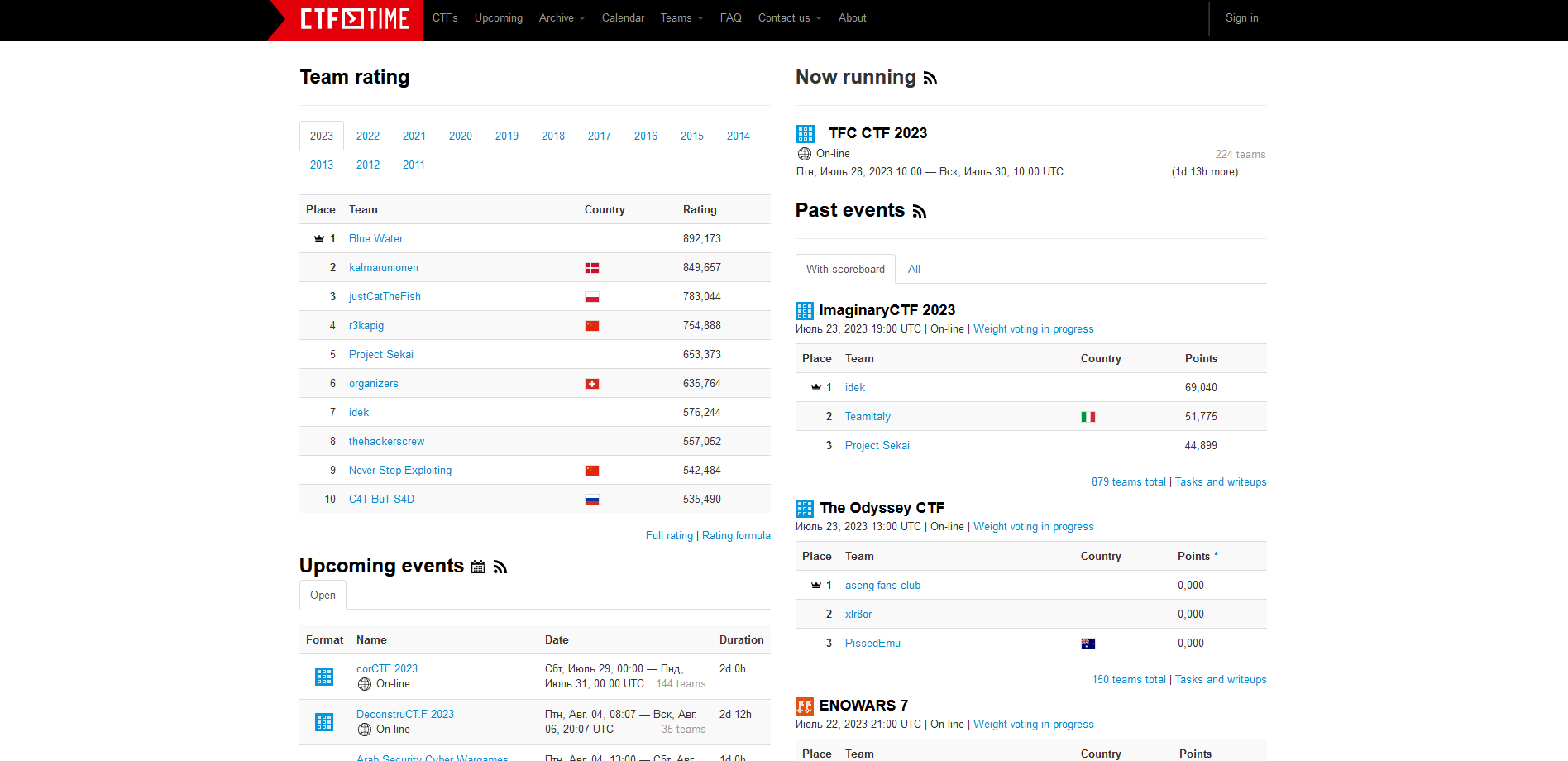


Рисунок 1.3.1. – Платформа “CtfTime”

На данной платформе возможна регистрация участников соревнований, а также формирование непосредственных команд. Пример отображения команды показан на рисунке 1.3.2.

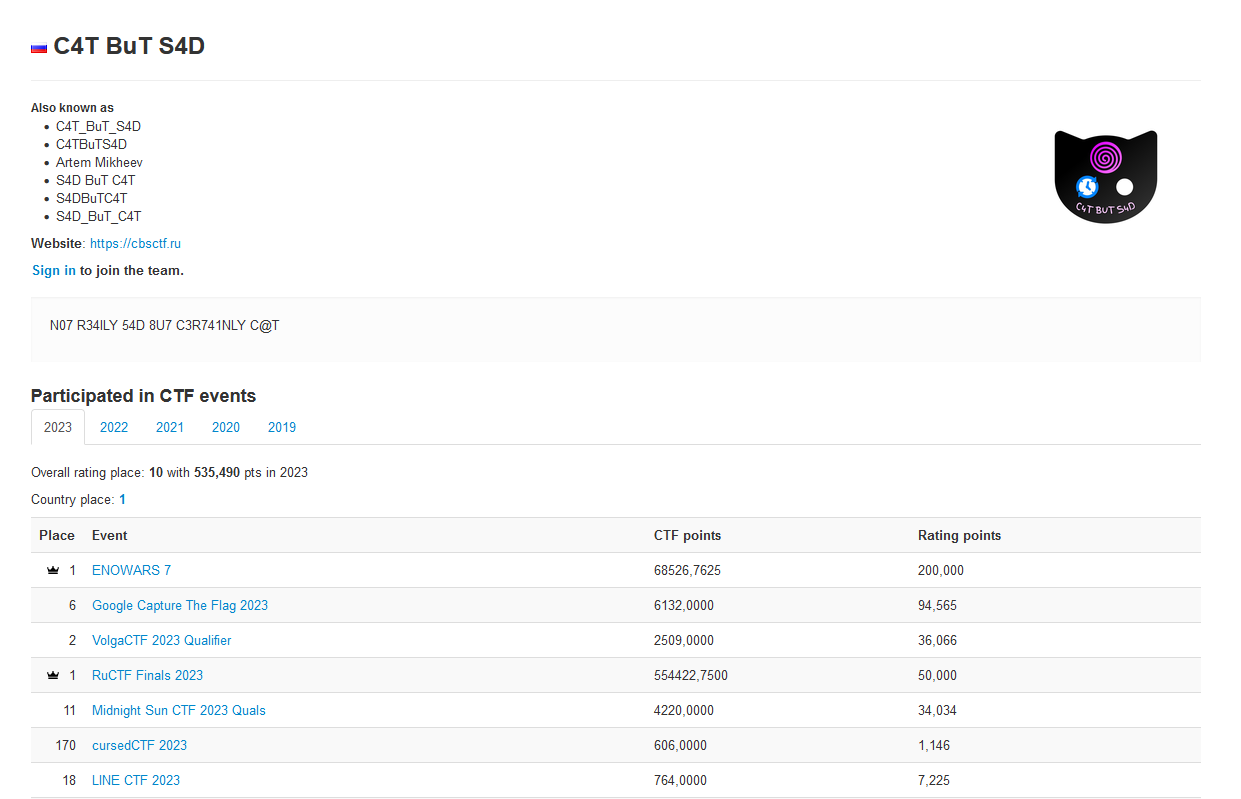


Рисунок 1.3.2. – Команда “C4T BuT S4D”

На платформе можно найти прошедшие, текущие и планирующиеся соревнования формата “CTF”. На рисунке 1.3.3 показан календарь с соревнованиями.

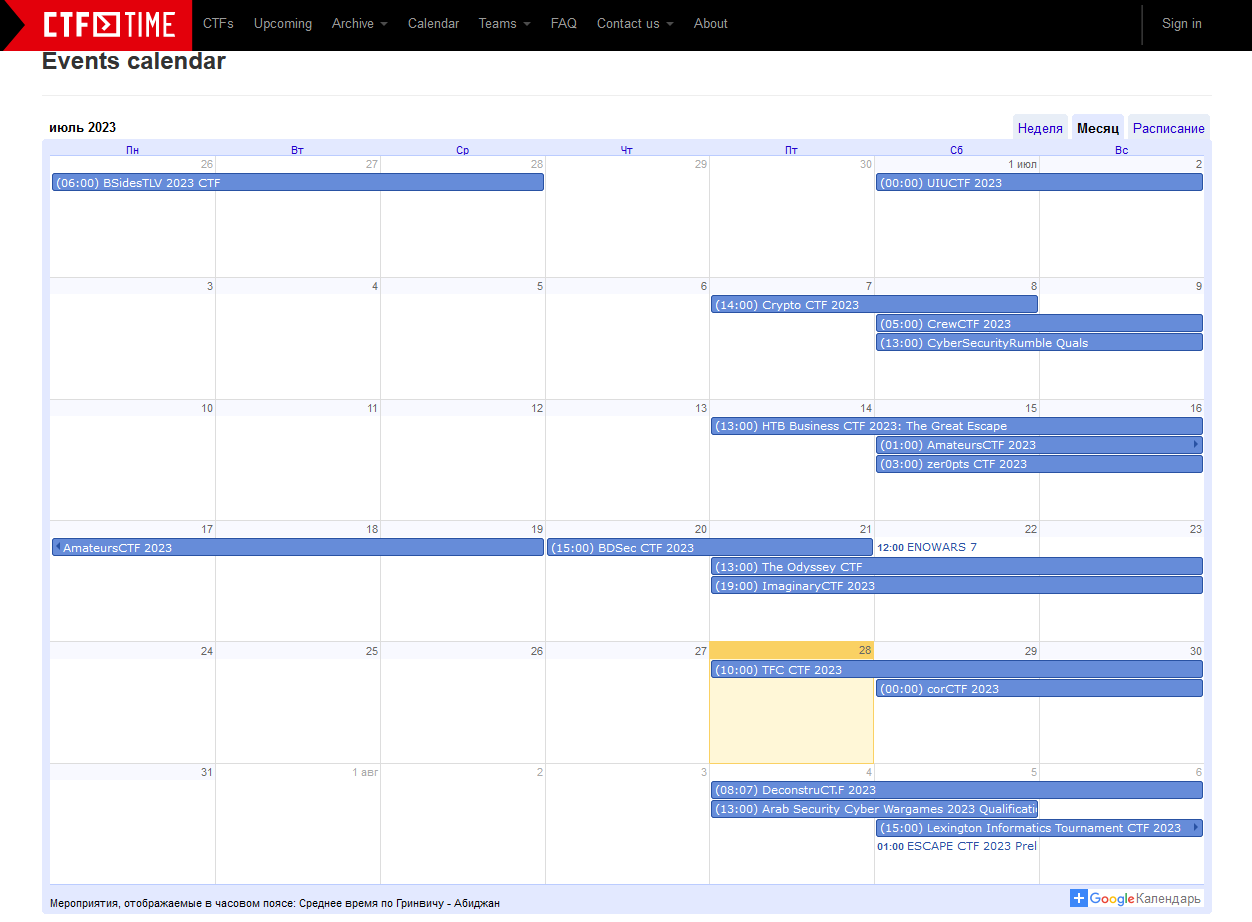


Рисунок 1.3.3. – Календарь соревнований

Визуализация непосредственного соревнования показана на рисунке 1.3.4.

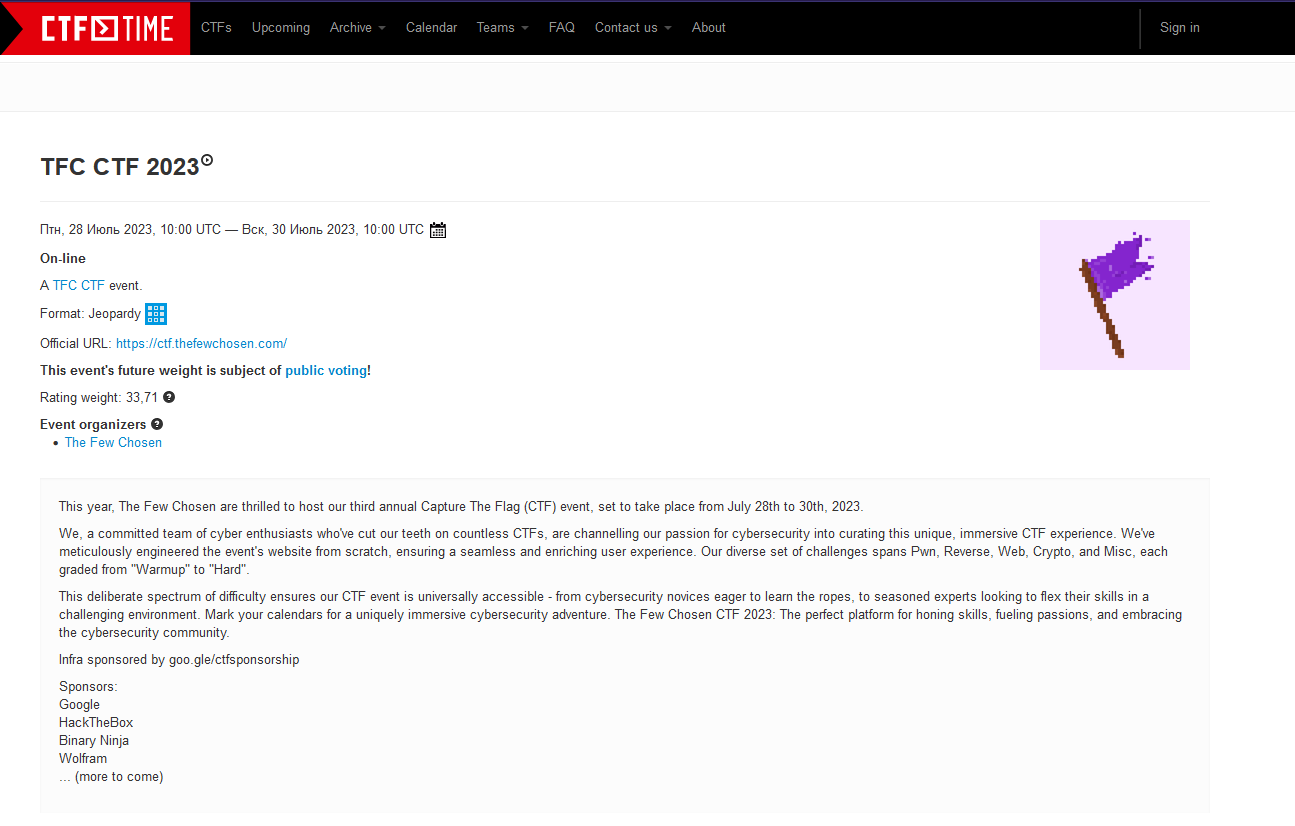


Рисунок 1.3.4. Пример соревнования.

Также на платформе предусмотрена система рейтинга. Рейтинг на платформе считается исходя из количества очков, набранных конкретной командой на различных “CTF”-ах.

На платформе также возможна фильтрация рейтинга по странам. Также существует глобальный мировой рейтинг. Рейтинг команд по России представлен на рисунке 1.3.5, а глобальный рейтинг представлен на рисунке 1.3.6.

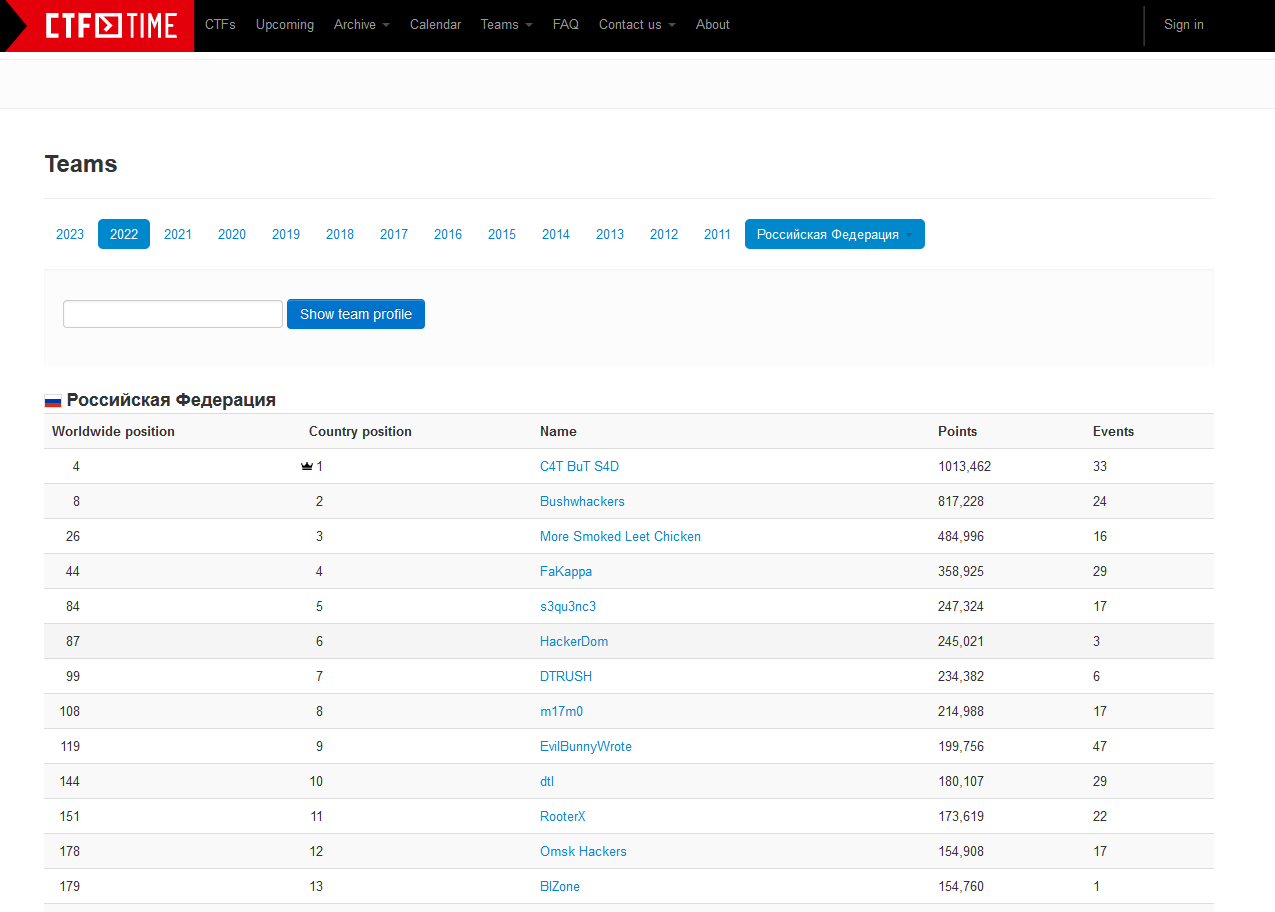


Рисунок 1.3.5. – Рейтинг Российских команд по “CTF”

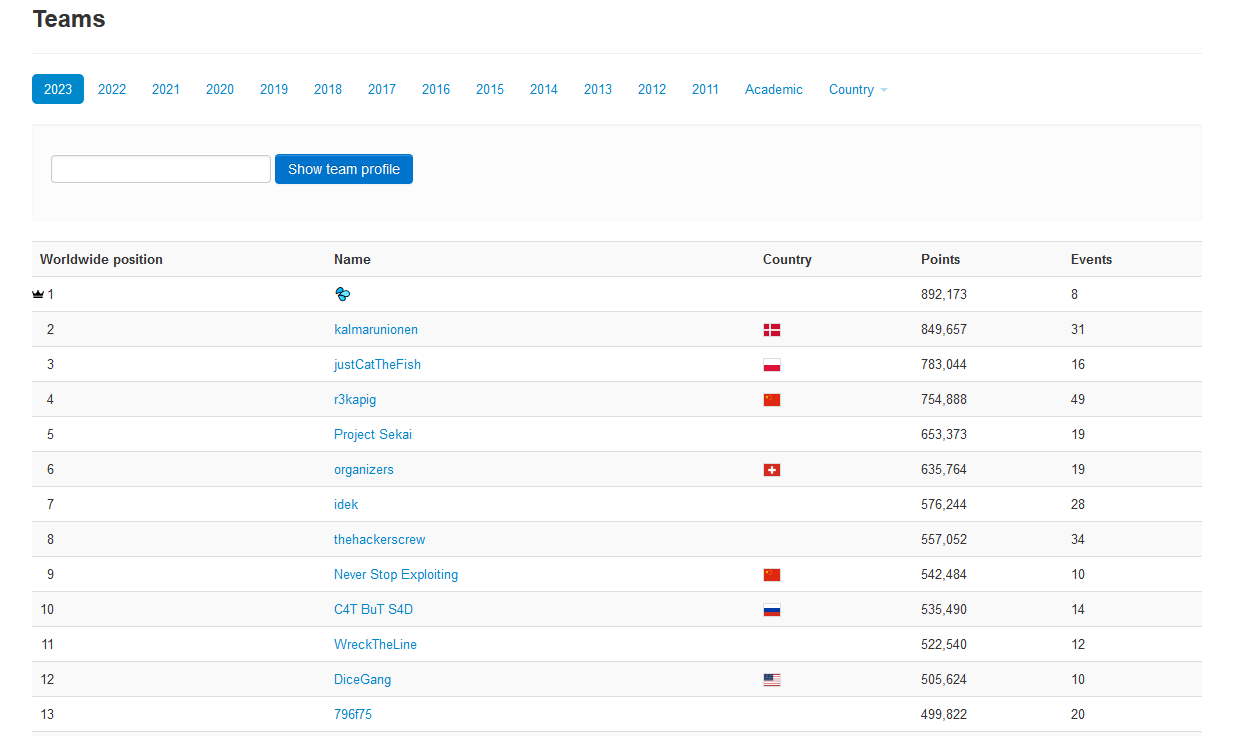


Рисунок 1.3.5. – Глобальный рейтинг команд по “CTF”

1. Основные виды заданий
   1. WEB

Категория заданий "WEB" в “CTF” — это одна из наиболее распространенных и интересных категорий, связанных с веб-безопасностью. Задания в этой категории обычно требуют от участников знаний и навыков веб-разработки, а также умения обнаруживать и эксплуатировать уязвимости в веб-приложениях.

Некоторые из типичных заданий в категории “WEB” “CTF” включают:

1. Уязвимые веб-приложения: Участникам предоставляется доступ к веб-приложению с различными уязвимостями, такими как инъекции “SQL”, межсайтовый скриптинг (“XSS”), кросс-сайтовая атака подделки межсайтового запроса (“CSRF”) и другие. Задача участников - обнаружить и эксплуатировать эти уязвимости для получения флагов или доступа к защищенным ресурсам.
2. Исследование “HTTP”-трафика: Участникам могут предоставляться журналы HTTP-запросов и ответов или дампы сетевого трафика веб-приложения. Их задача - проанализировать трафик, найти скрытые сообщения или уязвимости, а также определить методы аутентификации или авторизации.
3. Скрытые данные в коде страницы: Задания могут содержать веб-страницы с зашифрованными или скрытыми флагами в исходном коде “HTML”, “CSS” или “JavaScript”. Участникам нужно уметь обнаруживать и анализировать эти данные, чтобы получить флаги.
4. Шифрование и дешифрование: Участникам могут предоставляться зашифрованные данные или параметры, которые нужно расшифровать, используя различные методы криптографии.
5. Реверс-инжиниринг веб-приложений: Задания могут включать анализ исполняемых файлов веб-приложений или клиентских скриптов с целью обнаружения уязвимостей или скрытых флагов.

Как и в других категориях “CTF”, в категории “WEB” участникам предоставляется ограниченное время для решения задач, и они зарабатывают очки за каждый успешно найденный флаг. Задания в этой категории могут быть различными по сложности - от начального уровня до сложных задач, требующих глубоких знаний и опыта в области веб-разработки и веб-безопасности.

Категория “WEB” в “CTF” предоставляет участникам отличную возможность попрактиковаться в поиске уязвимостей в реальных веб-приложениях и научиться разрабатывать более безопасные веб-ресурсы. Это также помогает повысить осведомленность о веб-безопасности и популяризировать лучшие практики разработки веб-приложений.

* 1. Криптография

Криптография в "CTF" — это категория заданий, которая занимается анализом и созданием криптографических алгоритмов. Это важный аспект соревнований CTF, который проверяет знания криптографии у участников и их способность решать разнообразные задачи, связанные с шифрованием и дешифрованием данных.

Задания в категории "криптография" могут включать следующие типы:

1. Шифрование и дешифрование: Участникам могут предоставляться зашифрованные данные или тексты с использованием различных шифров, таких как шифр Цезаря, шифр Виженера, шифр Атбаш и другие. Задача участников - расшифровать эти данные и найти флаги, скрытые в них.
2. Криптоанализ: Задания могут предполагать анализ шифров или криптографических алгоритмов с целью выявления уязвимостей. Участники могут пытаться обнаружить паттерны или уязвимости в шифротекстах для извлечения ключей или флагов.
3. Криптографические головоломки: Задания могут включать различные криптографические головоломки, которые требуют логического мышления и знаний криптографии для решения. Это может быть что-то вроде задачи на нахождение простых чисел, генерации ключей или использования криптографических хеш-функций.
4. Криптография на основе каналов: Задания могут связывать криптографию с обменом информации через различные каналы связи. Участникам могут предлагаться задачи на защищенную передачу данных или обнаружение скрытых сообщений.

Участники соревнуются в решении задач в категории криптография и получают очки за каждый успешно найденный флаг. Задания могут иметь разный уровень сложности - от задач для новичков до более сложных проблем для опытных специалистов в области криптографии.

* 1. Реверс-инжиниринг

Реверс-инжиниринг (“Reverse Engineering”) в “CTF” — это категория заданий, которая проверяет навыки анализа и разбора программного обеспечения, таких как исполняемые файлы (бинарные файлы) или клиентские скрипты. Эта категория позволяет участникам исследовать работу программы на уровне машинного кода или исходного кода для обнаружения уязвимостей, поиска флагов или решения криптографических задач.

Задания в категории «Реверс-инжиниринг» могут включать следующие типы:

1. Анализ исполняемых файлов: Участникам предоставляют исполняемые файлы (например, исполняемые файлы “Windows .exe”, исполняемые файлы “Linux ELF” или “Android APK”) с кодом на машинном уровне. Задача участников - исследовать эти файлы, анализировать их структуру и выявлять интересующие участки кода.
2. Обратная разработка протоколов: Участникам могут предоставляться протоколы или форматы данных, используемые в программе, и задача состоит в их разборе и понимании, чтобы понять, как работает взаимодействие между компонентами системы.
3. Криптоанализ бинарных файлов: Задания могут предполагать анализ алгоритмов шифрования или хэширования, использованных в бинарных файлах, чтобы обнаружить уязвимости или найти флаги.
4. Обход "антиотладочной" защиты: Некоторые задания могут включать "антиотладочные" механизмы, предназначенные для затруднения анализа программы. Участникам нужно будет найти способы обойти такие механизмы и продолжить анализ.
5. "Обфускация" кода: В некоторых заданиях исходный код программы может быть специально "обфусцирован" (затруднен для чтения), и участникам придется разгадать эту "обфускацию" для понимания его работы.

Реверс-инжиниринг в CTF предоставляет участникам возможность лучше понять работу программного обеспечения на низком уровне и научиться идентифицировать и анализировать уязвимости. Успешное выполнение заданий в этой категории требует хорошего понимания архитектуры компьютеров, машинного кода, ассемблера и других технических аспектов программирования. Это также позволяет участникам развивать навыки решения сложных проблем и поощряет творческий подход к обнаружению и анализу уязвимостей.

* 1. Форензика

Форензика (“Forensics”) в “CTF” — это категория заданий, которая фокусируется на анализе данных и поиске цифровых следов, оставленных на компьютерных системах, устройствах или в сетевом трафике. Задания в этой категории имитируют работу цифровых следователей (цифровых форензиков) и требуют участников применять методы анализа данных, стеганографии, криптографии и другие техники для решения задач.

Задания в категории «Форензика» могут включать следующие типы:

1. Анализ файлов и метаданных: Участникам предоставляются файлы различных форматов (изображения, аудио, документы и т.д.), и их задача - найти скрытую информацию или флаги внутри файлов или в метаданных, таких как дата создания, автор и т.д.
2. Восстановление удаленных данных: Задания могут предполагать восстановление удаленных или скрытых файлов из образов дисков или физических устройств.
3. Анализ сетевого трафика: Участникам предоставляются записи сетевого трафика, и их задача - исследовать этот трафик для обнаружения ценной информации, такой как пользовательские учетные данные или коммуникации с использованием протоколов.
4. Скрытая информация в изображениях: Задания могут содержать изображения, в которых спрятаны флаги или другие данные с использованием стеганографических методов. Участникам нужно будет обнаружить и извлечь скрытую информацию.
5. Криптография и дешифрование: Задания могут включать зашифрованные данные или параметры, которые требуют расшифровки с использованием различных методов криптографии.
6. Анализ памяти: В некоторых заданиях участникам может быть предоставлен образ памяти компьютера или устройства, и их задача - анализировать память для поиска важной информации, такой как пароли или ключи.

Успешное выполнение заданий в категории «Форензика» требует умения анализировать и исследовать данные, использовать соответствующие инструменты для анализа цифровых следов и понимать методы обнаружения скрытой информации. Форензика в “CTF” помогает участникам развивать навыки цифрового расследования и повышать понимание методов защиты и обнаружения угроз в информационных системах. Это также позволяет участникам углубиться в аспекты кибербезопасности, связанные с анализом данных и обнаружением цифровых следов.

* 1. Стеганография

Стеганография в “CTF” — это категория заданий, которая фокусируется на обнаружении и извлечении скрытой информации из различных медиа-ресурсов, таких как изображения, аудиофайлы или текстовые документы. В стеганографии информация скрывается таким образом, чтобы она оставалась незамеченной визуально или аудиально.

Задания в категории «Стеганография» могут включать следующие типы:

1. Скрытые флаги в изображениях: Участникам предоставляются изображения, в которых скрыты флаги или другая информация с использованием стеганографических методов. Участники должны обнаружить и извлечь эту информацию, чтобы найти ответ на задание.
2. Аудио стеганография: Задания могут содержать аудиофайлы, в которых спрятаны флаги или другая информация. Участникам предстоит использовать соответствующие методы для обнаружения и извлечения скрытой информации.
3. Текстовая стеганография: В некоторых заданиях участникам могут предоставляться текстовые документы, в которых спрятаны флаги или другие данные с использованием различных методов стеганографии.
4. Обнаружение изменений: Задания могут включать обнаружение изменений в медиа-ресурсах, которые могли быть внесены с целью скрыть информацию.
5. Анализ цветовых каналов: В некоторых изображениях информация может быть скрыта в цветовых каналах (“RGB”) или в других аспектах изображения.

Успешное выполнение заданий в категории "Стеганография" требует умения обнаруживать скрытые данные, использовать различные инструменты и методы стеганографии для извлечения информации из медиа-ресурсов. Стеганография в CTF помогает участникам развивать навыки анализа изображений, аудиофайлов и текстовых данных на предмет скрытой информации. Это также позволяет участникам понять, как можно использовать стеганографию в целях скрытия информации и как обнаруживать такие методы для целей кибербезопасности.

1. Nimda CTF
   1. История

История “Nimda CTF” начинается в 2021 году, когда в “РТУ МИРЭА” студенческим союзом была проведена олимпиада по кибербезопасности на платформе “Discord”. В дальнейшем “Nimda” вырастет в полноценный “CTF” в виде “Jeopardy”, а потом и в виде “Attack-defense”.

* 1. Проведение в 2023 году
     1. Контингент

Как и всегда – “Nimda CTF” проектируется таким образом, чтобы дать шанс на решение заданий всем группам студентов, обучающихся на “IT” специальностях.

Прошлое соревнование (“Nimda CTF LateAutumn 2022”) прошло с рекордным количеством участников – 234. Статистика по предыдущим проведениям (до “Nimda CTF LateAutumn 2022”) “Nimda CTF” не собиралась и из-за этого невозможно дать объективный ответ по приросту числа участников.

* + 1. Планируемые задания

Задания планируются создаваться в следующих категориях:

* Криптография
* Стеганография
* WEB
* Реверс-инжиниринг
* Форензика

А также в других категориях.

Сложность заданий планируется на уровне прошлых заданий “Nimda CTF”, а также для примера сложности можно взять задания из популярного “CTF” – “UgraCTF”. На очный этап планируется заготовить 20-25 заданий. На финальный – 3-5.

* + 1. Планируемые этапы

Планируется два этапа соревнования:

1. “Jeopardy”: удаленный (онлайн) отборочный этап, исходя из результатов которого будут отобраны команды-участники для участия во втором этапе – “Attack-defense”.
2. “Attack-defense”: очный финальный этап, исходя из результатов которого будет определена команда-победитель соревнования.

Второй этап планируется провести в киберзоне «РТУ МИРЭА» по предварительной договоренности со студенческим союзом и непосредственно самой киберзоной.

* + 1. Планируемые даты проведения

Первый этап предполагается провести в середине февраля (10-20 числа) протяженностью в 24 часа. Второй этап предполагается провести в начале марта (1-10 числа) протяженностью в 4-6 часов.

* + 1. Планируемое количество участников в отборочном этапе

В этом году планируется участие не менее 200 человек исходя из положительной динамики роста числа участников с 2021 года.

* + 1. Планируемое количество участников в финальном этапе

Планируется участие 6-8 команд (т.е. ~30-40 человек).

* + 1. Потенциальные партнерства

Ожидается партнерство с «Лабораторией ИТ» вуза «РТУ МИРЭА», а также с членами академической команды «РТУ МИРЭА» в дисциплине “CTF” – “KKS”.

* + 1. Планируемая платформа проведения очного этапа

В данный момент идет разработка собственной “CTF” платформы, которая в потенциале может стать платформой проведения. В качестве других вероятных платформ выступают “Yatb” и “CTFd”.

* + 1. Планируемая платформа проведения финального этапа

Неизвестно.