CTF

Практика

Teach
Me
Skills

Собираемся и отмечаемся

Teach
Me
Skills

Вопросы по предыдущим темам или ДЗ

Teach Me Skills

Mini-quize по прошлым темам:

1. **Что мы можем получить при перехвате информации, передаваемой по радио каналу?**
2. **Можем ли мы произвести атаку класса MITM на физическом уровне?**
3. **По какой причине автоматизированные сканеры работают так долго?**

Teach Me Skills

Mini-quize по новой теме:

1. **Что такое CTF? О каких CTF соревнованиях || ресурсах вы знаете?**
2. **Какие основные направления в CTF?**
3. **Что такое стеганография и как она применяется в ИБ?**
4. **Как вы думаете бывает ли физический CTF?**
5. **Что необходимо для решения CTF?**
6. **Нужно ли сотрудникам ИБ решать crackme и CTF? И для чего?**

Teach
Me
Skills

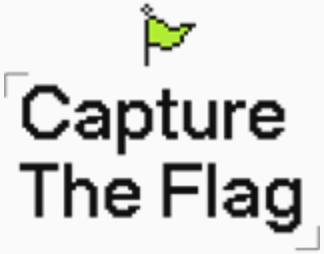
План занятия

1. Изучим основные направления CTF.
2. Рассмотрим различные площадки, обсудим какие стоит посещать.
3. Попробуем себя в роли «хакеров» на платформах CTF.
4. Попробуем различные направления в CTF.

Что такое Capture The Flag?

Teach Me Skills

Захват флага, **CTF** — это упражнение или соревнование, в котором производится поиск флагов, по различным направлениям. Флаги представляют собой определенную строку, данные или файл, который располагается в специально созданной инфраструктуре или же файле-ах. CTF может быть соревнованием или иметь образовательные цели.



Впервые CTF был проведен в 1993 году на **DEFCON**

Что нужно для CTF?

1. Умение гуглить
2. Упорство
3. Желание и свободное время
4. Компания единомышленников (Желательно)
5. Умение писать на каком-либо языке программирования (Python, Ruby)

Виды и типы CTF

Teach Me Skills

CTF можно подразделить по некоторым признакам:

1) Основные применяемые навыки
2) Тип доступа
3) Итоговая цель
4) Командный/личный

Виды и типы CTF

Teach Me Skills

Выделяют два основных формата проведения: task-based и attack-defense.

Task-based (Jeopardy)

- Задача – решить как можно больше заданий из различных категорий.
- Флаг – строка, полученная при решении задания.
- Баллы за каждый сданный флаг.
- Командный/индивидуальный зачёт.

Attack-Defense (Classic)

- Вам предоставляется образ с уязвимыми сервисами (сайтами, FTP и тп)
- Задачи:
  - Развернуть сервер;
  - Закрыть уязвимости сервисов;
  - Атаковать уязвимости сервисов у других команд.
- Флаг – строка, полученная в ходе успешной атаки противника.
- Баллы за атаку (сданный флаг) и за защиту (работоспособность сервисов).
- Командный зачёт.

Виды и типы CTF

Teach Me Skills

task-based ctf (*jeopardy*) — игрокам предоставляется набор заданий (*тасков*), к которым требуется найти ответ. Ответом является флаг — набор символов или произвольная фраза. Каждое задание оценивается различным количеством очков, в зависимости от сложности. Обычно выделяются следующие категории:

- **admin** - задачи на администрирование.
- **joy** - различные развлекательные задачи вроде коллективной фотографии или мини-игры.
- **ctb** - задачи на аудит удалённых машин (*crack the box*).
- **reverse** - исследование программ без исходного кода (*реверс-инжиниринг*).
- **stegano** - стеганография.
- **ppc** - задачи на программирование (*professional programming and coding*).
- **crypto** - криптография.
- **web** - задачи на веб-уязвимости, такие как SQL injection, XSS и другие.
- **forensics** - одна из сложных категорий заданий, сравнимая с *PWN*.

Teach Me Skills

Описание категорий и способы решения

admin

- Обычно задания, связанные с работой `сисадмина`: восстановление данных, виртуальные машины и т.д. Скорее всего, вам нужно будет просто погуглить, как делается та или инная вещь.

Joy

- Обычно какая-то `игра`, в которой нужно найти флаг. Например, пройти карту в какой-нибудь *Half-Life*.

Reverse

- Достаточно сложная категория. Обычно приходится дизассемблерировать, затем редактровать код на ассемблере.
- Но бывают и более простые задания. Сперва следует обратить внимание на `формат файла`, что он из себя представляет. Затем открыть бинарник в текстовом редакторе и пробежать по нему глазами в поисках чего-то интересного.

Stegano

- **Стеганография** - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.
- Чаще всего вам дается изображения в котором скрыт флаг. В самом простом случае он находится на картинке, но его не видно. Тут можно либо пробежаться по каналам, либо сделать `XOR` с оригинальным изображением, если оно есть. Программа для этого указана ниже .
- В более сложных случаях в изображении зашит не просто флаг, а какая-то другая информация, которую нужно дальше преобразовать в него.
- Так же есть стега с аудио-файлами, такие задания достаточно сложные.

PPC

- Это категория должна вам понравиться! Ничего искать не надо, просто напишите `программу` для автоматизации ваших действий.
- Обычно эти таски решаются на `python`, так как это самый удобный язык для прототипирования.
- Если вам необходимо делать `POST` и `GET` запросы используйте встроенную библиотеку `requests` в `python`. Если вам нужно куда-то подключаться используйте `сокеты`.

Виды и типы CTF

Teach Me Skills

Crypto

- Ознакомьтесь с базовыми `алгоритмами шифрования` тут. Поймите, какой подходит вам. Это пригодится!
- Так же бывают таски с `языками`. Погуглите этот язык и перевидите программу на нормальный для дальнейшего решения.
- Если вам дан код программы и выходные данные, просто разберитесь в коде и напишите декодер.

Web

- Внимательно осмотрите весь `html код`.
- Обратите внимание, какие *cookie* передаются.
- Посмотрите, что происходит при работе с сайтом: что отправляется и что принимается. Используйте встроенный в браузер `отладчик`.
- Проверьте сайт на наличие известных папок. Например, `/phpmyadmin` или `/admin`.
- Проверьте сайт на наличие `sql-injection`.
- Если вам необходимо отправить `POST` запрос с вашими параметрами или *cookies*, будет удобно использовать библиотеку `requests` в `python`.

Forensics

- Каких-либо универсальных методов решения тасков категории `forensic` нет. Никогда не знаешь, что тебе за инцидент попадется и как с ним справляться.
  - Чаще всего таски решаются использованием `binwalk`.
    - Получить подробную информацию о содержании файла и распаковать все, что внутри: `binwalk -e file`.

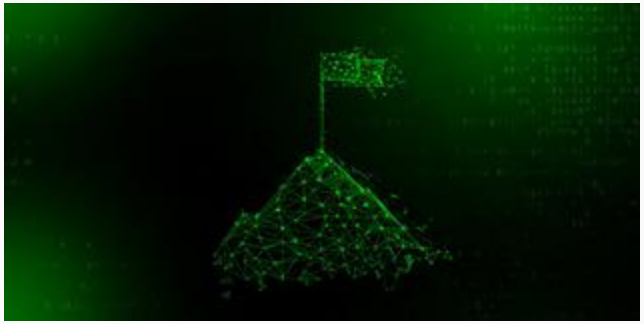
На каких площадках себя проверить

- CTF-соревнования проходят каждую неделю, а то и чаще. Расписание турниров удобно отслеживать на сайте CTFtime. Здесь же можно зарегистрироваться.
- Самое авторитетное соревнование — DEF CON CTF. Первый турнир серии был проведен на хакерской конференции без малого 30 лет назад и дал начало всем CTF. Чтобы попасть на DEF CON, нужно выстоять в жестком онлайн-этапе или выиграть одно из престижных международных соревнований — сейчас в мире 6 таких отборочных турниров.
- С 2019-го официальным отборочным турниром DEF CON CTF стал CTFZone, который в этом году прошел в конце апреля онлайн. Среди участников были команды из России, Китая, Италии, США, Польши, Японии. Обладатели первых трех мест получили денежные призы, а победитель, которым стала команда mslc из России,— еще и место в финале DEF CON CTF.
- Еще два крутых российских соревнования — RuCTF и Volga CTF. Они собирают команды со всего мира, но с одним условием: в отборочном турнире могут принять участие все, а в финале — только студенты и вчерашние выпускники.

Зачем нам CTF как ИБ специалисту?

Teach Me Skills

Участие в соревнованиях **Capture The Flag (CTF)** важно для специалистов по информационной безопасности, так как это предоставляет ряд преимуществ и развивает ключевые навыки.



Практический опыт решения разнообразных задач, таких как криптография, веб-безопасность и реверс-инжиниринг, помогает в быстром анализе и решении проблем.

Работа в команде на CTF способствует развитию навыков сотрудничества, а программирование и использование различных инструментов расширяют технические компетенции. CTF также обучает креативному мышлению и предоставляет возможность следить за актуальными трендами в кибербезопасности.

Успешное участие в CTF может повысить репутацию в сообществе и обновить знания специалиста, а также помочь в развитии навыков реагирования на инциденты безопасности.

Где мы можем потренироваться?

Teach Me Skills

Существует множество онлайн и офлайн площадок и событий, где можно участвовать в Capture The Flag (CTF) и развивать навыки в области информационной безопасности.
Некоторые из них:

Hack The Box (HTB): Онлайн-платформа с разнообразными задачами и машинами для взлома.
hackthebox.eu

OverTheWire: Платформа с вариантами CTF-задач, охватывающих различные области.
overthewire.org

picoCTF: Ежегодное онлайн-соревнование для начинающих и опытных участников.
picoctf.com

Google Capture The Flag (GCTF): Соревнование, организованное Google.
capturetheflag.withgoogle.com

DEFCON CTF: Один из самых престижных турниров CTF, проводимый на конференции DEFCON.
www.defcon.org

RuCTF (Russian Capture The Flag): Международное соревнование, организованное российскими командами.
ructf.org

HITB CTF: Capture The Flag, организованный на конференциях Hack In The Box (HITB).
conference.hitb.org

CodebyGames: Новая платформа для тренировки в направлении CTF, от ресурса Codeby.
codeby.games

Различные киберучения и киберполигоны.

Практика CTF

Codeby Games – это площадка для специалистов в сфере информационной безопасности и программистов, которая содержит задания по кибербезопасности на захват флага **(CTF).**

КОДЕБАЙ ИГРЫ

Возможные направления на платформе

Почему именно это платформа?
Идеально подходит для первоначального старта в CTF, имеет не малое количество направлений, новая платформа, в которой активно прибавляются задания.

codeby.games

Практическое решение CTF

Teach
Me
Skills

Спасибо за внимание!