Capture-the-Flag

Формат и виды задач

Гришаев Григорий

26 Марта 2024

LibreOffice

Что это такое?

CTF (Capture-the-Flag) — это соревнования 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 ещё раз.

Типы задач Jeopady

Web

Задачи на веб-уязвимости, такие как SQL injection, XSS и другие.

Reverse

Исследование программ без исходного кода (реверс-инжиниринг).

PWN

Эксплуатация уязвимостей в скомпилированных приложениях.

Crypto

Задачи на эксплуатацию алгоритмов шифрования и/или их реализаций.

Stegano

Задачи на обнаружение информации – не являющейся зашифрованной, но скрытой тем или иным способом.

Forensic

Расследование инцидентов.

OSINT

Поиск информации в открытых источниках.

Формат проведения соревнований

Attack-Defense

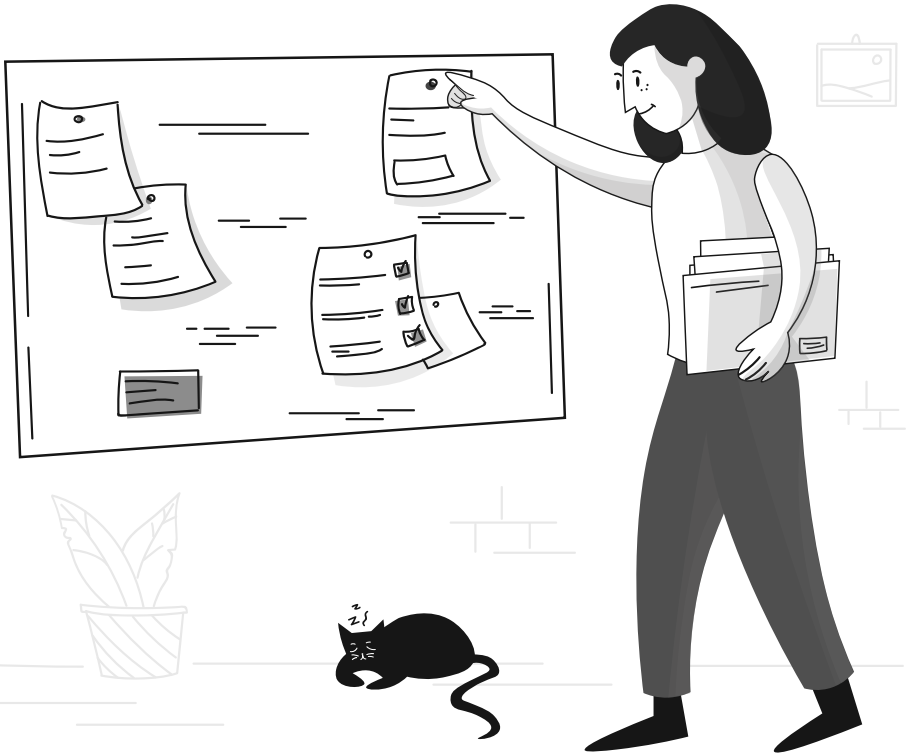
- Команды получают идентичные серверы с набором уязвимых сервисов, на которые жюри периодически посылает приватную информацию — флаги.
- Задача каждой команды заключается в том, чтобы найти и устранить уязвимости на своем сервере и воспользоваться найденными уязвимостями для получения флагов у соперников

Task-Based (Jeopardy)

- Игрокам предоставляется набор заданий (тасков), к которым требуется найти и отправить ответ.
- Чем сложнее таск, тем больше очков даётся за правильный ответ.

Формат занятий

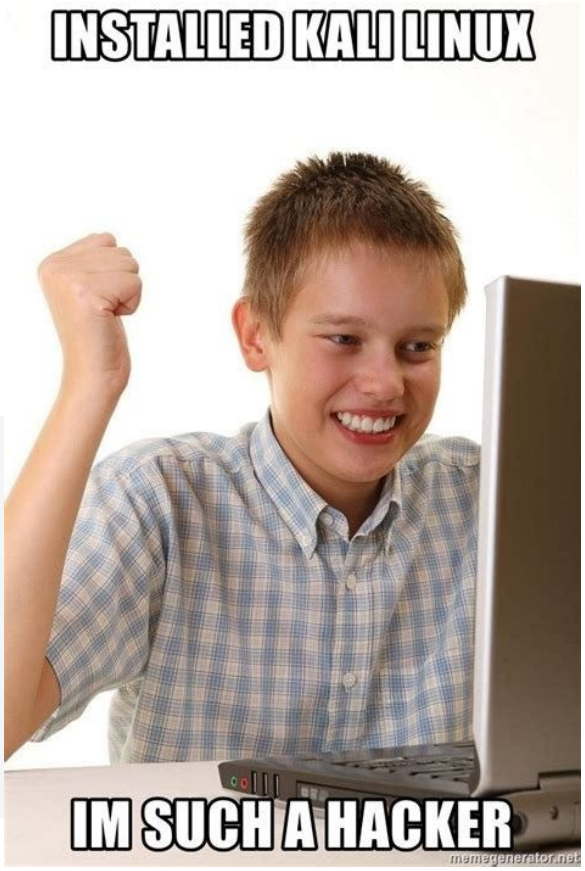
- Собираемся раз в неделю (вероятно, позже – раз в две);
- К каждому занятию 2-3 человека разбирают заинтересовавшую их задачку (например, с ресурсов, представленных в конце презентации) или готовит рассказ по какой-то теме;
- Темы (например, Docker или как пропатчить KDE2 под FreeBSD), о которых хочется побольше узнать можно писать в группу (и создадим онлайн документ для систематизации);
- На занятии докладчик рассказывает разобранную задачу, обсуждаем всё, что непонятно;
- Назначение подготовки – циклически по списку фамилий.



Подготовка доклада

- Рассказ в свободной форме (на доске или с использованием презентации);
- Желательно, чтоб была презентация/pdf-ка, которую можно будет потом залить в облако, чтоб любой желающий мог ознакомиться и в общих чертах понять произошедшее;
- Если в задачке упоминаются нетривиальные теоретические вещи, то следует дать хотя бы минимальное количество вводной информации о явлении/технологии.

Что следует иметь при себе



- Да, зачастую нужен будет Kali Linux;
- Kali Linux можно поставить в виде виртуальной машины (например, в VirtualBox), для многих систем виртуализации на официальном сайте Kali есть ссылка на скачивание.

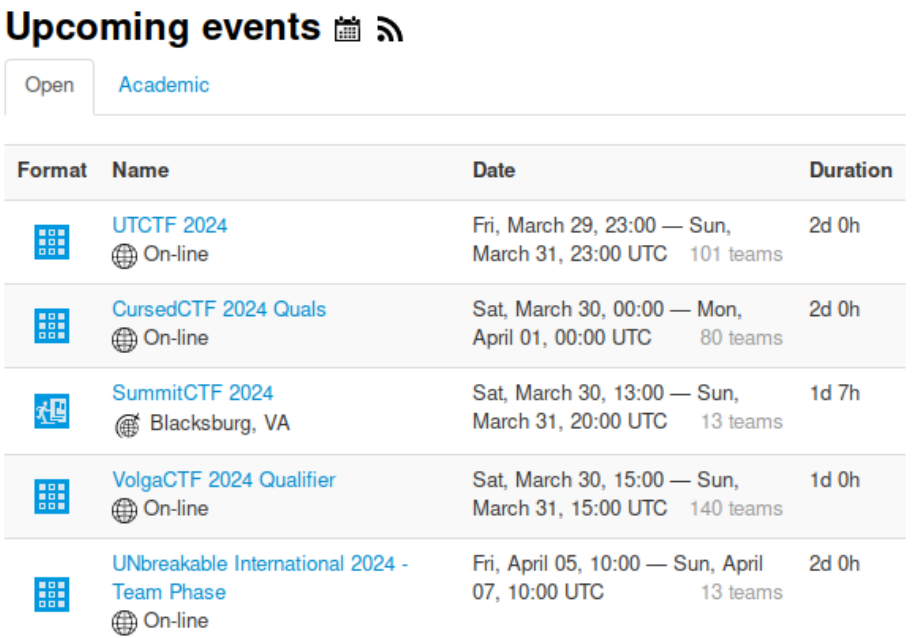
Ссылка на скачивание Kali

Ресурсы для тренировки

- https://vk.com/@spbctf-ctf-for-beginners - огромный список материалов и задачек почти по всем темам;
- https://overthewire.org/wargames/ - задачки на разные темы (Web, Crypto, Pwn, Reverse), решаемые, как правило, по SSH на сервере OTW. Обязательный к прохождению набор задачек – Bandit;
- https://cryptopals.com/ - криптография, надо писать свои собственные программки, реализующие различные алгоритмы и эксплуатирующие разнообразные уязвимости;
- https://standoff365.com/ - “киберполигон”, практика Attack-[Defense] на виртуальной инфраструктуре (не совсем CTF);
- https://www.hackthebox.com/ - большой каталог виртуальных машин, как для пентеста, так и для заданий вида CTF.

CTF Time (ctftime.org)

- Основной агрегатор CTF-соревнований;
- Чуть позже создадим команду на сайте и попробуем участвовать в соревнованиях (почти все проходят онлайн).



Upcoming events

Open | Academic

Format	Name	Date	Duration
	UTCTF 2024 On-line	Fri, March 29, 23:00 — Sun, March 31, 23:00 UTC 101 teams	2d 0h
	CursedCTF 2024 Quals On-line	Sat, March 30, 00:00 — Mon, April 01, 00:00 UTC 80 teams	2d 0h
	SummitCTF 2024 Blacksburg, VA	Sat, March 30, 13:00 — Sun, March 31, 20:00 UTC 13 teams	1d 7h
	VolgaCTF 2024 Qualifier On-line	Sat, March 30, 15:00 — Sun, March 31, 15:00 UTC 140 teams	1d 0h
	UNbreakable International 2024 - Team Phase On-line	Fri, April 05, 10:00 — Sun, April 07, 10:00 UTC 13 teams	2d 0h

Чат в Telegram