Itinerario de retos para la formación de profesionales

Diego López Montes
Máster Universitario de Seguridad de las tecnologías de la información y de las comunicaciones
TFM-Ad hoc

Jorge Chinea López
Victor Garcia Font

29/12/2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	Itinerario de retos para la formación de profesionales
Nombre del autor:	Diego López Montes
Nombre del consultor/a:	Jorge Chinea López
Nombre del PRA:	Victor Garcia Font
Fecha de entrega (mm/aaaa):	12/2018
Titulación:	Máster Universitario de Seguridad de las tecnologías de la información y de las comunicaciones
Área del Trabajo Final:	TFM-Ad hoc
Idioma del trabajo:	Español
Palabras clave	Retos, capturar la bandera

Resumen del Trabajo (máximo 250 palabras): Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.

Este trabajo va a analizar el uso de los retos dentro del ámbito de la ciberseguridad como herramienta para formación y evaluación de profesionales. Se va a realizar una taxonomía de los diferentes retos y la identificación de herramientas que ayuden a su organización. Como objetivo final, se desarrollará un CTF de demostración que permita mostrar el funcionamiento de estas herramientas pero que sea suficientemente escalable y extensible en el futuro para la celebración de un CTF real.

Abstract (in English, 250 words or less):

This paper will analyze the use of the challenges in the field of cybersecurity as a tool for training and evaluation professionals. A taxonomy of the different challenges and the identification of tools that help your organization will be carried out. The target is a demonstration of a CTF which will be developed to show the performance of these tools and if that is sufficiently scalable and extensible in the future to hold a real CTF.

Índice

Lista de figuras

1 Introducción

1.1 Contexto y justificación del Trabajo

Junto con la aparición de las Tecnologías de la Información, al mismo tiempo, surgió la necesidad de proteger de amenazas las tecnologías de la información, así como la información que estas recopilan, procesan y almacenan. Estas amenazas son robo, modificación o eliminación de la información, anulación del correcto funcionamiento de los sistemas, suplantación de identidad o fuga de información confidencial entre otros.

De esta necesidad de proteger los sistemas, surge una disciplina que analiza posibles vulnerabilidades, valora los riesgos, diseña y establece medidas de seguridad efectivas para evitar que puedan ser explotadas. Esta disciplina es conocida como seguridad informática, ciberseguridad o seguridad de tecnologías de la información.

La seguridad informática requiere de un constante estudio y actualización, puesto que los sistemas en desarrollo, a la vez que pueden estar protegiéndose de vulnerabilidades conocidas, muy posiblemente están desarrollando nuevas. Esta labor debe de ser realizada continuamente dentro de cada una de las organizaciones y debe involucrar en un modo u otro a cada miembro de esta.

Disponer de miembros dentro de la organización formados y entrenados para reconocer, mitigar y prever amenazas se hace especialmente importante para obtener altos niveles de seguridad en los sistemas y su información. Es por ello, por lo que han surgido multitud de bases de datos públicas de vulnerabilidades conocidas, manuales de seguridad, normativas, softwares de detección y anulación de amenazas, retos de ciberseguridad, etc.

En este trabajo se va a enfocar en los retos de ciberseguridad, entendidos tanto como una herramienta para la formación como para la evaluación de profesionales. Estos retos pueden ser de distintas clases y ser presentados de distintas formas, pero todos ellos tienen en común, que simulan ser un sistema o parte de él. El objetivo de dicho reto es utilizar dichas vulnerabilidades para explotarlas y comprometer lo máximo posible el sistema. A partir de estas líneas nos referiremos a esta clase de retos como CTF de sus siglas en inglés *Capture the flag* o traducido como *Capturar la bandera*.

Los retos CTF tienen como principal característica que se han introducido deliberadamente diferentes tipos de vulnerabilidades, normalmente de diferente dificultad y disciplina, que son de alguna forma asociadas a una *bandera* o en inglés *flag* que sirve como prueba de su descubrimiento. Dicho *flag* suele corresponder con una clave en forma de texto.

1.2 Objetivos del Trabajo

El presente trabajo tiene como objetivo reconocer el contexto y las motivaciones por las que se crean y celebran estos retos. Desarrollar una clasificación o taxonomía de los distintos tipos de retos que se pueden encontrar, desde los eventos organizados en universidades, pasando por los eventos realizados en los congresos de seguridad, hasta los ejercicios impulsados desde los gobiernos.

Posteriormente, se va a realizar un análisis y recopilación de herramientas y ejercicios existentes en Internet, que permitirán la realización y organización de esta clase de retos. En base a este análisis, se diseñará un reto estilo CTF.

Finalmente, se desarrollará un despliegue de una infraestructura preparada para la realización de un reto de demonstración. Este despliegue tiene como propósito ser una demostración sencilla, pero extensible, de una preparación a nivel técnico de un CTF. Debe ser lo suficientemente mínima para poder mantenerse funcionando en un ordenador de escritorio.

Todo este trabajo quedará documentado en el presente documento de memoria.

1.3 Enfoque y método seguido

Para el cumplimiento de los objetivos enumerados anteriormente, el trabajo transcurrirá en la siguientes fases o etapas:

1.3.1 Recopilación de la información

El trabajo comienza con una investigación alrededor del contexto, tipos y eventos de retos existentes. Esta fase, que es especialmente importante como primer paso para poder concretar los objetivos y poder realizar la planificación del trabajo, será una constante durante la realización de este, permitiendo aportar continuamente nuevos datos y enfoques.

1.3.2 Planificación

Entendiendo el contexto y objetivos del trabajo, se va a realizar la planificación donde se definirán las tareas a realizar, se estimarán y se representarán en la línea temporal mediante un diagrama de Gantt, así como los hitos que corresponden con las entregas de cada una de las PEC. También se recopilarán todos los recursos hardware, software, y servicios en línea que serán necesarios. Finalmente, se listarán los productos que deben quedar realizados al final del presente trabajo.

1.3.3 Realización del CTF de demostración

Para la realización del trabajo se va a realizar un CTF de demonstración en que sea sencillo de desplegar tantas veces como se necesite. Para ello, es necesario identificar las herramientas de automatización de despliegues sobre la que se va a trabajar y recopilar algunos ejercicios o pruebas públicas para incluir en el CTF.

1.3.4 Documentación

La documentación del trabajo será redactada en el presente documento de memoria. Esta tarea deberá ser continua desde el inicio hasta el final de la realización del trabajo. Se realizarán revisiones antes de la entrega de cada uno de los hitos y una antes de la entrega final.

También se prestará especialmente atención a la correcta recopilación de toda la bibliografía utilizada.

1.3.5 Repositorio

Los ficheros y fuentes utilizados y necesarios para el despliegue del CTF serán subidos a un repositorio público. En este trabajo se ha seleccionado Github como repositorio que utiliza el sistema de control de versiones de Git.

1.4 Planificación del Trabajo

1.4.1 Diagrama de Gantt

La representación sobre la línea temporal de las tareas definidas para el proyecto mediante un Diagrama de Gantt.

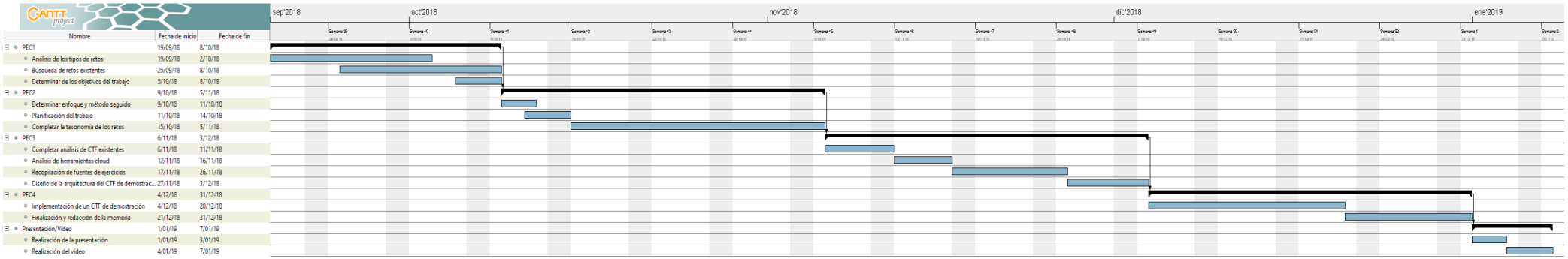


Ilustración 1 Diagrama de Gantt del trabajo

1.4.2 Recursos necesarios para la realización del trabajo

Listado de recursos tanto hardware como software necesarios para la realización del presente trabajo. También se enumeran las herramientas disponibles en línea utilizadas.

1.4.2.1 Recursos hardware

- Ordenador (portátil o sobremesa)
  - CPU x64
  - RAM Mínima 12GB
  - Disco duro con 100GB libres

1.4.2.2 Recursos software

- Microsoft Windows 10
- Microsoft Word 365
- GanttProject
- Adobe Reader
- Docker Toolbox (Windows)

1.4.2.3 Servicios en línea

- Draw.io (https://www.draw.io/)
- MindMeister (https://www.mindmeister.com)
- Gmail (https://mail.google.com/)
- GitHub (https://github.com/)

1.4.3 Hitos

El trabajo se divide en entregables parciales o PEC. Cada una de estas PEC se considera un hito del proyecto:

- **PEC1**: En la primera PEC se realiza un primer análisis de los tipos de retos, una búsqueda de los retos existentes y se determinan los objetivos del trabajo.
- **PEC2**: Se determina el enfoque y métodos que se van seguir, la planificación temporal y se completa una taxonomía de los retos. Identificando y recopilando diversas fuentes de información.
- **PEC3**: Se completan los análisis de los CTF existentes. Además de la recopilación de las diferentes herramientas para el despliegue de un reto en la nube, de retos o ejercicios disponibles en Internet y el diseño de la arquitectura de un reto de demonstración.
- **PEC4**: Se implementa un CTF de demonstración y se completa la redacción de la memoria con las conclusiones, bibliografía y anexos.
- **Video**: Se realiza la presentación del proyecto y posteriormente el video de defensa.

1.5 Breve sumario de productos obtenidos

1.5.1 Memoria

El presente documento de memoria debe incluir toda la información que ha sido necesaria para la realización del trabajo, desde los trabajos iniciales de obtención de información hasta las conclusiones derivadas de la realización del trabajo. Se presentará en formato PDF.

1.5.2 Código fuente

El código fuente resultante de la realización de este trabajo se presentará comprimido y empaquetado en el buzón de entrega. También se encontrará para acceso público en Internet en la plataforma de alojamiento de código GitHub.

El enlace para el repositorio: https://github.com/diegolopmon/CTF-demo

2 Análisis de los retos en el ámbito de la ciberseguridad

2.1 Motivaciones para la existencia de los retos

Cada día las tecnologías de la información están más presentes en nuestro entorno, desde el profesional hasta ocio. Tratan nuestros datos personales y son el medio para muchas de nuestras comunicaciones. Este crecimiento exige cada vez más profesionales especializados en seguridad informática. La firma *Cybersecurity Ventures*, predice que existirán 3.5 millones de vacantes abiertas en 2021 (Morgan, 2017).

Es, por tanto, que universidades, centros de formación y compañías estén en crecimiento titulaciones, cursos y planes de formación enfocados en la ciberseguridad. Paralelamente, la captación de estos profesionales dentro del mercado laboral es también otro reto, y ambos encuentran en los retos de ciberseguridad una herramienta muy potente.

Los retos de ciberseguridad desde la perspectiva del retado permiten un entorno de entrenamiento, de prueba de superación y autoevaluación y una forma de demostrar sus competencias. Por parte del organizador, son una plataforma donde puede evaluar a un equipo y sus integrantes, entrenarlos y también poner a prueba sus propios sistemas en un entorno simulado y controlado.

2.2 Taxonomía de los retos

Se va a realizar una taxonomía de los distintos tipos de retos, la cual, no solo permitirá hacer una clasificación de aquellos relacionados exclusivamente con la ciberseguridad sino con todos los retos o ejercicios donde se quieran poner a prueba la preparación de los participantes.

Los retos pueden ser clasificados atendiendo a los siguientes grupos de criterios:

- **Ámbito de participación:** Los retos pueden ser organizados para grupos tanto homogéneos como heterogéneos de participantes. Estos participantes pueden ser agrupados basándose en el sector al que pertenecen, ámbito geográfico o roles.
- **Modalidades:** Los retos presentan múltiples modalidades para su desarrollo y las reglas de este. Estas pueden ser de todos los participantes simulando el ataque conjuntamente, separados en grupos de ataque/defensa
- **Propósitos:** Cada reto se realiza buscando uno o varios propósitos que pueden ser de concienciación, evaluación o desarrollo.

2.2.1 Ámbito de participación

Los participantes pueden ser agrupados según los siguientes criterios:

- **Sector** en el que desempeñan su labor profesional o de formación. Dicho sector puede ser tanto el público entendiendo este como gobiernos, defensa, servicios de emergencia, etc. o el sector privado como pueden ser corporaciones y profesionales. También se puede diferenciar el sector de los estudiantes.
- **Geográfico**, el reto puede ser organizado con un alcance local, nacional o multinacional.
- **Roles** que van a asumir durante la ejecución del reto. Estos roles pueden ser de carácter técnico, de gestión o directivo.
- El **acceso** al reto puede ser de carácter abierto al público en general que desee participar, restringido a un conjunto limitado de participantes o totalmente privado.

2.2.2 Modalidades

Se identifican las siguientes modalidades de ejecución de retos:

- **Comprometer el sistema**: Comúnmente referenciada en inglés *Jeopardy*, se trata de resolver el reto individualmente o en equipo tratando de capturar las distintas banderas para conseguir las mejores puntuaciones, pero sin ataques entre los participantes.
- **Resolución de una crisis**: Contrariamente a la modalidad de *comprometer el sistema*, esta modalidad propone a los participantes una situación de un sistema atacado o que se encuentra atacado en tiempo real y estos deben plantear y realizar acciones de defensa para neutralizar o evitar daños en el sistema que defienden.
- **Ataque y defensa**: Este tipo de retos se trata en una competición entre dos equipos, uno es el encargado de reforzar el sistema y protegerlo mientras que el contrario es el encargado de realizar el ataque, etc. Se trata de una combinación de los dos anteriores.

2.2.3 Propósitos de los retos

Los retos pueden ser realizados por uno o varios propósitos o fines:

- La **concienciación de los participantes** implica que la realización del reto ha alterado la percepción acerca de la seguridad que los participantes tenían de los sistemas. Esto permitirá que posteriores tomas de decisiones, planificaciones y prioridades puedan ser realizadas desde nuevas perspectivas.
- Los retos son una simulación en la cual se pueden realizar una **evaluación de planes de seguridad y los sistemas** con el fin de que estos mejoren ante futuras amenazas.
- La **elaboración de nuevas tareas de mejora** puede entenderse como el propósito siguiente a los dos anteriores, donde en base a

una evaluación de los resultados del reto, se identifican una serie de mejoras para aplicar sobre los sistemas reales.

2.3 Frameworks abiertos

Existen frameworks o plataformas software que proveen las funcionalidades necesarias para la organización, preparación y gestión que los retos necesitan. Se trata generalmente de aplicaciones web donde los participantes reciben las instrucciones del reto y pistas que también pueden introducir los distintos flags que vayan obteniendo y pueden visualizar su progreso y el del resto de participantes.

2.3.1 FBCTF

Facebook CTF es una plataforma de código abierto para operar retos de tipo *Jeopardy* y estilo *King of the Hill*. Fue desarrollado por Facebook como herramienta educativa en el año 2013, se utilizó para organizar CTFs en institutos, universidades y conferencias de seguridad entre otros. En el año 2016 fue publicado su código fuente.

Ilustración 2 Captura de pantalla de FBCTF

Dispone de una interfaz web que es utilizada tanto por los organizadores de CTF para la configuración de cada uno de los desafíos, como por los participantes, para obtener la información de los retos, recibir pistas e introducir los *flags* obtenidos. Los participantes verán un mapamundi donde se activarán distintos países por parte de los organizadores, cada uno de estos países corresponde a un reto. El primer participante o equipo en resolver el reto obtendrá la conquista del país, características propias del estilo *King of the Hill*, obteniendo una serie de puntos.

En base a la cantidad de puntos totales se establece el ranking final. Estos puntos pueden también ser gastados en la obtención de pistas para cada uno de los retos.

2.3.2 CTFd

CTFd es una plataforma de código abierto para ejecutar CTFs. Dispone de un diseño sencillo y es adaptable mediante plugins y temas.

Se encuentra desarrollado en Python y Flask.

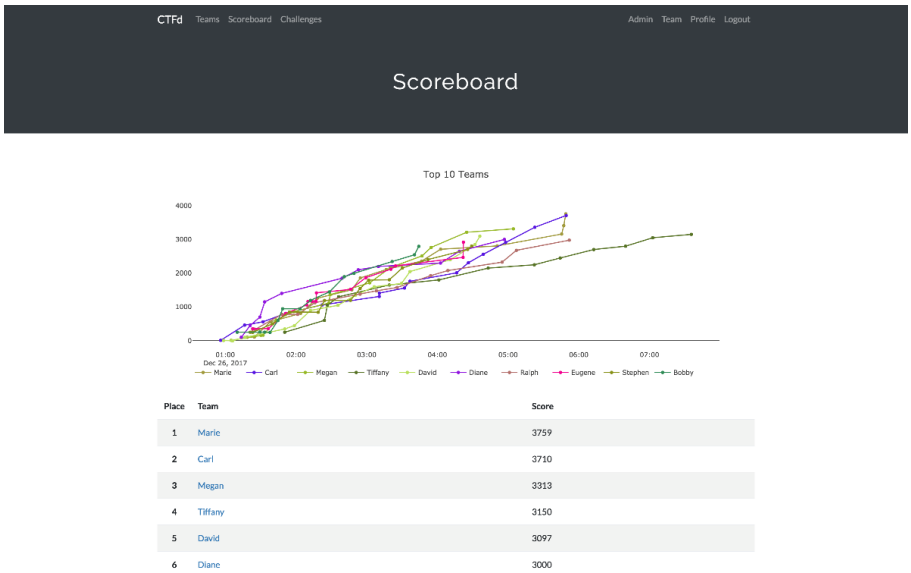


Ilustración 3 Captura de pantalla de CTFd

La gestión de retos, usuarios y marcadores puede ser realizada desde la misma interfaz web mediante los usuarios con permisos de administración. Adicionalmente, toda la configuración puede ser exportada e importada mediante ficheros, permitiendo así la existencia de ejercicios predefinidos.

Toda la persistencia de la plataforma se realiza contra una base de datos y permite soporte de web cache especialmente útil para eventos en los que concurren gran número de participantes.

Desde la web del proyecto https://ctfd.io se ofrecen servicios de hosting, extensiones de pago.

2.3.3 HackTheArch

HackTheArch es otro framework para CTFs de código abierto desarrollado por la Military Cyber Professionals Association (MCPA). Funciona como un servidor para los marcadores donde añadir retos y capturar y llevar seguimiento de los eventos de bandera capturada de los participantes.

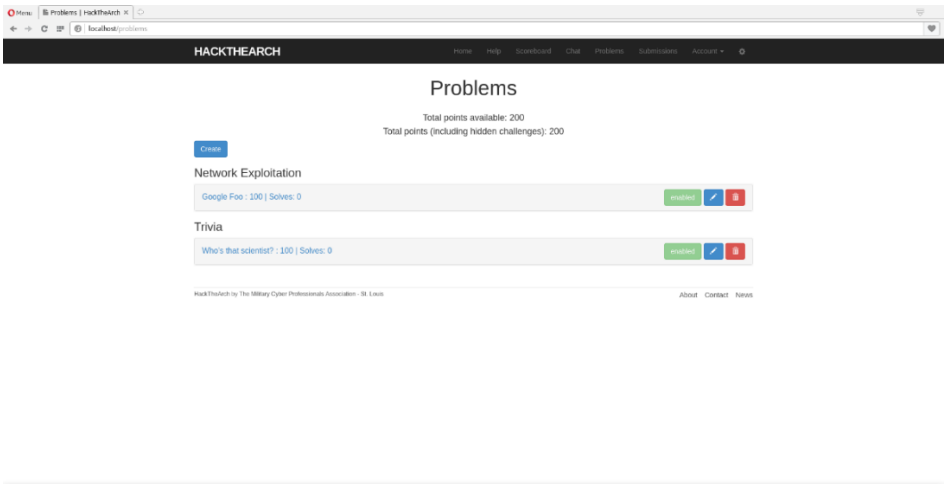


Ilustración 4 Captura de HackTheArch

2.4 CTFs en línea

A continuación, se van a desglosar algunos de los sitios web que permiten la realización de CTFs en línea. Estos sitios presentan plataformas muy útiles para el entrenamiento personal.

2.4.1 ctfs.me

ctfs.me es una web que dispone de retos online. El registro es libre y permite la realización de retos de distintos tipos y temáticas, que son realizados por la comunidad. Cada uno de los retos propuestos otorga unos puntos en base a su dificultad una vez resuelto y existe un ranking global. Regularmente, se realizan retos durante periodos de tiempo limitado con la misma mecánica.

Enlace: https://ctfs.me/challenges

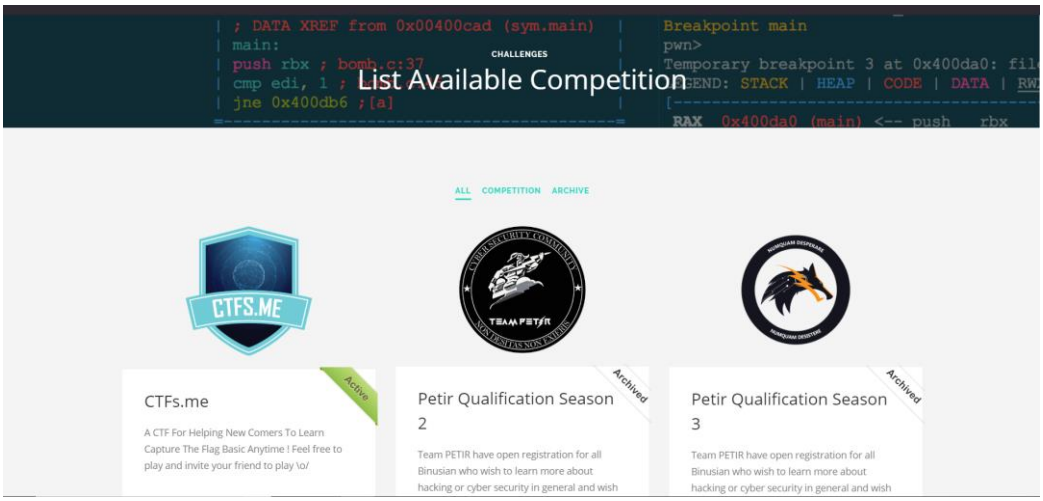


Ilustración 5 Captura de ctfs.me

2.4.2 Backdoor

Backdoor es una plataforma de retos online. Dispone de retos online que se encuentran siempre disponibles cuya resolución otorga puntos para un ranking global y también se realizan competiciones tanto en equipos como individuales.

Enlace: https://backdoor.sdslabs.co/

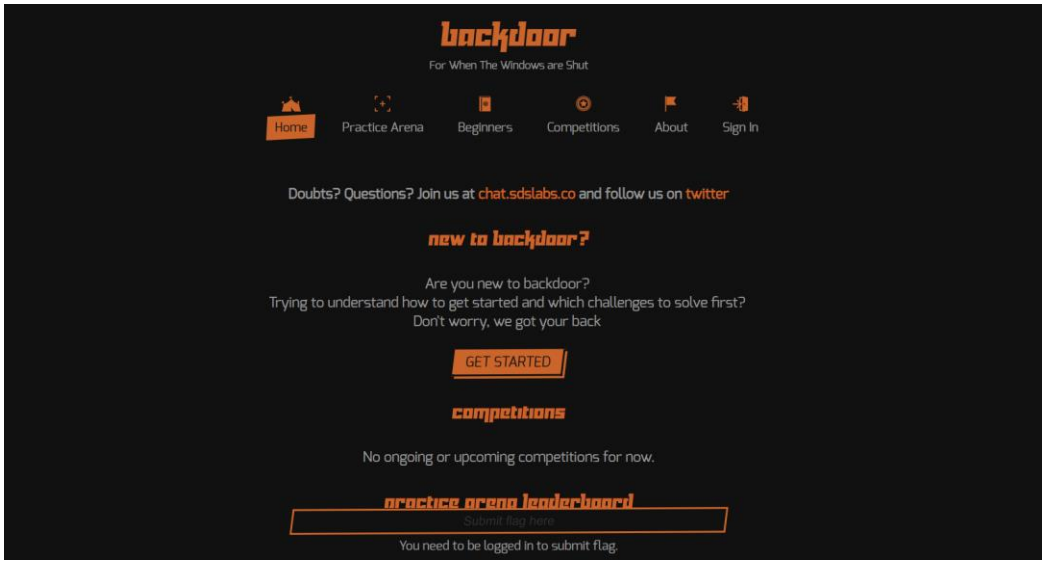


Ilustración 6 Captura de Backdoor

2.4.3 CTF Time

Una plataforma particular es *CTF Time*. Se trata de un archivo de competiciones CTF donde se recopilan una gran cantidad de ellos para que sea muy fácilmente saber sobre el calendario las fechas de celebración de cada uno y los distintos tipos. También recopila los resultados después de cada celebración con el fin de mantener un ranking global de equipos y participantes individuales.

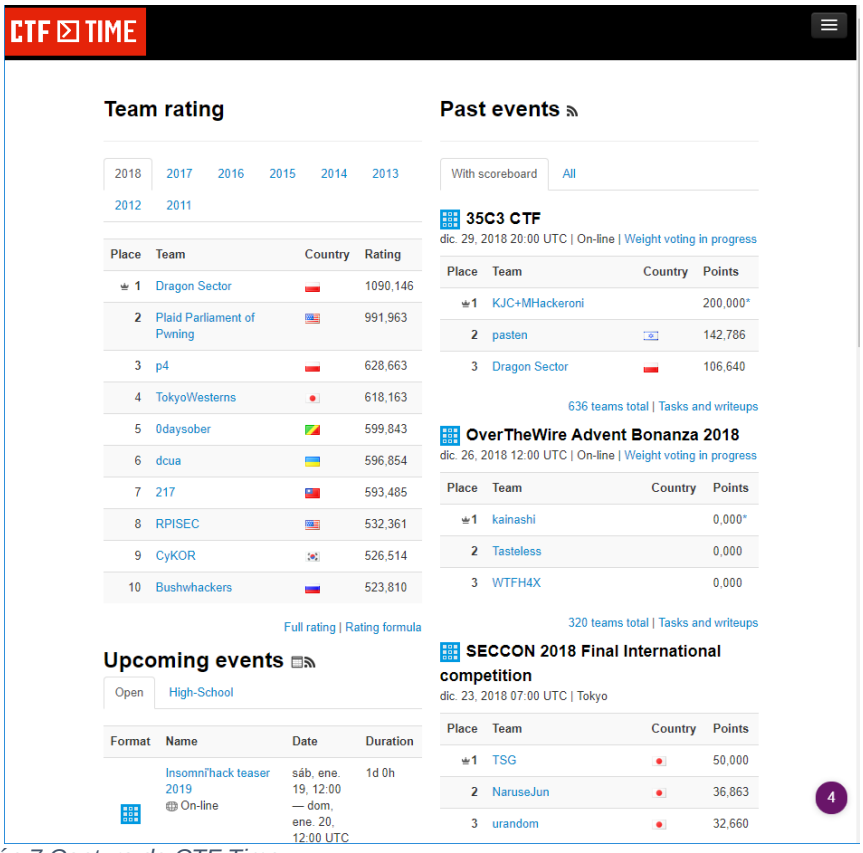


Ilustración 7 Captura de CTF Time

Enlace: https://ctftime.org

2.5 Fuentes públicas de retos

A diferencia de la sección anterior, aquí nos vamos a centrar en aquellas fuentes donde pueden obtenerse recopilaciones de retos para ser resueltos fuera de línea. La resolución de estos no tiene por qué resultar en un flag y no existe un ranking ni competición asociada a ellos, aunque si pueden ser usados como ejercicios individuales dentro de la celebración de un CTF.

2.5.1 Vulnhub

Vulnhub es una web que almacena materiales que pueden ser descargados en formato de imágenes de máquinas virtuales para ser ejecutados en un entorno local. Estas máquinas van acompañadas de una descripción y algunas veces de alguna pista acerca de las vulnerabilidades y flags que incluyen.

En la mayor parte de los retos es necesario disponer de un hipervisor para máquinas virtuales como, por ejemplo, *VirtualBox*.

Enlace: https://www.vulnhub.com/

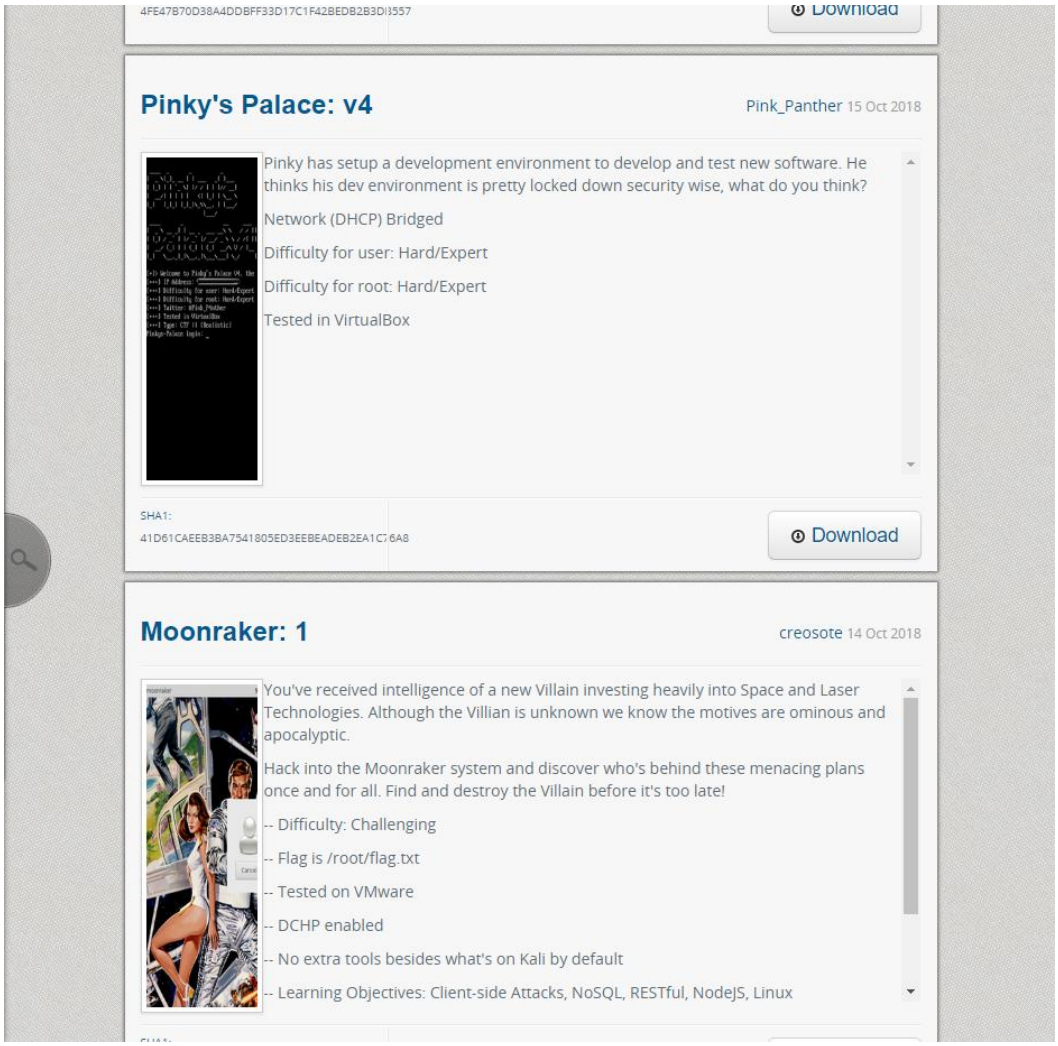


Ilustración 8 Captura de vulnhub.com

2.5.2 Retos de las celebraciones de CSAW CTF

Cada año la Universidad de Nueva York celebra la competición CTF entre varios equipos alrededor del mundo. Estas competiciones están enfocadas para principiantes. Posteriormente a su celebración, los retos con su código fuente son publicados en GitHub.

Enlace: https://github.com/osirislab

2.5.3 Proyecto OWASP Juice Shop

OWASP Juice Shop es una aplicación web insegura de código abierto. La aplicación, que simula ser un comercio online, contiene una gran cantidad de retos de distinta dificultad que los participantes deben descubrir.

La aplicación puede ser configurada con la modalidad de CTF, lo que permite generar un fichero con la configuración de retos que puede ser importada tanto en CTFd como en FBCTF. También el modo CTF activa la opción de *flags* y cuando un usuario descubre una vulnerabilidad,

aparece un dialogo mostrando el nombre y el flag del reto resuelto. No es nada recomendable disponer de una única instancia compartida para todos los participantes, puesto que los diferentes ataques que los usuarios realizasen sobre ella alterarían los resultados del resto de participantes.

Para que los participantes puedan ejecutar rápida y fácilmente una instancia de esta, el proyecto se distribuye en imagen Docker, que puede ser ejecutada rápida y fácilmente en un equipo local. El único requisito es, que la clave CTF configurada sea la misma para que la generación de los *flags* sea la correcta.

Al tratarse de un proyecto que tiene como objetivo la formación en seguridad, está ampliamente documentado e intenta cubrir varios aspectos de la seguridad en las aplicaciones web. Cada uno de los retos de los que dispone están asociados a una serie de pistas y soluciones consultables en su documentación.

Enlace: https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

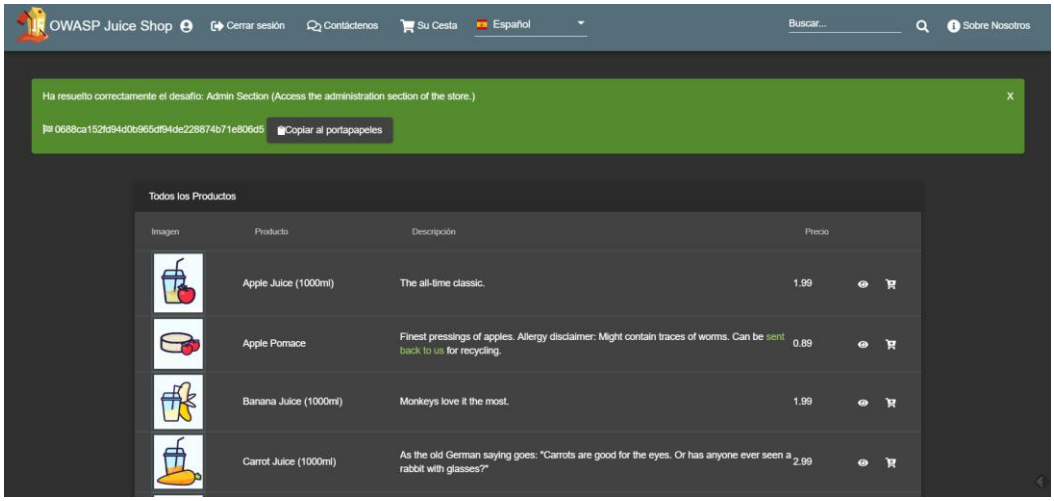


Ilustración 9 Captura de la página principal de OWASP Juice Shop

3 Diseño de un CTF

3.1 Descripción general del CTF de demonstración

Uno de los propósitos del presente trabajo es diseñar, desarrollar y demonstrar el despliegue de un CTF donde se pueda realizar la gestión de los usuarios, los retos, los *flags* y los resultados. Este debe desarrollarse con el objetivo de que sea extensible para soportar un CTF con varios retos y soporte para muchos usuarios. Para facilitar su desarrollo y demonstración, este CTF de demonstración debe ser lo suficientemente ligero para ejecutarse en un equipo de escritorio.

3.2 Análisis de herramientas para despliegues

Para que el despliegue del software que va a ejecutar el CTF, pueda ser replicado de una forma sencilla, rápida y segura se van a utilizar una serie de herramientas que facilitaran mucho el trabajo.

3.2.1 Docker

Docker es un proyecto de código abierto para la automatización del despliegue de aplicaciones dentro de contenedores añadiendo una capa de abstracción. Docker se sirve de características del Kernel de Linux para que los contenedores independientes se ejecuten dentro de una misma instancia de Linux evitando la sobrecarga que suponen las máquinas virtuales.

En la siguiente figura se muestran las diferencias entre máquinas virtuales y contenedores Docker:

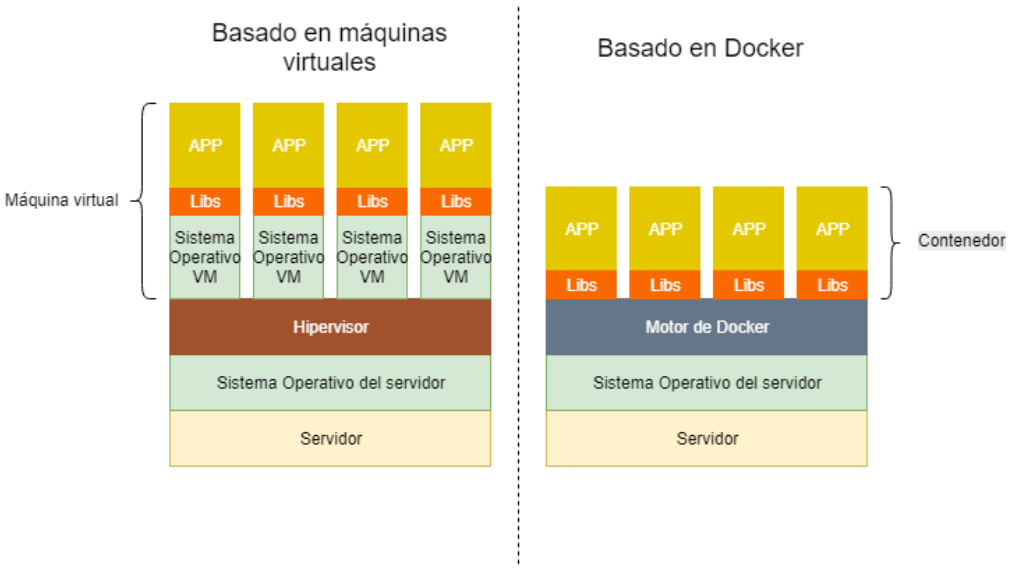


Ilustración 10 Comparativa entre las capas en máquinas virtuales y Docker

Como se puede apreciar en el caso de Docker, se elimina la necesidad de virtualizar un sistema operativo completo, pero se mantiene la portabilidad que sería necesaria para llevar este escenario de demostración a un entorno real de producción.

3.2.2 Docker Compose

Docker Compose es una herramienta para la definición de aplicaciones multicontenedores en Docker. Mediante un fichero de tipo YAML, se definen cada uno de los servicios que serán ejecutados en una misma máquina. De esta forma en un único fichero podremos definir cómo será desplegado el CTF, definiendo tanto cada uno de los componentes como las redes a las que serán conectados y las características de estas.

3.3 Arquitectura del CTF

3.3.1 Aspectos generales de la arquitectura

Entre los elementos que se deben desplegar, en los cuales se entra en más detalle en apartados siguientes, se distinguen el framework del CTF, los distintos entornos para cada una de las pruebas, bases de datos, etc.

Se establece el requisito que cada elemento desplegado sea independiente del resto, sin dependencias, permitiendo la atomicidad que facilitará la escalabilidad del sistema y aislar los elementos como se desee. Esto se podría conseguir mediante el uso de máquinas virtuales, pero su coste computacional es demasiado alto, es por ello, que se optará por contenedores.

Los contenedores ofrecen un modelo de implementación basado en imágenes, lo que permite compartir una aplicación o un conjunto de servicios con todos sus servicios en varios entornos. Una vez ejecutado el contenedor este se ejecuta en un entorno aislado en la máquina que lo hospeda de una forma mucho las ligera que lo haría si fuera una máquina virtual.

3.3.2 Componentes

El primer paso para definir la arquitectura es identificar los elementos que van a conformar el CTF de demonstración.

- **Framework**: Se ha seleccionado el framework *CTFd* para la realización de esta demonstración por ser el más fácilmente extensible de los analizados y la facilidad para su despliegue. Esta herramienta dispone de una interfaz web que permite la configuración y gestión del CTF por parte de los usuarios administradores, a la vez es donde los participantes encontrarán la descripción y recursos de los distintos retos, podrán registrar los

flags que descubran y consultar sus resultados y estadísticas propios y del resto de participantes.

- **Base de datos:** Para el almacenamiento de todos los datos relacionados con la celebración del CTF se desplegará una base de datos dedicada de la cual hará uso el framework, en nuestro caso, *CTFd* recomienda *MySQL* o *MariaDB*. Por su mejor rendimiento y licencia GPL se desplegará una base de datos *MariaDB*.
- **Cache:** CTFd usa Flask-Caching para implementar la lógica de caché. Se desplegará una base de datos en memoria *Redis*.
- **Web vulnerable:** Para la realización de la demostración se va a desplegar una aplicación web con varias vulnerabilidades y flags asociados. Se ha seleccionado la aplicación de *OWASP Juice Shop*. Esta aplicación web dispone de integración con *CTFd* permitiendo importarle todos los tokens generados. En esta demostración se desplegará junto al resto de componentes, pero en un CTF real este componente debería ser replicado tantas veces como participantes o equipos estén durante la celebración, puesto que está diseñado para mantener el estado conforme se van explotando las vulnerabilidades.

Cada uno de estos componentes corresponde a un contendor separado y deben estar conectados entre sí mediante una red virtual segura para evitar que esta resulte comprometida.

En esta arquitectura se diferencian dos redes:

- Red **default**: Esta red con carácter público debe ser la red por la que los participantes accedan a los recursos necesarios del CTF. En esta red exclusivamente deben ser conectados aquellos servicios estrictamente necesarios.
- Red **internal**: Esta red de carácter privado es la red que utilizarán los servicios para comunicarse entre sí. Por ejemplo, entre el framework y la base de datos. En esta red se conectarán todos aquellos servicios que no deban ser accesibles desde el exterior y aquellos que hagan uso de servicios internos.

En la siguiente figura se muestra la arquitectura completa:

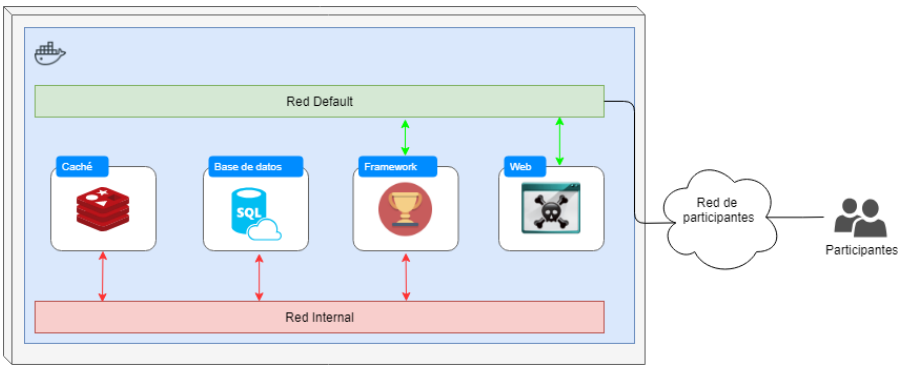


Ilustración 11 Arquitectura del CTF de demostración

4 Implementación del CTF

4.1 Orquestación

Todos los componentes del CTF van a ser orquestados desde un mismo fichero en el que se describen los siguientes parámetros principales:

- Nombre del contenedor
- Mapeo de puertos que expone
- Declaración de variables de entorno dentro de cada contenedor
- Volúmenes que se montan entre la máquina y el contenedor
- Dependencias entre los contenedores
- Redes a las que se conecta

Este fichero en formato *yml*, es interpretado por el programa *Docker-compose* mediante el siguiente comando ejecutado en la misma ruta en la que se encuentra el fichero *docker-compose.yml*:

```
docker-compose up -d
```

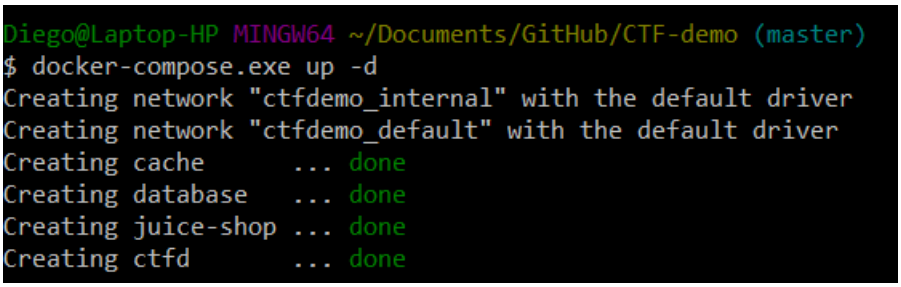


Ilustración 12 Traza de la ejecución de docker-compose up

Este deberá arrancar los siguientes contenedores:

- Ctfd
- Base de datos (MariaDB)
- Caché (Redis)
- Juice Shop

El fichero de *docker-compose* mencionado, se encuentra en el repositorio de Github:

https://github.com/diegolopmon/CTF-demo/blob/master/docker-compose.yml

4.2 Configuración

Una vez ejecutada la orquestación de todos los contenedores, estos iniciarán su arranque y una vez finalizado, se encontrarán en su estado por defecto.

La configuración cubre los siguientes aspectos:

- Configuración del reto en CTFd
- Importación del fichero de retos

4.2.1 Configuración del reto en CTFd

En la primera ejecución de CTFd este no se encuentra configurado. Para la configuración, se debe acceder a su interfaz web en el puerto *8000*.

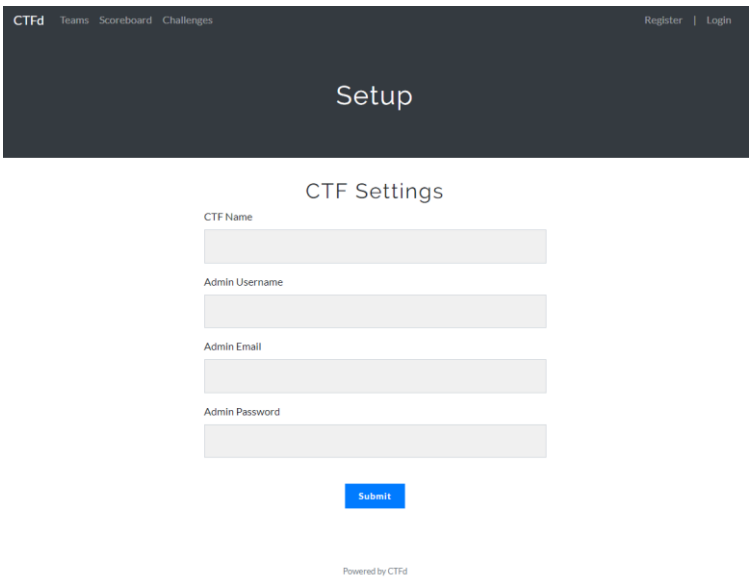


Ilustración 13 Captura de la configuración inicial de CTFd

Donde se deben especificar los parámetros de del Nombre del CTF y usuario, correo y contraseña del usuario administrador. Estos datos son suficientes para la configuración inicial del CTF.

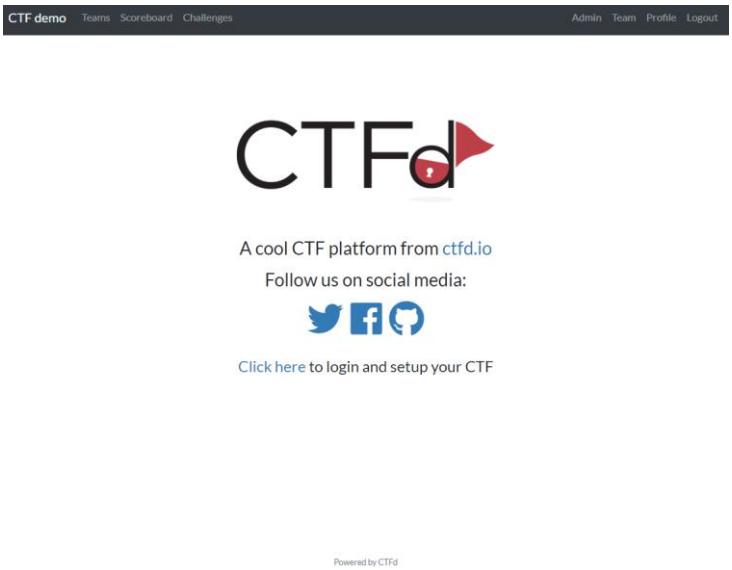


Ilustración 14 Captura de la página inicial de CTFd

4.2.2 Generación del fichero de retos

Una vez se ha configurado CTFd, el paso siguiente es la carga de retos. Los retos son generados por una herramienta de *OWASP Juice Shop* llamada *juice-shop-ctf*.

En el fichero *docker-compose* utilizado en el paso anterior, se han especificado dos variables de entorno en el contenedor de *Juice Shop*:

```
NODE_ENV=ctf
CTF_KEY=TFM
```

La variable *NODE_ENV* indica que Juice Shop será ejecutado en modo CTF y *CTF_KEY* indica que la clave generadora de los flags será *TFM*. La clave generadora es importante que sea la misma en la configuración de *Juice Shop* que la que se utilice en la herramienta de *juice-shop-ctf*, de esta forma se importarán los mismos flags que los que existen dentro de la aplicación.

El primer paso es instalar *juice-shop-ctf*, mediante el instalador de *npm* de Node.js:

```
npm install -g juice-shop-ctf-cli
```

Después ejecutar:

```
Juice-shop-ctf
```

A continuación, se realizan las siguientes 5 preguntas:

1. **“CTF framework to generate data for?”** Se dan dos opciones, CTFd y FBCTF. En este caso, se seleccionará la de *CTFd*.

2. **"Juice Shop URL to retrieve challenges?"** La URL de un servidor de *Juice Shop* desde donde la herramienta obtiene los retos existentes.
3. **"Secret key URL to ctf.key file?"** Admite tanto la clave para generar los flags o una URL a un fichero donde se encuentra esta clave. Para este caso, esta debe ser *"TFM"*.
4. **"Insert a text hint along with each challenge?"** Es un seleccionable entre las siguientes opciones:
    a. **"No text hints"** No añadirá ninguna pista a los retos.
    b. **"Free text hints"** Incluirá pistas gratuitas a los retos (desvelarlos no consume puntos).
    c. **"Paid text hints"** Incluirá pistas con coste a los retos. El coste es el 10% de puntos del valor total del reto una vez conseguido.
5. **"Insert a hint URL along with each challenge?"** Es un seleccionable entre las siguientes opciones:
    a. **"No hint URLs"** No añadirá ninguna URL como pista a los retos.
    b. **"Free hint URLs"** Incluirá URL's como pistas gratuitas a los retos.
    c. **"Paid hint URLs"** Incluirá URL's como pistas con coste a los retos. El coste es el 20% de puntos del valor total del reto una vez conseguido.

Una vez contestadas todas las preguntas se generará un fichero comprimido *.zip*.

En el repositorio se encuentra un fichero de importación ya previamente generado para *CTFd* con todas las pistas activadas con coste:

https://github.com/diegolopmon/CTF-demo/blob/master/OWASP_Juice_Shop.2018-12-07.CTFd.zip

4.2.3 Importación del fichero de retos

Este fichero, será importado dentro de CTFd de la siguiente forma:

1. Acudir a la pestaña de *Admin*.
2. Acudir a la pestaña de *Config*.
3. En el menú de configuración ir al submenú de *Backup.*
4. Ir a la pestaña *Import*.
5. Seleccionar el fichero *.zip* generado anteriormente.
6. Asegurarse que solamente se encuentra activada la opción de *Challenges*.
7. Pulsar el botón amarillo de *Import*.

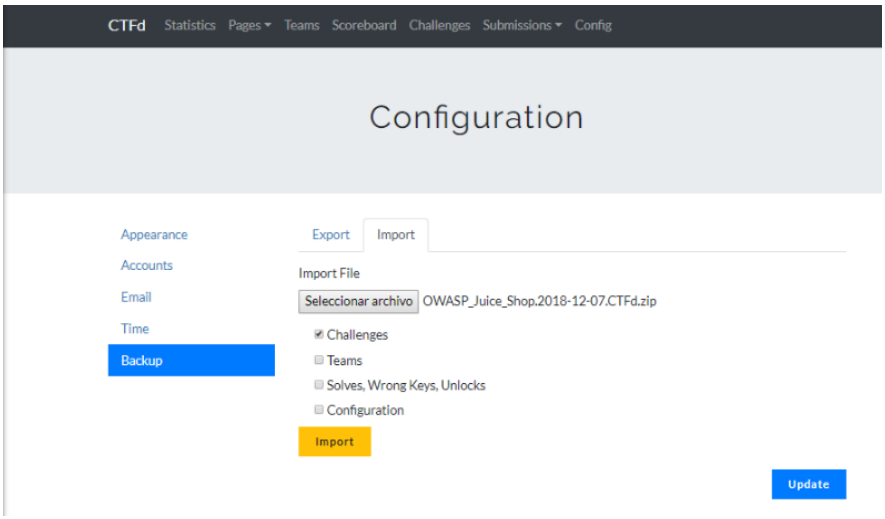
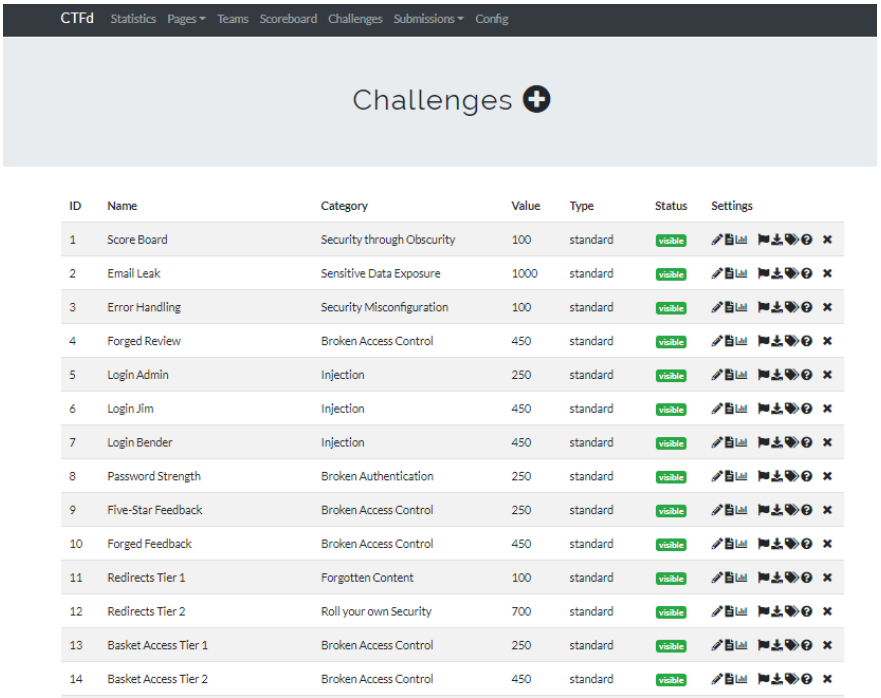


Ilustración 15 Captura del apartado de importación de configuraciones de CTFd

Todos los retos serán importados y podrán ser visibles desde la pestaña de *Challenges*:



ID	Name	Category	Value	Type	Status	Settings
1	Score Board	Security through Obscurity	100	standard	visible	
2	Email Leak	Sensitive Data Exposure	1000	standard	visible	
3	Error Handling	Security Misconfiguration	100	standard	visible	
4	Forged Review	Broken Access Control	450	standard	visible	
5	Login Admin	Injection	250	standard	visible	
6	Login Jim	Injection	450	standard	visible	
7	Login Bender	Injection	450	standard	visible	
8	Password Strength	Broken Authentication	250	standard	visible	
9	Five-Star Feedback	Broken Access Control	250	standard	visible	
10	Forged Feedback	Broken Access Control	450	standard	visible	
11	Redirects Tier 1	Forgotten Content	100	standard	visible	
12	Redirects Tier 2	Roll your own Security	700	standard	visible	
13	Basket Access Tier 1	Broken Access Control	250	standard	visible	
14	Basket Access Tier 2	Broken Access Control	450	standard	visible	

Ilustración 16 Captura del apartado de configuración de retos de CTFd

5 Conclusiones

En este trabajo se han analizado el contexto en el que surgen los retos, su taxonomía y se han recopilado varias herramientas, eventos y retos existentes, con especial atención a los eventos tipo CTF. También, se ha desarrollado una demostración de cómo podría ser orquestada una infraestructura para la celebración de un evento CTF, con la gestión centralizada de los participantes, retos y resultados, de una forma escalable y sencillamente portable.

La utilización de retos con propósitos educativos, de entrenamiento y de evaluación, no es nada reciente, ni exclusivos en el ámbito de la seguridad. Han sido llevados a ámbitos militares, universidades y organizaciones privadas. Su celebración no solo aporta un medio de formación, sino que permite evaluar el estado de formación de los participantes y facilita lecciones para mejorar diversos aspectos que se vean envueltos dentro del entorno simulado.

En la fase inicial del presente trabajo, se preveía la necesidad de desarrollar muchos más elementos necesarios para el CTF de ejemplo de los que finalmente han sido necesarios. Frameworks como los vistos de CTFd y FBCTF puestos a disposición a cualquiera que quiera utilizarlos e incluso extenderlos, hacen que sea mucho más sencilla técnicamente la organización de esta clase de eventos. También, su uso extendido, permite mayores niveles de seguridad y madurez en el software. Es por ello, que después del análisis de estas herramientas, se tomó la decisión de utilizarlas para orquestar un ejemplo de su uso en lugar de desarrollar unas nuevas desde cero.

Era necesario que todo lo aprendido y desarrollado en este trabajo pudiera formar parte de los primeros pasos de un evento de tipo CTF. Es por ello que el enfoque multiplataforma, escalabilidad y de automatización han estado siempre presentes en todas las decisiones, diseños e implementaciones.

Futuras líneas de trabajo podrían explorar como este trabajo podría aplicarse sobre distintos entornos de producción. Por ejemplo, llevarlo a una organización que disponga de una infraestructura real que pueda ser replicada parcial o totalmente en un entorno simulado. Diseñar distintos retos, no solo a nivel técnico, sino a más niveles que permitan la participación de más roles como pueden ser los equipos de administración, legal, dirección, etc. Si bien el ejemplo mostrado ha sido entorno a una web vulnerable que disponía de una gran cantidad de vulnerabilidades, este permite ser extendido para cualquier tipo de reto siempre que sea basado en la obtención de *flags*.

6 Glosario

- **CTF**: Siglas en inglés "*Capture the flag*" o "*Capturar la bandera*". Modalidad de juego que consiste en intentar atrapar el máximo número de banderas o hitos.
- **SQL:** Siglas en inglés de "*Structure Query Language*" es un lenguaje de dominio específico utilizado para la administración de bases de datos relacionales.
- **XSS:** Del inglés "*Cross-site scripting*" es un tipo de vulnerabilidad propio de las aplicaciones Web que permite la inyección de código.
- **Jeopardy**: Traducción al español de *compromiso*. En el contexto de los retos de seguridad es la modalidad en la que se busca comprometer un sistema con vulnerabilidades.
- **Framework**: Herramienta o entorno de trabajo que sirve para enfocar una problemática específica, mediante artefactos y estructuras prediseñadas.
- **PEC**: Acrónimo de "*Prueba de Evaluación continua"*, son las entregas que se realizan en el aula virtual de una asignatura que permiten la evaluación de esta.
- **PDF**: Siglas en inglés de *Portable Document Format*. Es un formato estándar de almacenamiento para documentos digitales.
- **YAML**: Del acrónimo recursivo, que significa *YAML Ain't Markup Language* (otro lenguaje de marcado más). Es un formato de serialización de datos inspirado en XML y JSON.
- **URL**: Siglas en ingles de *Uniform Resource Locator* (Identificador de recursos uniforme), se utiliza para referenciar recursos en una red, por ejemplo, Internet.

7 Bibliografía

CFT TIME. CTF? WTF? (s.f.). Recuperado el 30 de Septiembre de 2018, de https://ctftime.org/ctf-wtf/

Collado, P. (17 de Julio de 2015). *Capture The Flag*. Recuperado el 02 de Julio de 2018, de Security Artwork: https://www.securityartwork.es/2015/07/17/capture-the-flag

CTFd. (06 de octubre de 2018). Obtenido de GitHub: https://github.com/CTFd/CTFd

ENISA. (2012). *On National and International Cyber Security Exercises - Survey, Analysis and Recommendations.*

Facebook Capture the Flag. (s.f.). Obtenido de GitHub: https://github.com/facebook/fbctf

HackTheArch. (06 de octubre de 2018). Obtenido de GitHub: https://github.com/mcpa-stlouis/hack-the-arch

Marinescu, P. (15 de junio de 2016). *YouTube*. Recuperado el 06 de octubre de 2018, de #HITB2016AMS CommSec Track D2 - Facebook Presents Capture The Flag: https://youtu.be/z_Xic03zor0

Morgan, S. (31 de Mayo de 2017). *Cibersecurity Ventures*. Obtenido de https://cybersecurityventures.com/jobs/

OWASP Juice Shop Project. (05 de Diciembre de 2018). Recuperado el 12 de Diciembre de 2018, de https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

Pablos, R. (26 de Febrero de 2014). *CERTSI Blog*. Recuperado el 29 de Septiembre de 2018, de https://www.certsi.es/blog/ctf-entrenamiento-seguridad-informatica

Red Hat. (s.f.). *¿Qué es Docker?* Recuperado el 23 de 11 de 2018, de https://www.redhat.com/es/topics/containers/what-is-docker

8 Anexos

8.1 Resolución de un ejercicio de ejemplo

A continuación, se muestra, desde el punto de vista de un participante del CTF, como sería el procedimiento desde la resolución de uno de los retos planteados hasta el registro del flag obtenido.

El primer paso, es el establecimiento de la conexión con un navegador web, tanto con el portal de CTFd como de la web de Juice Shop.

CTFd estará escuchando en el puerto 8000:

Ilustración 17 Captura de la página inicial de CTFd

Juice Shop, por otro lado, escuchará en el puerto 3000:

Ilustración 18 Captura de la página inicial de OWASP Juice Shop

Para este ejemplo, se va a utilizar el usuario administrador de CTFd que ha sido de alta en el capítulo *Configuración del reto en CTFd*. El reto será el titulado *Admin Section*:

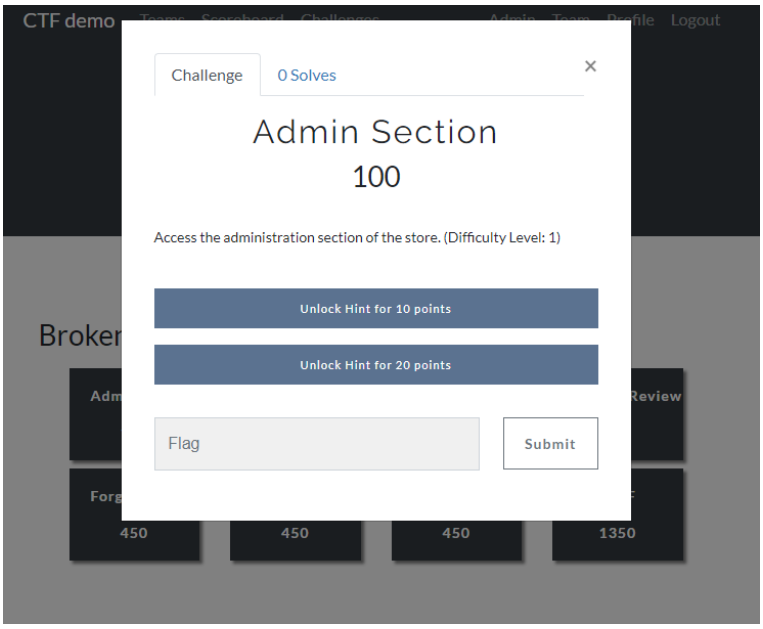


Ilustración 19 Captura de la descripción de un reto en CTFd

Según la descripción de este reto, hay que conseguir acceso a la sección de administración de la tienda.

La solución a este reto es acceder a la URL http://<servidor>:3000/administration

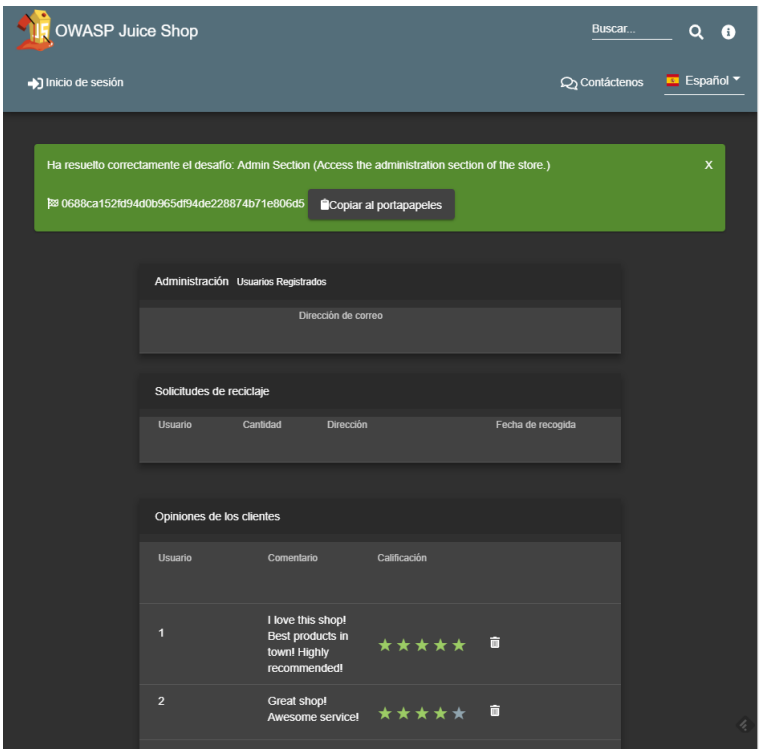


Ilustración 20 Captura que muestra la correcta resolución de un reto en OWASP Juice Shop y su flag asociado

En la parte superior se muestra un aviso indicando la resolución del reto y el flag correspondiente. Una vez copiado en el portapapeles, cambiar a CTFd para registrarlo:

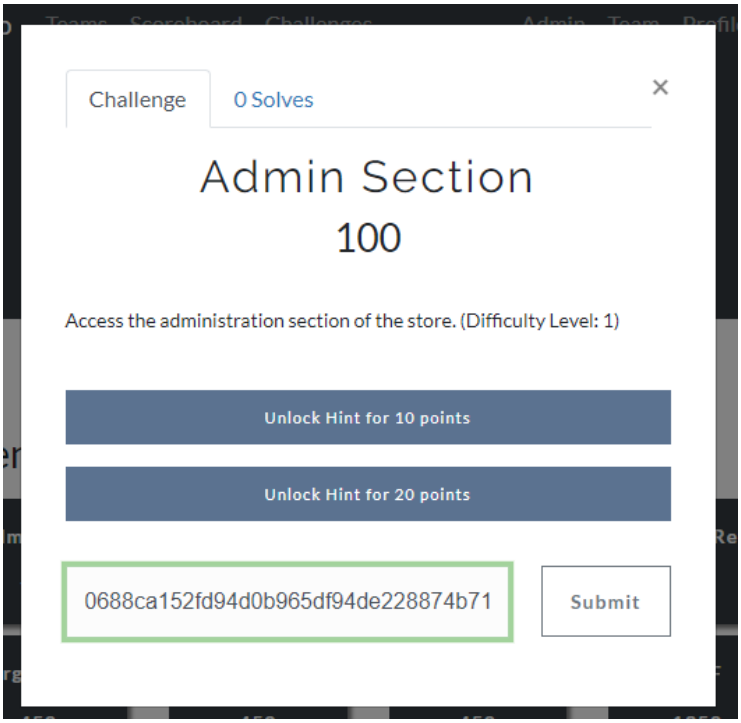


Ilustración 21 Captura del procedimiento de registro de un flag en CTFd

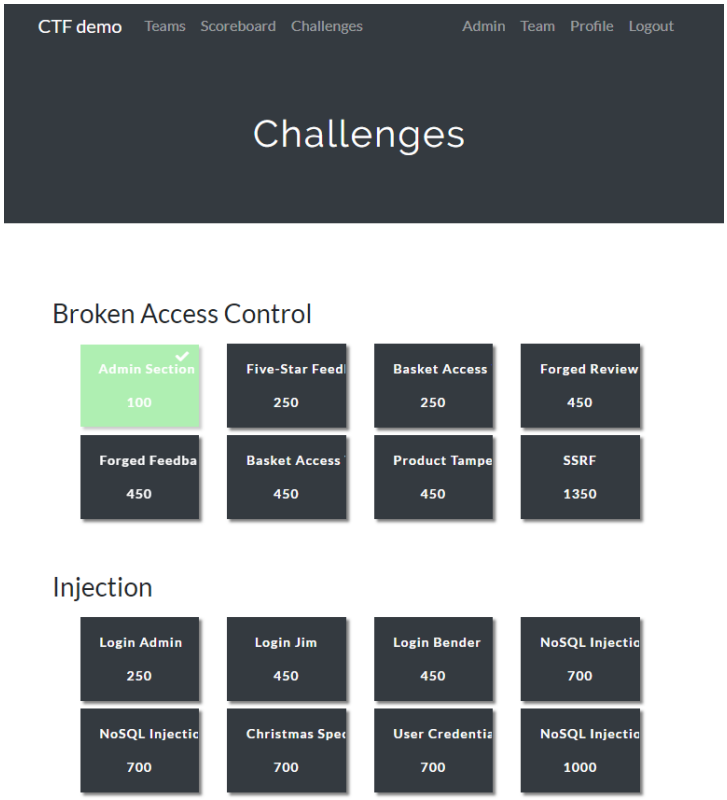


Ilustración 22 Captura que muestra el reto en verde como resuelto