Платформа CTF

Соревнование проводится на **CTFd** — open-source платформе для Jeopardy-CTF. Она развёрнута локально и доступна по предоставленной ссылке/IP.

Функционал:

- Регистрация/вход участников.
- Отображение категорий и заданий с указанием сложности и баллов.
- Описания заданий, прикреплённые файлы для скачивания.
- Поле для ввода флага (CTF{...}) и мгновенная проверка.
- Динамическая система баллов (уменьшаются с каждым новым солвом).
- Таблица лидеров (scoreboard) в реальном времени.
- Таймер соревнования (если установлен).

Описание категорий заданий

В нашем CTF-соревновании задания разделены на 8 категорий, охватывающих основные направления информационной безопасности. Всего около 43 заданий разной сложности (от easy до hard), с динамическими баллами.

OSINT (Open Source Intelligence) — 10 заданий Категория посвящена сбору и анализу информации из открытых источников. Участники ищут флаги с помощью поисковых систем, соцсетей, метаданных файлов, Google Dorking, анализа утечек данных и корреляции информации о людях или организациях.

Форензика (Forensics) — 4 задания Анализ цифровых следов и артефактов: работа с PCAP-файлами (Wireshark), дампами памяти (Volatility), образами дисков, восстановление удалённых файлов и file carving (binwalk).

MISC (Miscellaneous) — 3 задания Разнородные задачи, не вписывающиеся в другие категории: головоломки, простые скрипты, кодировки, базовая стеганография и креативные挑战, требующие нестандартного мышления.

Криптография (Crypto) — 8 заданий Взлом шифров, хэшей и криптографических протоколов: классические шифры (Цезарь, Виженер), RSA/AES/ECC, крэкинг хэшей (Hashcat), криптоанализ с помощью CyberChef и SageMath.

Стеганография (Stego) — 9 заданий Извлечение скрытой информации из медиафайлов: LSB в изображениях, спектрограммы аудио, работа с инструментами steghide, binwalk, Stegsolve и outguess.

Reverse (Reverse Engineering) — 5 заданий Реверс-инжиниринг бинарных файлов: статический и динамический анализ в Ghidra, IDA Pro или Radare2, поиск флагов в crackme, обход обфускации и анти-отладки.

Web — 2 задания Эксплуатация уязвимостей веб-приложений (OWASP Top 10): SQL-инъекции, XSS, CSRF, SSRF, IDOR и другие, с использованием Burp Suite или ZAP.

Linux — 2 задания Глубокое знание командной строки Linux в сильно ограниченной среде (без установки ПО, пайпов, скриптов и интернета). Задачи на поиск альтернативных способов с использованием coreutils и встроенных shell-возможностей.

В CTF-соревновании приняли участие 10 студентов 3-го курса группы ИБ-1-23. На решение заданий было отведено 3 часа.

Результаты CTF-соревнования

Таблица лидеров (Player Progression, Top 10)

По итогам 3-часов, и дополнительного времени, места распределились следующим образом:

Player Progression (Top 100)

Rank	User	Score	Официальная докум... 50pt	Сбор QR 100pt	Тыквенная сеть 100pt	Скобки 100pt	Хакерская конферен... 100pt	Улица 100pt
1	Ayan	3150	✓	✓	-	-	✓	-
2	Мырза	2500	-	-	✓	✓	✓	✓
3	Nurlis	2200	✓	✓	-	✓	✓	✓
4	argen	2150	✓	-	✓	-	✓	✓
5	Yrysbek	2050	✓	✓	-	-	✓	✓
6	Kasym	1950	✓	✓	-	✓	✓	✓
7	Kalys	1930	✓	✓	-	-	✓	-
8	Azhar	1900	-	✓	✓	-	-	-
9	omurbek	1700	✓	-	-	-	✓	-
10	Emir_Alypsatarov	850	-	-	-	-	-	-

Итоговые результаты CTF (реальные, по основному времени)

Важное уточнение: Эта таблица отражает **реальные результаты** по итогам основного 3-часового лимита соревнования (без учёта продлённого времени). Предыдущие данные (Player Progression и диаграммы) включали солвы после дедлайна, когда некоторые участники продолжили работу. Здесь показан честный срез на момент окончания — топ-4 участников, все с видимыми результатами (Visibility: visible).

- Победители: **1-е место: Ayan** (2800 баллов)
- **2-е место: Мырза** (2300 баллов)
- **3-е места: Azhar, Nurlis** (по 1700 баллов)

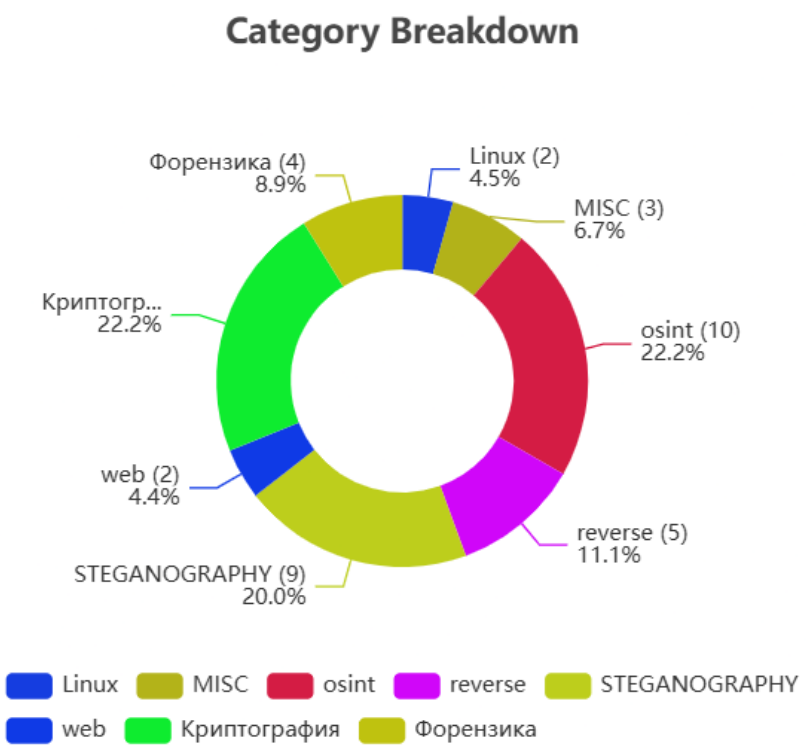
Place	Пользователь	Bracket	Score	Visibility
1	Ayan		2800	visible
2	Мырза		2300	visible
3	Azhar		1700	visible
4	Nurlis		1700	visible

Распределение решённых заданий по категориям (Category Breakdown)

Круговая диаграмма показывает, сколько заданий из каждой категории было решено хотя бы одним участником (в процентах от общего числа заданий):

- **osint** (10 заданий) — 22.2%
- **STEGANOGRAPHY** (9) — 20.0%
- **Криптография** (8) — 22.2%
- **reverse** (5) — 11.1%
- **Форензика** (4) — 8.9%
- **MISC** (3) — 6.7%
- **web** (2) — 4.4%
- **Linux** (2) — 4.5%

Самыми популярными категориями стали OSINT, Стеганография и Криптография — на них пришлось более 64% всех солвов.



Распределение набранных баллов по категориям (Point Breakdown)

Эта диаграмма отражает, сколько баллов в сумме участники набрали за каждую категорию (в процентах от общей суммы баллов):

- **osint** — 1750 баллов (23.6%)
- **Криптография** — 18.2%
- **STEGANOGRAPHY** — 1250 баллов (16.9%)

- **reverse** — 900 баллов (12.2%)
- **Форензика** — 650 баллов (8.8%)
- **web** — 550 баллов (7.4%)
- **Linux** — 650 баллов (8.8%)
- **MISC** — 300 баллов (4.1%)

OSINT принёс наибольшее количество баллов благодаря большому числу заданий и высокому проценту солвов. Самыми «дорогими» по баллам оказались Linux и Web — несмотря на малое количество заданий, они дали значительный вклад в общий счёт топ-игроков.