EL ÚLTIMO HACKER: UN CTF INSPIRADO EN AVATAR

NICOLÁS ALMAGRO SORIA
ASIR 05/2025
2º Curso

Declaración de Autoría

Yo, Nicolás Almagro Soria, declaro formalmente que el presente proyecto titulado "El último hacker: un CTF inspirado en Avatar" es original y producto de mi trabajo, dedicación y esfuerzo durante el período de desarrollo correspondiente al proyecto final de ciclo de Administración de Sistemas Informáticos en Red. Todos los elementos, ideas, y aportaciones presentes en este proyecto son el resultado de mi investigación, diseño, implementación y evaluación.

Cualquier recurso externo utilizado, ya sea información, código fuente, imágenes u otros, ha sido adecuadamente citado y referenciado.

Entiendo que cualquier intento de plagio o falsificación de información en este proyecto conllevará consecuencias académicas y éticas, por lo cual asumo la responsabilidad de mi trabajo.

Fecha: _____

Firma: _____

RESUMEN

El presente Trabajo de Fin de Grado se desarrolla en torno a la construcción de una máquina con distintos retos de hacking ético y la ciberseguridad, del tipo Capture The Flag (CTF), que consiste en la preparación de entornos donde practicar los retos diseñados, para que los competidores puedan aprender y desarrollar distintas habilidades según el reto que se esté resolviendo en ese momento. Dentro del mismo podemos también incluir entender nuevas herramientas, aumentar conocimientos de la ciberseguridad, proporcionar una forma de entrenamiento…

Primero definiremos los CTF, estos son competiciones diseñadas para poner a prueba las habilidades de los participantes en diversas áreas de la ciberseguridad y las telecomunicaciones seguras. Estas competiciones que se han vuelto populares tanto en entornos educativos como profesionales, sirven como herramientas de aprendizaje y evaluación. [1]

Según esta categoría se han desarrollado un conjunto de 6 retos, que se explicarán a continuación, junto al conocimiento que aportan:

1) El servicio FTP: Obtener información de servidores sin tener un usuario en el propio sistema.
2) Archivos ZIP: Crear diccionarios de claves y lanzarlos con el método de fuerza bruta a archivos cifrados con contraseña.
3) Página web: Descifrar cadenas cifradas en distintos tipos de cifrados y obtener información del código de una página web.
4) El servicio SSH: Revisión de archivos del sistema y descarga de estos de manera segura y sin que el sistema lo detecte.
5) Estenografía: Ocultar información en los metadatos de una imagen de manera sencilla y como obtener esos metadatos de una imagen modificada
6) Cifrado

Palabras clave: CTF, ciberseguridad, flag o bandera, servicio y servidor.

ÍNDICE

INTRODUCCIÓN

1.1 CONTEXTO

En un mundo cada vez más digital, con una frecuencia cada vez más alta de nuevas creaciones o innovaciones tecnológicas, ha cambiado de manera muy profunda como interactuamos, trabajamos o vivimos en el mundo. La abundancia de dispositivos inteligentes, la comunicación constante y la progresiva dependencia de sistemas digitales han creado un ecosistema complejo y dinámico, donde la información se ha convertido en el mayor valor incalculable.

Sin embargo, esta misma velocidad de creación o innovación ha aumentado exponencialmente la superficie de ataque para los atacantes o "hackers". Los delincuentes que pueden estar motivados por distintos motivos, desde enriquecerse económicamente hasta espionajes a través de medios electrónicos, han diseñado y creado complejas técnicas para explotar las vulnerabilidades de los sistemas y redes informáticas. La complicación de estas amenazas, unida a la velocidad con la que se detectan nuevas vulnerabilidades, ofrece un desafío constante a los profesionales de la ciberseguridad. No solo se trata de proteger información confidencial, sino también de garantizar la integridad y la disponibilidad de los sistemas críticos en momentos de necesidad.

1.2 PROPÓSITO

Este Trabajo Fin de Ciclo (TFC) se centra en el diseño, desarrollo e implementación de un CTF temático enfocado en las vulnerabilidades de los servicios que ofrece un servidor web con el objetivo de proporcionar una experiencia de aprendizaje práctica y atractiva para estudiantes de informática o principiantes en el mundo de la ciberseguridad.

Primero se explicará que es un CTF, este es una competición de seguridad informática o prueba de entrenamiento en la cual los contendientes tienen que resolver un conjunto de desafíos relacionados con seguridad informática o ciberseguridad. Estos retos pueden ser de distinto tipo:

- Criptografía: Implica descifrar o cifrar una parte de los datos.
- Esteganografía: La tarea consiste en encontrar información oculta en todo tipo de archivos.
- Binario: Ingeniería inversa o explotación de un archivo binario.
- Web: Explotación de páginas web.
- Pwn: Atacar un servidor. [2]

El objetivo principal es capturar banderas o "flags" que son la prueba de que se ha completado con éxito un reto, y cuentan puntos para el resultado final. Existen distintas modalidades de CTF, cada uno dirigida con un enfoque y una forma de competencia. Las más comunes son:

1. CTF de Estilo Jeopardy: Los participantes deben conseguir las banderas de los retos propuestos por los organizadores de la competición. [3] Figura 1

Figura 1 Equipo participando en una competición de CTF en la DEF CON 17

2. CTF de Estilo Ataque/Defensa: Los participantes son divididos en grupos y se deben de encargar de defender su sistema mientras atacan el sistema de otros grupos y consiguen las correspondientes banderas. [3]
3. CTF de Estilo Mixto: Una combinación de elementos de los estilos Jeopardy y Ataque/Defensa. Los equipos resuelven desafíos para ganar puntos y pueden usar esos puntos para mejorar sus capacidades defensivas o atacantes para atacar a otros equipos. [3]

Como se ha comentado anteriormente, el CTF es temático y el tema es Avatar: La Leyenda de Aang [4]. Esta es una serie animada que sigue las aventuras de Aang, un niño de doce años y el último superviviente de los Nómadas Aire. La historia se desarrolla en un mundo conformado por 4 naciones, representando cada una un elemento natural: agua, tierra, fuego y aire. El Avatar, una persona capaz de dominar los 4 elementos es la persona encargada de mantener el equilibrio entre las naciones y el equilibrio entre el mundo y reino de los espíritus.

2. JUSTIFICACIÓN DEL PROYECTO Y MOTIVACIÓN

2.1 Justificación de la elaboración del proyecto

La necesidad de profesionales capacitados en ciberseguridad justifica la creación de un Capture The Flag (CTF). Los CTF ofrecen una manera atractiva y distinta de aprender y practicar habilidades muy necesarias en el ámbito de la seguridad, siendo mejor en algunos casos a métodos más tradicionales de enseñanza.

Este trabajo ayuda a la formación de personas capacitadas mejor preparadas para hacer frente a los retos del mundo digital actual, ofreciendo una experiencia práctica que refuerza el aprendizaje teórico. Además, un CTF puede ser útil como herramienta de evaluación, ya que permite identificar partes de mejora en la formación y proporciona un conocimiento inmediato.

La naturaleza competitiva del CTF promueve el aprendizaje colaborativo y la resolución de problemas de equipo, habilidades que son muy importantes en el mundo laboral actual.

2.2 Motivación de la realización del proyecto

La motivación principal a hacer este proyecto es colaborar en la mejora de la educación de la ciberseguridad a través de recursos prácticos, atractivos e innovadores. La creación de un CTF permite:

- Desarrollar habilidades: Los participantes ponen en uso conocimientos teóricos como programación, redes, criptografía y análisis de vulnerabilidades de sistemas y servicios.
- Fomentar aprendizaje activo: Solucionar desafíos mejora en el pensamiento crítico y creativo.
- Promover el trabajo en equipo: En muchos de los retos es necesario la colaboración entre distintos participantes, lo que mejora en sí las relaciones.
- Satisfacción personal: Diseñar y desarrollar un CTF, y ver que otros participantes la superan, me llena orgullo.

3. OBJETIVOS Y ALCANCE

En el siguiente apartado se explicarán los objetivos y las limitaciones que se han alcanzado con el desarrollo de este Trabajo de Fin de Grado.

3.1 Objetivo principal

El objetivo principal es la creación y desarrollo de un sistema educativo interactivo con diseño de un Capture The Flag (CTF) dirigido principalmente a principiantes en el campo de ciberseguridad y el mundo del hacking ético. El sistema facilitará el aprendizaje y práctica de aptitudes básicas de ciberseguridad mediante retos distintos.

3.2 Objetivos específicos

Los siguientes objetivos forman parte del objetivo principal presentado:

- Instalación, configuración y utilización de distintos servicios administrados en un servidor.
- Creación de un formulario basado en PHP que hará de plataforma CTF y que recoge los datos y los comprueba con una base de datos.
- Creación y administración de una base de datos.
- Configuración y utilización de sistemas Linux Ubuntu Server.
- Aprendizaje de creación de vulnerabilidades y como detectarlas y solucionarlas.
- Diseño de una empresa que enseña sobre la ciberseguridad

Las limitaciones a las que se han enfrentado durante de la del proyecto son:

- Conocimientos técnicos: Crear un CTF y crear una plataforma para registrar banderas requiere conocimiento en distintos ámbitos. La falta de experiencia en algunos de estos ha limitado la calidad en algunos de los retos.
- Recursos limitados: Como material principal se ha dispuesto del ordenador del alumno, el cual no posee unas características más potentes que pueden ser utilizados para la realización del CTF.
- Tiempo: Diseñar y desarrollar un CTF es un proceso que utiliza mucho tiempo. La creación de los desafíos y pruebas además de sus comprobaciones requieren de un tiempo que ha sido limitado por la realización de otras responsabilidades.

4. ESTADO DEL ARTE/MARCO TEÓRICO

4.1. Introducción

Las plataformas de CTF han alcanzado una gran importancia como herramientas pedagógicas en el campo de la formación de ciberseguridad, ofreciendo un medio interactivo y desafiante para que tanto como personas principiantes o personas más profesionales pongan a prueba, experimenten y mejoren sus habilidades. La exigencia de medios educativos eficientes, accesibles y adaptados a diferentes niveles de experiencia ha aumentado de forma significativa y se han buscado diferentes soluciones que se han desarrollado y publicado para hacer frente a esta demanda.

Existen distintos tipos de plataformas CTF:

4.2. Plataformas de código abierto

CTFd: Esta es una plataforma muy popular y muy utilizada para crear o publicar CTFs. Permite gestión individual y de equipos, es también adecuada para que estudiantes y profesionales practiquen desafíos simulados de seguridad de la información. [5]

Root Me: Sitio web que ofrece desafíos en ámbitos como criptografía o vulnerabilidades de manera legal y gratis.

4.3. Plataformas comerciales

Hack The Box: Es la plataforma más utilizada en la industria debido a la gran variedad de desafíos de ciberseguridad y laboratorios virtuales. Ofrece máquinas virtuales a las que se pueden acceder mediante VPN donde practicar retos web, móviles entre otros. [5]

TryHackMe: Plataforma muy recomendada para iniciantes en el campo de ciberseguridad. Además de proporcionar desafíos para resolver, también ofrece guías y explicaciones para mejorar la comprensión de vulnerabilidades y técnicas de explotación. [5]

4.4. Plataformas educativas

PicoCTF: Es un espacio de práctica no competitivo donde se puede explorar y resolver desafíos de competencias lanzadas anteriormente, encontrar desafíos nuevos y no revelados anteriormente y construir un base de conocimiento de habilidades de ciberseguridad en entornos seguros. [6]

OverTheWire: Página diseñada para aprender temas de seguridad mediante pruebas de capturar la bandera desde niveles básicos a niveles más profesionales.

4.5. Diseño de los desafíos en CTF

Al diseñar desafíos eficientes hay que tener en cuenta diversos elementos, como la dificultad, que no sean muy similares a otros y las distintas habilidades que se necesitan para superarlos. Los retos pueden ser de distintos tipos, algunos son:

- Web: Desafíos con vulnerabilidades en aplicaciones web como Inyección SQL.
- Redes: Analizar el tráfico, sniffing o explotación de protocolos de red.
- Criptografía: Retos en los que los que los participantes descifren mensajes o rompan algoritmos de cifrado.
- Reversa: Desafíos que implica analizar código binario para descubrir vulnerabilidades.

5. ANÁLISIS Y DISEÑO

A continuación, se presentará el análisis detallado de los requisitos y el diseño propuesto para el Trabajo de Fin de Grado.

5.5 Análisis de Requisitos

El análisis de requisitos es necesario para que el proyecto cumpla con las expectativas y con los objetivos educativos. A continuación, se detallarán más profundo:

- Selección de equipo por parte de los usuarios: Los usuarios deben poder elegir un equipo para poder participar en la competición.
- Registro de banderas: Los participantes pueden registrar las banderas que han conseguido.
- Sistema de puntuación: La plataforma calcula y suma las puntuaciones conseguidas por cada equipo.
- Soporte para diferentes tipos de desafíos: La plataforma acepta diversos tipos de desafíos como criptografía o web.

5.6 Diseño de la solución propuesta

La arquitectura de la plataforma CTF se divide en distintas capas:

- Presentación: Interfaz de usuario web donde se explica de qué trata la CTF, se puede seleccionar el equipo con el que participar y registrar las banderas.
- Para la página web se utiliza código HTML, CSS y PHP.
- Datos: Base de datos para almacenar la información de los equipos, sus puntuaciones, las banderas y el resultado.
- Máquinas virtuales: Los equipos virtualizados donde se realizará la CTF y el equipo virtualizado que contendrá el formulario con la base de datos.
- Red: Todas las máquinas, es decir, la maquina atacante, la máquina vulnerable y la máquina con la plataforma para registrar banderas, se encuentran en una red NAT. Dentro de esta pueden comunicarse todas entre sí, además de disponer de conexión a internet de ser necesario. Figura 2

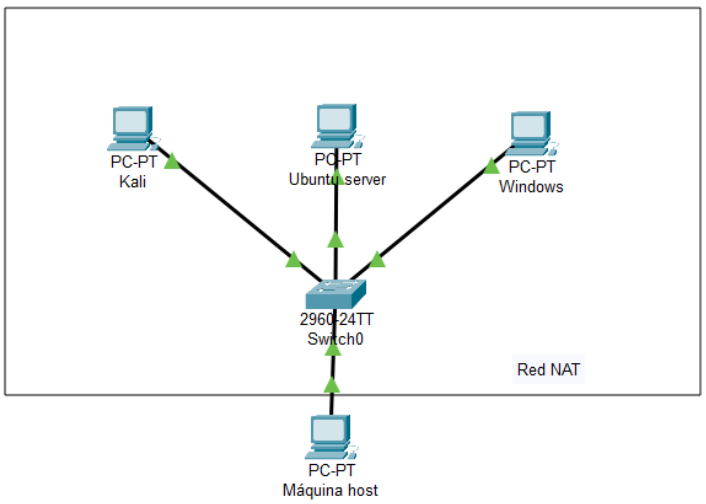


Figura 2 Mapa CPT de una Red NAT

6. FASES Y SECUENCIACIÓN

6.1. Fases del proyecto

1ª Etapa: Investigación. Búsqueda de información sobre la creación de CTF: Sistemas operativos que se pueden llegar a utilizar, vulnerabilidades que se pueden crear en base a los requisitos necesarios y material para el diseño de empresa que hay que realizar.

2ª Etapa: Creación de los sistemas. Elección de un sistema de virtualización de equipos y selección de los sistemas operativos donde se crearán la CTF y la página web donde registrar las banderas. También se crearán las distintas máquinas.

3ª etapa: Servicios y vulnerabilidades. Elección, instalación y configuración de los servicios del servidor para las vulnerabilidades, además de introducir las banderas dentro de la máquina.

4ª Etapa: Formulario PHP y base de datos. Creación de una página web con los lenguajes de HTML, CSS y PHP. Esta contendrá un formulario donde se introducirán las banderas de la CTF y se comprobará con la base de datos.

5ª Etapa: Creación de la empresa: Esta etapa se hará a lo largo del proyecto. El objetivo de esta etapa es diseñar una empresa en base a los requisitos solicitados y que sea relacionada con el proyecto.

6.2. Diagrama de la realización del proyecto

Figura 3

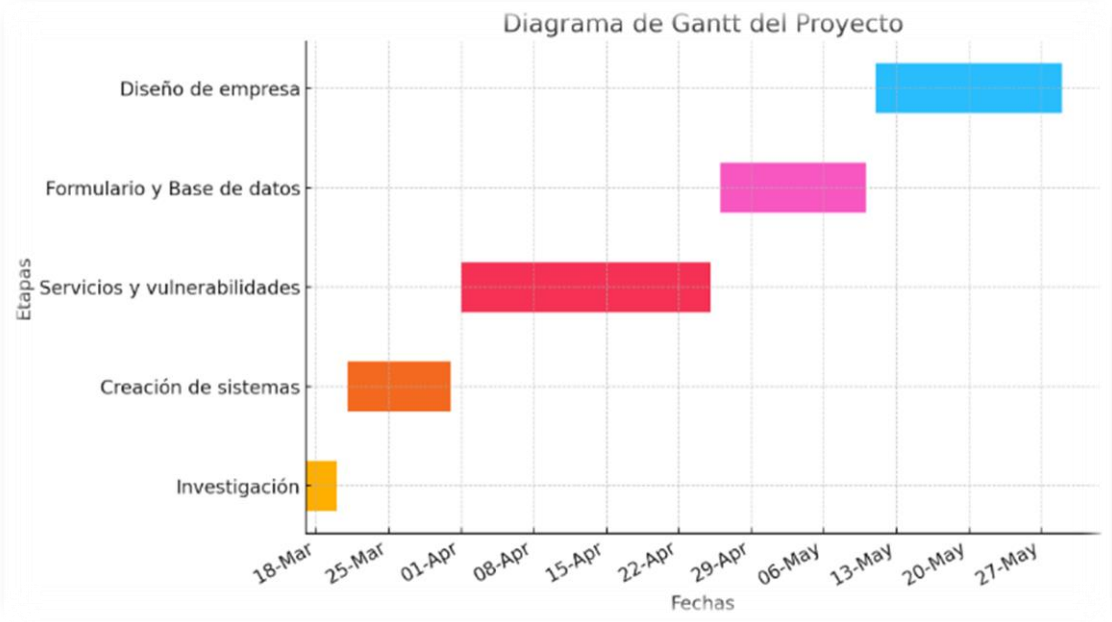


Figura 3 Diagrama de Gantt

7. METODOLOGÍA Y DESARROLLO

En este apartado se explicará el diseño, desarrollo e implementación de una plataforma de Capture The Flag (CTF) y una página web que será un formulario donde comprobar las banderas y las puntuaciones mientras se participa en el juego. El índice que seguirá para explicar toda la sección es el siguiente:

- Creación de máquinas virtuales
- Diseño, desarrollo e implementación de las flags
- Instalación de un servidor XAMPP y creación de la página web.

7.1. Creación de las máquinas virtuales

7.1.1. Marco teórico de las máquinas virtuales

Antes de empezar a explicar el proceso de creación, se explicará que es una máquina virtual. Existen dos tipos de máquinas virtuales, diferenciadas por su funcionamiento, las de sistema y las de proceso.

Una máquina virtual de proceso es aquella que en vez de emular un ordenador por completo, ejecuta procesos concretos como aplicaciones de manera aislada en su entorno de ejecución [7].

Una máquina virtual de sistema es aquella que emula a un ordenador completo. En otras palabras, es un software que se hace pasar por otro dispositivo como un ordenador, de manera que se pueden ejecutar otros sistemas operativos en su interior. Estos tiene su propio disco duro, memoria, tarjeta gráfica y otros componentes hardware aunque en este caso sean virtuales [7]

Aunque los componentes son virtuales, realmente sí que existen debido a que se toman de la máquina host o anfitrión. Aunque otros dispositivos no existen físicamente como los CD-ROM que solo llevan el contenido de una imagen ISO.

7.1.2. Elección del sistema de virtualización y del sistema operativo de la máquina vulnerable

Para la creación y uso de máquinas virtuales se ha elegido VirtualBox. Esta es una aplicación que sirve para crear máquinas virtuales con instalación de sistemas operativos. Lo que quiere decir es que independientemente del sistema operativo (Windows, GNU/Linux o MacOS) puede crear máquinas virtuales de cualquier otro sistema operativo y utilizarlo con los recursos del sistema que está utilizando.

Esta aplicación puede servir para probar aplicaciones de otros sistemas sin necesidad de instalarlos en el ordenador o tener que comprar otro. También otros usos que tiene es comprobar la funcionalidad de otros sistemas operativos y la instalación de aplicaciones peligrosas sin que afecte al ordenador anfitrión. [8]

Se ha elegido la aplicación de VirtualBox por los siguientes motivos:

- Gratuito y de código abierto: Lo que permite usar sin ningún coste.
- Fácil de usar: Interfaz gráfica intuitiva que facilita la creación y administración de máquinas virtuales.

- Buen rendimiento: Las máquinas virtuales en VirtualBox realizan un buen rendimiento para la mayoría de tareas, aunque este se puede ver reducido por las limitaciones de la máquina anfitrión.

Debido a que la máquina virtual necesita un Sistema Operativo (SO) se buscó uno para esta. Se eligió el sistema operativo de Ubuntu, y debido a que queremos simular que la máquina es un servidor, se eligió más concretamente, Ubuntu Server 20.04 LTS, una versión ya vista y utilizada durante la realización del curso.

7.1.3. Descarga de las ISO e instalación en las máquinas virtuales

Para crear la creación de la máquina vulnerable en VirtualBox se necesitará la Imagen del Sistema Operativo (ISO). Para ello se accede a la página web oficial de Ubuntu y descargaremos la ISO que buscamos. Figura 4

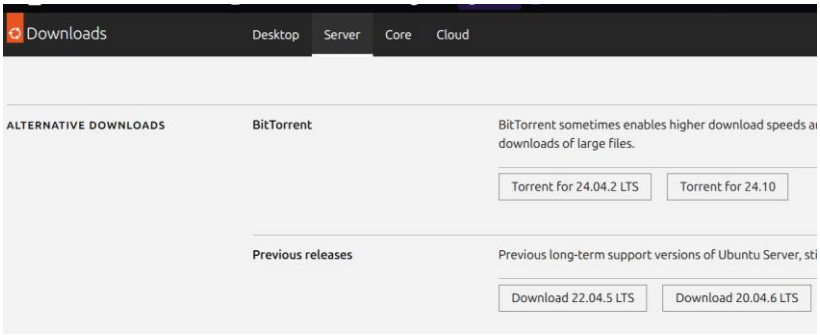


Figura 4 Página oficial de Ubuntu

Una vez instalada la ISO, se accede a VirtualBox. Dentro de este, se hace clic en “Nueva”, para crear una máquina virtual nueva y se configuran las características de Sistema, Almacenamiento y Red. Las características elegidas se basan en lo que será necesario para la máquina y sin superar el límite de la máquina host. Figura 5

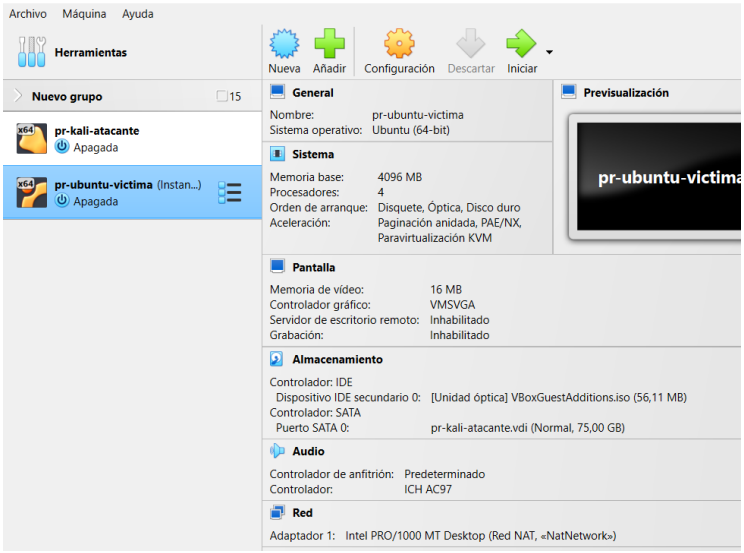


Figura 5 Configuración de la máquina virtual de Ubuntu

Por último, para terminar la creación de las máquinas virtuales, se inicia la máquina y se sigue el proceso de instalación del sistema operativo. Por último, una vez finalizada la instalación se inicia sesión con el usuario creado durante la instalación, para comprobar que el sistema operativo se ha instalado correctamente. Figura 6

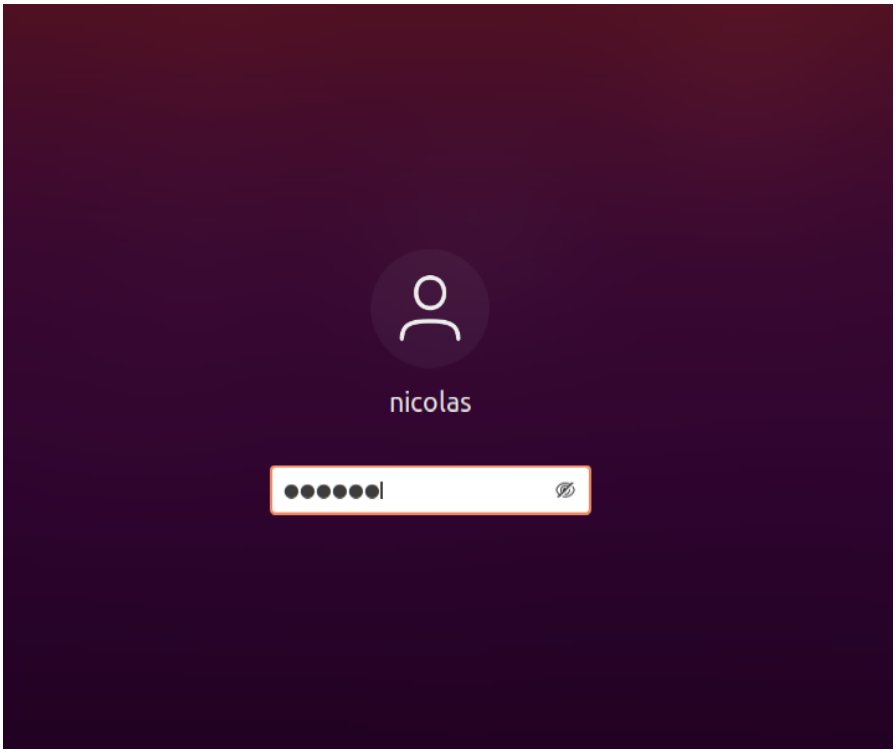


Figura 6 Inicio de sesión del servidor de Ubuntu

Para la simulación de la máquina atacante se utilizará un sistema operativo que cuenta con todas las herramientas y aplicaciones necesarias para realizar las vulnerabilidades durante el ataque. Se ha elegido el sistema operativo Kali, sistema operativo que también se utilizó durante la realización de las clases, pero que, además también se ha elegido debido a que es un sistema diseñado específicamente para auditorias de seguridad y pruebas de penetración.

7.1.4 Marco teórico de los adaptadores de red de VirtualBox

Ahora como último paso de la configuración de máquinas virtuales necesitaremos que se puedan conectar entre ellas y enviarse distintos comandos.

Actualmente en VirtualBox existen siete tipos de configuraciones de adaptador de red disponibles, que son:

- NAT: Network Address Translation, es decir, Traducción de Direcciones de Red. Este permite a la máquina virtual conectarse a Internet, pero no puede ver a otras máquinas en la red virtual. [9]

- Adaptador puente: Este adaptador permite que la máquina virtual tenga conexión a Internet además también le permite conectarse con otras máquinas, ya que sale a Internet con la IP de la máquina host. [9]
- Red interna: Adaptador totalmente opuesto al adaptador NAT, ya que con este configurado no tienes conexión con Internet, pero puedes comunicarte con cualquier dispositivo que se encuentre en la red. [9]
- Adaptador Solo-Anfitrión: En este modo de conexión, la máquina virtual solo puede verse con la máquina anfitriona y viceversa. Además, si la máquina anfitriona tiene conexión a Internet, la máquina virtual también la tendrá. [9]
- Red NAT: Es el mismo adaptador que NAT, pero con la diferencia que crea una red virtual, con la que todas las máquinas conectadas a esa red y con ese adaptador podrán tener conexión a Internet y además poder verse entre ellas. [9]
- Controlador genérico: Este adaptador permite que el usuario elija su propio adaptador para la máquina virtual, lo que permite que se puedan usar adaptadores de red no disponibles en VirtualBox. [9]
- No conectado: Este es un adaptador desconecta a la máquina virtual de la red virtual. [9]

Para la realización de este proyecto se ha elegido utilizar una red NAT ya que se necesitaban conectar ambas máquinas y la máquina virtual vulnerable necesitaba la descarga y actualización de algunos servicios.

7.1.5 Creación de la red NAT

Para crear una Red NAT en VirtualBox se hace de la siguiente manera: se hace clic en "Herramientas" y seleccionamos "Redes NAT". Se vuelve a hacer clic en "Crear" y se le configura el rango de IPs privada que quiere que ofrezca la red. Por último, se configura el adaptador de red en todas las máquinas a "Red NAT". Figura 7

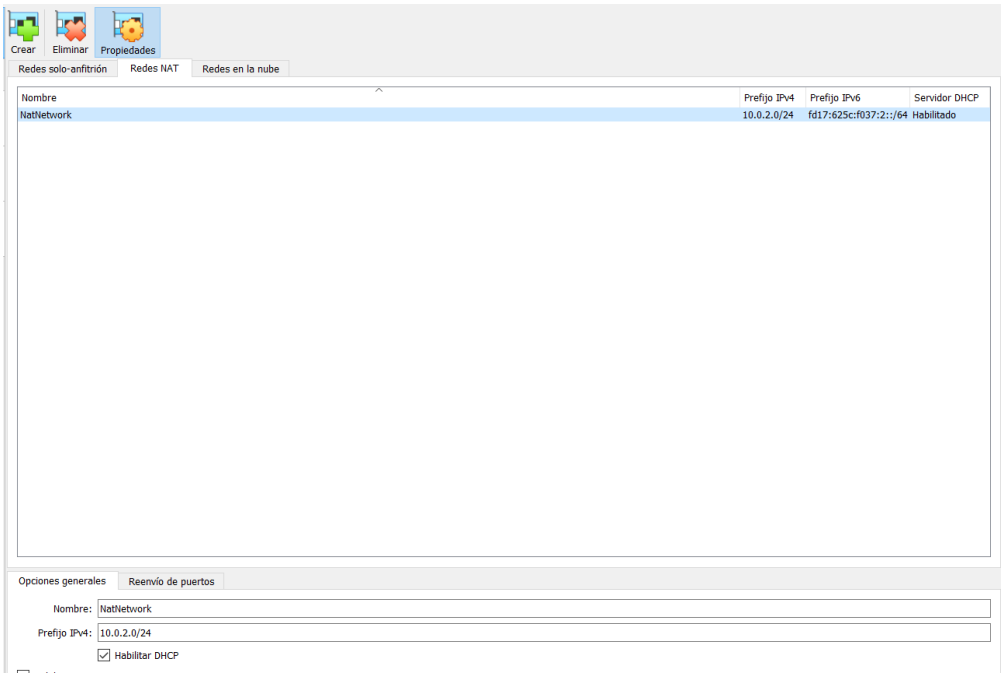


Figura 7 Creación de una red NAT

7.2. INSTALACIÓN DE SERVICIOS Y VULNERABILIDADES

Como siguiente paso a realizar en el Trabajo de Fin de Ciclo (TFC), se instalarán una serie de servicios a Ubuntu Server. El orden de instalación de los servicios será según se utilizarían en la realización del CTF. Así que se comenzará con el servicio de FTP.

7.2.1 Marco teórico del servicio FTP

El servicio File Transfer Protocol (FTP), también conocido como Protocolo de Transferencia de Archivos es un protocolo de la capa de Aplicación del modelo TCP/IP que facilita el uso compartido de ficheros entre sistemas conectados a redes TCP/IP. Este permite a los usuarios acceder a sistemas remotos y listar ficheros y directorios, transferir ficheros hacia o hasta el sistema remoto y realizar acciones adicionales como renombrar, borrar o cambiar permisos. Y todo esto independientemente del sistema operativo que utilice el usuario.

Existen diversos tipos de acceso a servidores FTP los cuales pueden usar los clientes:

- Acceso Anónimo: El usuario no necesita poseer una cuenta de usuario privada. Para poder utilizar esto en el servidor, este debe tener configurado que se pueda iniciar sesión de manera anónima. El nombre del usuario será Anonymous y no necesitará contraseña. Generalmente puede leer o copiar ficheros públicos, pero no puede acceder más allá del directorio principal del servidor.
- Usuario: Para poder acceder el usuario deberá iniciar sesión con su nombre de usuario y contraseña. En este tipo de conexión al usuario se le permitirá subir, descargar y modificar archivos.
- Invitado: Para este tipo de conexión el usuario necesita disponer de un usuario y una contraseña, pero no tendrá acceso a todos los archivos del servidor.

7.2.2. Primera bandera

Como servicio de FTP en el servidor se ha instalado VSFTPD. Este es uno de los servidores FTP más potentes y completos en Linux. Se ha elegido este servicio FTP debido a la sencillez de instalación y de uso. Para la instalación de este servicio utilizaremos el comando “apt install vsftpd”. Figura 8

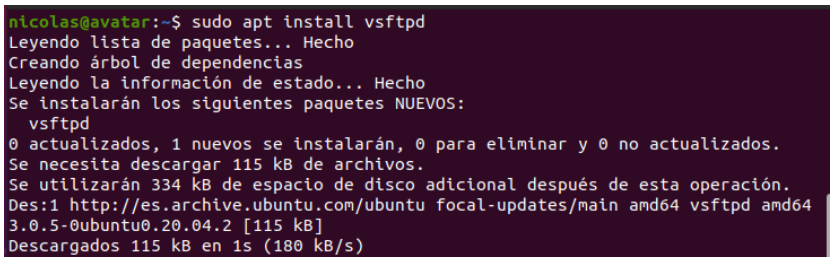


Figura 8 Comando para la instalación de VSFTPD

A continuación, se abre el archivo de configuración con un editor de texto, en este caso nano, la ruta “/etc/vsftpd.conf/”. En el archivo de configuración se accede al parámetro “anonymous_enable”. Este permite que los usuarios sin un usuario puedan iniciar sesión con el

usuario Anonymous. Para permitir el acceso anónimo se quita el comentario en el parámetro y se indica con un "Yes" que lo permita. Figura 9

Figura 9 Configuración de usuario anónimo

Ahora se realizan los dos archivos que se colocarán dentro de la carpeta del usuario anónimo dentro del servidor de FTP. El primer archivo con extensión ".txt", incluye la primera bandera del CTF (Flag{Aang-aprende-aire-control}) y un pequeño texto relacionado a la temática de esta CTF. Al final del texto se menciona el segundo archivo y partes de la contraseña para abrir ese archivo. Figura 10

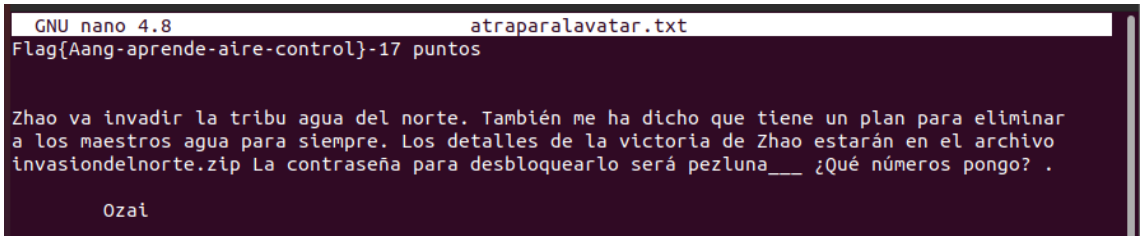


Figura 10 Archivo de texto con la primera bandera

7.2.3 Segunda bandera

El segundo archivo incluye un texto que será otra vez relacionado con la temática del CTF, además de incluir la segunda bandera (Flag{Aang-aprende-agua-control}) del CTF.

Para dificultar el acceso al archivo se decide bloquearlo por contraseña y ocultarlo. Para bloquear el archivo se utiliza zip (Formato de fichero utilizado para comprimir uno o más archivos en un solo elemento). El comando que se utiliza para comprimir el archivo y bloquearlo es "zip –encrypt nombredelfichero.zip archivo-original". Y para ocultar el archivo se renombra con un punto delante ".invasiondelnorte.zip". Después, se utiliza el comando "mv" para mover ambos archivos al directorio del servidor FTP.

Por último, se comprueba que tanto el servidor FTP como los archivos funcionan y están bien configurados. Para ello, primero se inicia sesión en la máquina Kali con el usuario anónimo y se

descargan los dos archivos. Como el segundo archivo estaba oculto se comprueba que aparece correctamente al ejecutar el comando “ls -a”, que sirve para listar los archivos incluyendo los ocultos.

Después para comprobar que funciona correctamente el zip con la contraseña, se crea un diccionario con las pistas de la contraseña con la herramienta crunch (herramienta para generar archivos de contraseñas). Para crear el diccionario utilizaremos el comando “crunch 10 10 –t pezluna%%% -o dic.txt”. La explicación breve del comando es “10 10” tamaño mínimo y máximo de la contraseña, “-t” el patrón que sigue la contraseña y “-o” indica que el diccionario generado se guarde en el archivo “dic.txt”.

Por último, se lanza con fcrackzip (programa de Linux para lanzar ataques de fuerza bruta) el comando “fcrackzip –D –p diccionario.txt invasiondelnorte.zip” para sacar la contraseña del zip. Una vez se ha comprobado que funciona todo correctamente se pasa al siguiente servicio.

7.2.4. Marco teórico del protocolo HTTP

Para esta tercera bandera se necesita un servidor con HTTP. Este es un protocolo de la capa de Aplicación del modelo TCP/IP que está diseñado para facilitar el acceso a los usuarios a información almacenada en servidores lejanos, también da acceso a otras páginas web del mismo servidor o de otros mediante hiperenlaces. Las páginas o documentos web son almacenados en un directorio denominado “sitio” y utilizado una página a modo de índice (index.html).

Para implementar el servicio se utiliza un servidor web. Este es un programa informático que utiliza HTTP para atender las peticiones de los clientes web y proporcionarles los recursos solicitados. Se ha elegido el servidor Apache como servidor web, ya que es el que se ha visto y utilizado durante el curso.

7.2.5 Instalación del servidor HTTP

Para instalarlo se utiliza el comando de “apt install apache2”. Figura 11

```
nicolas@avatar:~$ sudo apt install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
0 actualizados, 9 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.829 kB de archivos.
Se utilizarán 7.976 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Figura 11 Comando de instalación del servidor Apache en Ubuntu

A continuación, se configura la página que se mostrará. Figura 12

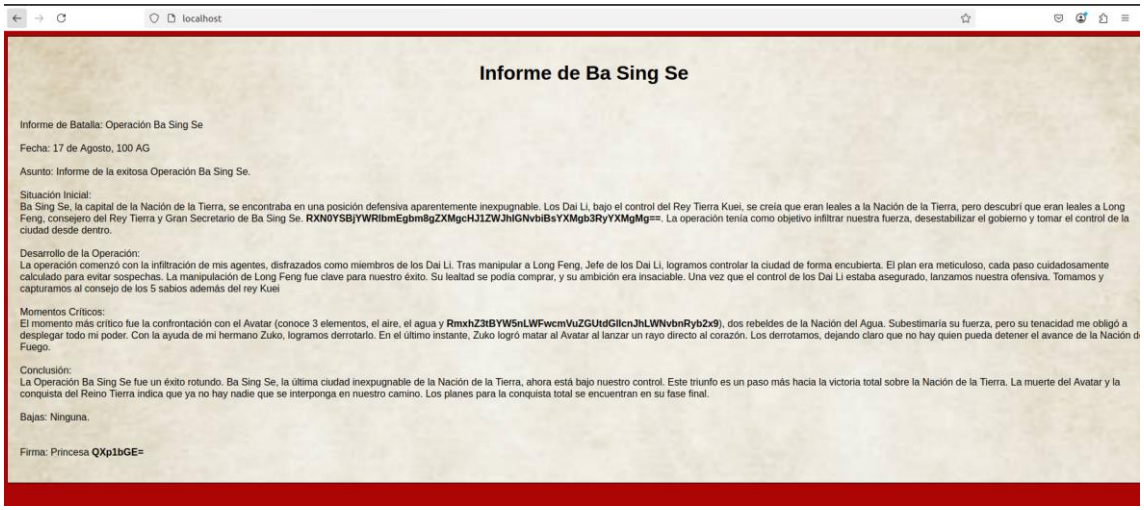


Figura 12 Página web utilizada para la tercera bandera

Seguidamente se explica un poco más el código de la página. La página se pensó en una carta informando del estado de una ciudad de la serie después de un ataque. Por ello, se metió todo el contenido dentro de un contenedor y se puso una imagen de fondo que se repitiese hasta rellenar el contenedor para dar la sensación de una carta de la época. El resto de la página está en un color rojo similar al color de la nación al que es enviada la carta.

Dentro de la carta se incluyen tres cadenas codificadas en Base64. La primera cadena de la página es una cadena de relleno, la segunda cadena contiene la bandera (Flag{Aang-aprende-tierra-control}) y la tercera y última cadena es un usuario de la máquina vulnerable, que utiliza el nombre de un personaje de la serie.

Base64 es un sistema de numeración posicional que utiliza 64 como base. Es la mayor potencia que puede ser representada usando únicamente los caracteres imprimibles de ASCII. Esto ha propiciado su uso para codificación de correos electrónicos, PGP y otras aplicaciones [10]. Para cifrar las cadenas se ha utilizado la página web CyberChef. Esta es una herramienta online que permite la codificación y descodificación de manera sencilla, sin necesitar utilizar múltiples herramientas ni utilizar lenguajes de programación para realizar diferentes acciones. Cyberchef está orientado a un público más técnico, pero también es ideal para estudiantes y gente no tan técnica en diferentes métodos de cifrado. [11]

La contraseña del usuario dado en la cadena se encuentra en un comentario de código de la página. Para poder leer el código se debe hacer los siguiente, hacer clic con el botón derecho sobre la página web y en el menú desplegado clicar sobre la opción “Inspeccionar”. A continuación, se abrirá una ventana lateral donde podremos ver el código de la página.

Como último paso se realizará la comprobación de que funciona correctamente. Se hace accediendo a la máquina Kali y en el navegador se coloca la dirección de la máquina Ubuntu y el puerto 80, confirmado que aparece la página web. Por último, se comprueba si se puede inspeccionar el contenido de la página para saber que se puede obtener la contraseña.

7.2.6. Marco teórico del protocolo SSH

Para esta cuarta bandera se utiliza el protocolo SSH. SSH (Secure Shell) es un protocolo de capa cuatro del modelo TCP/IP que permite el acceso remoto a una máquina, a través de un canal seguro, ya que encripta la información. Este protocolo es utilizado para realizar la conexión con servidores, debido que el protocolo es más seguro que otros más antiguos como telnet.

El protocolo SSH (Secure Shell) está basado en el modelo de arquitectura cliente/servidor para establecer conexiones seguras. Las tres partes que componen la arquitectura son:

- Cliente SSH: Es la aplicación que se utiliza para conectarse a un servidor remoto. Los diferentes clientes SSH en los sistemas operativos son OpenSSH en sistema Linux o Putty en sistemas Windows. [12]
- Servidor SSH: Se ejecuta el servidor remoto al que se quiere acceder. Este servidor está configurado para aceptar conexiones SSH y autenticar a los usuarios. [12]
- Autenticación: Cuando el usuario se intenta conectar a un servidor remoto, el cliente SSH y el servidor SSH inician un proceso de autentificación. Esto normalmente implica un nombre de usuario y una contraseña, aunque también puede ser una clave SSH. [12]

7.2.7. Instalación del servidor SSH

Se realiza la instalación del servicio, ya que la idea es que el atacante utilice el servicio para probar el usuario y contraseña que ha encontrado previamente.

Para implementarlo se instala openssh-server. Esto se realiza con el comando “apt install openssh-server”. Figura 13

```
nicolas@avatar:~$ sudo apt install openssh-server
[sudo] password for nicolas:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  ncurses-term openssh-sftp-server ssh-import-id
Paquetes sugeridos:
  molly-guard monkeysphere ssh-askpass
Se instalarán los siguientes paquetes NUEVOS:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 actualizados, 4 nuevos se instalarán, 0 para eliminar y 11 no actualizados.
Se necesita descargar 689 kB de archivos.
Se utilizarán 6.018 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
```

Figura 13 Comando para la instalación del servidor de OpenSSH

Posteriormente a instalar el servidor, se crea el usuario que se dio en la página web. Para hacerlo se utiliza “adduser Azula”. Después, se introducen los datos del usuario y se configura su contraseña. Figura 14

```
root@naciondelfuego:/home/nicolas# adduser Azula --force-badname
Allowing use of questionable username.
Adding user `Azula' ...
Adding new group `Azula' (1001) ...
Adding new user `Azula' (1001) with group `Azula' ...
Creating home directory `/home/Azula' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for Azula
```

Figura 14 Creación de un usuario en Ubuntu

Una vez creado el usuario, se cambia al directorio principal del usuario recién creado. Dentro de este se crea un archivo llamado “bss.txt”. Este en su interior contiene la cuarta flag.

Cuando se creó la máquina virtual del servidor, se instaló una interfaz gráfica para facilitar el trabajo. Debido a esto, cuando se arrancaba la máquina, permitía elegir directamente con qué usuario se empezaba, lo que revelaba los nombres de usuario. Para solucionarlo, se abre con un editor de texto la configuración del administrador de sesión y se deshabilita que aparezca al inicio la lista de usuarios del sistema. Figura 15

```
  GNU nano 4.8              /etc/gdm3/greeter.dconf-defaults              Modified
# picture-options='zoom'
#  - Or no background at all
[org/gnome/desktop/background]
# picture-options='none'
# primary-color='#000000'

# Login manager options
# =====================
[org/gnome/login-screen]
#logo='/usr/share/images/vendor-logos/logo-text-version-128.png'

# - Disable user list
 disable-user-list=true
# - Disable restart buttons
```

Figura 15 Configuración para deshabilitar los usuarios

7.2.8. Quinta bandera

En esta bandera se utiliza el método de esteganografía. Esta es la práctica de ocultar información dentro de otro mensaje u objeto físico para evitar su detección, los portadores. Actualmente se puede usar para ocultar cualquier tipo de archivo digital, como texto, imágenes, vídeos o audios. Luego dichos datos ocultos se extraen en su destino. [13]

Para ocultar el mensaje se ha utilizado la herramienta de exiftool. Exiftool es una herramienta de línea de comandos gratuita y de código abierto que se utiliza para leer, escribir y editar metadatos en una amplia gama de tipos de archivos. [14]

Los metadatos son “datos” sobre otros datos. En general, un grupo de metadatos se refiere a un grupo de datos que describen el contenido informativo de un objeto al que se denomina recurso. [15]

Exiftool se puede utilizar para varias tareas entre ellas:

- Extraer información de los metadatos de los archivos. Esta información puede ser muy útil para determinar la autenticidad de un archivo, la ubicación geográfica de una imagen o un vídeo, o para identificar el dispositivo que se utilizó para crearlo.
- Editar los metadatos de los archivos. Esto puede ser útil para corregir errores o para añadir información adicional.
- Escribir metadatos en nuevos archivos. Esto puede ser útil para añadir información adicional a los archivos, como el nombre de autor o la fecha de creación.

Para instalarlo se ha utilizado el comando “apt install exiftoll”, y el comando que se ha utilizado para añadir información a los metadatos de la imagen ha sido “exiftool –sección=”mensaje” imagen”. Figura 16

```
nicolas@naciondelfuego:~$ exiftool -UserComment="Flag{Aang-aprende-fuego-control}" bss.jpeg
    1 image files updated
nicolas@naciondelfuego:~$ exiftool -Description="User:Ozai" bss.jpeg
    1 image files updated
nicolas@naciondelfuego:~$ exiftool -Keywords="Passwd:ReyF*nix-3**" bss.jpeg
    1 image files updated
```

Figura 16 Inserción de los metadatos en la imagen

La imagen con los mensajes se ha movido al directorio del usuario Azula, ya que es donde debe encontrarlo el atacante. Figura 17

```
root@naciondelfuego:/home/nicolas# exiftool bss.jpeg
ExifTool Version Number         : 11.88
File Name                       : bss.jpeg
Directory                       : .
File Size                       : 14 kB
File Modification Date/Time     : 2025:04:23 16:48:43+00:00
File Access Date/Time           : 2025:05:20 17:03:12+00:00
File Inode Change Date/Time     : 2025:04:23 16:48:43+00:00
File Permissions                : rw-rw-r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 1
Y Resolution                    : 1
Resolution Unit                 : None
Y Cb Cr Positioning             : Centered
Exif Version                    : 0232
Components Configuration        : Y, Cb, Cr, -
User Comment                    : Flag{Aang-aprende-fuego-control}
Flashpix Version                : 0100
Color Space                     : Uncalibrated
Current IPTC Digest             : d3bb6a1eeeab261e7c8c4d738a1ac018
Keywords                        : Passwd:ReyF*nix-3**
Application Record Version      : 4
XMP Toolkit                     : Image::ExifTool 11.88
Description                     : User:Ozai
Image Width                     : 300
```

Figura 17 Metadatos de la imagen modificada

7.2.9. Marco teórico del cifrado simétrico

Para la última bandera del CTF se utilizará el cifrado simétrico. El cifrado es el proceso de transformar un texto sin formato legible en un texto cifrado ilegible para ocultar datos sensibles a usuarios no autorizados.

Casi en todos los dispositivos lo que hace la gente para proteger los datos y las comunicaciones se basa en el cifrado.

El cifrado simétrico, también conocido como criptografía de clave simétrica o cifrado de clave secreta, es uno de los métodos principales de cifrado junto con el cifrado asimétrico. El cifrado simétrico funciona creando una única clave compartida para cifrar y descifrar datos confidenciales. La principal ventaja del cifrado simétrico es que, por lo general, es sencillo y eficiente a la hora de proteger los datos. [16]

7.2.10. Sexta bandera

El planteamiento para esta bandera es cifrar con cifrado simétrico un archivo y esconder la clave en un directorio preparado del servidor. Para ello se instala el programa GNU Privacy Guard (GPG). Este es uno de los sistemas más directos para cifrar datos en informática, y también una herramienta de código abierto. [17]

Lo primero que se hará es crear el archivo que contendrá la pista para encontrar el archivo con la clave. Después de crearse se guardaré en el directorio principal del usuario dado en la bandera de esteganografía. Figura 18

```
root@naciondelfuego:/home/nicolas# cat ReyFenix.txt
Yo, el Rey Fénix Ozái mañana quemaré el Reino Tierra por completa con el cometa
Sozin y así lograré lo que no pudieron ni mi abuelo ni mi padre, gobernar sobre
las 4 naciones. También mañana me aseguraré de 'buscar' al 'Avatar' y evitar que
 se interponga entre mis planes.

Rey Fenix.
```

Figura 18 Mensaje en el directorio del usuario Ozai

La pista son dos palabras entre comillas (“buscar” y “Avatar”). Se marcan estas porque el usuario debe utilizar el comando “find” para buscar un directorio en la máquina llamado “Avatar”.

A continuación, se crea el fichero que contiene la clave para resolver el cifrado del archivo que contiene la bandera. El contenido de este archivo consta de un texto diciendo que casi se ha acabado la CTF y te da la contraseña del archivo. Por último, incluye un pequeño texto extra indicando donde está el archivo de la bandera en caso de que el usuario no lo haya encontrado previamente a encontrar este archivo. Figura 19

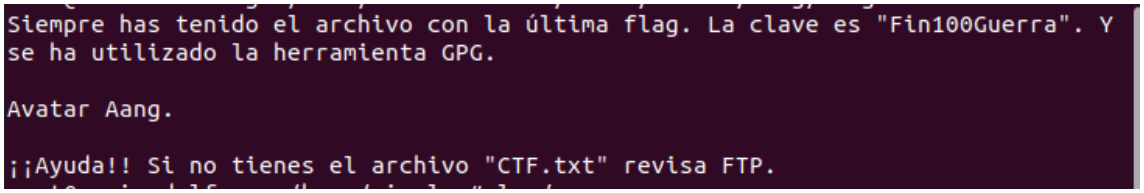


Figura 19 Mensaje en directorio preparado

Por último, se cifra el archivo con la bandera. Para ello se utiliza el comando "gpg –c CTF.txt". Luego se mueve al directorio del servidor de FTP, ya que la idea es que el usuario tenga el archivo desde el principio, pero no lo pueda desbloquear hasta el final de la realización del CTF.

7.3 Creación de un formulario web y una base de datos

7.3.1. Creación de la máquina virtual

Para la creación del formulario y la base de datos se necesitará otra máquina virtual que ofrezca la página web y a ella pueda acceder el usuario que realiza el CTF.

Por ello lo primero que se hará es los pasos realizados previamente en la creación de la máquina virtual de la máquina vulnerable. Descargar la ISO necesaria de la web oficial, en este caso, Windows 10. Después se realiza el proceso de configurar el sistema virtualizado, se añade a la red NAT de las otras dos máquinas y se instala su Sistema Operativo (SO).

7.3.2. Marco teórico e instalación de Apache

A continuación, se instala la aplicación de Apache. Apache es un servidor web HTTP de código abierto. Actualmente está desarrollado y mantenido por una comunidad de usuarios en torno a la Apache Software Foundation. La funcionalidad principal de este servicio web es servir a los usuarios todos los ficheros necesarios para visualizar la web. Las solicitudes de los usuarios se hacen normalmente mediante un navegador como Google Chrome, Firefox, Safari entre otros.

Apache tiene una estructura basada en módulos, que permite activar y desactivar funcionalidades adicionales, por ejemplo, módulos de seguridad como mod_security, módulos de caché como Varnish, o de personalización de cabeceras como mod_headers. También permite ajustar los parámetros de PHP de tu hosting de forma personalizada mediante el fichero .htaccess. [18]

Para realizar la instalación de Apache, se busca el sitio web oficial de la aplicación XAMPP y se descarga el instalador. Lo ejecutamos y se sigue el proceso de instalación, marcando que se quiere instalar las extensiones de Apache y MySQL.

7.3.3. Creación de las páginas web

A continuación, se crean y se describe el contenido de los archivos para las páginas web. La primera página es una introducción para explicar de qué trata el CTF, su temática y por último incluye un conjunto de botones para seleccionar con que equipo participa el usuario en el CTF. Figura 20

Figura 20 Página de introducción

Una vez seleccionado un equipo, nos lleva a la siguiente página que contiene los campos para el registro de las banderas. Dentro de esta página el usuario puede registrar las banderas que encuentra durante la prueba, puede ver la puntuación de su equipo y por último existe la opción también de que pueda cambiar de equipo. Figura 21

Figura 21 Página para el registro de banderas

7.3.4 Base de datos

Para crear la base de datos se abre PHP My Admin desde XAMPP. Una vez abierta la página se crea un usuario al que se le otorgan todos los permisos para poder crear y modificar la base de

datos al completo sin complicaciones. A continuación, se desarrolla el contenido de la base de datos.

La base de datos contiene dos tablas:

- 1ª Tabla (Equipos): Contiene los equipos con sus respectivas puntuaciones
- 2ª Tabla (Banderas): Contiene las banderas del CTF.

Como último paso se creará un script que haga una copia de la base de datos a la semana. Para ello creamos un archivo ".bat" donde se hará una conexión a la base de datos con nuestro usuario y contraseña [19]. Además, se guarda la fecha de cuando se hace la copia de seguridad y se introduce en el nombre del archivo de la copia. Figura 22

```
@echo off
:: Obtener día, mes y año
set dia=%date:~0,2%
set mes=%date:~3,2%
set anio=%date:~8,2%

set filename=copia-seguridad-%dia%-%mes%-%anio%.sql

C:\xampp\mysql\bin\mysqldump.exe --host=127.0.0.1 --user=nas --password=123456 --databases ctfavatar --result-file=%filename%

pause
```

Figura 22 Script para la copia de la base de datos

Para hacer que se haga de manera automática una vez a la semana, se configura el archivo ".bat" como tarea básica en el Programador de Tareas de Windows.

7.4 Subida de las máquinas virtuales a un repositorio de GitHub

El último paso del desarrollo del proyecto es subir las OVAs de la máquina Ubuntu y de la máquina Windows a un repositorio de GitHub para que las personas que lo quieran, puedan realizarlo. Figura 23

Figura 23 Logo GitHub

7.4.1. Preparación de las máquinas

Primero se comprobará que todas las configuraciones son correctas, una vez hecho se exportarán a .ova (Open Virtual Appliance) para facilitar su subida a otras plataformas.

Para exportar ambas máquinas desde VirtualBox se siguen los siguientes pasos:

- Se selecciona la máquina virtual
- Se hace clic en Archivo > Exportar servicio virtualizado

- Se elige donde se guarda el archivo

Se realizan estos pasos dos veces, una para cada máquina.

7.4.2. Creación del repositorio de GitHub

Posteriormente se crea un repositorio en GitHub para subir las dos máquinas y la documentación necesaria para poder usarlas en un archivo ReadMe.md. También se subió el Trabajo de Fin de Ciclo (TFC) al repositorio

Enlace al repositorio público: https://github.com/NAS-2224/TFG-2024-2025

7.4.3. Subida de los archivos .ova a MEGA

Debido al tamaño de ambas máquinas no se podían subir a GitHub, por lo que se utilizó el servicio de almacenamiento en la nube de MEGA para alojarlas. Los pasos seguidos fueron:

- Creación de una cuenta de MEGA
- Subida de los archivos .ova
- Obtener los enlaces de descarga pública de ambos archivos
- Incluir ambos enlaces en el ReadMe.md

8. EVALUACIÓN Y RESULTADOS

En la siguiente sección de este Trabajo de Fin de Grado (TFC) se presentarán los resultados obtenidos tras finalizar el proyecto y cómo se han evaluado para considerar que se han realizado correctamente.

8.1 Resultados obtenidos

- Número de retos creados: Se creó un total de 6 retos de baja y media dificultad.
- Registro: Se diseñó un formulario de PHP que es capaz de recoger las banderas introducidas por los usuarios y hacer las comprobaciones con la base de datos.
- Empresa: Se diseñó los siguientes apartados de una empresa: forma jurídica, análisis del sector y de la empresa, recursos humanos, plan de inversiones y gastos, financiación, ayudas y subvenciones, plan de tesorería, cuenta de resultados y balance.

8.2 Evaluación de los resultados

Los resultados han sido evaluados de la siguiente manera:

- Se ha comprobado que todos los retos funcionan desde la máquina virtual de Kali simulando ser un participante del CTF.
- Se han rellenado los campos de registro en las páginas web de todos los equipos y se ha comprobado que las revisa con la base de datos y en caso de ser correcta que sume la puntuación a los equipos.
- Se han corregido todos los errores encontrados durante correcciones previas al resultado final.

9. CONCLUSIÓN Y TRABAJO FUTURO

En la siguiente sección de este Trabajo de Fin de Grado (TFC) se presentarán a la conclusión alcanzada tras finalizar este proyecto y posibles mejoras que se pueden hacer para mejorar el resultado final.

9.1 Conclusión

Este Trabajo de Fin de Grado (TFC) ha consistido en el diseño y desarrollo de una plataforma de tipo Capture The Flag (CTF) centrada en el apartado de ciberseguridad, acompañada por un sistema de verificación de banderas mediante un formulario PHP conectado a una base de datos y como último, el diseño empresarial de una Sociedad Limitada (S.L.)

A lo largo del proyecto se ha confirmado la utilidad de los CTF como herramientas que te forman y evalúan en el ámbito de la seguridad informática, fomentando tanto el aprendizaje práctico como el pensamiento crítico. Además, durante la realización del trabajo se ha podido aplicar conocimientos conseguidos durante el ciclo, especialmente seguridad informática, administración de sistemas operativos y desarrollo web.

Aunque es una versión de básica, el sistema implementado ofrece una base sólida para seguir creando una plataforma más completa. De igual manera el enfoque en el apartado empresarial aporta un valor adicional sobre como este proyecto puede ser utilizado en empresas en las que su trabajo principal sea la ciberseguridad.

El TFC ha cumplido sus objetivos principales. Aun así, también ha demostrado áreas en las que se puede mejorar y ampliar, que se explicarán a continuación como parte del trabajo futuro.

9.2 Trabajo futuro

A partir de la conclusión obtenida, se plantean las siguientes mejoras y extensiones para el proyecto:

- Narración interactiva según la elección del jugador: Ampliar el número de banderas en la máquina vulnerable y según el equipo que seleccione el usuario al realizar el CTF tenga que buscar las banderas correspondientes a su equipo.
- Mayor número de equipos: Crear más equipos con los que participar en el CTF para los casos en los que participen más equipos de los creados en la página web y en la base de datos.
- Mejora en el diseño del formulario web: Se quiere mejorar el diseño visual del formulario para ser más atractivo y entendible para los usuarios.
- Integración con contenedores (Docker): Diseñar y crear el entorno completo dentro de un contenedor para facilitar su despliegue y reutilización.

10. PARTE EMPRESARIAL

10.1 Forma Jurídica

FORMA JURÍDICA	Sociedad limitada
CARACTERÍSTICAS	
Razón social / Denominación	CyberTeach S.L.
Objeto social / Finalidad	La finalidad de la empresa es enseñar hacking ético a personas con interés en la seguridad informática. Esto se dará a conocer a través de desafíos que simulan escenarios reales de ciberseguridad. Las personas instruidas desarrollan distintas habilidades como detectar y actuar ante vulnerabilidades.
Domicilio social / Dirección	Av. de los Alfares, 19.
Promotor / Socios	Número de socios: 3 Datos de los socios Juan Sánchez Montes con el DNI 06587946ª y número de tlf 465 12 38 12. Selene Espada Noheda con el DNI 04672369Z y número de tlf 489 34 76 12 Nicolás Almagro Soria con el DNI 07953124N y número de tlf 237 94 61 55
Responsabilidad patrimonial de los socios	Los socios responden con su patrimonio personal hasta el límite de su aportación a la empresa.
Capital social / Aportación	El capital mínimo que deben aportar los socios para formar una sociedad limitada es de 3000 €. Los socios en total han aportado 35.000 €. Juan ha aportado 5.000 €, Selene ha aportado 14.000 € y Nicolás Almagro Soria ha aportado 16.000 €.
Régimen fiscal	La Sociedad Limitada tributa por el Impuesto de Sociedades.
JUSTIFICACIÓN DE LA ELECCIÓN	
He elegido esta forma jurídica por los siguientes motivos: -Ante las deudas no se recurrirán a mis bienes personales sino a los bienes aportados a la empresa. -El número mínimo de socios para formar la empresa es de un socio, por lo que podría formar la empresa por mí mismo. -El capital mínimo necesario para constituir la sociedad limitada es de 3000€. -La empresa formada al tener menos de 2 años el porcentaje del Impuesto de Sociedades es del 15% y el 3º año del 25%. Se ha elegido montar la empresa en esa ubicación debido a los siguientes motivos: -Cercanía a institutos y la universidad, donde se realizan ciclos/carreras relacionados con la informática y la ciberseguridad. -La ubicación de la empresa está bien comunicada con el resto de la ciudad y hay zonas de aparcamiento cercanas para los trabajadores que vengan en coche o moto. -La ubicación tiene una alta conectividad como alta velocidad de internet y baja latencia que es muy necesario para la empresa.	

10.2 Análisis del sector y de la empresa

10.2.1. Fortalezas

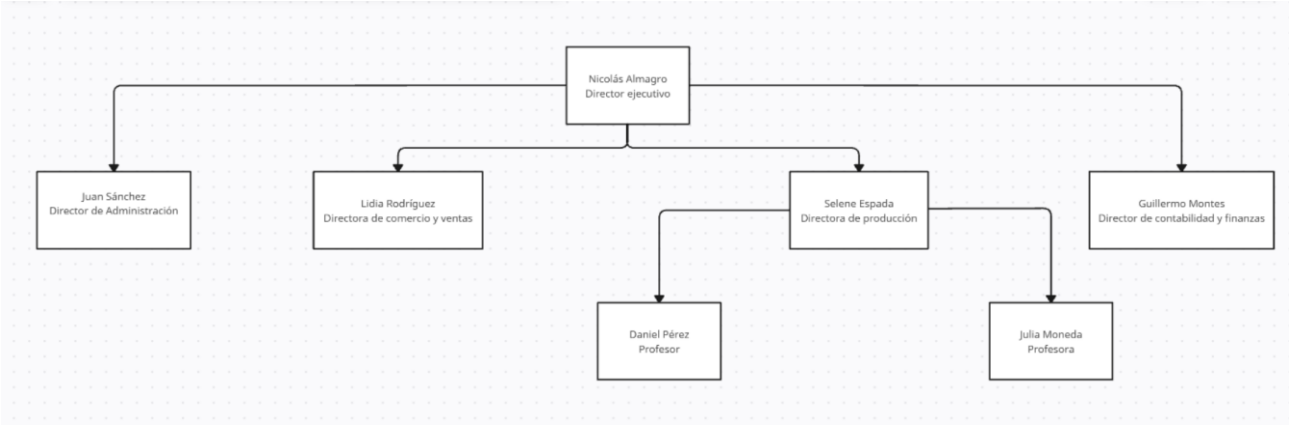
Fortalezas	Debilidades
Formación práctica: CyberTeach ofrece una formación práctica y enfocada en solucionar problemas reales como CTF.	Recursos limitados en comparación a otras grandes empresas.
Facilidad para poder realizar la formación: La empresa ofrece formación online y presencial para adaptarse a la situación de cada estudiante.	Precios más elevados debido a la formación especializada que se ofrece.
Equipo docente altamente cualificado y con experiencia en trabajar y enseñar ciberseguridad.	Actualizar el contenido constantemente requiere un gran coste.
Material didáctico actualizado con las últimas tendencias de ciberseguridad.	Falta de una mayor inversión en publicidad y marketing.
Oportunidades	**Amenazas**
Crecimiento del sector: La ciberseguridad es cada vez más importante y hay necesidad de aprender sobre esta.	Alta competencia en el sector de la formación de ciberseguridad.
Posibilidad de colaboración con institutos y universidades para ofrecer prácticas y empleo a los estudiantes.	Riesgo de ciberataques que pueda afectar a la reputación de la empresa.
Nuevos nichos: Que los estudiantes se especialicen en cosas más específicas en ciberseguridad como IoT, Blockchain…	Cambios en la legislación que afecten a la formación.
Desarrollar nuevos cursos o programas de formación de ciberseguridad.	Escasez de financiación de los bancos por ser una nueva empresa.

10.3. Recursos humanos

10.3.1. Estructura organizativa de la empresa

Personal que lo lleva en la empresa	El director ejecutivo sería la persona encargada del área de dirección	El director administrativo sería la persona encargada del área administrativa	El director comercial sería la persona encargada del área comercial	El director de producción y dos trabajadores de producción se encargarían del área de producción.	El dirección de contabilidad y finanzas se encargaría del área de contabilidad y finanzas
Tareas realizadas en la empresa	La dirección empresarial se encargaría de la planificación, organización, coordinación, dirección, liderazgo y control de la empresa	La administración se encargaría de la redactar, archivar y revisar los documentos de la empresa, coordinar servicios de mensajería y logística de la empresa, desarrollar y supervisar registros y archivos de contabilidad, informar y atender a clientes y ayudar a otros departamentos	El área comercial se encargaría del diseño de objetivos y estrategias, establecer objetivos de ventas, diseñar campañas y promociones, venta y negociación.	El área de producción se encargaría de la planificación y gestión de la producción, garantía de calidad, mantenimiento de equipos, realización del inventario, minimizar costos de producción.	Se encargaría de gestionar facturación emitida y recibida, registro de todas las operaciones económicas, cumplimentar los libros contables, elaborar balances e inventarios patrimoniales, establecer el nivel de liquidez y la solvencia de la empresa, abonar las nóminas a los trabajadores, efectuar controles financieros para evitar errores o detectar fraudes.
Departamentos	Área de dirección	Área administrativa	Área comercial o de ventas	Área de producción	Área de contabilidad y finanzas

10.3.2. Organigrama de la empresa



10.3.3. Diseño de puestos de trabajo

<table>
<tr><th>Descripción del puesto</th><th>Condiciones laborales</th><th>Perfil profesional</th></tr>
<tr><td>Denominación:
Enseñanza</td><td>Salario:
2.925,94 € brutos/mes
12 pagas
Salario obtenido de las tablas salariales del:
XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública</td><td>Formación y titulación:
Curso de especialización de ciberseguridad
Máster universitario en Seguridad Informática</td></tr>
<tr><td>Departamento:
Producción</td><td>Horario y jornada:
De 09:30 a 13:30 y de 16:00 a 20:00</td><td>Conocimientos específicos:
Amplios conocimientos en ciberseguridad</td></tr>
<tr><td rowspan="3">Tareas a realizar:
Impartición de clases
Resolución de dudas de alumnos
Preparación de materiales didácticos
Desarrollar entornos de prueba de ciberseguridad</td><td>Lugar de trabajo:
Aulas dentro de la empresa</td><td>Experiencia profesional:
3 meses en empresas de ciberseguridad
3 meses en empresas de informática</td></tr>
<tr><td rowspan="2">Tipo de contrato:
Contrato formativo para la obtención de la práctica profesional.
Tiempo de contrato:
8 meses</td><td>Habilidades profesionales:
Habilidades pedagógicas
Habilidades de comunicación</td></tr>
<tr><td>Actitudes y habilidades personales:
Ordenado
Simpático
Puntual
Cooperativo</td></tr>
</table>

<table>
<tr><th>Descripción del puesto</th><th>Condiciones laborales</th><th>Perfil profesional</th></tr>
<tr><td>Denominación:
Comercio y ventas</td><td>Salario:
2.645,27 € brutos/mes
12 pagas
Salario obtenido de las tablas salariales del:
XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública</td><td>Formación y titulación:
Ciclo formativo de grado medio de gestión administrativa
Ciclo formativo de grado superior de Administración y Finanzas</td></tr>
<tr><td>Departamento:
Comercio y ventas</td><td>Horario y jornada:
De 09:30 a 13:30 y de 16:00 a 20:00</td><td>Conocimientos específicos:
Marketing digital
Conocimiento en ventas y comercio</td></tr>
<tr><td rowspan="2">Tareas a realizar:
Desarrollo de estrategia comercial
Marketing y generación de leads
Relaciones con clientes corporativos</td><td>Lugar de trabajo:
Oficina de comercio y ventas</td><td>Experiencia profesional:
3 meses en empresas de informática
3 meses en empresas similares</td></tr>
<tr><td rowspan="2">Tipo de contrato:
Contrato formativo para la obtención de la práctica profesional.
Tiempo de contrato:
8 meses</td><td>Habilidades profesionales:
Buena organización y planificación
Resolución de problemas</td></tr>
<tr><td>Actitudes y habilidades personales:
Ordenado
Simpático
Puntual
Cooperativo</td></tr>
</table>

Descripción del puesto	Condiciones laborales	Perfil profesional
Denominación: Contabilidad y finanzas	Salario: 2.645,27 € brutos/mes 12 pagas Salario obtenido de las tablas salariales del: XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública	Formación y titulación: Ciclo formativo de grado medio de gestión administrativa Ciclo formativo de grado superior de Administración y Finanzas
Departamento: Contabilidad y finanzas	Horario y jornada: De 09:30 a 13:30 y de 16:00 a 20:00	Conocimientos específicos: Contabilidad y fiscalidad Finanzas corporativas
Tareas a realizar: Contabilidad general y cumplimiento Gestión financiera Gestión de costos y precios Gestión de pagos y cobros	Lugar de trabajo: Oficina de administración	Experiencia profesional: 3 meses en empresas de informática 3 meses en empresas similares
	Tipo de contrato: Contrato formativo para la obtención de la práctica profesional. Tiempo de contrato: 8 meses	Habilidades profesionales: Buena organización y planificación Resolución de problemas
		Actitudes y habilidades personales: Ordenado Simpático Puntual Cooperativo

10.3.4. Coste salarial

	Puesto de trabajo	Salario mensual (SB + complementos)	Seguridad Social al mes		Seguridad Social Total al mes	Seguridad Social Al año (12 meses)	Total salarios al año (12 pagas)	Total salarios anuales + Seguridad Social
			Trabajador	Empresa				
Trabajador 1	Director de comercio y ventas	2.645,27 € brutos/mes	356,58 €	843,84 €	1200,42 €	14.405,04 €	31.746,24 €	46.151,24 €
Trabajador 2	Director de contabilidad y finanzas	2.645,27 € brutos/mes	356,58 €	843,84 €	1200,42 €	14.405,04 €	31.746,24 €	46.151,24 €
Trabajador 3	Profesor	2.925,94 €	394,42 €	933,37 €	1327,79 €	15933,48 €	35.111,28 €	51.044,76 €

10.3.5. Evaluación de riesgos

PLAN DE PREVENCIÓN			
Empresa	CyberTeach S.L.		
Elaborado por: Nicolás Almagro Soria			
Actividad de la empresa: Enseñanza de seguridad informática y ciberseguridad			
Modelo organizativo: Mi plan de prevención de riesgos consiste en asegurar que los trabajadores de la empresa no sufran riesgos durante su jornada laboral y que los medios de la empresa tampoco se vean dañados. En este plan identificamos los posibles riesgos a los que se enfrenta la empresa en su trabajo a diario, como de dañino puede ser y cómo podemos prevenirlo. En caso de ser necesario se consultará con un servicio de Prevención de Riesgos Laborales Ajeno.			
Funciones en materia preventiva	Empresario		
	Delegado de prevención		
	Trabajadores		
Evaluación de riesgos			
Descripción del riesgo	**Evaluación del riesgo**	**Medidas preventivas**	**Responsable**
Incendio en la empresa	Probabilidad baja Extremadamente dañino (Riesgo moderado)	Sistemas contra incendios Extintores	Empresario
Inundación	Probabilidad baja Extremadamente dañino (Riesgo moderado)	Seguro para todo tipo de aparato eléctrico o electrónico	Empresario
Corte de corriente	Probabilidad baja Dañino (Riesgo tolerable)	Sistemas de alimentación ininterrumpida	Empresario
Divulgación de información por parte de los trabajadores	Probabilidad media Dañino Riesgo moderado	Concienciación a los trabajadores Contratos de confidencialidad	Trabajadores
Hackeo	Probabilidad media Muy dañino Riesgo importante	Firewall Antivirus	Delegado de prevención
Cansancio visual de los trabajadores	Probabilidad media Ligeramente Dañino Riesgo bajo	Pantallas con filtros de luz azul	Empresario
Síndrome del túnel carpiano	Probabilidad baja Ligeramente dañino Riesgo bajo	Ratones ergonómicos	Empresario
Rotura de los dispositivos	Probabilidad media Ligeramente dañino Riesgo tolerable	Concienciar a trabajadores y alumnos del material	Empresario

10.4. Plan de inversiones y gastos

El siguiente plan indica todos los recursos necesarios para el lanzamiento y funcionamiento de la empresa de enseñanza de ciberseguridad CyberTeach SL. Se divide en dos partes principales: recursos humanos y recursos materiales.

10.4.1 Recursos humanos

Instructores:

Número:

2 instructores (al comenzar), con posibilidad de aumentar si aumenta la necesidad en la empresa.

Salario Anual por instructor:

35.111,28 € anuales

Capacitación de los trabajadores:

Inversión al año para formar de manera continua a los instructores para que se mantengan actualizados con las últimas novedades de ciberseguridad (2500 € por instructor).

Administración:

Número:

1 Director de administración

Socio de la empresa

Comercio y ventas:

Número:

1 director de comercio y ventas

Salario anual del trabajador:

31.746,24 € anuales

Coste total anual (Comercio y ventas):

30.321,53 €

Producción:

Número:

1 Director de producción

Socio de la empresa

Contabilidad y finanzas:

Número:

1 director de contabilidad y finanzas

Salario anual del trabajador:

31.746,24 € anuales

Coste total anual (Contabilidad y finanzas):

30.321,53 €

10.4.2. Recursos materiales

INVERSIONES INICIALES		COSTE	
		Alquiler	Compra
Edificio / Local	La ubicación del local sería en la Cuenca capital, en Avenida de los Alfares nº 2. La superficie sería 50 m^2 las 2 aulas para clases, 24 m^2 para las 2 oficinas, 20 m^2 para la sala de reuniones, 20 m^2 de espacios comunes y 10 m^2 de almacén. En total serían 124 m^2.	1860€ / mes 22.320€ / año	
Reformas / Instalaciones	Las reformas que se van a hacer al local son las siguientes: Seguridad: Sistema de seguridad con cámaras de vigilancia, control de acceso y alarma. Iluminación: Instalación de una estructura de luz eficiente y adecuado para cada área del local. Climatización: Sistema de climatización para la comodidad de los empleados. Por último se le dará un diseño general de modernidad.		5000 €
Maquinaria / Equipos	Detalla el tipo y el número necesarios. Decide si lo adquieres en propiedad o lo alquilas y valora el coste.	€ / mes € / año	0
Herramientas/Utillaje	Detalla el tipo y el número necesarios.	0	
Mobiliario	Aulas: 10 Mesas para profesor y alumnos, 10 sillas para profesor y alumnos. Oficinas: 5 escritorios, 5 sillas, 3 armarios archivadores, 3 estanterías de oficiona, 1 mesa de reuniones y 5 taquillas. Zona descanso: Mesa café, 7 sillas, 1 microondas, 1 cafetera y 1 neverita	€ / mes € / año	10.000 €0
Equipos informáticos	Los equipos necesarios para la empresa serían: Ordenadores portátiles: 7 portátiles Servidores: 1 Equipos de red: 2 Pizarras interactivas: 2 Software de seguridad: 1		9750 €
Vehículos	Detallar el modelo y tipo de vehículo Decide si lo adquieres en propiedad o lo alquilas y valora el coste.	€ / mes € / año	0
	INVERSIÓN INICIAL TOTAL	22.380 €	24.750 €

Nicolás Almagro Soria

10.4.3 Gastos iniciales

GASTOS INICIALES	*COSTE*	FUENTE DE FINANCIACIÓN
Constitución y puesta en marcha	1.191, 36 €	Recursos propios
Stock, (existencias/materia prima mínimas si fuesen necesarias)	0 €	Recursos propios
Seguros, (vehículos, local)	565 €	Recursos propios
Publicidad	2.700 €	Recursos propios
Servicios, (gestoría, agua, luz, internet, prevención riesgos laborales)	4.850 €	Recursos propios
GASTOS INICIALES TOTALES	**9306,36 €**	

10.5 Financiación y ayudas

10.5.1 Financiación de inversiones

FUENTES DE FINANCIACIÓN	IMPORTE	
Recursos propios (Autofinanciación)	35.000 €	La financiación propia es aportada por los ahorros de tres amigos, es decir, los tres socios de la empresa. En total los socios han aportado un total de 35.000 €, lo que representa al 55% de la financiación total de la empresa. Esta aportación es muy importante para comienzo y desarrollo de la empresa, ya que demuestra la confianza de los socios en el futuro negocio. La distribución de la financiación se divide de la siguiente manera: Socio 1: Juan ha aportado 5.000 € Socio 2: Selene ha aportado 14.000 € Socio 3: Nicolás ha aportado 16.000 €.
Préstamo Bancario (Financiación ajena)	19.436,36 €	Para la financiación ajena se va a solicitar un prestamos bancario y solicitar ayudas o subvenciones al estado. La empresa ha solicitado un préstamo bancario a la entidad financiera de CaixaBank. Esta ha sido elegida tras analizar las distintas ofertas ofrecidas por las distintas entidades y considerando cuál es la más favorable para la empresa. Condiciones del préstamo: 19.436,36 € Tipo de interés: Interés fijo 7% anual. El tipo de interés se ha considerado adecuado debido al riesgo del proyecto y las condiciones del mercado financiero actual. Se ha fijado un interés fijo para asegurar la devolución del préstamo por parte de la empresa. Plazo de devolución: 60 meses (5 años). Se ha eligió este plazo para poder hacer una liquidación gradual de la empresa sin comprometer la liquidez de esta en los primeros años de funcionamiento. Ayudas y subvenciones del Estado No se han podido encontrar ayudas que pueden beneficiar a la empresa.
TOTAL	54.436,36 €	La cantidad aquí recogida ha de coincidir con la inversión inicial total.

10.5.2 Amortización del préstamo

Cantidad solicitada (préstamo)	19.436
Entidad financiera que lo concede	Caixabank
A pagar el primer año	3.887,27
Número de cuotas al año	12
Interés anual (TAE en ICO)	7,00%
Cuota mensual	336.35 €

Amortización				
Número	Importe de la Cuota	Interés	Principal	Saldo
0	-	-	-	3.887,27 €
1	336,35 €	22,68 €	313,68 €	3.573,59 €
2	336,35 €	20,85 €	315,51 €	3.258,09 €
3	336,35 €	19,01 €	317,35 €	2.940,74 €
4	336,35 €	17,15 €	319,20 €	2.621,54 €
5	336,35 €	15,29 €	321,06 €	2.300,48 €
6	336,35 €	13,42 €	322,93 €	1.977,55 €
7	336,35 €	11,54 €	324,82 €	1.652,73 €
8	336,35 €	9,64 €	326,71 €	1.326,02 €
9	336,35 €	7,74 €	328,62 €	997,40 €
10	336,35 €	5,82 €	330,53 €	666,86 €
11	336,35 €	3,89 €	332,46 €	334,40 €
12	334,40 €	1,95 €	332,45 €	- €
	TOTALES	148,96 €	3.885,32 €	

10.6. Plan de tesorería, cuenta de resultados y balance

10.6.1. Previsión de tesorería

ENTRADAS	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembr	Octubre	Noviembre	Diciembre	Total
Capital aportado por los socios	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	2.916,67 €	35.000,04
Prestamo	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	1.619,70 €	19.436,40
Ventas	20.000 €	22.000 €	25.000 €	30.000 €	35.000 €	40.000 €	25.000 €	25.000 €	35.000 €	40.000 €	40.000 €	40.000 €	377.000,00
Subvenciones													0,00
Total Entradas	24.536,37	26.536,37	29.536,37	34.536,37	39.536,37	44.536,37	29.536,37	29.536,37	39.536,37	44.536,37	44.536,37	44.536,37	431.436,44
SALIDAS	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembr**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Intereses Prestamo primer año	22,68 €	20,85 €	19,01 €	17,15 €	15,29 €	13,42 €	11,54 €	9,64 €	7,74 €	5,82 €	3,89 €	1,95 €	148,98
Devolucion prestamo primer año	336,35 €	336,35 €	336,35 €	336,35 €	336,35 €	336,35 €	336,35 €	336,35 €	336,35 €	336,35 €	336,35 €	334,40 €	4.034,25
Cuota de autonomo	240,00	240,00	240,00	240,00	240,00	240,00	240,00	240,00	240,00	240,00	240,00	240,00	2.880,00
Materiales y stock mínimo a la venta													0,00
Sueldo de autonomo	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Alquiler y fianza	1.860 €	1.860 €	1.860 €	1.860 €	1.860 €	1.860 €	1.860 €	1.860 €	1.860 €	1.860 €	1.860 €	1.860 €	22.320,00
Gastos constitución puesta en marcha	99,28 €	99,28 €	99,28 €	99,28 €	99,28 €	99,28 €	99,28 €	99,28 €	99,28 €	99,28 €	99,28 €	99,28 €	1.191,36

Elementos de transporte (compra)	0,00												0,00
Elementos de transporte (renting)	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Mobiliario	833.33 €	833.33 €	833.33 €	833.33 €	833.33 €	833.33 €	833.33 €	833.33 €	833.33 €	833.33 €	833.33 €	833.33 €	0,00
Utiles y herramientas	0,00												0,00
Seguros	565 €	565 €	565 €	565 €	565 €	565 €	565 €	565 €	565 €	565 €	565 €	565 €	6.780,00
Maquinaria	0,00												0,00
Servicios subcontratados	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Publicidad	425 €	425 €	425 €	425 €	0 €	0 €	0 €	0 €	250 €	250 €	250 €	250 €	2.700,00
Salarios	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	14.413,37 €	172.960,44
Seguridad Social	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	7.410,38 €	88.924,56
Edificios y otras construcciones	0,00												0,00
Equipos y programas informáticos	812,50 €	812,50 €	812,50 €	812,50 €	812,50 €	812,50 €	812,50 €	812,50 €	812,50 €	812,50 €	812,50 €	812,50 €	9.750,00
Suministros	202,08 €	202,08 €	202,08 €	202,08 €	202,08 €	202,08 €	202,08 €	202,08 €	202,08 €	202,08 €	202,08 €	202,08 €	2.424,96
Total salidas	26.386,64	26.384,81	26.382,97	26.381,11	25.954,25	25.952,38	25.950,50	25.948,60	26.196,70	26.194,78	26.192,85	26.188,96	314.114,55
ENTRADAS MENOS SALIDAS	-1.850,27	151,56	3.153,40	8.155,26	13.582,12	18.583,99	3.585,87	3.587,77	13.339,67	18.341,59	18.343,52	18.347,41	117.321,89

Saldo en el banco	51.224,96 €	49.913,23 €	51.701,50 €	41.217,95 €	53.430,50 €	50.643,05 €	47.855,60 €	45.068,15 €	57.031,15 €	44.412,05 €	61.375,32 €	64.977,68 €	**64.977,68 €**
Saldo en cuenta de credito	5.593,47 €	5.084,04 €	4.575,61 €	4.067,18 €	3.558,75 €	3.050,32 €	2.541,89 €	2.033,46 €	1.525,03 €	1.016,60 €	508,17 €	0 €	**6.100,90 €**
Pago Cuenta impuestos IS				25.464,05						25.464,05		25.464,05	76.392,16
Pago Cuenta impuestos IRPF				25.464,05			28.293,39			28.293,39			82.050,84

10.6.2 Cuenta de resultados

CUENTA DE RESULTADOS

Ingresos		**Gastos**	
Ingresos de explotacion		*gastos de explotacion*	
Ventas	377.000,00	Alquiler	22.320,00
		A. mobiliario	0,00
		A. maquinaria	0,00
		A. inmovilizado	0,00
		A elementos transporte	0,00
		A. Útiles y herramientas	0,00
		A. informática	211,25
		Sueldo autonomo	0,00
		Seguro	0,00
		Materias primas	0,00
		Servicios subcontratados	0,00
		Publicidad	0,00
		Salarios	172.960,44
		Seguridad social	88.924,56
		E. Transporte	0,00
		Suministros	2.424,96
		Cuota autónomo	2.880,00
		Gastos constitución puesta en marcha	99,28
		TOTAL	289.820,49
Ingresos financieros	*54.436,44*	*Gastos financieros*	*148,98*
resultado explotacion	***377.000,00***	***289.820,49***	***87.179,51***
resultado financiero	54.436,44	148,98	54.287,46
resultados ordinarios			***141.466,97***
resultado del ejercicio			141.466,97
RESULTADO DESPUES DE IMPUESTOS IS			65.074,81
RESULTADO DESPUES DE IMPUESTOS E.I			59.416,13

10.6.3 Balance patrimonial

BALANCE PREVISIONAL			
Activo		**Pasivo**	
Activo no corriente	**601,25**	**Neto Patrimonial**	**176.467,01**
Edificios y otras construcciones	0,00	Capital	35.000,04
Amortización del inmovilizado	0,00	Pérdidas y ganancias	141.466,97
Mobiliario	0,00	Subvenciones	0,00
Amortización mobiliario	0,00		
Equipos informáticos	812,50		
Amortización equipos informáticos	-211,25		
Maquinaria	0,00		
Amortización Maquinaria	0,00		
E. Transporte	0,00	**Pasivo no corriente**	**-2.414,55**
Amortización E. Transporte	0,00	Prestamo	-2.414,55
Útiles y herramientas	0,00		
Amortización útiles y herramientas	0,00		
Activo corriente	**64.977,68**	**Pasivo Corriente**	**6.100,90**
Existencias		Cuenta de credito	6.100,90
Créditos pendientes de cobro			
Efectivo			
Banco cuenta corriente	64.977,68		
Total	**65.578,93**	**Total**	**180.153,36**

11. BIBLIOGRAFÍA Y REFERENCIAS

Bibliografía

[1] Universidad Politécnica de Cartagena, Qué es un CTF en ciberseguridad, Cartagena: TrustLab, 2024.

[2] Geodesical Technology S.L., «¿Qué es un CTF?,» Madrid, 2024.

[3] ivOt_, «¿Qué es un CTF y por qué son importantes si trabajas, estudias o te gusta la ciberseguridad ?,» Wikipedia, 29 de septiembre de 2023.

[4] M. D. D. y. B. Konietzko, «Avatar: La Leyenda de Aang,» Nickelodeon, 2005.

[5] CyberTalents, «Top 6 Platforms to Run your CTF On,» Delaware, 2025.

[6] Universidad Carnegie Mellon, «picoCtf is for everyone,» Pittsburgh, 2025.

[7] I. Ramírez, «Máquinas virtuales: qué son, cómo funcionan y como utilizarlas.,» Xataka, 2020.

[8] Y. Fernández, «VirtualBox: qué es y cómo usarlo para crear una máquina virtual con Windows u otro sistema operativo,» Xataka, 2020.

[9] «Tipos de redes en VirtualBox,» Archive Hixec, 2023.

[10] Viewerwiki, «Base64,» Wikipedia, 2024.

[11] Sergio de Luz, «CyberChef: La herramienta todo en uno que cualquier informático utilizará alguna vez,» Redes Zone, 2016.

[12] F. G. Zúñiga, «SSH: qué es y cómo funciona este protocolo,» arsys, 2025.

[13] «¿Qué es la esteganografía? Definición y explicación,» Kaspersky, 2024.

[14] Alberto, «ExifTool, la herramienta de extracción de metadatos para imágenes, vídeos, etc,» Seo, IA y Ciberseguridad, 2024.

[15] Leonpolanco, «Metadatos,» Wikipedia, 2025.

[16] Annie Badman, Matthew Kosinski, «¿Qué es el cifrado simétrico?,» IBM, 2024.

[17] C. Cilleruelo, «GNU Privacy Guard,» keepcoding.

[18] Iván Camino, «¿Qué es Apache y para qué sirve?,» dinahosting, 2022.

[19] a. Malbarez, «Como Realizar Un backup Automático en MySQL,» stackoverflow, 2018.

[20] Angellstvrou92, «Capture the flag (cybersecurity),» Wikipedia, 3 de marzo de 2025.

12. ANEXOS

12.1 Código PHP para el formulario

```
<?php

//Para que se puedan utilizar y guardar variables globales en el usuario

session_start();

/**

 * @author NAS

*/


// Conexión a la base de datos.

   //IP del servidor

   $servidor = "127.0.0.1";

   // Usuario con el que nos conectamos a la BBDD.

   $usuario = "nas";

   // Password

   $clave = "123456";

   // BBDD a la que me conecto

   $baseDeDatos = "ctfavatar";

   // Almaceno los datos y la función musqli_connect en la variable de sesión $enlace

   $enlace = mysqli_connect ($servidor, $usuario, $clave, $baseDeDatos);


   // Función de recogida de datos

   function recoge($key, $type = "")

   {

      if (!is_string($key) && !is_int($key) || $key == "") {

         trigger_error("Function recoge(): Argument #1 (\$key) must be a non-empty string or an
integer", E_USER_ERROR);

      } elseif ($type !== "" && $type !== []) {
```

```
        trigger_error("Function recoge(): Argument #2 (\$type) is optional, but if provided, it must be an empty array or an empty string", E_USER_ERROR);
    }
    $tmp = $type;
    if (isset($_REQUEST[$key])) {
        if (!is_array($_REQUEST[$key]) && !is_array($type)) {
            $tmp = trim(htmlspecialchars($_REQUEST[$key]));
        } elseif (is_array($_REQUEST[$key]) && is_array($type)) {
            $tmp = $_REQUEST[$key];
            array_walk_recursive($tmp, function (&$value) {
                $value = trim(htmlspecialchars($value));
            });
        }
    }
    return $tmp;
}
    //Recogida de datos de los campos
    if(isset($_POST['formulario'])){

        $equipo     = recoge("equipo_seleccionado");

        $banderas = [
        recoge("band1"),

        recoge("band2"),

        recoge("band3"),

        recoge("band4"),

        recoge("band5"),
```

```
recoge("band6"),
];

//Variables para puntos por bandera y recuento de puntos de equipos
$puntosbandera = 20;
$puntosequipo = 0;

// Comprobar si se ha rellenado los campos
foreach ($banderas as $index => $bandera) {
    if ($bandera === "") {
        // Se continua haciendo el bucle si detecta un campo vacío
        continue;
    }

// Comprobar la bandera en la base de datos
 //Preparamos la consulta con la base de datos
$stmt = mysqli_prepare($enlace, "SELECT COUNT(*) FROM banderas WHERE flags = ?");
//Asigna el contenido de la variable a la consulta (?)
mysqli_stmt_bind_param($stmt, "s", $bandera);
//Ejecución de la consulta
mysqli_stmt_execute($stmt);
//Asigna el resultado de la consulta preparada
mysqli_stmt_bind_result($stmt, $banderaExiste);
//Guarda el resultado en la variable
mysqli_stmt_fetch($stmt);
//Limpia la variable donde se preparó la consulta
mysqli_stmt_close($stmt);

// Comprobación de que si el resultado de la query es correcto
if ($banderaExiste != 0) {
```

```
            //Si lo es suma el valor de la bandera a la puntuación del equipo
            $puntosequipo += $puntosbandera;
        }
    }

    // Comprueba los puntos del equipo
    if ($puntosequipo > 0) {
    //
        $stmt = mysqli_prepare($enlace, "UPDATE equipos SET puntuacion = /*Comprueba que la puntuación no sobrepase la puntuación máxima*/LEAST(puntuacion + ?, 100) WHERE naciones = ?");
        mysqli_stmt_bind_param($stmt, "is", $puntosequipo, $equipo);
        mysqli_stmt_execute($stmt);
        mysqli_stmt_close($stmt);
    }

    //Vuelta a la página de cada equipo después de hacer las comprobaciones
    switch ($equipo) {
        case 'Tribus-Agua':
            header("Location: agua.html");
            break;
        case 'Nómadas-Aire':
            header("Location: aire.html");
            break;
        case 'Reino-Tierra':
            header("Location: tierra.html");
            break;
        case 'Nación-Fuego':
            header("Location: fuego.html");
            break;
    }
}
```

```
// Reiniciar la puntuación de los equipos si el usuario cambia de equipo
if (isset($_POST['quitar_puntos'])) {
    // Variable para recoger el equipo
    $equipoReset = recoge("equipo_seleccionado");
    //Preparamos la consulta
    $stmt = mysqli_prepare($enlace, "SELECT COUNT(*) FROM equipos WHERE naciones = ?");
    //Asigna el contenido de la variable a la preparación de la consulta
    mysqli_stmt_bind_param($stmt, "s", $equipoReset);
    //Ejecutamos la consulta
    mysqli_stmt_execute($stmt);
    //Asigna el resultado en la variable
    mysqli_stmt_bind_result($stmt, $existe);
    //Guarda el resultado en la variable
    mysqli_stmt_fetch($stmt);
    //Limpia la variable donde se guardó la consulta
    mysqli_stmt_close($stmt);

    // Si el equipo existe reseteará la consulta
    if ($existe > 0) {
        // preparamos la actualización de la tabla
        $stmt = mysqli_prepare($enlace, "UPDATE equipos SET puntuacion = 0 WHERE naciones
= ?");
        //Asigna el contenido de la variable a la consulta
        mysqli_stmt_bind_param($stmt, "s", $equipoReset);
        //Ejecuta la consulta
        mysqli_stmt_execute($stmt);
        //Limpia la variable
        mysqli_stmt_close($stmt);
        }
```

```
    //Redirecciona a la página principal una vez termina
    header("Location: index.html");
    exit();
}

//Recogida de datos en caso de que el usuario quiera ver la puntuación
if (isset($_POST['ver_puntos'])) {
    $equipo = recoge("equipo_seleccionado");
    //Guarda el valor de la variable en una variable global
    $_SESSION['equipo'] = $_POST['equipo_seleccionado'];
    //Redirecciona a la página de la puntuación
    header("Location: puntuaciones.php");
    exit();
}

?>
```