**Главная страница:**

Capture the Flag или CTF в ИБ — это соревнования в информационной безопасности в форме командной игры, главная цель которой — захватить «флаг» у соперника в приближенных к реальности условиям.

Команды решают прикладные задачи, чтобы получить уникальную комбинацию символов (флаг). Далее участники отправляют флаг в специальную платформу и получают подтверждение, что задача решена верно или стоит попытаться дать ответ еще раз.

На данном сайте вы можете поближе познакомиться с данным видом соревнований и узнать о работе сборной команды CTF Московского Политеха.

В разделе “Информация о сайте” находится информация о составителях сайта

В разделе “О команде” вся работа команды ctf с сентября 2022.

В разделе “Курс молодого бойца” вы можете больше узнать о соревнованиях Capture the Flag.

В разделе “Статьи” подобраны интересные статьи связанные с соревнованиями ctf и информационной безопасностью.

В разделе “WriteUps” собраны подробные решения заданий ctf от участников команды.

**Раздел Информация о сайте:**

Сайт создан участниками проекта “Сборная CTF” Лаборатории внутренней разработки.

Скрыпник Василий - создание и оформление сайта.

Игумнова Карина - координация участников, базовая информация в разделах, “Курс молодого бойца”, статья “Еще больше полезных инструментов”.

Коржов Арсений - статья “Полезные ссылки для CTF”.

Щипунов Тимофей - статьи “Начало начал – сканирование” и “Brute-force-атака с помощью BurpSuite”.

Евсеев Григорий - writeup “Разбор интересных задач CTFLEARN”

Шаталов Вадим - writeups “OSINT InfoSec 2022 T1” и “ugractf стеганография Задача E\*. Разрез”

Кочева Елизавета - статья в раздел Crypto “Что это такое?” и статья в раздел OSINT “Что это такое?”

Огурцова Карина - статья в раздел Crypto “Криптография, криптосистемы, ключи и алгоритмы”

Раимов Хасан - статья раздел “Exploiting / PWN” и статья раздел “FORENSIC”

Иванов Дмитрий - статья “Задачи со случайностями”

Хоанг Тхань Лич - статья “Web в CTF”

Сиплатов Алексей - статья “Сканер уязвимостей на Python”

Женин Михаил - статья “RCE”

**Раздел О команде:**

Цель студенческой CTF команды anakta — привлечение студентов, заинтересованных в получении практических навыков в сфере информационной безопасности, совместное обучение и участие в соревнованиях.

На данный момент наша команда занимает 93 место по стране.

С актуальной информацией о нашем участии можно ознакомиться здесь (ссылка <https://ctftime.org/team/150251>).

В этом семестре нам удалось поучаствовать в 13 соревнованиях

CSAW CTF Qualification Round 2022

Даты: Птн, 09 Сен. 2022, 19:00 MSK — Вск, 11 Сен. 2022, 19:00 MSK

Формат: Jeopardy

SekaiCTF 2022

Даты: Птн, 30 Сен. 2022, 19:00 MSK — Вск, 02 Окт. 2022, 19:00 MSK

Формат: Jeopardy

Capture the Intruder

Даты: 14-16 октября 2022 года

Формат: Jeopardy

Участвовало 10 команд

Кубок CTF

Первый этап (Отборочный) – участвуют все желающие (online), начало 19 ноября в 12:00, окончание 20 ноября в 12:00

Участвовало 2 команды

M\*CTF Quals

Даты: Онлайн с 14.00 29 октября до 14.00 30 октября

Формат: Task-Based

Hack The Boo от Hack The Box

Даты: Сбт, 22 Окт. 2022, 16:00 MSK — Чтв, 27 Окт. 2022, 15:59 MSK

Формат: Jeopardy, одиночное участие

EKOPARTY CTF 2022

Даты: 2 ноября (среда) 20:00 MSK — 4 ноября(пятница) 22:00 MSK

Формат: Jeopardy

N1CTF 2022

Даты: Sat, 05 Nov. 2022, 03:00 MSK — Mon, 07 Nov. 2022, 03:00 MSK

Формат: Jeopardy

p4ctf 2022

Даты: Sat, 05 Nov. 2022, 13:00 MSK — Sun, 06 Nov. 2022, 13:00 MSK

Формат: Jeopardy

ISITDTU CTF 2022 Quals

Даты: 12 ноября суббота 08:00 MSK — 13 ноября воскресенье 08:00 MSK

Формат: Jeopardy

YetiCTF

Даты: 26 по 27 ноября, длительность 24 часа

Формат: task-based

TUCTF 2022

Даты: Птн, 02 Дек. 2022, 20:00 MSK — Вск, 04 Дек. 2022, 20:00 MSK

Формат: Jeopardy

InfoSec CTF 2022

Даты: Сбт, 03 Дек. 2022, 10:00 MSK — Вск, 04 Дек. 2022, 10:00 MSK

Формат: Jeopardy

Топ игроков, внесших большой вклад в соревнования:

Коржов Арсений

Шаталов Вадим

Скрыпник Василий

**Индивидуальная работа участников**

Помимо командной работы, каждый член команды тренировался отдельно на разных сайтах.

Наши участники проходили курсы и решали задания на:

* CTFLearn
* HTB Academy
* ugractf
* hackerdom
* overthewire
* vulnhub
* awesome-ctf

**Раздел Курс молодого бойца:**

**Capture the Flag (CTF)** — это игра, в которой участники пытаются захватить флаг противников и защитить свой. Популярной ее сделали командные шутеры вроде Quake и Team Fortress, но в какой-то момент хакерам пришла идея спроецировать CTF на информационную безопасность.

Хакерский CTF хоть и построен на правилах классического Capture the Flag, однако с годами очень сильно видоизменился. Сейчас CTF в контексте информационной безопасности может означать даже соревнования, которые далеки от обычного захвата флага. Множественные эксперименты с правилами и механикой проведения привели к появлению массы типов и разновидностей CTF. Вот основные из них.

**Attack-Defence**

В классической схеме каждая команда получает выделенный сервер или небольшую сеть для поддержания её функционирования и защиты. Во время игры команды получают очки за корректную работу сервисов своего сервера и за украденную информацию (флаги) с серверов противников. Обычно после окончания соревнований команды-участники публикуют свои решения у себя на сайтах, так что всегда можно ознакомиться с решением интересующей задачи.

**Task-Based CTF**

Это наиболее популярный вид CTF, поскольку он проще других в реализации. Вместо того чтобы ломать друг друга, команды делают определенные задания. За решение заданий дают флаг — сдав его, команда получает очки. Обычно в таком CTF есть несколько веток заданий — каждая по своей дисциплине. Вот несколько самых популярных:

Admin — задачи на администрирование. Чаще всего задания для Линукса

Reverse — исследование программ без исходного кода (реверс-инжиниринг)

PPC — задачи на программирование (professional programming and coding). Нужно обследовать код, найти или написать (нечто вроде спортивного программирования на минималках, сейчас редко встречается).

Crypto — классическая криптография. Задачи на расшифровку некого сообщения, в котором сидит флаг.

Web — задачи на веб-уязвимости, такие как SQL injection, XSS и другие.

Osint – разведка по различным источникам. Чаще всего найти информацию о человеке, месте, времени и т.д.

Stegano - в этой дисциплине участники пытаются вытащить скрытую информацию из какого-нибудь мультимедийного файла, документа, текста или образа чего-либо

Forensic - имитирует различные задания на расследование инцидентов и анализ образов и файлов. Вполне могут попасться задания, связанные с восстановлением удаленных файлов и скрытых разделов.

В ветку Misc попадают любые задания, которые не относятся к другим группам. Это может быть и конкурентная разведка, и какие-нибудь развлекательные задания.

Узнать больше о каждой категории можно здесь:

Механика проведения task-based CTF бывает разная. Например, более сложные задания могут открываться по мере решения более простых. Или бывает так, что команда, решившая задание первой, получает дополнительные баллы. Однако в целом идея остается прежней — кто решил больше заданий, тот набрал больше баллов и тот в итоге побеждает.

**Mixed**

Существуют CTF, которые объединяют черты attack-defence и task-based: командам требуется не только защищать свои сервисы и атаковать чужие, но и решать задания. В этом случае правила проведения могут быть любыми и ограничиваются лишь воображением организаторов. Яркий пример можно было встретить на PHDays 2014. Текста регламента хватило на небольшую книжечку, и разобраться в механике было не так-то просто.

**Немного про сами соревнования**

В мире каждую неделю проводится как минимум один CTF, а то и несколько. Организуют их, как правило, команды, которые сами постоянно участвуют в подобных соревнованиях. Полный список всех CTF с датами проведения можно найти на сайте ctftime.org.

Немало CTF проходит и в России. Большинство из них студенческие, однако есть пара соревнований, которые известны на международном уровне, — RuCTFE и PHDays. RuCTFE — это attack-defence CTF, который проводится командой HackerDom. Он имеет очень высокий рейтинг среди международных CTF, и, как следствие, победа на RuCTFE — пропуск на DEF CON CTF.

Многие задания в CTF будут совершенно случайными и беспрецедентными, и для их решения потребуется просто логика, знания и терпение. Не существует надежного способа подготовиться к ним, но по мере того, как вы будете выполнять больше CTF, вы сможете распознать и получать больше подсказок о том, как их решить.

**Основные термины и сленг CTF и кибербезопасности**

A&D (АД, дефенс) — Attack-Defense CTF. Отличительная особенность — наличие у каждой команды сервера, на котором базируется несколько уязвимых приложений (сервисов).

АСМ — ассемблер, язык программирования низкого уровня.

БД — база данных, место хранения данных. Чаще всего имеется в виду БД с логинами и паролями.

Бейс — base. Чаще всего употребляется в терминах кодирования информации. Например, base64 или base32 (стандарты кодирования данных).

Бекдор — back door, сознательно оставленная лазейка, предоставляющая доступ к данным или контроль над сервисом. Бекдор может быть как программным, так и аппаратным.

Бинарник — файл с бинарным (исполняемым) кодом, он же exeшник.

Брут (он же брутфорс) — brute force, грубая сила. Метод, чья суть — полный перебор всех возможных вариантов ответа. Чаще всего применяется при взломе паролей или сдаче уцуцужных флагов.

В хексах — выражение, означающее представление данных в шестнадцатеричном (hexadecimal) виде. Чаще всего относится к целым к числам, символам, и байтам.

Дамп — dump, файл с информацией об объекте или процессе. Обычно говорят о дампе сетевого трафика,прошивки устройства или базы данных.

Деструктивная атака — как правило используется в контексте A&D. Атака, направленная на разрушение общей инфраструктуры сети, запрещена правилами.

Зип-бомба — так же известна как «архив смерти» или decompression bomb. Файл, который при распаковке начинает распаковку себя же самого. Закидывание таких бомб на сервер является деструктивной атакой. Примером является 42.zip.

Куки — cookie. Данные, идентифицирующие текущего пользователя и/или текущую сессию.

Курить, раскурить — анализировать исходный код или данные.

Курл — cURL, программа для отправки http-запросов.

Лог — log, запись событий. Логи сервера.

Локпикинг — lock picking, взлом замков. Является «дополнительной активностью» на некоторых оффлайн-соревнованиях, а также способом «взлома» физической защиты.

Метаданные — любые данные, которые хранят в себе файлы. Например, геолокация в фотографиях или исполнитель аудиозаписи.

Парсить — parse, обрабатывать / разбирать / анализировать данные (например, вытаскивать из строки числа).

Пейлоад - payload, полезная нагрузка. Строка, эксплуатирующая некоторую уязвимость.

Пинговать — ping. Используется админами для проверки доступности сайта или наличия интернета на машине. Также используется в смысле «донести информацию до кого-то» или «достучаться до кого-то».

Пывнить — pwn, овладевать. Применительно при эксплуатации бинарных уязвимостей.

Райтап (врайтап, writeup) — описание процесса решения таска.

Реквест — request, запрос. Как правило в значении запрос к сервису.

Сервис — как правило в контексте A&D — (уязвимое) приложение, развернутое на сервере. Например, веб-страница.

Сниффить — sniff, «разнюхивать». Перехват и анализ сетевого трафика.

Сорцы — source (исходный). Исходный код приложения или чего-то еще.

Соль — случайная строка, добавляемая к хешируемым данным.

Сплойт — программа, эксплуатируящая уязвимость.

Ссш (эс-эс-аш) — ssh, secure shell. Программа для защищённого удалённого доступа.

Суп — Beautiful Soup, парсер веб страниц. Является модулем питона.

Таски — задания. Применительно к task-based CTF, причем сам task-based CTF также может называться «таски» или «тасковый CTF».

Трафик — применительно к A&D. Данные, которые передаются внутри сети. В основном в значении «данные, которые поступают к нам от других пользователей сети».

Уцуцуга — в простонародье «угадайка». Нестандартная, нетривиальная задача с таким же нетривиальным решением.

Ферма — применительно к A&D. Программа, которая обрабатывает переданные ей флаги, автоматически их сдает и визуализирует полученные очки. Например, DestructiveFarm.

Форк-бомба — fork bomb (вилковая бомба). Скрипт, который бесконечно генерирует свои же копии. Используется как деструктивная атака.

Хардкод — hardcode, жёсткий код. Практика, встречающаяся в разработке ПО, при которой переменные задаются напрямую и заранее, в противовес получению их значений в процессе выполнения. Например, захардкоженные пароли в старых прошивках роутеров.

Хедер — header, заголовок. Чаще всего имеются ввиду http-заголовки.

Хеш — число или строка, результат хеш-функции.

Хост — в контексте виртуальных машин: основная система. В остальных случаях: компьютер, рабочая станция.

Шелл-код — shellcode, набор инструкций, который обеспечивает доступ к командной оболочке системы, т.е. с его помощью можно выполнить любую команду. Библиотеку шелл-кодов можно найти на сайте shell-storm.

**Некоторые инструменты и ресурсы для подготовки к соревнованиям или испытаниям хакеров CTF**

Trail of Bits CTF Guide — один из лучших гайдов для новичков

Practice CTF List / Permanent CTF List - хорошая коллекция и ресурс CTF, которые давно работают.

Awesome CTF — тщательно подобранный список фреймворков, библиотек, ресурсов и программного обеспечения Capture The Flag (CTF).

Vulnhub — уязвимые машины, которые вы можете использовать для практики или для своей лаборатории пентестов

CTF Resources — репозиторий и архив общих тем для CTF и что-то вроде того же, что и Trail of Bits CTF Guide.

SecurityCTF на Reddit — /r/securityCTF

Forensics Wiki - вики, предназначенная для компьютерной криминалистики.

**Раздел Статьи:**

Информационная безопасность требует постоянного обучения. Важной частью каждого соревнования ctf является изучение и исследование новых методов или необычных ситуаций.

В ctf командах участники часто обмениваются новой информацией и учатся вместе в процессе.

**Раздел WriteUps:**

WriteUp (врайтап, райтап) - это подробные описания процесса решения и получение флага. В некоторых ctf райтапы являются обязательной частью соревнования. Райтапы пишут сами команды (в более редких случаях организаторы соревнований), поэтому методы решения могут быть разными.

Райтапы по решенным заданиям публикуются после окончания соревнования. Их можно найти на ctftime на страницах самих соревнований и в общем разделе Writeups. Также участники публикуют райтапы на своих сайтах.

При решении задания тоже рекомендуется писать для себя райтап или просто помечать, что делаешь, чтобы лучше понимать действия и при удачном решении можно было легко вспомнить, что делал, чтобы написать свой райтап.

Многие задания в CTF похожи и может получится найти решение задания просто прогуглив его. Никто не запрещает пользоваться Интернетом как угодно. Единственное правило, нельзя выпрашивать/воровать флаги у других команд.

Участники нашей команды также составили некоторые райтапы на задания из соренований, в которых мы успели поучаствовать: