https://habr.com/ru/articles/519762/

https://ctfnews.ru/what-is-ctf/

https://proglib.io/p/capture-the-flag

https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/344675.php

https://rb.ru/opinion/ctf/

Соревнования CTF (Capture the Flag) – это соревнования в области информационной безопасности, где команды участников соревнуются между собой в решении задач по ИБ.

На CTF-соревнованиях участникам предлагаются различные задачи, которые проверяют их знания и навыки в области информационной безопасности, такие как нахождение уязвимостей в программном обеспечении, криптографический анализ, эксплуатация уязвимостей итд.

Соревнования CTF помогают участникам развивать свои навыки в области информационной безопасности, а также научиться работать в команде.

Категории заданий.

1. Reverse Engineering:

Одна из самых сложных категорий, начинать с неё точно не рекомендую. В тасках на реверс вам будут давать бинарники (исполняемые файлы под винду или линукс – EXE и ELF, но иногда и что-то другое) различных форматов. Вашей задачей будет дизассемблировать этот файл, получить ассемблерный или Си-подобный код и проанализировать его, понять логику программы и написать алгоритм, который добудет вам флаг. Это в простом случае, в сложном же между открытием файла в дизассемблере и получении флага может пройти 10 часов.

Пример простого задания – дизассемблировав файл вы понимаете, что флаг собирается из кодов символов, которые изначально стоят в неправильном порядке. Вам нужно переписать символы в нужном порядке и сдать флаг.

Навыки – дизассемблирование, бинарный патчинг, чтение ассемблерных инструкций, знания особенностей различных архитектур.

2. Cryptography:

Крипта также является довольно сложной категорией, если углубляться в неё и решать сложные таски. Суть тасков вытекает из названия категории – нужно будет анализировать различные криптографические алгоритмы, такие как RSA, AES, различные вариации шифров перестановки и замены, проводить криптоанализ текста и разбираться с свойствами больших чисел, то бишь здесь вам пригодится математика. Эту категорию не стоит боятся, часть тасков здесь вполне себе решаемая. Почти на каждом ивенте встречаются задания на RSA, XOR, one time pad и на различные кодировки по типу Base64. Советуем изучить эти темы в первую очередь, они станут отправной точкой.

Пример простого задания – дана строка «VXYsIHNldnJhcQ==». Находим декодер из Base64, получаем нечитаемый текст, применяем шифр Цезаря со сдвигом на 13 символом и получаем ответ.

Навыки – основные алгоритмы шифрования, операции с большими числами, модулярная арифметика, теория чисел, написание дешифраторов на любом языке программирования

3. Web:

Одна из наиболее разнообразных категорий. Как можно было догадаться из названия, здесь вам придётся работать с сайтами, искать на них забытые файлы, анализировать логику работы приложения, искать в ней уязвимости, а также изучать, как происходит взаимодействие с сервером, понимать что и каким образом передаётся от клиента. Для начала стоит изучить базовый веб-стек хотя бы на уровне чтения кода – JS, PHP, HTML, далее идем в Инструменты разработчика в вашем браузере и учимся пользоваться ими. Изучаем какие стандартные файлы есть на сайтах, что такое HTTP-заголовки и методы, а дальше начинаем изучать веб-уязвимости, такие как SQL инъекции, XSS, SSRF, SSTI, LFI, RCE и куча других аббревиатур, за которым скрываются довольно простые действия. Например, типичный таск на веб это обход проверки пароля в форме авторизации с помощью SQL инъекции. Пароли хранятся в базе данных, когда поступает запрос на авторизацию, сайт сравнивает пару логин\пароль с тем, что у него есть в БД и отдаёт ответ. Если пользовательский ввод не обрабатывается, то мы можем изменить логику проверки и получить доступ к аккаунту пользователя, не зная его пароль.

Навыки – понимание веб-стека (как работают сайты, заголовки, флаги), OWASP Top 10

4. Forensic:

В данной категории вы будете учиться работать с файлами различных форматов, поэтому первым делом отправляемся в гугл и смотрим, что такое Magic Bytes и как по ним определять, что за файл перед нами. Данная категория включает в себя несколько основных задач: определение формата файла, работа с образами дисков и дампами оперативной памяти, анализ сетевого траффика, атаки на подбор пароля к архивам, конвертация из одного формата в другой. Обхватить всё это сразу довольно сложно, поэтому советуем двигаться последовательно, от одного направления к другому. Простейший таск, с которым вы можете столкнуться – дан дамп сетевого траффика в формате pcapng. Такие файлы открываются через утилиту для перехвата и анализа траффика Wireshark. Открываем файл через него и анализируем его содержимое. В самом простом варианте флаг будет записан либо в заголовке одного из пакетов, либо будет передана картинка, которую можно эскпортировать и прочитать флаг с неё.

5. Steganography:

Одна из лучших категорий для начинающих. В основном здесь представлены лёгкие задачки, суть которых сводится к одному – у нас есть обычный файл, в котором сокрыта информация невидимая невооружённым взглядом. Это может быть добавление информации в конец картинки, наложение одной картинки на другой методом LSB, кодирование в аудио файл сигналов азбуки морзе, которые не слышно при простом включении записи и много чего ещё. Советуем начать именно с этой категории, побольше гуглите, ищите инструменты и онлайн сервисы, подходящие к вашей ситуации.

Навыки – понимание устройства различных файлов

6. PWN:

Эта категория требует участников для проведения эксплуатации уязвимостей в программах. Участники должны будут искать и использовать уязвимости в имеющихся программах. Обычно выдаётся бинарный файл, что отсылает нас к реверсу, но в данной категории нам нужно проэксплуатировать уязвимость не в выданном нам бинарном файле, а на удалённом сервисе.

Навыки – работа с бинарными файлами, определение и эксплуатация уязвимостей, таких как – Buffer overflow, format string attack, ROP-цепочки

7. OSINT:

Тоже довольно простая и интересная категория, которая не требует обширных знаний чтобы начать решать её. По сути осинт это новое звучное определение для термина «гуглить». Суть тасков сводится к тому, что по описанию в задании нужно найти в интернете определённую информацию. Вам может быть дано фото памятника, найдя на гугл-картах который, в отзывах вы найдёте флаг, или же по никнейму пользователя в одной соцсети, нужно найти его аккаунт в другой и забрать флаг оттуда. Звучит довольно просто и интересно, но будьте готовы к тому, что организаторы захотят поиздеваться над вами и сделают таск с довольно неочевидным решением.

Навыки – научитесь гуглить, находить разную информацию.

В отрыве от соревнований, который обычно проводятся по выходным, можете тренироваться решать таски на данных платформах:

1. CodebyGames- платформа с тасками, которая идеально подойдёт для начала. Таски разной сложности, от элементарных до прям сложных.
2. Forkbomb – платформа от SpbCTF с тасками и разборами на них. Довольно старый ресурс, с которого многие начинали свой путь в ctf. На их youtube канале много полезных видео.
3. CTF Club – преемники SpbCTF. Проводят оффлайн сходки, которые рекомендуем посетить. Также есть платформа с тасками
4. CTF Learn – зарубежная платформа с тасками.
5. FreeHackQuest – платформа с заданиями с разных CTF
6. picoCTF – платформа с архивами заданий с прошедших ивентов.

(список, разумеется неполный, существует ещё много ресурсов для подготовки, мы выделили те, которые используем сами)

Где искать инфу, теорию:

Итак, вот прошёл ивент, вы что-то порешали, много осталось страшным и непонятным, что же делать?

1. После каждой CTF обязательно смотрите разборы заданий. Обычно организаторы выкладывают их к себе на гитхаб, но если они ленивцы, то ждите разборы от участников на ctftime или иных ресурсах. Пытайтесь повторить действия из разбора, добавляйте в закладки онлайн-инструменты, устанавливайте приложения, которые были рассмотрены в разборе.
2. Во время самих ctf гуглите столько, сколько сможете. Зачастую организаторы «вдохновляются» другими ивентами и делают похожие

задания, так что можно найти почти готовый эксплойт, немного изменить/дописать его и решить тасочку.

3. Различные шпаргалки, репозитории с готовыми пэйлоадами, методиками, такие как:
    a. https://github.com/payloadbox/command-injection-payload-list
    b. https://book.hacktricks.xyz
    c. https://github.com/payloadbox
    d. https://github.com/swisskyrepo/PayloadsAllTheThings
    e. https://dvd848.github.io/CTFs/CheatSheet.html
    f. https://github.com/Rajchowdhury420/CTF-CheatSheet
4. Помимо непосредственной подготовки к решению тасков, рекомендуем проходить комнаты на TryHackMe и HackTheBox. Там вы получите более фундаментальные знания, которые помогут лучше ориентироваться в тасках, понимать что же хотят от вас организаторы и как это делается.

Где участвовать?

https://ctftime.org/event/list/upcoming - на данном сайте регистрируете свою команду, выбираете понравившийся ивент, переходите на сайт конкретной ctf и регистрируетесь там, поставив на CTFtime галочку, что вы участвуете. Решаете на сайте ctf задания, после окончания ивента приходят очки, которые идут в глобальный зачёт.

Самое главное – не бойтесь неудач. Первые несколько ивентов скорее всего покажутся сложными, непонятными, но чем больше практики у вас будет, тем проще будет решать таски. Мы сами, когда только начали участвовать в ctf, по сути не знали ничего. Постепенно, участвуя в различных ивентах, мы узнавали для себя много нового, учились пользоваться различными инструментами, поднимали теоретическую базу. Надеюсь, хоть кто-то дочитает до этого момента)

В общем, пробуйте, не бойтесь неудач и всё получится.

По всем вопросам можете писать в тг - @L0ki_2