# **Введение в CTF**

На этом занятии подробно раскрывается термин CTF и рассматриваются виды соревнований и распространённых заданий.

## **Что такое CTF**

CTF (Capture The Flag) — это соревнования в области информационной безопасности, где участники стремятся найти и захватить флаги — секретные коды или файлы. В соревнованиях предлагаются различные задания, проверяющие знания и навыки в различных категориях. CTF помогает участникам развивать свои навыки и обмениваться опытом, одновременно стимулируя демонстрацию интеллекта и креативности при решении сложных задач.



## **Цели и задачи CTF-соревнований**

Цели CTF-соревнований — развитие и проверка навыков участников в области информационной безопасности. Ключевые категории заданий: криптография, веб-эксплуатация, реверс-инжиниринг и другие.

Участники развивают умения анализа систем, выявления уязвимостей и их эксплуатации. CTF-соревнования дают практический опыт в информационной безопасности, способствуют обмену знаниями между участниками и профессионалами. Мероприятия помогают повысить квалификацию и подготовить к решению реальных задач.

## **Основные виды CTF-соревнований**

Соревнования выделяются двумя популярными форматами: **Jeopardy** и **Attack-Defense**.



### **Jeopardy**

Jeopardy (или Task Based) — один из самых популярных форматов, где участники решают разнообразные задачи в нескольких категориях: криптография, веб-эксплуатация, реверс-инжиниринг, стеганография и другие. За каждую решённую задачу команда получает очки, которые зависят от сложности задания.



### **Attack-Defense**

В формате Attack-Defense команды делятся на атакующих (red team) и защищающихся (blue team). Атакующие ищут и эксплуатируют уязвимости в системах соперников, а защищающиеся пытаются их устранить. Очки даются за успешные атаки и снимаются за уязвимости, найденные соперниками.

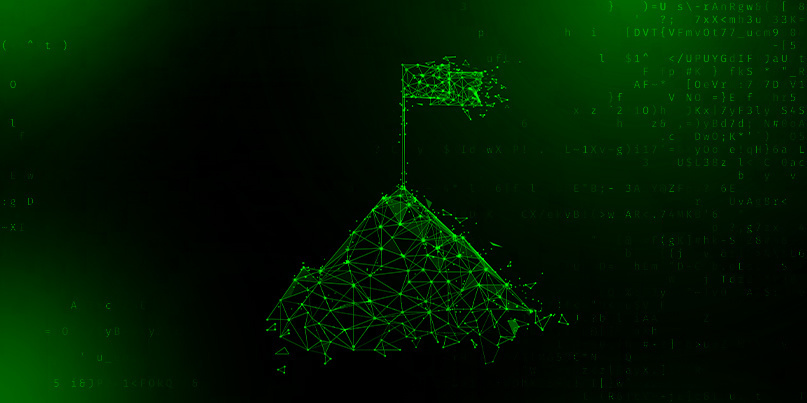


## **Категории заданий в CTF**

* **Криптография** — шифрование, дешифрование и анализ криптографических систем.
* **Веб-эксплуатация** — уязвимости веб-приложений (SQL-инъекции, XSS и др.).
* **Реверс-инжиниринг** — анализ кода и его обратное проектирование.
* **Форензика** — анализ цифровых следов, восстановление данных.
* **Стеганография** — скрытие информации в изображениях, аудио или видеофайлах.
* **OSINT** — сбор информации из открытых источников.
* **PWN** — эксплуатация уязвимостей программного обеспечения.
* **Развлечения** — головоломки и неординарные задания.
* **Квесты/Машины** — задания с повышением привилегий.
* **Active Directory** — задания, связанные с корпоративными сетями и контролем доменов.

## **Виды и типы флагов**

Флаги в CTF могут быть разных типов и форматов. Обычно формат флага представляет собой **название\_ивента{флаг}**, например: CODEBY{th1s\_1s\_a\_f4k3\_fl4g}.



## **Глоссарий**

### **Jeopardy**

* **Таск** — задание, за решение которого дается флаг.
* **Флаг** — уникальный код для подтверждения успешного выполнения задания.
* **Хинт** — подсказка для помощи в решении задания.
* **Скорборд** — таблица с результатами команд.

### **Attack-Defense**

* **Vulnbox** — сервер с уязвимыми сервисами.
* **Сервис** — уязвимое приложение на Vulnbox.
* **FP (Flag Points)** — очки за захват флага.
* **Эксплойт** — программа для автоматизации атак.

## **CTF-инструментарий**

Важные инструменты для участников CTF:

### **Active Directory**

* impacket-GetNPUsers, enum4linux-ng, evil-winrm, ldapsearch, crackmapexec, kerbrute, smbclient, bloodhound, adalanche.

### **Квесты**

* linpeas, linux-exploit-suggester, pspy, GTFOBins.

### **Веб**

* Burp Suite, OWASP ZAP, sqlmap, Nikto, DirBuster, Wfuzz, Nmap, Acunetix, Nuclei, Chrome DevTools, XSSer.

### **Стеганография**

* Exiftool, Steghide, Outguess, Stegsolve.

### **Форензика**

* Audacity, Bkhive, Samdump2, Foremost, NetworkMiner, Volatility.

### **Криптография**

* John the Ripper, Hashcat, XORTool, RSATool, FeatherDuster.

### **Реверс-инжиниринг**

* IDA Pro, dnSpy, Frida, Ghidra, OllyDbg, x64dbg.

### **PWN**

* GDB, Radare2, pwntools, AFL, Angr, QEMU.

Этот список поможет участникам сделать первые шаги в CTF-соревнованиях, хотя инструменты не заменяют знаний и опыта.

## **Домашнее задание**

1. Зарегистрироваться на [GitHub](https://github.com/) и изучить его основные функции.
2. Начать отслеживать репозиторий: <https://github.com/Nikevich/ctf_miet>.