TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

UNIVERSIDAD DE ALMERIA

ESCUELA SUPERIOR DE INGENIERÍA

Laboratorio de ciberseguridad en un entorno virtualizado

Curso 2020/2021

Alumno/a:

Alejandro Roca López

Director/es:

Julio Gómez López

Nicolás Padilla Soriano

Laboratorio de ciberseguridad en un entorno virtualizado

Trabajo Fin de Grado

Alumno: Alejandro Roca López

Director: Julio Gómez López

Codirector: Nicolás Padilla Soriano

Grado en Ingeniería Informática

Escuela Superior de Ingeniería

Universidad de Almería

Curso 2020/2021

Agradecimientos

Es importante comenzar por uno de los aspectos más importantes de este trabajo, siendo este todo aquello que tengo que agradecer a las personas que me han apoyado y han confiado en mis capacidades para realizar este trabajo.

Me gustaría empezar con Julio Gómez López, que aceptó desde un primer momento tutorizar este trabajo de fin de grado, teniendo en cuenta que aún no había cursado su asignatura y ni siquiera había llegado a conocerme, un acto de confianza muy grande, por el que estoy muy agradecido. Quiero destacar que desde el primer hasta el último día se ha implicado de lleno, estando ahí siempre que ha sido necesario, es por ello por lo que si he tenido la oportunidad de hacer este proyecto, ha sido en mayor parte gracias a él.

También nombrar a mi codirector Nicolas Padilla Soriano, persona que desde la primera reunión ha estado proponiendo diferentes puntos de vista e ideas que quizás nunca me hubiera llegado a plantear. Gracias a esto considero que mi trabajo es ahora más útil tanto a nivel de autoaprendizaje, como para evaluar a estudiantes.

De una forma muy especial Agradecer a mi familia, amigos y pareja por estar ahí ya no solo durante la realización de este proyecto, sino durante toda la carrera, apoyándome en los momentos en los que me he podido sentir más perdido y motivándome a dar siempre un poco más en los momentos en los que todo iba bien. He de reconocer que gran parte de mi determinación actual se la debo a ellos, ya que siempre han confiado en que yo soy capaz de todo y más, consiguiendo que a veces hasta yo mismo me lo llegue a creer.

Finalmente agradecer tanto a la Universidad de Almería como a los profesores que me han acompañado durante el transcurso de esta experiencia, haciendo de la UAL mi casa, un lugar donde he pasado muchos grandes momentos y algunos malos, pero sobre todo un lugar que me ha servido de guía para avanzar hacia un futuro mejor.

Resumen

En las últimas décadas se ha experimentado un gran desarrollo tecnológico, lo que ha conllevado que cada vez existan más dispositivos capaces de conectarse a internet. Si a esta situación le sumamos la poca importancia que se le ha dado a la seguridad informática hasta hace unos pocos años, se puede llegar a entender como las amenazas cibernéticas se han convertido en un problema real de nuestra sociedad. Esto ha provocado el aumento de contratación de profesionales en esta área, llegando hasta el punto en el que la demanda es mayor que la oferta.

Con el fin de ayudar a aquellas personas interesadas en formarse en la rama de la seguridad informática y cubrir la situación actual de necesidad de personal, surge este proyecto, el cual consiste en la creación de una red en un entorno virtual, desde cero, la cual contará con diferentes máquinas virtuales vulnerables. El proyecto está orientado en forma de reto, consiguiendo de esta manera ampliar los conocimientos de los usuarios que lo realicen, así como poner a prueba los adquiridos anteriormente de una manera dinámica y divertida.

El proyecto cuenta con un portal web de seguimiento, el cual resulta muy útil para los usuarios, proporcionando pistas e información según el nivel de dificultad para enfocar el reto. Este portal es la continuación de un manual de juego, en el que se explica cómo desplegar el laboratorio y comenzar los retos.

Durante este trabajo de Fin de Grado se abarca el completo desarrollo del laboratorio de prácticas, comenzando desde el estado el arte, diseño e implementación del mismo. Además, se muestran los manuales que tiene a su disposición el usuario final, tanto para desplegar la red como para guiarlo durante todo el proceso.

Palabras clave

Seguridad Informática, analista de seguridad informática, entornos de virtualización, retos, entrenamiento.

Abstract

In the last decades there has been a great technological development, which has led to an increasing number of devices capable of connecting to the Internet. If we add to this situation the little importance that has been given to computer security until a few years ago, it is possible to understand how cyber threats have become in a real problem in our society. This has led to an increase in the hiring of professionals in this area, reaching the point where the demand is higher than offer.

In order to help those interested people in training in the field of computer security and covering the current situation of personnel needs, this project appears, which consists of the creation of a network in a virtual environment, from scratch, which will have different vulnerable virtual machines. The project is oriented in the form of a challenge, thus managing to broaden the knowledge of the users who carry it out, as well as testing those previously in a dynamic and fun way.

The project has a monitoring web portal which is very useful for users, providing clues and information according to the level of difficulty to approach the challenge. This portal is the continuation of the game manual, which explains how to deploy the laboratory and start the challenges.

During this End of Degree project, the complete development of the practical laboratory is covered, starting from the state of the art, design and implementation. In addition, the manuals available to the end user are shown, both to deploy the network throughout the process.

Keywords

Computer Security, computer security analyst, virtualization environments, challenges, training

Índice

Índice de ilustraciones

Índice de tablas

Abreviaturas

MV	Máquina Virtual
SO	Sistema Operativo
LFI	Local File Inclusion
RFI	Remote File Inclusion
XSS	Cross-Site Scripting
RCE	Remote Code Ejecution

Capítulo 1
Introducción

1. Introducción

1.1 Motivación

Hasta donde pueden llegar mis recuerdos, no existe un pasado en el que no me sintiera atraído tanto por la tecnología, como por el cómo ésta consigue funcionar. Pero fue realmente con 12 años cuando decidí que tenía claro que iba a aprender todo lo que pudiera relacionado con el mundo de los ordenadores, y es que allí estaba el primer ordenador al que pude tener acceso, el cual me permitía hacer cualquier cosa que se me ocurría casi por arte de magia, es decir la misma electricidad que alumbraba mi casa era capaz de detectar el movimiento de mi mano en forma de puntero, para mí eso no tenía explicación.

Conforme fueron pasando los años mi interés por el mundo de los ordenadores siguió aumentando sin parar, lo que supuso que descubriera rápidamente el mundo de la Seguridad Informática, el cual desde un primer momento me llamó mucho la atención, pero por mucho que lo intentaba no conseguía encontrar la manera de empezar aprender, ya que, no tenía los conocimientos básicos necesarios y no sabía dónde practicar sin cometer ningún acto ilegal.

Aunque lo que realmente me ha llevado a hacer este proyecto fue cuando un amigo me mostró una página web donde podías comprometer máquinas virtuales en un entorno controlado y seguro. En ese momento realmente decidí poner todo mi esfuerzo en el aprendizaje de ciberseguridad, con el fin de superar nuevos retos, lo que conllevó a que me tirara más de un mes para completar mi primera máquina en esta plataforma.

Tras el esfuerzo y trabajo que he tenido que poner en los últimos años para aprender lo que sé actualmente sobre esta rama, surge la motivación de llevar cabo este proyecto, intentando de cierta forma ayudar a todas esas personas que como yo quieren comenzar a aprender sobre este mundo y no saben cómo empezar o dónde practicar.

Además, me gustaría destacar la importancia que tiene para mí un mundo con un mayor número de profesionales y gente con conocimientos en este sector, intentado de esta manera construir un futuro más seguro en internet para las personas y empresas.

1.2 Objetivos

El objetivo principal de este TFG es una contribución a la formación en seguridad informática orientado a todos los usuarios con un nivel medio o avanzado en informática, a través de la creación de un laboratorio de ciberseguridad en un entorno virtualizado enfocado como un reto para el usuario.

Los objetivos del TFG son los siguientes:

- Mostrar los aspectos más importantes de la seguridad informática, vulnerabilidades, repercusión en el mundo laboral, aprendizaje del uso de sistemas GNU/Linux, herramientas de virtualización, etc. para obtener una base con la que empezar a trabajar.
- Dar a conocer las plataformas de entrenamiento dedicadas a la ciberseguridad más importantes del mercado. Las cuales se usarán de base para el diseño de los distintos retos que se implementarán en las máquinas del laboratorio de ciberseguridad.
- Analizar y diseñar el entorno virtualizado utilizando una red de máquinas virtuales que replique la arquitectura de red de una empresa. Para cada una de las máquinas virtuales se analizará el sistema operativo a utilizar, los servicios que se ejecutarán y sus respectivas configuraciones.

- Aprender los aspectos más importantes de las diferentes vulnerabilidades de los sistemas informáticos: su uso y la forma de asegurarla.
- Aprender los aspectos más importantes de las herramientas que permiten asegurar un sistema informático.
- Implementar y probar el entorno virtualizado, con todas las vías de ataque que se hayan concretado durante la fase de análisis y diseño.
- Elaborar un informe que recoja todos los pasos seguidos en la realización del proyecto, así como una guía para el usuario que vaya a utilizar el entorno.

1.3 Planificación

En este caso se contará con ocho fases de desarrollo que serán necesarias completar para realizar el trabajo, estas fases sumarán un total de 300h:

1. **Reuniones (20 horas):** Reuniones con el profesorado en las que se definirán los requisitos del proyecto, el diseño de la red, las vulnerabilidades y resolución de posibles dudas.
2. **Estado del arte (50 horas):** Investigación sobre el estado actual de la formación en ciberseguridad en el ámbito académico, herramientas de virtualización más usadas en el mercado, ejemplos de máquinas virtuales vulnerables, tipos diferentes de vulnerabilidades y servicios más comunes en internet.
3. **Análisis (25 horas):** Una vez realizada la labor de investigación y determinados los límites en los que nos podemos mover, comienza la fase de análisis, en la que se determinara el hardware y software necesario, así como los conocimientos teórico-técnicos que se quiere que obtenga el usuario tras la realización del laboratorio.
4. **Diseño (20 horas):** En esta fase se realizará un diseño lo más detallado posible sobre la cantidad de máquinas virtuales que compondrá la red, así como sus sistemas operativos y las vulnerabilidades de cada una de ellas.
5. **Evaluación individual (35 horas):** Aquellas vulnerabilidades propuestas para formar parte de la red final, serán evaluadas en máquinas virtuales independientes en las que se medirán si estas pueden ser explotadas correctamente y se le atribuirá un nivel de dificultad.
6. **Implementación (60 horas):** Implementación de la red virtual a partir de un router basado en un sistema operativo Linux, el cual conectará el resto de las máquinas virtuales testeadas anteriormente, así como un cliente en la red externa que simulará tráfico a los distintos servicios de la red.
7. **Evaluación global (30 horas):** Se realizará una evaluación completa de la red en la que se comprobará que el usuario pueda tener acceso y explotar todas las vulnerabilidades propuestas, así como el correcto funcionamiento de todos los servicios.
8. **Documentación del proyecto (60 horas):** La documentación se realizará en dos fases:
   - **Documentación enfocada para el profesional que vaya a utilizar el entorno virtualizado.** Se documentará en forma de retos y dicha documentación irá ayudando al usuario con pistas y permitirá mostrar la consecución de los diferentes retos de seguridad.
   - **Documentación de todas las fases del proyecto.** A continuación, un diagrama Gantt en el que se muestra la cronología del proyecto por semanas:

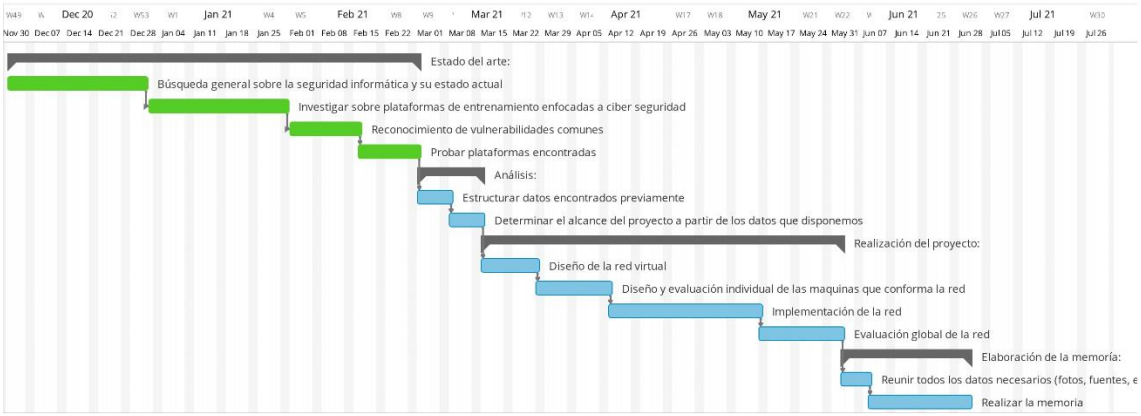

Ilustración 1-1: Cronograma etapas del TFG en semanas

1.4 Estructura de la memoria

Esta memoria está compuesta por cinco capítulos:

- **Introducción.** En este primer capítulo se expone la motivación, objetivos, planificación, estructura de la memoria y herramientas utilizadas, consiguiendo de esta forma determinar la naturaleza del proyecto.
- **Estado del arte.** Este capítulo recogerá la investigación previa realizada para conseguir los objetivos de este proyecto. En esta fase inicial de recolección de información se muestra la evolución de la seguridad informática en las últimas décadas, conceptos básicos sobre ataques y vulnerabilidades, diferencias entre términos del sector, datos sobre la formación en el área y además, se recopila y analizan datos sobre plataformas usadas por los profesionales del sector para poner a prueba sus conocimientos.
- **Diseño del laboratorio**. Corresponde con uno de los capítulos más importantes de la memoria, en el que se especifica la información sobre todas las máquinas que componen el entorno, siendo esta la necesidad de hardware, las vulnerabilidades y conexiones con las que cuenta cada una de ella, con el fin de definir las redes que compondrán el laboratorio.
- **Implementación.** Durante este capítulo se muestra la creación de máquinas virtuales, el desarrollo de las vulnerabilidades que componen el laboratorio y el desarrollo de la web de seguimiento.
- **Conclusiones y trabajo futuro.** En el último capítulo de la memoria se encuentran las conclusiones tras el esfuerzo de realizar el proyecto y las posibilidades a otros proyectos futuros podrían ser desarrollas partiendo del creado en esta memoria.

Además, la memoria cuenta con dos apéndices bastantes importantes.

- **Manual de juego.** El primer apéndice corresponde con un manual de juego, el cual será otorgado a aquellas personas que quieran realizar el laboratorio. Este manual cuenta con toda la información necesaria para desplegar el entorno y comenzar el desafío según los conocimientos del usuario.
- **Fichas técnicas de vulnerabilidades.** El segundo apéndice consiste en todas las fichas técnicas de las vulnerabilidades existentes en el entorno. En dichas fichas se recoge toda la información sobre estas, como puede ser detalles para llevarlas a cabo, próximos pasos tras explotar la vulnerabilidad, objetivos a conseguir, etc.

1.5 Herramientas utilizadas

La herramienta más importante utilizada en este proyecto se trata del software VMware Workstation [1], la cual consiste en un programa de virtualización que permite la ejecución segura de distintos sistemas operativos en forma de máquinas virtuales desde un mismo ordenador. Por lo tanto, esta herramienta es la utilizada tanto para desarrollar el laboratorio de ciberseguridad, como para que el usuario final pueda desplegarlo en su ordenador personal.

Continuando con la parte de software, a parte de esta herramienta de virtualización, también se va a hacer uso de un gran número de utilidades instaladas en Kali Linux [2], siendo este un SO enfocado para la realización de diversas tareas de seguridad de la información, como pueden ser pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa. Mediante las herramientas proporcionadas por este SO se realizarán todas las pruebas necesarias para verificar el correcto funcionamiento del proyecto, así como, la comprobación de que todas las vulnerabilidades funcionen según lo esperado.

Finalmente, en lo referente a la parte de hardware, se va a utilizar un ordenador doméstico de gama media, en la parte de virtualización de la red virtual.

Capítulo 2
Estado del arte

2. Estado del arte

No se puede hablar de seguridad informática sin tener en cuenta la evolución que esta ha experimentado durante los últimos años, conllevando consigo la creación de nuevos términos que últimamente son bastantes conocidos, pero que no todos tienen claros sus significados: ciberespacio, ciberguerra y ciberseguridad.

Con este marco global ya definido, se van a tratar las necesidades de formación en ciberseguridad del mundo actual, así como aquellas plataformas que ayudan a los interesados en el sector a seguir aumentando sus conocimientos, como a poner a pruebas los mismos.

2.1 Evolución de la seguridad informática

Con el fin de entender la evolución que se ha experimentado en esta área desde su comienzo hasta la actualidad, se va a realizar una breve explicación tomando como referencia el artículo “Cómo ha evolucionado la ciberseguridad en los últimos 25 años y cómo ha sido la evolución de seguridad en las empresas” [3], el cual, está basado en artículos del Instituto Nacional de Ciberseguridad (INCIBE) [4].

La evolución de la seguridad informática viene ligada con la evolución que han experimentado las empresas durante los últimos 30 años, comenzando por la década de los 70, cuando la seguridad de estas se basaba en la confianza y el sentido común de sus empleados para garantizar la seguridad de la organización, sin embargo, con los progresos tecnológicos que se dieron durante esa época dieron lugar a que esta “seguridad” quedara obsoleta.

El principal motivo que impulsó un cambio de tendencia en la seguridad de las empresas fue la aparición del malware, convirtiéndose este en los principales motores de la seguridad de la información a nivel mundial debido a la globalidad de sus objetivos.

Con la aparición de estos programas malignos y la popularización de los ordenadores personales durante la época de los 80 [5], apareció la primera generación de ciberamenazas caracterizada por la capacidad de réplica de estos programas. Aunque la presencia de Internet aún no se había extendido, estas amenazas podían distribuirse a través de disquetes, CDs o memorias USB, lo que supuso la creación de los primeros productos comerciales de antivirus tradicionales y la contratación de guardias por parte de las empresas para la protección física de ciertas instalaciones.

Ya en la década de los 90, llegó el internet tal y como lo conocemos hoy en día [6], lo que trajo consigo la segunda generación de ataques informáticos, provocada por aquellos cibercriminales que cada vez estaban más especializados en técnicas para robar dinero, comenzando a desarrollar técnicas que fueron las precursoras de la ciberdelincuencia actual. Ante esta situación, surgió la necesidad de desarrollar el primer firewall, con el fin de intentar mantener a las empresas protegidas de estos delincuentes, pero la seguridad de estas empresas seguía siendo insuficiente, ya que los empleados no contaban con ninguna concienciación sobre el uso de internet, la información se guardaba en dispositivos extraíbles sin ningún tipo de seguridad y la seguridad física en las instalaciones seguía sin ser suficiente.

En los años 2000 se produjo un incremento muy notable en el aumento de las vulnerabilidades que se encontraron, provocado por el cambio de tendencia producido en los ataques, los cuales empezaron a ser dirigidos a sistemas operativos, hardware y aplicaciones, viéndose estos ampliados por la adopción masiva del email y las redes sociales, las cuales ofrecían posibilidades de realizar ataques de ingeniería social.

Aunque las empresas intentaron adaptarse a estos ataques combinando firewalls y antivirus, asentando las bases de las infraestructuras empresariales de hoy en día, no fue suficiente, en mayor medida a causa de la velocidad a la que los ataques evolucionaban en sofisticación e impacto. Esto llevó consigo la aparición de organizaciones criminales durante la década de los años 2010, los cuales comenzaron a explotar vulnerabilidades de día 0 (zero-day) [7], conllevando consigo que estos ataques fueran más sigilosos y difíciles de identificar. Ante la situación de no poder reconocer las amenazas, se comenzó a desarrollar herramientas de detección de amenazas y a concienciar tanto a los empleados como a los ciudadanos sobre la seguridad de la información, naciendo de esta manera la primera ley de protección de infraestructuras críticas.

Finalmente, durante los últimos años hemos podido ver las capacidades de estas organizaciones criminales en ataques como el WannaCry [8], que afectó a más de 300.000 ordenadores en 99 países, el NotPetya, que causó pérdidas de 300 millones de dólares, y el ataque producido hace unos meses en 2021 al SEPE bajo el virus Ryuk, que conllevó a la paralización de varios servicios de esta entidad [9]. Es por ello por lo que, conforme se siga evolucionando tecnológicamente, seguirán apareciendo nuevas vulnerabilidades, haciendo el papel de los profesionales de este sector cada vez más importantes para garantizar la seguridad de los ciudadanos y empresas.

2.2 Ataques informáticos

Se entiende por ataque o amenaza informática a cualquier condición del entorno del sistema de información (p.ej. persona, máquina) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo) [10].

Las amenazas pueden ser categorizadas en cuatro categorías generales:

- **Interrupción:** Este consiste en un ataque contra la disponibilidad, en el cual un recurso del sistema es destruido o deja de estar disponible.
- **Intercepción:** Un ataque contra la confidencialidad en el que una entidad no autorizada consigue acceso a un recurso.
- **Modificación:** Consiste en la manipulación de recursos por una entidad no autorizada, correspondiéndose con un ataque contra la integridad
- **Fabricación:** Se trata de un ataque en contra de la autenticidad, en el cual una entidad no autorizada inserta objetos falsificados en un sistema.

Además, estos ataques se pueden clasificar en:

- **Ataques pasivos:** En este tipo de ataques, el atacante no altera la comunicación, sino que simplemente se encarga de monitorizarla con el fin de obtener información de lo que se está trasmitiendo.
- **Ataques activos:** Estos ataques implican la modificación o creación de datos, creando un falso flujo de estos. Además, estos se pueden dividir en cuatro categorías: suplantación de identidad, reactuación, modificación de mensajes, denegación de servicio.

Finalmente, en la tabla 2-1, extraída del libro mencionado anteriormente, se puede observar un resumen de los ataques más habituales.

Tabla 2-1: Tipos de ataques

Nombre	Descripción
Sistemas	
Explotar bugs del software	Utilizar fallos de seguridad en el software para atacar un sistema.
Romper contraseñas	Fuerza bruta o ataques basados en diccionarios que permiten obtener las contraseñas del sistema o de un determinado servicio.
Red	
Barridos de ping	Utilización del protocolo ICMP para determinar los equipos activos de una red.
Confianza transitiva	Aprovechar la confianza UNIX entre usuarios o hosts para tomar sus privilegios.
DNS spoofing	Falsificación de una entrada DNS que apunta a un servidor no autorizado
DoS	Ataque de denegación de servicio (DoS), que consiste en saturar un sistema para impedir la utilización correcta del sistema.
Fuzzer	Ataque que permite generar datos aleatorios para enviarlos a un servidor y detectar posibles fallos en su funcionamiento.
Hijacking	Permite a un usuario robar una conexión de un usuario que ha sido autentificado en el sistema.
Man in the middle	A través del ataque ARP spoofing el atacante se sitúa en medio de la comunicación entre varios equipos para realizar otros ataques, como sniffer, spoofing, phishing, etc.
Mensajes de control de red o enrutamiento fuente	Se envían paquetes ICMP para hacer pasar los paquetes por un router comprometido.
Navegación anónima	No se considera directamente un ataque, pero la suelen utilizar los atacantes para realizar sus fechorías. Se denomina “navegación anónima” cuando un usuario utilizar diferentes servidores proxy para ocultar su dirección IP.
Phising	Ataque informático que consiste en falsificar un sitio web para poder obtener las contraseñas de sus usuarios.
Reenvío de paquetes	Retransmisión de paquetes para engañar o duplicar un mensaje (p.ej. una transferencia).
Sniffer	Programa o equipo que registra todo el tráfico de una red. Se utiliza especialmente para obtener las contraseñas de los sistemas.
Spoofing	El atacante envía paquetes con una dirección fuente incorrecta. Las respuestas se envían a la dirección falsa. Pueden usarse para: (1) Acceder a recursos confiados sin privilegios (2) Para DoS (Deny of Service) directo como indirecto o recursivo.
VLAN Hopping	Técnica que permite tener acceso a tráfico de red de otra VLAN que normalmente es inaccesible.
Servidores web	
Inyección SQL	Ataque que consiste en modificar las consultas SQL de un servidor web para poder realizar consultas SQL maliciosas.
LFI (Local File Inclusión)	Ataque informático que consiste en hacer que un servidor ejecute un script que está alojado en el mismo servidor.
RFI (Remote File Inclusion)	Ataque informático que consiste en hacer que un servidor ejecute un script que está alojado en una máquina remota.

XSS (Cross site scripting)	Consiste en engañar al servidor web para que ejecute un script malicioso en el navegador del cliente que visita una determinada página.
Aplicaciones	
Crack	Software que permite romper la protección de una aplicación comercial.
Keylogger	Software o hardware que registra todas las pulsaciones de teclado que se realizan en el sistema.
Rootkit	Software que se instala en un sistema y oculta toda la actividad de un usuario (el atacante).
Troyano	Software que se instala en el ordenador atacado que permite al atacante hacerse con el control de la máquina.
Virus	Software que se copia automáticamente y que tiene por objeto alterar el normal funcionamiento del equipo sin el permiso o el conocimiento del usuario.
Varios	
Ingeniería social	Atacante que consiste en convencer a un usuario legítimo para que facilite información (contraseñas, configuraciones, etc.).
Rubber-hosse	Utilizar soborno o tortura para obtener una determinada información.

2.3 Vulnerabilidades

Una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos [11].

Aunque comúnmente se confunden los términos de vulnerabilidad y ataque o amenaza informática hay que destacar que estos no son iguales, ya que como se puede observar si analizamos las definiciones de estos términos, todas las vulnerabilidades sí son ataques o amenazas informáticas, pero no todos estos son vulnerabilidades.

2.3.1 CVE

En el área de la seguridad informática el termino vulnerabilidad suele ir muy ligado al de CVE (Common Vulnerabilities and Exposures), o en español vulnerabilidades y exposiciones comunes, el cual hace referencia a una lista de vulnerabilidades de seguridad conocidas, de las cuales se proporcionan todos los datos públicos existentes, como pueden ser: descripción de la vulnerabilidad, versiones afectadas, actualizaciones necesarias (si existen) o posibles soluciones para mitigar su alcance, referencias a páginas webs donde se ha publicado dicha vulnerabilidad o se ha puesto a prueba. Aparte, todas las CVE deben ir correctamente identificadas, utilizando el formato de la ilustración 2-1.

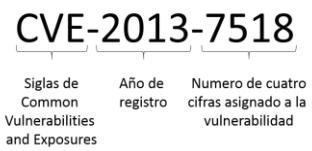

Ilustración 2-1: Formato CVE

Gracias a esto se puede consultar información sobre cualquier vulnerabilidad de la que se disponga su identificación, en sitios web como:

- https://cve.mitre.org/
- https://www.incibe-cert.es/
- https://nvd.nist.gov/
- https://vuldb.com/

2.3.2 Tipo de vulnerabilidades

En el caso de las vulnerabilidades, existen cuatro niveles principales en las que éstas se pueden clasificar, dependiendo de su nivel de impacto y severidad:

- **Crítico.** Las vulnerabilidades marcadas con un nivel crítico son aquellas que permiten a un atacante ejecutar código arbitrario o acceder a datos confidenciales. Debido a la alta peligrosidad de estas vulnerabilidades, se recomienda corregirlas inmediatamente.
- **Alto.** Los problemas marcados con gravedad alta permiten a los atacantes acceder a los recursos y datos de la aplicación vulnerable, consiguiendo de esta manera robar datos de sesión o datos privados de la aplicación y del servidor. En este caso también se recomienda corregir inmediatamente las vulnerabilidades de este nivel, ya que pueden dar lugar a que los atacantes encuentren otras vulnerabilidades de mayor impacto.
- **Medio.** Las vulnerabilidades encontradas en este nivel suelen ocurrir debido a errores y deficiencias en la configuración de la aplicación. Aprovechando estos problemas de seguridad los atacantes consiguen acceso a la información confidencial de la aplicación o servidor.
- **Bajo.** Las vulnerabilidades de este nivel incluyen la fuga de información, errores de configuración y la falta de medidas de seguridad. Estas se caracterizan en que a diferencia con los niveles vistos anteriormente (crítico, alto y medio), estos hallazgos tienen un efecto limitado.

2.3.3 Herramientas para explotar vulnerabilidades

En el área de la seguridad informática las vulnerabilidades son algo muy importante que se deben tener en cuenta en el día a día de cualquier administrador de sistemas, ya que cada año se descubren más y éstas pueden suponer riesgos para los sistemas a los que afectan. Debido a la gran cantidad y su correcta identificación, desde hace unos años se comenzó a crear herramientas con el fin de encontrar y poner a prueba la seguridad de los sistemas de información.

Existen una gran cantidad de utilidades con este fin, tanto es así, que incluso existen Sistemas Operativos dedicados a la ciberseguridad, como pueden ser Kali o Parrot, que cuentan con un gran número de estas herramientas: Nessus, Metasploit, Nmap, Burp Suit, etc.

Concretamente se va a profundizar un poco más en el caso de Metasploit, ya que ésta es una de las herramientas más utilizadas y más útil que se puede encontrar. Esta utilidad cuenta con una base de exploits de diferentes vulnerabilidades, la cual permite al usuario una vez detectada la vulnerabilidad ponerla a prueba en caso de que el exploit se encuentre en la base, permitiendo ver el alcance y el daño que ésta puede llegar a causar.

En la ilustración 2-2 se observa un ejemplo de la ejecución de Metasploit, en la que se muestra un resumen de la cantidad de módulos que contiene dicha herramienta.

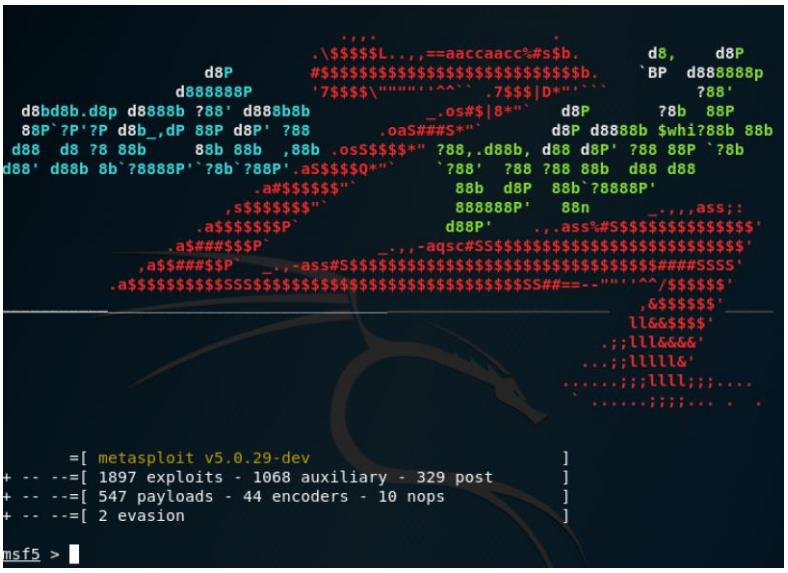

Ilustración 2-2: Metasploit

2.3.4 ¿Qué hacer después de una vulnerabilidad?

A la hora de comprobar la seguridad de un sistema es importante ponerse en la piel del atacante, es por ello por lo que una vez detectada una vulnerabilidad se debe intentar realizar las acciones que llevaría a cabo un intruso, con el fin de detectar otras posibles vulnerabilidades y observar el alcance que éstas pueden tener en el sistema.

En el caso de las vulnerabilidades de nivel medio o bajo, nos proporcionan información para seguir creando nuestro "vector de ataque". Por lo tanto, es necesario obtener más información que nos permita acceder a una vulnerabilidad más grave, con el fin de comprometer el sistema. Si se encuentra alguna vulnerabilidad más importante (alta o crítica) que permita acceder al sistema mediante un usuario no privilegiado (no root), el atacante deberá buscar diferentes vías para conseguir escalar privilegios y hacerse dueño del sistema, aparte se pueden analizar los ficheros de configuración y servicios activos, con el fin de encontrar nuevas vulnerabilidades en el sistema.

Además, al acceder al equipo de una red, puedes utilizar dicho equipo para analizar la red en la que esta se encuentra con el fin de encontrar nuevos objetivos.

Finalmente, en el caso de que se explote una vulnerabilidad crítica que permita al atacante obtener acceso con los máximos privilegios en el sistema, este debe de intentar mantener sus privilegios, tratar de ocultar su rastro e intentar que la máquina sea suya, para ello se suelen utilizar herramientas como rootkits, que permiten ocultar la información de un usuario especifico.

2.4 Ciberespacio, ciberseguridad y ciberguerra

2.4.1 Ciberespacio

Se conoce a William Gibson como el creador de la noción de ciberespacio, introduciéndolo por primera vez en un relato denominado Johnny Mnemonic en 1981, aunque el término no se dio a conocer hasta su siguiente novela Neuromante en 1984, la cual obtuvo el Premio Philip K. Dick, el Premio Hugo y el Premio Nébula, popularizando este concepto. También hay que destacar que este concepto deriva del término cibernética, el cual fue acuñado por Norbert Wiener en la década de 1940 para hacer referencia al estudio de las analogías entre los sistemas de comunicación y de control de las máquinas con los seres vivos.

El ciberespacio se define como “un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas” [12].

En la actualidad se suele relacionar este término a Internet, sin embargo, el ciberespacio es mucho más que Internet, este consiste en un espacio creado por el hombre para su servicio que se rige según sus propias leyes, el cual se ha visto impulsado con el avance tecnológico experimentado en las últimas décadas, ocasionando la gran dependencia que nuestra sociedad tiene sobre él.

Al enfocar este concepto sobre el mundo de la seguridad informática se pueden observar los siguientes aspectos:

- Este inmenso espacio permite a los delincuentes realizar ataques desde cualquier parte del mundo, logrando de esta manera mantener el anonimato y dificultar las labores de rastreo.
- Cualquier persona puede realizar un ataque sin necesidad de una gran inversión económica o en recursos humanos, causando efectos desproporcionados y daños.
- El ciberespacio no entiende de horas, cualquier dispositivo conectado a este es susceptible de ser atacado en cualquier momento.
- El aumento del nivel de complejidad de los ataques que se producen obliga a aquellas posibles víctimas a requerir de unos conocimientos técnicos avanzados con el fin de poder defenderse

2.4.2 Ciberseguridad

La ciberseguridad es el área de las ciencias de la computación encargada del desarrollo y la implementación de los mecanismos de protección de la información y de la infraestructura tecnológica [13].

Desde los inicios de Internet para uso personal a partir de los años noventa, tanto nuestro modo de vida como sociedad han experimentado una adaptación a esta nueva tecnología, llegando hasta el punto en el que, si esta tecnología llegara a desaparecer o se viera comprometida, el mundo entero podría llegar a descontrolarse.

Esta gran inmersión que ha tenido Internet en la vida de las personas se debe en su mayor parte al desarrollo que han experimentado los smartphones durante los últimos años, así como, a la creación de todo tipo de aplicaciones informáticas, que han dado lugar a que sus usuarios puedan realizar casi cualquier actividad desde su dispositivo móvil, como pueden ser realizar cualquier trámite en un banco o comprar un producto.

Con el avance que han supuesto estas tecnologías, las relaciones de nuestra sociedad se han visto sometidas a un cambio, donde ciudadanos y gobiernos no consiguen encontrar la manera de convivir en este ciberespacio. Esto se debe principalmente a la evolución que han experimentado los cibercriminales, los cuáles han pasado de ser adolescentes, que cometían ciberdelitos simplemente para satisfacer su curiosidad o demostrar lo que eran capaces de hacer, a bandas criminales, mafias e incluso organizaciones terroristas que utilizan los vacíos legales de este ciberespacio para llevar a cabo sus fechorías.

Aunque es cierto que durante los últimos años la inversión de las empresas en ciberseguridad ha sido menor que la inversión en la protección de sus activos físicos (muebles, dispositivos…), se está viendo un cambio de tendencia en este aspecto, producida principalmente por la situación provocada por el Covid-19, provocando que los ciudadanos incorporen a su vida cotidiana el comercio electrónico, el teletrabajo, el consumo de ocio digital o la teleeducación, volviéndose estos elementos, que antes cada vez estaban más presentes, en algo indispensables. Esto ha conllevado que las personas se den

ahora más cuenta que nunca de la importancia de la ciberseguridad, dando lugar a la siguiente frase "La ciberseguridad nunca ha sido tan visible y quizás nunca hemos sido tan conscientes de la dependencia que tenemos de ello" de Félix Barrio, gerente de Ciberseguridad para la Sociedad del INCIBE [14].

Esta situación ha derivado a que el número de amenazas cibernéticas se haya multiplicado en los últimos años de manera exponencial [15], produciéndose además un cambio en la naturaleza de éstas. Se ha pasado de amenazas conocidas, puntuales y dispersas, a amenazas de gran sofisticación con objetivos muy concretos y persistentes.

Tal y como se observa en la ilustración 2-3 sacada del informe The Global Risks Report 2021 [16], en el que se observan los sucesos de riesgo global según su interconexión actual entre riesgos económicos, medioambientales, geopolíticos, sociales y tecnológicos, se puede observar que para un futuro próximo y medio se encuentra un fallo en ciberseguridad, demostrando la importancia que estos pueden tener para el mundo actual.

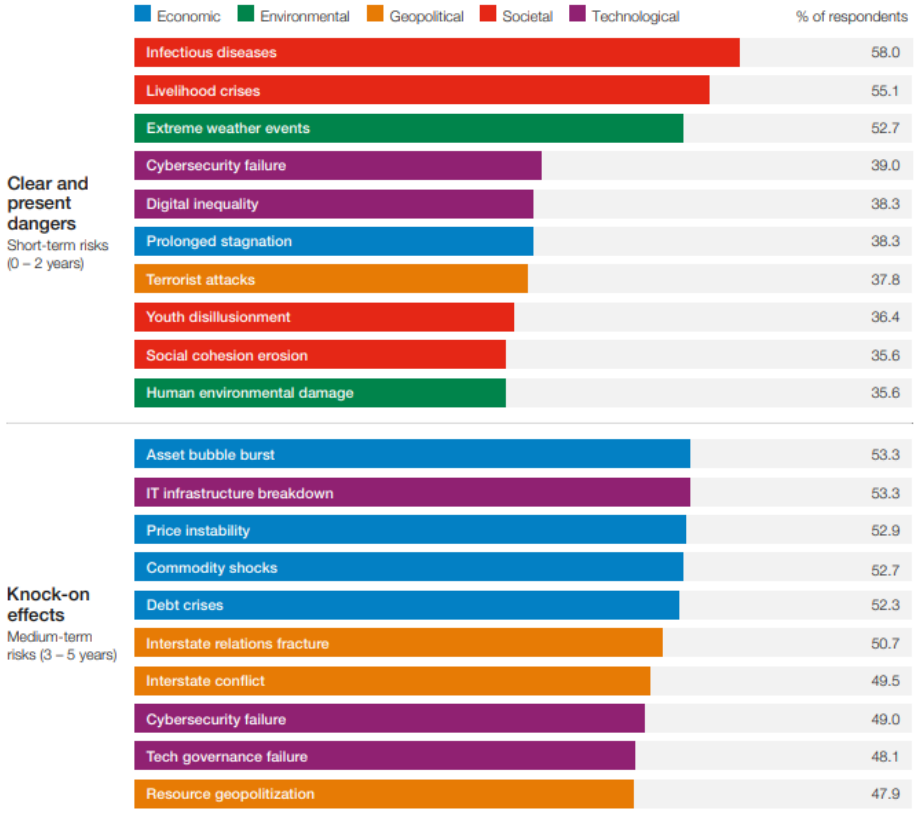

Ilustración 2-3: Horizonte global de riesgos

Teniendo en cuenta que nos encontramos en un mundo en el que todo funciona a través de Internet, no es de extrañar que un fallo de ciberseguridad pueda suponer una catástrofe para el mundo entero, encontrándose por encima incluso de lo que supondría un ataque terrorista. Es por estos motivos, que debemos considerar esta área de las ciencias como una necesidad, ya que en el caso de que no estemos preparados, el día de mañana puede suceder una catástrofe.

Esta situación ha acelerado el aumento de la importancia de la ciberseguridad para las empresas, generando la necesidad de más profesionales en el sector y aumentado entorno al 70% la inversión realizada en esta área durante el año 2021.

2.4.3 Ciberguerra

Desde el comienzo de la historia el ser humano ha luchado por todo espacio que ha podido dominar (cielo, tierra y mar), por ello no es de extrañar que en este nuevo ciberespacio tampoco reine la paz. Con el fin de hacer referencia a estos conflictos, que toman el ciberespacio y las tecnologías de la comunicación e información como campo de batalla [17] se crearon los términos guerra informática, guerra digital o ciberguerra.

Estudios recientes demuestran como en la actualidad es más fácil derrotar a un enemigo atacando a su infraestructura informática, que llevando a la práctica cualquier otro tipo de ataque físico. Convirtiéndose esta estrategia en un arma, ya sea en ofensivas militares entre países, ataques de ciberdelincuentes a entidades gubernamentales… Con esto llegamos a entender como el malware se ha convertido en las armas de esta época, construidas con el fin de anular los sistemas informáticos del enemigo, convirtiéndose por tanto los combatientes en expertos en informática y telecomunicaciones. Aunque por norma general las víctimas de estos ataques de gran calibre suelen estar dirigidos a sistemas financieros, bancarios y militares, se han visto numerosos casos donde se ven afectados los sistemas de comunicación de un país.

Estos ataques han aumentado en número y envergadura durante estos últimos años, encontrándose entre los más comunes los ataques de denegación de servicios distribuido (DDos), el secuestro de dispositivos a través del envenenamiento del DNS y la utilización de técnicas para incapacitar los antivirus con el fin de poder enviar malware para que se ejecuten sin restricciones.

Pero, la amenaza más importante a la que nos enfrentamos en esta época consiste en la propagación de datos confidenciales, pudiendo estos llegar a comprometer incluso a una nación entera, así como el peligro de que sea eliminada información vital. También se da el caso de propagación de información falsa a través de la red, provocando que los ciudadanos cambien su punto de vista sobre un tema en específico, consiguiendo de esta manera controlar la opinión de la gente sobre un producto, las causas de un accidente, etcétera.

Para entender la gravedad de esta guerra informática, nos vamos a fijar en el caso del exploit EternalBlue [18], el cual fue desarrollado por la NSA (National Security Agency) y filtrado por el grupo de cibercriminales Shadow Brokers el 14 de abril de 2017, dando lugar a que se usara en el ataque mundial de ransomware con WannaCry el 12 de mayo de 2017, afectando a más de 99 países y causando estragos en empresas de salud, telecomunicaciones, suministros electicos… en todo el mundo.

Por estos motivos se debe tener en cuenta que la ciberguerra no solo afecta a los bandos que la conforman, sino también a los civiles de todos los estados que dependan de la tecnología para que todo siga funcionando correctamente.

2.5 Formación en ciberseguridad

Partiendo de la situación descrita en el apartado anterior, en la que nos encontramos ante un enorme ciberespacio expuesto a amenazas continuas y con una velocidad de crecimiento acelerada por los desafíos que ha traído el covid-19 desde el punto de vista de la seguridad informática, no es de extrañar que el aumento de la demanda de profesionales de este sector se haya visto disparada durante los últimos años, ocasionando la falta de personal cualificado para cubrir esta alta demanda.

Esta brecha continuará creciendo durante los próximos años, sobre todo, si a esta situación le sumamos las predicciones que hablan de que en cinco años habrá más de 26 ciudades inteligentes,

que para el 2030 habrá una red global compleja conformada por 200 mil millones de dispositivos y que por cada individuo existirán más de 20 dispositivos conectados.

Teniendo en cuenta la alta demanda que existe, es muy importante formar a nuevos profesionales en esta área. Para ello en primer lugar se va a observar los perfiles que actualmente están siendo más contratados, correspondiéndose con aquellos que cuentan con al menos un título de grado, y es que cada vez hay más universidades alrededor del mundo que ofrecen carreras de grado en ingeniería informática, pero como esta no es aún una titulación que pueda encontrarse en todas las instituciones, ha ocasionado que muchos profesionales se formen a través de certificaciones y de manera autodidacta, llegando haber un 12% de profesionales que solo cuentan con estudios de educación secundaria finalizados.

2.6 Plataformas de entrenamiento

Las plataformas de entrenamiento son aquellas que permiten a los usuarios tanto poner a prueba, como aprender nuevos conocimientos sobre analista de seguridad o hacking en un entorno controlado. Esto implica que la utilización de técnicas que podrían considerarse ilegales en el mundo exterior, se puedan llevar a cabo en este entorno sin realizar ningún daño real y por lo tanto de una manera legal. Dichas plataformas pueden llegar a ser muy variadas, pero la mayoría coinciden en tener acceso a una gran variedad de ataques que se clasifican según el tipo, nivel de dificultad, etc.

Con la situación en la que nos encontramos actualmente caracterizada por la falta de personal formado en seguridad informática y la importancia que ha cobrado esta durante los últimos años, ha dado lugar a la creación de varias plataformas de entrenamiento con mucho nivel de desarrollo, llegando incluso a realizarse competiciones basadas en las mismas prácticas que se realizan en estas plataformas.

A continuación, veremos algunos ejemplos de estas plataformas, así como de máquinas vulnerables que podemos encontrar en ellas, aunque cabe destacar que siempre podemos crear nuestra máquina, siendo esto tan sencillo como descargarse alguna versión de SO (Sistema Operativo) o de software desactualizado y comprobar las vulnerabilidades que existen en dicho sistema o servicio.

2.6.1 THM (TryHackMe)

En primer lugar, se va a hablar de THM (https://tryhackme.com) [19], esta plataforma puede ser considerada de las más apropiadas para principiantes, ya que, aunque cuente con máquinas y retos de diferentes niveles, ésta cuenta con las soluciones a todos ellos, para que se puedan consultar en caso de quedarse atascado. A parte, cuentan con una gran cantidad de retos sencillos en los cuales se explican paso a paso todo lo que se debe hacer para comprometer el objetivo. Estos casos vienen muy bien para aquellos usuarios inexpertos que se están iniciando en este mundo.

Otro aspecto positivo es que, aunque trabajan con máquinas virtuales online, éstas son creadas para cada usuario de forma independiente, consiguiendo de esta manera evitar que otros usuarios puedan modificar la máquina o que ésta se sature si hay demasiados usuarios intentando comprometerla, tal y como veremos que sucede en otras plataformas.

Ilustración 2-4: Web TryHackMe

Una vez que tenemos una visión general de esta plataforma veamos tres ejemplos de máquinas vulnerables disponibles.

Anonymous

La primera máquina para analizar se trata de una GNU/Linux para la cual, tal y como se ve en la Ilustración 2-5, se realizan una serie de preguntas para medir nuestro progreso. Cabe destacar que las preguntas "user.txt" y "root.txt" son comunes para casi todos los CTF (Capture The Flag), ya que, a través de estos dos archivos se comprueba si se ha conseguido entrar al sistema y si se ha conseguido privilegios de administrador. También hay que destacar que la web cuenta en algunas ocasiones con un botón "Hint", el cual proporciona una pequeña pista para poder seguir avanzando en el reto propuesto.

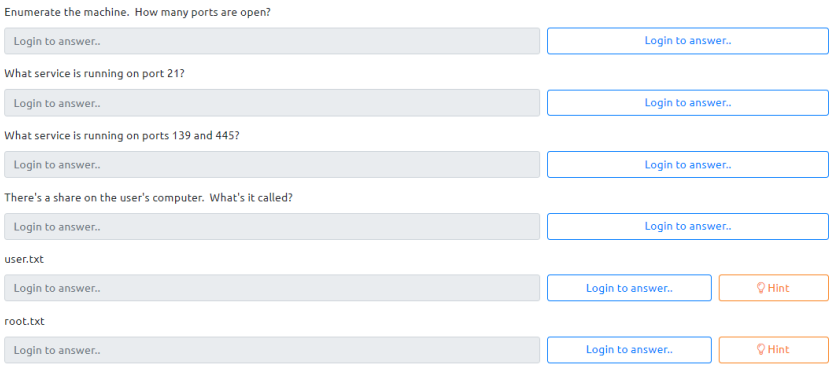

Ilustración 2-5: Progreso en máquina Anonymous

En el caso de esta MV, el propio nombre es una pista, ya que, para resolverla se necesita acceder mediante el usuario Anonymous al servicio ftp, el cual permite modificar un script que se ejecuta periódicamente. Con esto se llega a entender como cualquier elemento en estas plataformas puede llegar a ser una pista, aunque a veces nos tropecemos con algún rabbit hole, que viene a significar como un camino sin salida.

Finalmente, en la Tabla 2-2 se observa un resumen de las características de esta máquina, la cual será utilizada para realizar una comparativa entre las distintas máquinas que se analicen.

Tabla 2-2: Resumen Anonymous

Nombre	Anonymous
URL	https://tryhackme.com/room/anonymous
Modo: MV / Online	Online
Nº de MVs que utiliza	1
SO que utiliza	GNU/Linux
Se enfoca en modo de un reto	Sí
Tiene documentación	Sí
Tiene soporte (foro...)	Sí
Dificultad	Media

Overpass

Esta máquina, tal y como se observa en la Tabla 2-3, trata de un sistema GNU/Linux, con un nivel de dificultad fácil, aunque en este caso tan solo cuenta con las preguntas de "user.txt" y "root.txt". De la misma forma que en la MV anterior, el nombre es una pista, ya que, para conseguir el acceso a la máquina necesitarás sobrepasar un panel de login que se encuentra en el servicio web que tiene activo.

Aparte, tal y como se mencionó en la descripción de esta plataforma, aunque esta máquina virtual no cuente con pistas, ni preguntas que vayan dirigiendo tu proceso por el camino correcto, sí que cuenta con una documentación que se puede consultar en cualquier momento permitiendo a aquellos usuarios más inexpertos seguir avanzando en el caso de que se queden atascados en un punto.

Tabla 2-3: Resumen Overpass

Nombre	Overpass
URL	https://tryhackme.com/room/overpass
Modo: MV / online	Online
Nº de MVs que utiliza	1
SO que utiliza	GNU/Linux
Se enfoca en modo de un reto	Sí
Tiene documentación	Sí
Tiene soporte (foro...)	Sí
Dificultad	Fácil

Startup

La última máquina que se analizará de esta plataforma, aparte de estar planteada como un reto como las demás, cuenta con el extra de que la proponen como una situación "real", en la cual una empresa ha montado su servidor web y pide al usuario que realice una prueba de penetración para intentar obtener un ingrediente secreto que usan para sus productos, siendo el mismo la respuesta que necesitas para completar el reto.

En el resto de los aspectos es bastante similar a las anteriores, tal y como se observa en la Tabla 2-4 de características.

Tabla 2-4: Resumen Startup

Nombre	Startup
URL	https://tryhackme.com/room/startup
Modo: MV / online	Online
Nº de MVs que utiliza	1
SO que utiliza	GNU/Linux
Se enfoca en modo de un reto	Sí
Tiene documentación	Sí
Tiene soporte (foro...)	Sí
Dificultad	Fácil

2.6.2 HTB (HackTheBox)

La siguiente plataforma para analizar se trata de HTB (https://www.hackthebox.eu) [20], siendo de las plataformas más conocidas de este sector, sino la que más. Esto se debe principalmente a que esta fue una de las primeras plataformas de MVs online vulnerables, aparte de que el nivel de sus máquinas suele ser más complejo que el de sus principales competidores, llegando éstas a ser parte de la formación de muchos profesionales que optan a certificaciones de gran reconocimiento, como puede ser la OSCP [21].

Hay que destacar que no todo es tan bueno en esta plataforma, ya que cuenta con el inconveniente de que las máquinas vulnerables no son creadas para cada usuario específicamente, sino que existe, por norma general, una única máquina para todos los usuarios, lo que supone que en algunas ocasiones la experiencia del usuario se vea afectada por el resto de usuario de la plataforma.

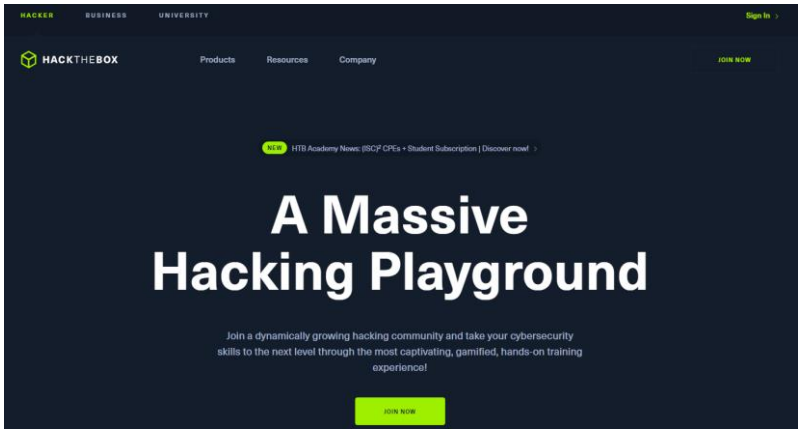

Ilustración 2-6: Web HackTheBox

También es cierto que al llevar tanto tiempo en funcionamiento, se ha formado una gran comunidad, a la cual se le pueden consultar dudas, ya que no existen soluciones publicadas para las máquinas (de acceso gratuito) como en el caso de THM. Esto es así, porque HTB tiene un sistema de puntuación interno, el cual clasifica a los usuarios según sus máquinas superadas.

Doctor

En el caso de las MVs de esta plataforma, solo existe una manera de comprobar que se ha obtenido acceso a la máquina, siendo ésta, facilitar el contenido de los archivos “user.txt” y “root.txt”.

La máquina Doctor de esta plataforma se encuentra retirada. Esto significa que aparte de que para tener acceso a ella se debe ser miembro VIP, lo que conlleva un pago mensual a la plataforma, ésta cuenta con documentación que ilustra cómo se resuelve la máquina, ya que una vez que se retiran, dejan de contar para la clasificación de la plataforma y por lo tanto la comunidad publica sus resoluciones. En la Tabla 2-5 se muestra las características de esta MV.

Tabla 2-5: Resumen Doctor

Nombre	Doctor
URL	https://www.hackthebox.eu/home/machines/profile/278
Modo: MV / online	Online
Nº de MVs que utiliza	1
SO que utiliza	GNU/Linux
Se enfoca en modo de un reto	No
Tiene documentación	Sí
Tiene soporte (foro...)	Sí
Dificultad	Media

Worker

Worker es otra máquina de dificultad media. No obstante, se debe tener en cuenta que el grado de exigencia de las MVs de nivel medio en esta web es equiparable con aquellas de nivel difícil en otras plataformas, suponiendo estos retos asumibles por muy pocos usuarios. Sus características se muestran en la Tabla 2-6.

Tabla 2-6: Resumen Worker

Nombre	Worker
URL	https://www.hackthebox.eu/home/machines/profile/270
Modo: MV / online	Online
Nº de MVs que utiliza	1
SO que utiliza	Windows
Se enfoca en modo de un reto	No
Tiene documentación	No
Tiene soporte (foro...)	Sí
Dificultad	Media

CrossFitTwo

Finalmente, no se podía dejar pasar esta plataforma sin ver una de sus máquinas de máximo nivel de dificultad (Tabla 2-7), siendo ésta una de las máquinas con más nivel que puedes encontrar ahora mismo en el mercado. Tras observar la Ilustración 2-7, se puede entender su grado de complejidad teniendo en cuenta que solo 297 usuarios han conseguido llegar al archivo “user.txt”, mientras que para el resto de las máquinas suele haber más de dos mil usuarios que consiguen esta meta. La Tabla 2-7 resume sus características.

Ilustración 2-7: Estadísticas CrossFitTwo

Tabla 2-7: Resumen CrossFitTwo

Nombre	CrossFitTwo
URL	https://www.hackthebox.eu/home/machines/profile/299
Modo: MV / online	Online
Nº de MVs que utiliza	1
SO que utiliza	GNU/Linux
Se enfoca en modo de un reto	No
Tiene documentación	No
Tiene soporte (foro...)	Sí
Dificultad	Muy difícil

2.6.3 MVs offline

Aunque en el mercado predominen las plataformas de entrenamiento online, gracias a las facilidades que estas suponen para el usuario final, pudiendo acceder a estas máquinas sin tener que gastar los recursos de su ordenador en mantenerla, también existen varias plataformas que facilitan MVs que se pueden descargar y desplegar en tu propio ordenador, trabajando de esta manera en tu entorno legal y asegurando que puedes practicar con ellas, sin ningún inconveniente legal o de conexión.

Es por ello por lo que a continuación, se van a mostrar algunos ejemplos de estas máquinas para permitir ver la diferencia con las anteriores en una comparación final.

Vulnhub

Vulnhub (https://www.vulnhub.com/) es una plataforma en la que cualquier usuario puede subir sus propias máquinas vulnerables con el fin de ayudar al resto de usuarios a practicar, siendo esta la única que permite a los usuarios llevar a cabo esta acción entre las que hemos visto. Gracias al apoyo que ha tenido esta idea, la página cuenta actualmente con más de 600 retos y MVs con los que poder practicar.

Además, cuenta con seis niveles de dificultad que comprenden niveles desde “Muy Fácil” a “Muy Difícil”, dependiendo de unas pautas impuestas por la propia página, consiguiendo de esta manera ayudar a los usuarios a encontrar aquellas máquinas que más le convencen. Aparte, este sistema de clasificación es más realista que en algunas plataformas.

En este caso vamos a realizar una tabla comparativa de una máquina virtual denominada “hacksudo: FOG”, creada por el autor Vishal Waghmare, con un nivel de dificultad fácil, tal y como se muestra en la siguiente Tabla 2-8.

Tabla 2-8: Resumen hacksudo: FOG

Nombre	hacksudo: FOG
URL	https://www.vulnhub.com/entry/hacksudo-fog,697/
Modo: MV / online	Offline
Nº de MVs que utiliza	1
SO que utiliza	GNU/Linux

Se enfoca en modo de un reto	Sí
Tiene documentación	Sí
Tiene soporte (foro...)	Sí
Dificultad	Fácil

Metasploitable2

En este caso, aunque no se va a hablar de una plataforma de entrenamiento como tal, nos encontramos ante Metasploitable2 (https://docs.rapid7.com/metasploit/metasploitable-2/), una máquina virtual preconfigurada con una serie de configuraciones y vulnerabilidades pensadas para permitir al usuario depurar sus técnicas de hacking utilizando exploits como, por ejemplo, mediante el uso de la herramienta metasploit.

Existen tres versiones de Metasploitable. La primera de ellas data de hace 9 años, la segunda de hace 6 años y la tercera (Metasploitable3), la versión más reciente de esta máquina virtual vulnerable, de hace cuatro de años. Se ha escogido la segunda ya que ésta cuenta con bastantes vulnerabilidades muy fáciles de explotar (Tabla 2-9), convirtiéndola en una perfecta candidata para personas con muy poca formación en el área.

En el caso de esta máquina la encontraremos disponible para las plataformas de virtualización VMware, VirtualBox y KVM, siendo VMware la recomendada por los desarrolladores de esta máquina.

Tabla 2-9: Resumen Metasploitable2

Nombre	Metasploitable2
URL	https://fwhibbit.es/toolkits-para-hacking-iii-maquinas-vulnerables-para-practicar
Modo: MV / online	MV
Nº de MVs que utiliza	1
SO que utiliza	GNU/Linux
Se enfoca en modo de un reto	No
Tiene documentación	Sí
Tiene soporte (foro...)	No
Dificulta	Muy Fácil

2.6.4 Comparativa entre plataforma de entrenamiento

Tras analizar distintas plataformas de entrenamiento que ponen a disposición de los usuarios varias MVs vulnerables, ya sean online u offline, con las que probar e incrementar los conocimientos en el área de la seguridad informática de una forma legal y segura, se ha elaborado la tabla 2-10, en la que se recoge información de interés sobre cada una de estas plataformas. Además, se ha añadido una última fila en la que se muestra información sobre el laboratorio que se ha propuesto para este Trabajo Fin de Grado.

Tabla 22-100: Tabla comparativa

	Diferentes modos de dificultad para la misma MV	Guía de usuario	Entornos con varias MVs	Seguimiento del progreso
TryHackMe	No	Sí	No	Sí
HackTheBox	No	No	No	Sí
Vulnhub	No	No	No	No
Metasploitable	Sí	No	No	No
Laboratorio propuesto	Sí	Sí	Sí	Sí

Como se muestra la tabla, casi todas las plataformas diseñan sus máquinas virtuales enfocándose en una dificultad determinada, en vez de realizar entornos en los que usuarios de todos los niveles puedan conseguir superar los objetivos. Sin embargo, en el caso del laboratorio propuesto, se pretende conseguir que todos los usuarios puedan conseguir superar la totalidad de los retos del entorno.

Otros aspectos muy importantes a tener en cuenta son la falta de seguimiento del progreso realizado dentro de una máquina concreta y la falta de guías que sirvan de ayuda a los usuarios más inexpertos durante el proceso de resolución de una máquina. Estos hechos se han visto muy claramente en las descripciones de estas plataformas de entrenamiento, las cuáles muestran como la única información proporcionada es conseguir los archivos “user.txt” y “root.txt”, e incluso ni esa información en casos como Vulnhub o Metasploitable. Este ha sido el motivo principal que ha conllevado el desarrollo de un portal web de seguimiento dentro del entorno, el cual actuará tanto de guía como de indicador de progreso para los usuarios que utilicen este laboratorio.

Aunque la carencia más importante que se ha hallado tras analizar los datos obtenidos ha sido la falta de entornos con más de una máquina virtual. De esta forma, no se pueden emular entornos reales de virtualización con varias MVs, de distintos SO, que se comuniquen entre ellas en el que el usuario pueda poner a prueba sus conocimientos. A raíz de esta necesidad surge este proyecto fin de carrera, el cual será enfocado a modo de reto y contará con varios niveles de dificultad para adaptarse a la mayor cantidad de perfiles posibles.

Finalmente, gracias a este trabajo de análisis se desarrollará el diseño de nuestro proyecto, teniendo en cuenta aquellas vulnerabilidades más comunes que se suelen encontrar en estas plataformas, así como, clasificar éstas según su nivel de dificultad con criterios más sólidos sobre la materia.

Capítulo 3
Diseño del laboratorio

3. Diseño del laboratorio

3.1 Introducción

En este capítulo se muestra el diseño y características del laboratorio de seguridad que se va a implementar durante la realización del proyecto. Para diseñar el laboratorio de seguridad se han tenido en cuenta las siguientes premisas:

- Red heterogénea con máquinas virtuales de diferentes sistemas operativos que permitan tipos de ataques según su naturaleza o nivel de dificultad.
- Diferentes tipos de vulnerabilidades que permitan vectores de ataque a nivel de servicio, servidor web, local, red y ajeno al sistema.
- Distintas opciones de configuración inicial según el nivel de dificultad elegida por el usuario.
- Reducción del consumo de recursos de CPU y RAM, asegurando que un ordenador de gama media pueda desplegar el laboratorio completo.
- Posibilidad de ejecutar toda la red en conjunto o de probar las máquinas de forma independiente unas de otras.

Para realizar el diseño de la plataforma se han establecido las siguientes fases:

- **Esquema de red.** Creación de un esquema de red general en el que se basará el laboratorio.
- **Interrelaciones de los sistemas.** Se muestran las conexiones que existirán en la red entre los distintos sistemas que la componen.
- **Especificaciones de los equipos.** Se expone toda la información inicial de las máquinas que componen la red.
- **Vulnerabilidades del sistema.** Para cada equipo de la red, se detalla su funcionamiento, así como el nivel de dificultad de las vulnerabilidades del sistema.
- **Puesta en marcha.** Se ha construido un manual para el proceso de despliegue y puesta en marcha de las máquinas virtuales del entorno. El manual se encuentra disponible en el Apéndice I.- Manual del juego.

3.2 Esquema de red

En la ilustración 3-1 se muestra el esquema de red del laboratorio de seguridad. En este esquema se puede diferenciar entre dos redes que se encuentran interconectadas entre sí y con acceso a Internet mediante un router:

- **La red de servidores** que será en la que se encuentren todos los servidores.
- **La red interna** en la que se encontrará el cliente.

La red está compuesta por 5 máquinas que se gestionan de la siguiente forma:

- **3 servidores.** La red de servidores cuenta con tres servidores con varios servicios activos.
- **1 router.** Un router para dar acceso a Internet y dirigir el tráfico de la red de servidores hacia a la interna y viceversa.
- **1 cliente.** Un cliente encargado de simular tráfico desde la red interna hacia la red de servidores.

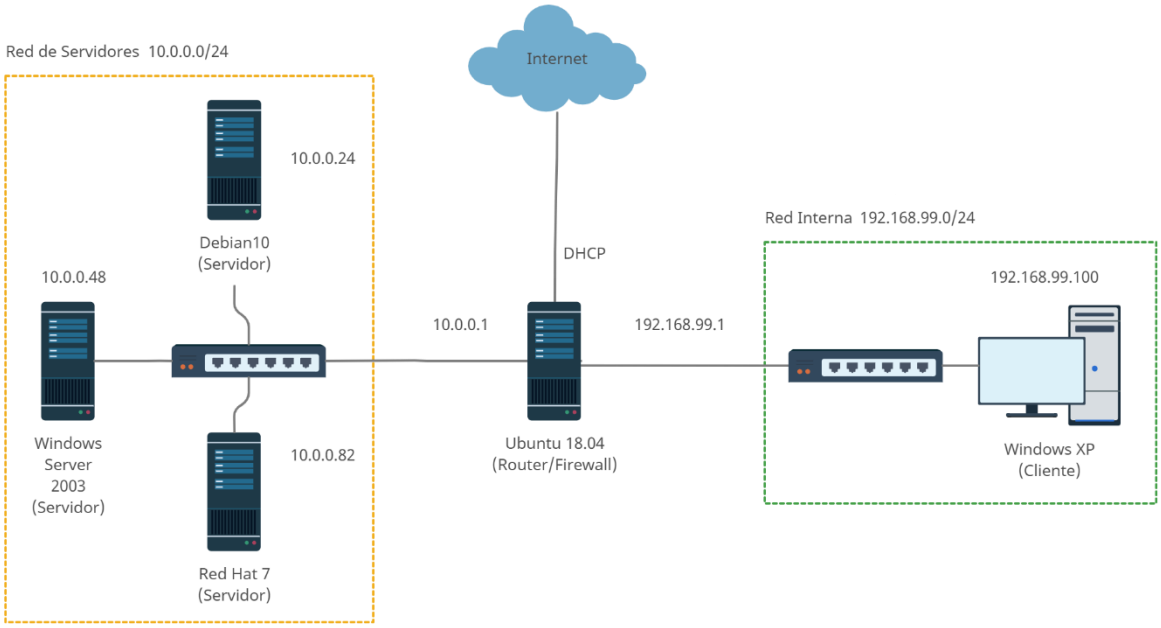

Ilustración 3-1: Esquema de red

Con el esquema de red definido, en la Tabla 3-1 se indica las direcciones IP asociadas a cada máquina y sus respectivas puertas de enlace.

Tabla 3-1: Tabla Esquema de Red 1

Máquina Virtual	Dirección IP	Puerta de enlace
Debian 10	10.0.0.24	10.0.0.1
Windows Server 2003	10.0.0.48	10.0.0.1
Red Hat 7 (Seawolf)	10.0.0.82	10.0.0.1
Ubuntu 18.04 LTS	DHCP	DHCP
Windows XP	192.168.99.100	192.168.99.1

3.3 Interrelaciones de los sistemas

En la ilustración 3-2 se muestra el esquema lógico de la red en el que se observan las comunicaciones entre los distintos sistemas que conforman el laboratorio.

Para diferenciar entre los distintos tipos de conexiones que se dan entre los sistemas, estas se van a representar por flechas de diferentes colores:

- **Flecha Naranja.** Indican las redirecciones de puertos que existirán entre el router y los servidores, para poder acceder a sus servicios desde las redes externas a la red de servidores
- **Flecha Verde.** Indica una conexión de subida de archivos a un servicio FTP
- **Flecha Azul.** Corresponde con el tráfico que simula nuestro sistema cliente en la red.

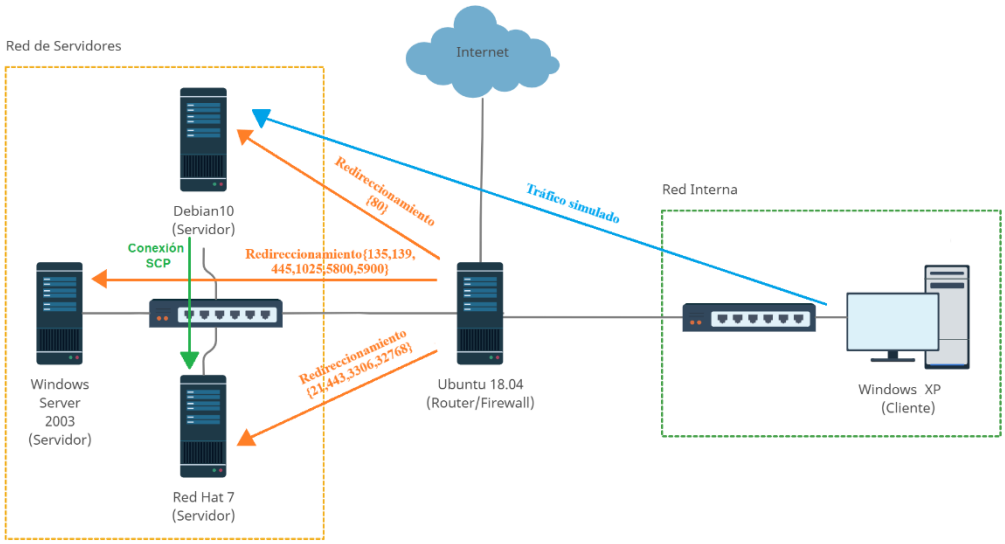

Ilustración 3-2: Esquema Lógico de red

3.4 Especificaciones de los equipos

A continuación, se muestran las especificaciones de los diferentes sistemas que conforman la red del proyecto.

3.4.1 Red Hat 7.1 (Seawolf)

El servidor Red Hat se utiliza para dar servicio a un portal web, además de disponer de un servicio ftp para las copias de seguridad. A continuación, en las tablas 3-2 y 3-3 se pueden observar las características de esta máquina.

Las especificaciones iniciales se muestran en la Tabla 3-2 y los servicios activos en la Tabla 3-3.

Tabla 3-2: Especificaciones Red Hat 7.1

Dispositivo	Resumen
Disco duro	4 GB
Tarjeta de red	1 Host-Only
Memoria RAM necesaria	256 MB
Procesadores	1
Sistema Operativo	Red Hat 7.1 (Seawolf)

Tabla 3-3: Red Hat 7.1 (Servidor) - Puertos y servicios

Puerto	Servicio
21	WU-FTPD wu-2.6.1-16
22	OpenSSH 2.5.2p2
80	Apache 2.0.47
111	RPC
443	Apache 2.0.47
3306	MySQL 4.0.14
32768	RPC

En los puertos 80 y 443 se encuentra el servicio apache para la implementación de un portal web. Para este servicio, se ha diseñado 5 retos sobre hacking web (ilustración 3-3), con los que los usuarios podrán poner a prueba sus conocimientos.

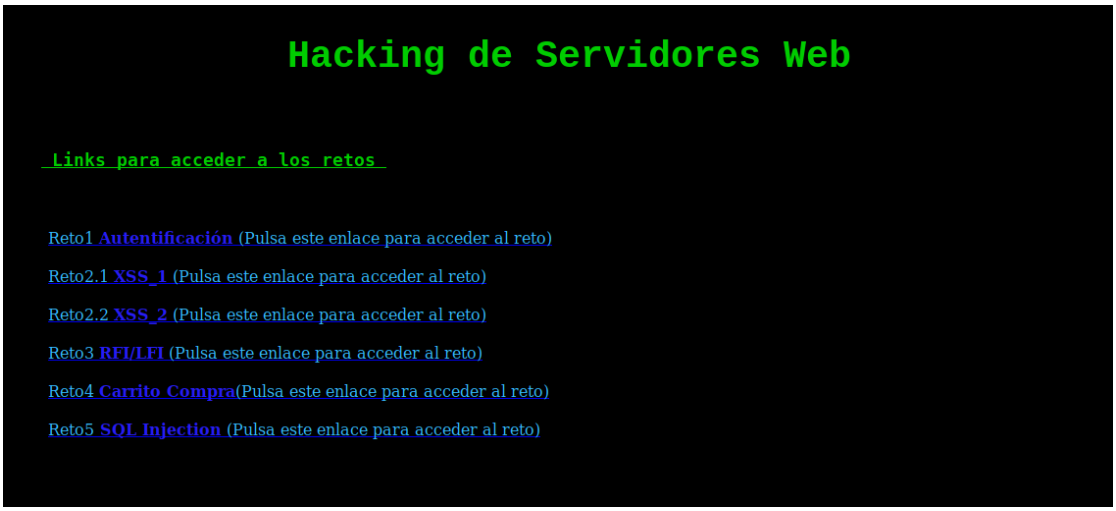

Ilustración 3-3: Web: Hacking de Servidores Web

3.4.2 Windows Server 2003

Este servidor simula estar en fase de desarrollo, por lo que solo cuenta con los servicios necesarios para su correcto funcionamiento y utilidades de acceso para el control remoto.

Las especificaciones para esta máquina se muestran en la Tabla 3-4 y los servicios activos disponibles en la Tabla 3-5.

Tabla 3-4: Especificaciones Windows Server 2003

Dispositivo	Resumen
Disco duro	4 GB
Tarjeta de red	1 Host-Only
Memoria RAM necesaria	512 MB
Procesadores	1
Sistema Operativo	Windows Server 2003

L

Tabla 3-5: Windows Server 2003 (Servidor) - Puertos y servicios

Puerto	Servicio
135	Microsoft Windows RPC
139	Microsoft Windows netbios-ssn
445	Microsoft Windows 2003 microsoft-ds
1025	Microsoft Windows RPC
1026	Microsoft Windows RPC
1027	Microsoft Windows RPC
5800	RealVNC 4.0
5900	VNC (protocol 3.8)

3.4.3 Debian 10

El servidor mantendrá un servicio web, el cual contiene información sobre ataques relacionados con archivos (RFI, LFI y File Upload), y permite a los usuarios crear nuevos usuarios e iniciar sesión en el portal.

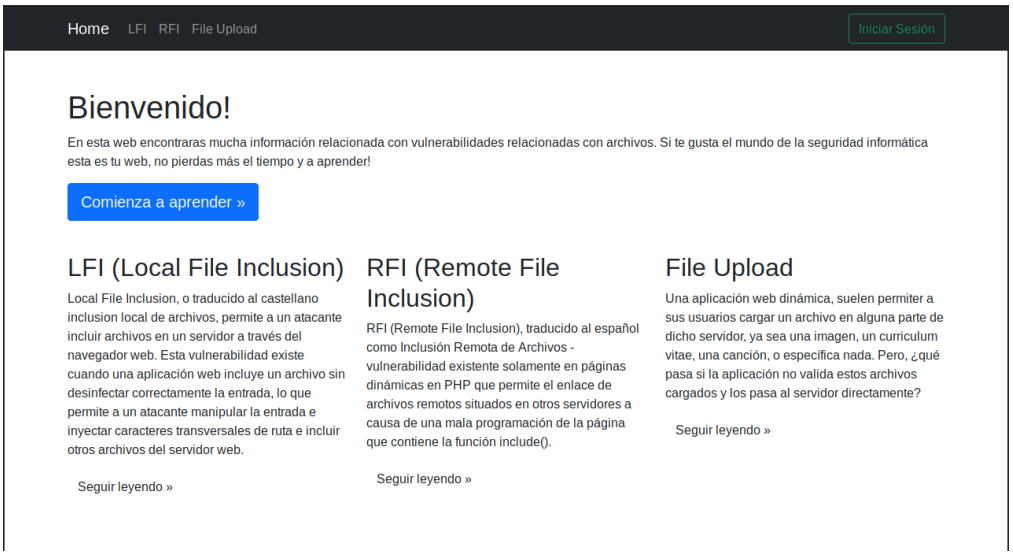

Ilustración 3-4: Web Vulnerabilidades de archivos

Las especificaciones de esta máquina se muestran en la Tabla 3-6 y los servicios activos disponibles en la Tabla 3-7.

Tabla 3-6: Especificaciones Debian 10

Dispositivo	**Resumen**
Discos duros:	10 GB
Tarjeta de red:	1 Host-Only
Memoria RAM necesaria:	1 GB
Procesadores	1
Sistema Operativo:	Debian 10

Tabla 3-7: Debian 10 (Servidor) - Puertos y servicios

Puerto	**Servicio**
22	OpenSSH 7.9p1
80	Apache httpd 2.4.38

3.4.4 Ubuntu 18.04 LTS

Esta máquina actúa como router y se encarga de organizar el tráfico de la red para permitir las conexiones entre las dos redes que hemos creado y el acceso a internet de éstas.

Las especificaciones para esta máquina se encuentran en la Tabla 3-8 y los servicios que tiene activos en la Tabla 3-9.

Tabla 3-8: Especificaciones Ubuntu 18.04 LTS

Dispositivo	Resumen
Discos duros:	8 GB
Tarjeta de red:	2 Host-Only 1 NAT
Memoria RAM necesaria:	1 GB
Procesadores	1
Sistema Operativo:	Ubuntu 18.04 LTS

Tabla 3-9: Ubuntu 18.04 (Router) - Puertos y servicios

Puerto	Servicio
22	OpenSSH 7.9p1
8080	Apache httpd 2.4.38

Además, a partir de cualquier red que no sea la de servidores, el router cuenta con redirecciones de puertos a varios servicios, lo que conlleva que finalmente se mostraran los servicios activos que aparecen en la Tabla 3-10.

Tabla 3-10: Ubuntu 18.04 (Router) - Puertos y servicios externos

Puerto	Servicio	Servidor de destino
21	WU-FTPD wu-2.6.1-16	Red Hat 7
22	OpenSSH 7.9p1	Localhost
80	Apache httpd 2.4.38	Debian 10
135	Microsoft Windows RPC	Windows Server 2003
139	Microsoft Windows netbios-ssn	Windows Server 2003
443	Apache 2.0.47	Red Hat 7
445	Microsoft Windows 2003 microsoft-ds	Windows Server 2003
1025	Microsoft Windows RPC	Windows Server 2003
3306	MySQL 4.0.14	Red Hat 7
32768	RPC	Red Hat 7
5800	RealVNC 4.0	Windows Server 2003
5900	VNC (protocol 3.8)	Windows Server 2003
8080	Apache httpd 2.4.38	Localhost

Además, cuenta con una consola de administración, desplegada en el servicio web del puerto 8080, la cual permite a un usuario autentificado ejecutar algunos comandos restringidos en el sistema (ilustración 3-5).

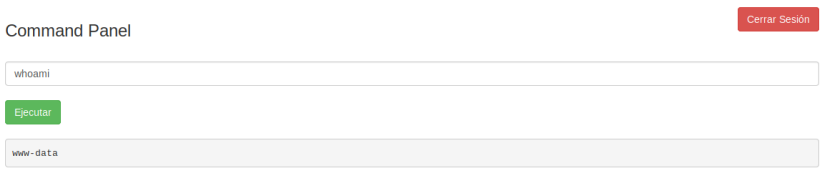

Ilustración 3-5: Panel de administración web

3.4.5 Windows XP

Esta máquina actúa como cliente desde la red interna, enviando tráfico simulado a nuestros servidores de la red interna. Las características de esta MV se muestran en la Tabla 3-11.

Tabla 3-11: Especificaciones Windows XP

Dispositivo	Resumen
Discos duros:	8 GB
Tarjeta de red:	1
Memoria RAM necesaria:	256 MB
Procesadores	1
Sistema Operativo:	Windows XP

3.5 Vulnerabilidades del laboratorio de entrenamiento

3.5.1 Esquema general

Una vez ya definidas todas las máquinas que se van a utilizar, y la manera en que éstas interactúan entre sí, vamos a comenzar a ver todas las vulnerabilidades que se van a poder explotar.

Dependiendo de su naturaleza, las vulnerabilidades pueden ser de cuatro tipos:

- **A nivel de servicio (S).**
- **A nivel de servidor web (W).**
- **A nivel local (L).** P.ej. escala de privilegios, aprovechar una mala configuración del sistema, etc.
- **A nivel de red (R).**
- **Ajena al sistema (A).** A partir del acceso de otro servidor se puede comprometer el sistema.

Y dependiendo de su dificultad pueden ser de tres tipos:

- **Fácil (★).**
- **Medio (★).**
- **Difícil (★).**

En la ilustración 3-6 se muestra un esquema red en el que se observa el tipo de vulnerabilidades y su dificultad en cada sistema, creado a partir de los descriptores especificados.

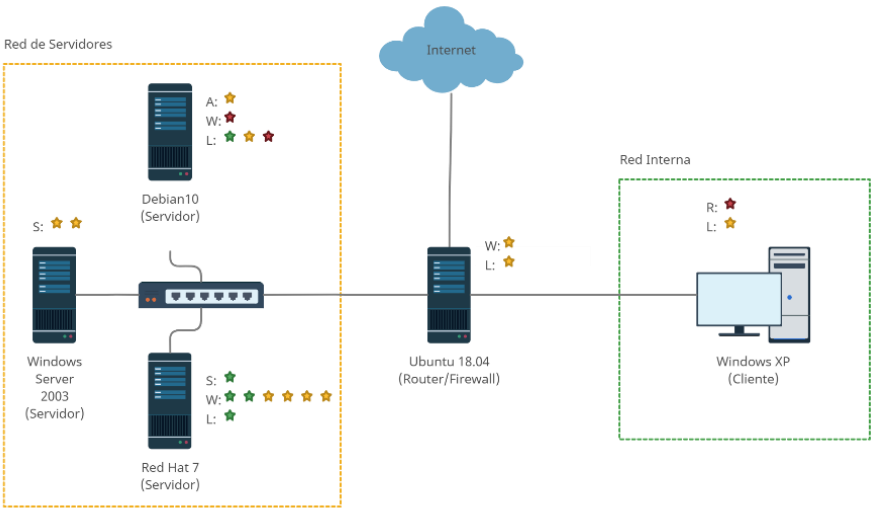

Ilustración 3-6: Esquema de vulnerabilidades

Como se observa en el esquema anterior, el laboratorio dispone de un total de 18 retos para poner a prueba y reforzar los conocimientos del usuario en el sector de la seguridad informática.

3.5.2 Determinando los vectores de ataque

A continuación, se analizarán todos los vectores de ataques disponibles en el laboratorio de ciberseguridad.

En el caso de nuestro laboratorio dispondremos de dos modos de dificultad a la hora de comenzar el desafío, dependiendo de la red en la que se ubique el atacante, tal y como vemos en las ilustraciones 3-7 y 3-8.

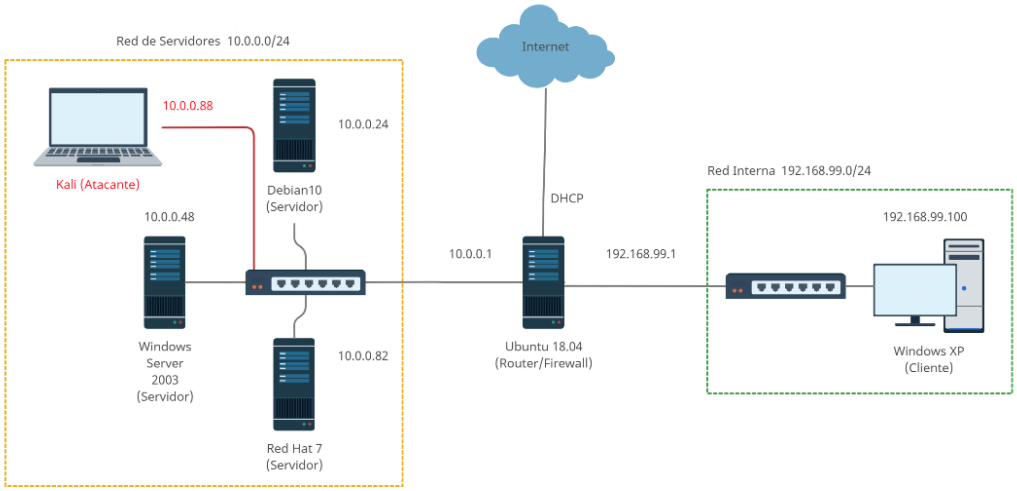

Ilustración 3-7: Esquema de red con atacante 1

El esquema de la ilustración 3-7 se corresponderá con el nivel más sencillo del laboratorio, en el cual el atacante se encuentra en la Red de Servidores, teniendo acceso directo a todos los servidores. También se observa que no se podrá interceptar el tráfico del cliente, aunque se sigue incluyendo en el sistema ya que este cuenta con una vulnerabilidad que no necesita conexión a la red para ser explotada, por lo que se seguirá necesitando.

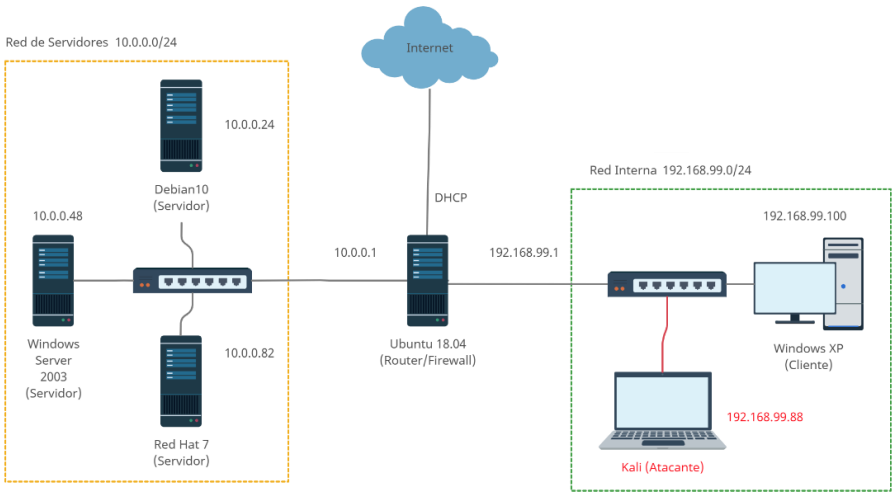

Ilustración 3-8: Esquema de red con atacante 2

Para sacar el máximo potencial a la estructura del proyecto, teniendo acceso a la interceptación de tráfico del cliente, el atacante debe situarse en la red interna, tal y como se muestra en la ilustración 3-8. Esto significaría un aumento de dificultad para el usuario, el cual no tendría acceso directo a la red de servidores, dando lugar a que la única fuente de información sea el router.

Ya con las distintas opciones de dificultad inicial definidas, los cinco objetivos principales del laboratorio son:

1. Ganar acceso al servidor Ubuntu 18.04
2. Ganar acceso al servidor Red Hat 7
3. Ganar acceso al router Windows Server 2003
4. Ganar acceso al servidor Debian 10
5. Ganar acceso al cliente Windows XP

Aunque estos objetivos no son suficientes para completar el laboratorio en su totalidad, ya que existen varios retos repartidos por todas las máquinas y varias vías de conseguir el acceso a dichas máquinas, permitiendo al usuario explorar nuevas formas de lograr el mismo objetivo.

3.5.3 Vulnerabilidades

A continuación, en la Tabla 3-12, se muestra el listado de todas las vulnerabilidades y su nivel de dificultad.

Tabla 3-12: Lista de vulnerabilidades

Máquina	Vulnerabilidad
Red Hat 7.1	WU-FTPD wu-2.6.1-16 Fuerza bruta XSS (Cross-site scripting) SQL Inyection LFI (Local File Inclusion) RFI (Remote File Inclusion) Modificación de parámetros GET Crackear contraseñas
Windows Server 2003	Remote Overflow (MS03-026) RealVNC 4.0
Debian 10	Copia de seguridad desprotegida Subida de archivos Escalada de privilegios mediante Cron Escalada de privilegios mediante Capabilities Sudoers
Ubuntu 18.04	Bypass de ejecución de comandos Escalada de privilegios mediante SUID
Windows XP	Man in the middle Password cracker

En el Apéndice II.- Fichas técnicas de vulnerabilidades, se encuentran todas las fichas técnicas de las vulnerabilidades del laboratorio. Se puede acceder a cualquiera de estas fichas a través de los hipervínculos asociados en la tabla anterior. Analicemos las vulnerabilidades de todas las MVs de una forma más general.

Red Hat 7.1 (Servidor)

En este servidor se encuentran varias vulnerabilidades a explotar, la primera de ellas se da en el servicio WU-FTPD wu-2.6.1-16, el cual está activo en el puerto 21. En concreto, esta versión de wu-ftpd cuenta con una vulnerabilidad de tipo **RCE (Remote Command Execution)** con el identificador CVE-2001-0550 [22], la cual nos permite ejecutar comandos en el sistema bajo el usuario root.

Por otro lado, este servidor dispone de una página web que contiene cinco retos, los cuáles permitirán al usuario practicar ataques de:

- Fuerza bruta
- XSS (Cross-site scripting)
- SQL Inyection
- LFI (Local File Inclusion)
- RFI (Remote File Inclusion)
- Falsificación de parámetros GET

Utilizando las vulnerabilidades LFI y RFI se puede obtener acceso al fichero **/etc/passwd** del sistema, el cual contiene los hashes de las contraseñas de los usuarios, permitiendo de esta manera al atacante crackear los mimos y obtener las credenciales de login a la máquina.

Windows Server 2003 (Servidor)

Para el servidor Windows existe con un vector de ataque en el servicio RPC activo en el puerto 135, el cual permite la **ejecución remota de comandos**. Debido a la importancia de esta vulnerabilidad (CVE-2003-0352), se encuentra categorizada como crítica en el Microsoft Security Bulletin MS03-026 [23].

Otro vector de ataque disponible en este servidor se encuentra en el servicio RealVNC 4.0 que se ejecuta en el puerto 5800, el cual permite hacer un bypass consiguiendo observar las acciones del servidor remotamente. Aunque esta vulnerabilidad no dá acceso directamente al sistema, es importante que se tenga conocimiento de ésta, ya que puede dar lugar a graves agujeros de seguridad.

Debian 7 (Servidor)

En este último servidor se han desarrollado diferentes vías de escalada de privilegios, así como dos maneras diferentes de acceder al sistema.

Comenzando por el acceso al sistema, la primera vía será mediante el servidor web, el cual nos permitirá explotar la capacidad de subir archivos. Por ello, se podrá subir una revershell, aunque hay restricciones que dificultan el proceso. La otra forma de conseguir acceso es mediante una clave privada rsa que se encuentra en una copia de seguridad del directorio home alojada en el servicio FTP del servidor **Red Hat 7**, la cual nos permitirá acceder directamente mediante ssh al sistema.

Por otro lado, para la escalada de privilegios se dispone de tres vías potenciales. La primera se lleva a cabo mediante una capability de tipo setuid que permite cambiar nuestra id de usuario a 0 para convertirnos a root. La segunda consiste en la explotación de un permiso otorgado al usuario del sistema en el archivo */etc/sudoers*. La última se trata de un script modificable por todos los usuarios, que es ejecutado como root cada minuto, ya que se encuentra en las tareas *crontab*.

Ubuntu 18.04 (Router)

El router cuenta con una consola administrativa en su servicio web, la cual está disponible tanto desde la red de servidores como desde la interna, aunque con algunas restricciones de comandos y protegida mediante un panel de login.

Una vez conseguido el acceso al sistema se dispondrá de una vulnerabilidad de escalada de privilegios, generada por una mala configuración de los permisos SUID en un archivo binario.

Windows XP (Cliente)

Por último, el cliente será vulnerable a la obtención de contraseñas del sistema mediante un ataque con tablas Raimbow [24] a los hashes de la máquina.

Además de la vulnerabilidad, esta MV simulará tráfico hacia la red interna, por lo que será vulnerable a un ataque MITM (Man-in-the-middle), el cual nos permitirá obtener credenciales de usuario tanto para la consola de administración del router como para el usuario administrador del servicio web del servidor Debian 7.

3.6 MV Atacante

Se proporcionará una máquina con el sistema operativo Kali Linux, cuyas especificaciones podemos encontrar en la tabla 3-13, con todas las herramientas necesarias para la resolución del laboratorio instaladas, aunque el uso de ésta será opcional, ya que realmente el usuario final podrá utilizar otra máquina virtual si lo considera más oportuno, aunque se recomienda el uso de la proporcionada ya que contará con una web de seguimiento del progreso.

Tabla 3-13: Especificaciones Kali

Dispositivo	**Resumen**
Disco duro:	20 GB
Tarjeta de red:	1
Memoria RAM necesaria:	2 GB
Procesadores	4
Sistema Operativo:	Ubuntu 18.04 LTS

3.6.1 Web de seguimiento

La MV Atacante proporcionada en el laboratorio, cuenta con acceso a un sitio web de seguimiento desplegada en dicha máquina, la cual permite al usuario introducir datos de las máquinas que vaya descubriendo e información sobre las vulnerabilidades que encuentre. De esta forma, se podrá medir el progreso del usuario dentro del laboratorio, así como facilitar pistas y consejos según el nivel de dificultad que se haya escogido inicialmente.

Destacar que con el fin de evitar que el usuario pueda hacer trampas, siempre que se añada una nueva vulnerabilidad o máquina a la web de seguimiento, ésta sólo se añadirá si se proporcionan al menos dos datos descriptivos, disminuyendo de esta manera la probabilidad de que el usuario acierte datos por azar.

Capítulo 4
Implementación

4. Implementación

Este capítulo recoge el proceso de implementación que se ha llevado a cabo para crear el laboratorio de ciberseguridad, partiendo desde la configuración de red que se ha realizado a cada máquina virtual del laboratorio, hasta la creación de las distintas vulnerabilidades que contienen las máquinas del entorno y el portal web de seguimiento para los usuarios.

Al ser una de las finalidades de este proyecto el hecho de que los usuarios que utilicen este laboratorio puedan aprender y enfoquen este como un reto, no se van a mostrar los procesos de resolución de las vulnerabilidades en este documento, evitando de esta manera que se suban dichas soluciones a Internet y puedan ser accesibles por cualquier usuario.

En el caso de que un docente quiera utilizar este proyecto para realizar una evaluación del mismo, se ha creado un documento independiente denominado “Resolución de vulnerabilidades críticas”, el cual será entregado a los directores de este TFG, conteniendo las soluciones a las vulnerabilidades en las que puedan existir alguna dificultad o confusión durante su explotación.

4.1 Configuración básica del entorno

En esta sección se parte del hecho de que todas las máquinas virtuales han sido creadas previamente. Este proceso de creación no se detalla, ya que ha consistido en la instalación por defecto de las imágenes de sistemas operativos utilizadas e incluso en algunos casos, se ha partido desde una máquina previamente creada.

Durante el proceso de creación de las máquinas virtuales es importante tener en cuenta que las máquinas virtuales deben seguir las especificaciones que se han definido en la fase de diseño, ya que sino podría conllevar un aumento de la cantidad de recursos necesarios para poder desplegar el laboratorio completo.

4.1.1 Configurar direcciones IP

Todas las máquinas que conforman la estructura del laboratorio, independientemente de su sistema operativo, deben contar con una IP estática para el correcto funcionamiento del entorno.

Aunque según el sistema operativo la asignación de una IP estática se realizaría de forma diferente, a continuación, se va a mostrar el proceso para asignar estas direcciones a las tres interfaces de red que contiene la máquina virtual Ubuntu 18.04.

En el caso de este sistema operativo, la dirección IP de una determinada interfaz de red se asignará en el fichero */etc/netplan/00-installer-config.yaml*, en el cual se especifican las características de cada interfaz, tal y como se muestra en la ilustración 4-1.

En dicha ilustración se muestran las siguientes configuraciones para cada una de las interfaces de red del sistema:

- **ens33.** Esta interfaz corresponde con la conectada a la red NAT, siendo la encargada de realizar las comunicaciones entre las máquinas de las redes internas y externa. Por este motivo la dirección IP de esta máquina será asignada mediante el protocolo DHCP.
- **ens34.** La IP de esta interfaz, conectada a la red Host-only, corresponde con la puerta de enlace utilizada en la red de servidores. Es por ello por lo que se le asigna la dirección estática 10.0.0.1/24.
- **ens38.** Dicha interfaz, conectada a la red Host-only, es la puerta de enlace para la red interna, lo que supone que se le debe asignar la dirección IP 192.168.99.1/24

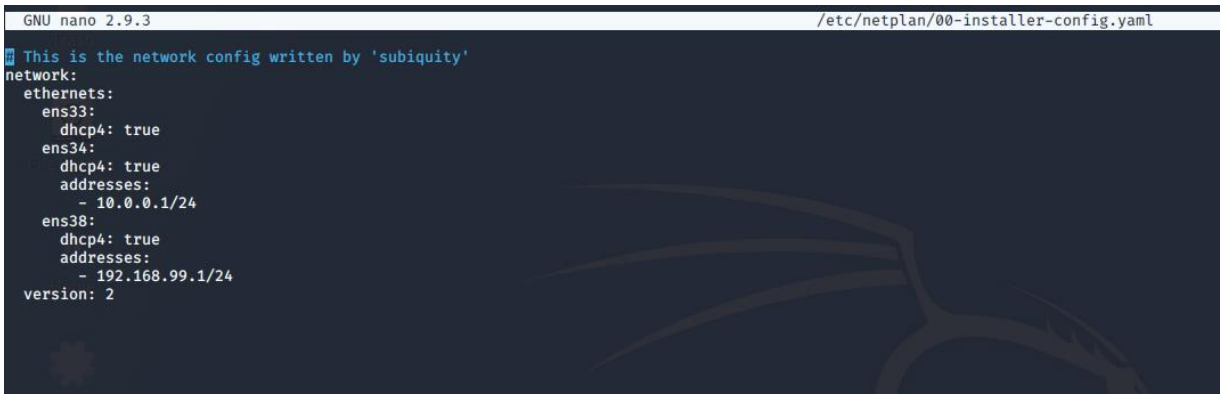

Ilustración 4-1: Configuración de red

La configuración de red que se ha llevado a cabo en el resto de las máquinas del laboratorio consiste en la asignación de la dirección IP estática y puerta de enlace definida en el esquema de red general del capítulo anterior para la interfaz de cada máquina virtual.

4.2 Configuración de la red

Una vez configuradas las direcciones IP de todas las máquinas, se configurará la MV Ubuntu 18.04, para que actúe como router, con el fin de permitir la conexión entre las distintas redes del entorno y el acceso a internet desde las mismas.

En primer lugar, para utilizar una máquina GNU/Linux como enrutador, hay que activar el mecanismo de redirección de paquetes entre interfaces de red del sistema denominado "IP forwarding". Esto se realiza cambiando la configuración de la utilidad sysctl, herramienta que permite cambiar valores en el kernel en tiempo real. El archivo de configuración de esta herramienta se encuentra en */etc/sysctl.conf*, al que se le añade la siguiente línea "net.ipv4.ip_forward=1", consiguiendo de esta forma que cada vez que se inicie el sistema se active el "IP forwarding".

En la ilustración 4-2 se puede observar el script *reglas-red.sh*, el cual contiene todas las reglas necesarias para el correcto funcionamiento del entorno. Estas reglas definidas mediante la utilidad *iptables*, utilizan el mecanismo de retrasmisión de paquetes activado anteriormente, con el fin de conseguir que tanto la red interna, como la red de servidores tengan acceso a la red externa, así como, definir todas las redirecciones de puertos existentes entre el router y los servidores, para todos los usuarios que intenten acceder desde la red externa o interna.

Hay que tener en cuenta que los cambios que realiza la utilidad *iptables* son temporales. Por tanto, cada vez que se reinicie la máquina se pierden todas las reglas que se han definido en el script. Por este motivo se ha instalado la herramienta *iptables-persistent*, la cual carga las reglas almacenadas en el archivo */etc/iptables/rules.v4* al iniciar el sistema. De esta forma se ha conseguido evitar ejecutar el script cada vez que se inicie el router.

Finalmente, hay que aclarar que este script se ha creado y dejado en la ubicación */root/reglas-red.sh* con dos fines principales, siendo el primero de ellos facilitar la tarea de realizar cambios en la estructura de la red, y el segundo, tratar de dejar una pista sobre cómo está estructurada la red a los usuarios que consigan comprometer dicha máquina.

```
 GNU nano 2.9.3                          reglas-red.sh

iptables -F
iptables -t nat -F
#Red de servidores
iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -d 0/0 -j MASQUERADE
iptables -A FORWARD -s 10.0.0.0/24 -j ACCEPT
iptables -A FORWARD -s 0/0 -d 10.0.0.0/24 -j ACCEPT
#Red Interna
iptables -t nat -A POSTROUTING -s 192.168.99.0/24 -d 0/0 -j MASQUERADE
iptables -A FORWARD -s 192.168.99.0/24 -j ACCEPT
iptables -A FORWARD -s 0/0 -d 192.168.99.0/24 -j ACCEPT

#Redirecciones de puertos para red interna y externa
iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 21 -j DNAT --to-destination 10.0.0.82:21
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 21 -j DNAT --to-destination 10.0.0.82:21

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.24:80
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.24:80

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 135 -j DNAT --to-destination 10.0.0.48:135
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 135 -j DNAT --to-destination 10.0.0.48:135

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 139 -j DNAT --to-destination 10.0.0.48:139
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 139 -j DNAT --to-destination 10.0.0.48:139

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 443 -j DNAT --to-destination 10.0.0.82:80
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 443 -j DNAT --to-destination 10.0.0.82:80

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 445 -j DNAT --to-destination 10.0.0.48:445
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 445 -j DNAT --to-destination 10.0.0.48:445

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 1025 -j DNAT --to-destination 10.0.0.48:1025
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 1025 -j DNAT --to-destination 10.0.0.48:1025

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 3306 -j DNAT --to-destination 10.0.0.82:3306
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 3306 -j DNAT --to-destination 10.0.0.82:3306

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 32768 -j DNAT --to-destination 10.0.0.82:32768
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 32768 -j DNAT --to-destination 10.0.0.82:32768

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 5800 -j DNAT --to-destination 10.0.0.48:5800
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 5800 -j DNAT --to-destination 10.0.0.48:5800

iptables -t nat -A PREROUTING -i ens33 -p tcp --dport 5900 -j DNAT --to-destination 10.0.0.48:5900
iptables -t nat -A PREROUTING -i ens38 -p tcp --dport 5900 -j DNAT --to-destination 10.0.0.48:5900

iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

iptables -A FORWARD -j DROP

iptables-save > /etc/iptables/rules.v4
```

Ilustración 4-2: reglas-red.sh

4.3 Desarrollo de portales webs vulnerables

Existen tres máquinas virtuales del laboratorio que cuentan con portales webs entre sus servicios desplegados, los cuáles han sido desarrollados para poner en práctica diferentes tipos de vulnerabilidades webs.

Este apartado se centra en mostrar las estructuras de dichos portales web, con el fin de explicar los objetivos con los que han sido desarrollados y las vulnerabilidades que estos ofrecen. Hay que destacar que el objetivo principal de los portales web no es el diseño ni la utilidad de dichos portales, sino que se han desarrollado con el fin de contener distintas vulnerabilidades y guiar al usuario para que pueda encontrarlas.

4.3.1 Debian 10

El primer portal web que se va a mostrar corresponde con el de la máquina Debian 10, el cual se muestra en la ilustración 4-3. Este portal consiste en un blog de tres entradas, en las que se han documentado tres tipos diferentes de ataques informáticos webs, relacionados con archivos.

Para el diseño de esta página web se ha utilizado la biblioteca multiplataforma de código abierto bootstrap 5 (https://getbootstrap.com/docs/5.0), que ha permitido centrar la atención en el desarrollo y el contenido sin preocupaciones por las modificaciones necesarias en el css para que la web se vea bien estéticamente.

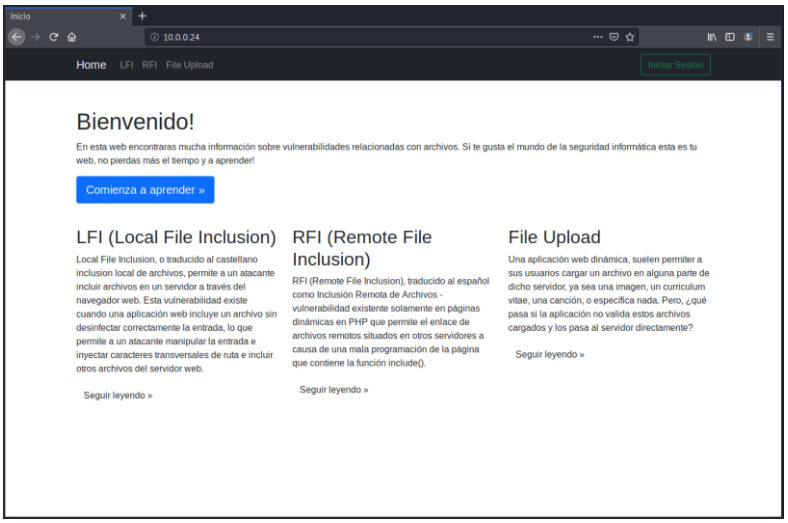

Ilustración 4-3: Portal web Debian 10

Al acceder a la entrada sobre cualquier tipo de vulnerabilidad documentada en el blog, la información mostrada es limitada, obligando de esta forma a disponer de una cuenta para poder leer el contenido completo, tal y como se muestra en la ilustración 4-4. Este detalle ha sido diseñado de esta forma, con el fin de obligar al usuario a registrarse en la web, guiándolo hacia la vulnerabilidad que contiene, que se encuentra en el panel de configuración del usuario que se muestra más adelante.

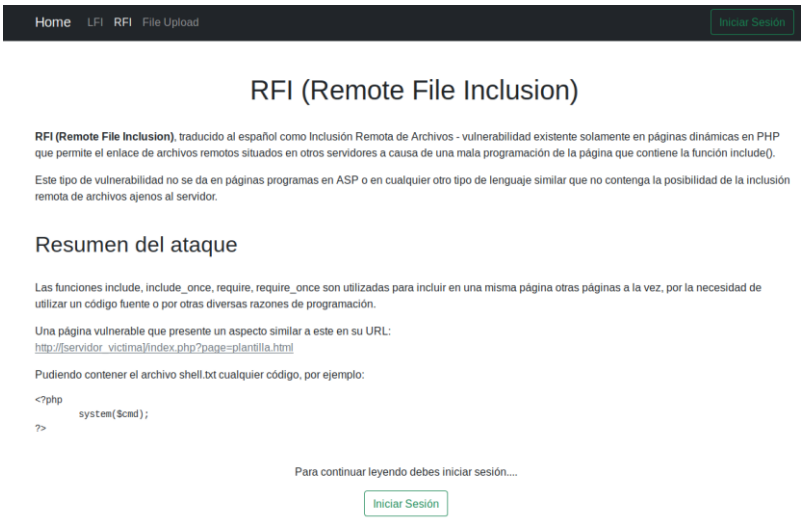

Ilustración 4-4: Información sobre RFI

La gestión de los usuarios del sistema se lleva a cabo mediante una base de datos de una única tabla en la que se guardan algunos datos sobre los usuarios registrados. Una vez registrado e iniciada la sesión con un usuario válido de la base de datos, creado mediante un panel de registro que existe en el portal, además de poder leer todas las entradas del blog por completo, el usuario tendrá acceso a un área en la que se mostrarán los datos del usuario, así como a dos formularios que permiten cambiar la foto de perfil y modificar la contraseña, tal y como se muestra en la ilustración 4-5.

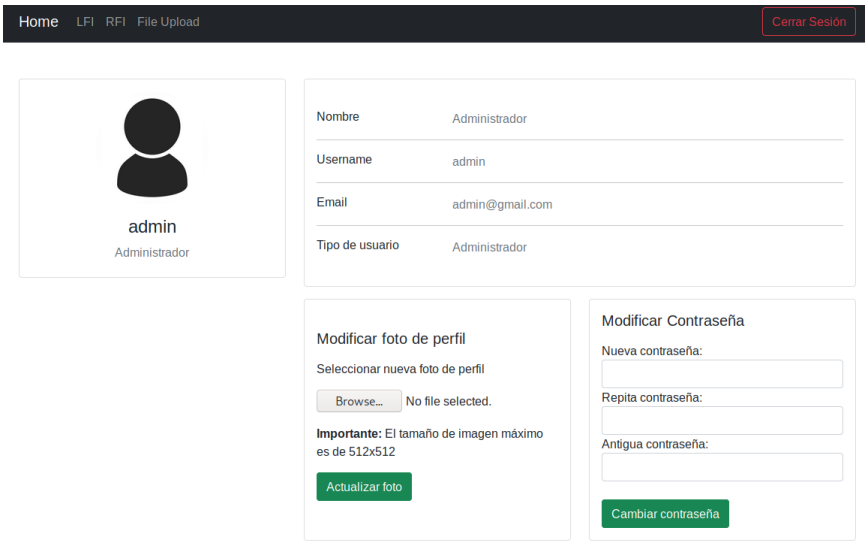

Ilustración 4-5: Configuración del usuario

Se va a profundizar en el código PHP de la página de configuración de cuenta, más concretamente en la función *subirArchivo()*, ejecutada cada vez que se intenta modificar la foto de perfil y en la que se encuentra la vulnerabilidad de este portal.

```php
function subirArchivo(){
        //datos del archivo
        $tipo_archivo = $_FILES['input-b4a']['type'];
        $tamano_archivo = $_FILES['input-b4a']['size'];
        $tmp_name = $_FILES["input-b4a"]["tmp_name"];
        $name = $_FILES["input-b4a"]["name"];
        $ruta = "/var/www/html/imagenes/";
        $tamañoImganen = getimagesize($tmp_name);
        if(!(strpos($tipo_archivo, "application") === false)){
                $message = "Parece que estas intentando subir un tipo de archivo no permitido, solo se aceptan imangenes";
                return $message;
        }elseif((strpos($tipo_archivo, "gif") === false && strpos($tipo_archivo, "jpeg") === false && strpos($tipo_archivo, "jpg") === false && strpos($tipo_archivo, "png") === false)){
                $message = "La extensión del archivo no es válida, solo se acepta: png, jpg, jpeg y gif.";
                return $message;
        }elseif($tamañoImganen === false){
                $message = "El archivo no es válido";
                return $message;
        }elseif($tamañoImganen[0] > 512 || $tamañoImganen[1] > 512){
                $message = "Tamaño máximo permitido 512*512";
                return $message;
        }else{
                include 'includes/db.php';
                $name =  $mysqli->real_escape_string($name);
                $username = $_SESSION['username'];
                if (move_uploaded_file($tmp_name, "$ruta$name")){
                        $result = $mysqli->query("UPDATE user SET img ='$name' WHERE username='$username'");
                        mysqli_close($mysqli);
                        return false;
                }else{
                        $message = "Ha ocurrido un error inexperado, disculpe las molestias";
                        mysqli_close($mysqli);
                        return $message;
                }
        }
        return false;
}
```

Ilustración 4-6: Función subirArchivo()

Como se puede observar, esta función cuenta con varias condiciones que se deben cumplir antes de subir el archivo al servidor, comprobando de esta forma que no sea peligroso para el sistema. Sin embargo, aquellos usuarios más experimentados pueden llegar a lograr evadir todas estas restricciones e introducir un archivo malicioso en el sistema.

El proceso de explotación de esta vulnerabilidad se encuentra detallado en el documento mencionado anteriormente “Resolución de vulnerabilidades críticas”, ya que ésta puede llegar a ser una de las vulnerabilidades más complejas del laboratorio, si se intenta realizar sin ninguna pista.

4.3.2 Red Hat 7.1

En el caso de esta máquina, aportada por la dirección del proyecto, se han realizado cambios con el fin de alinearla con el propósito y los objetivos del proyecto.

Esta máquina contiene un portal web, consistente en cinco retos sobre hacking de servidores web. En la ilustración 4-7 se muestran la página principal del portal, así como todos los retos que la componen.

A continuación, se enumeran todos los retos disponibles y se explica cómo se han creado las vulnerabilidades asociadas a los mismos:

- **Reto1 (Fuerza bruta).** Este reto se ha creado mediante un formulario que solicita un código de cuatro cifras válido al usuario y lo envía a través de POST. Como no se cuenta con restricciones de intentos ni ningún tipo de seguridad adicional, permite al usuario efectuar un ataque de fuerza bruta, consiguiendo de esta forma encontrar el código valido.
- **Reto2 (XSS).** Para esta vulnerabilidad se muestra una variable obtenida mediante un parámetro GET en el campo *value* de un elemento *input*, sin ningún tipo de preprocesamiento. Al no ser tratada correctamente la variable, permite al usuario romper la "caja de texto" e introducir código javascript y html.
- **Reto3 (LFI y RFI).** Ambas vulnerabilidades disponibles en este reto vienen dadas por el uso incorrecto de la función *include()* de PHP, a la cual se le pasa un archivo mediante un parámetro GET, sin realizar ninguna comprobación sobre el mismo. Esto permite al usuario cambiar dicho parámetro y apuntar a cualquier otro fichero del sistema al que tenga acceso el usuario que sostiene el servicio, e incluso cargar un fichero alojado en un servidor externo.
- **Reto4 (Modificación de parámetros GET).** En este caso, se ha diseñado una web de compra de vehículos, en la que el usuario puede seleccionar un vehículo y añadirlo a la cesta. Finalmente, a la hora de pagar se pasan mediante parámetros GET la cantidad y el precio del vehículo, permitiendo al usuario cambiarlo y conseguir comprar un coche por un euro.
- **Reto5 (SQL Inyection).** Este reto cuenta con un panel login conectado a una base de datos. La vulnerabilidad se encuentra en que no se realiza ninguna verificación de la entrada del usuario, permitiendo de esta forma la inyección de código SQL.

Ilustración 4-7: Retos hacking de servidores web

4.3.3 Ubuntu 18.04

En esta máquina, utilizada como router, se ha creado un portal web, simulando un área restringida, como se observa en la ilustración 4-8, para el uso de una consola administrativa protegida por un panel de login.

En este caso se ha desarrollado utilizando la biblioteca multiplataforma de código abierto bootstrap 4 (https://getbootstrap.com/docs/4.0), la cual ha sido utilizada para centrar elementos e imágenes, establecer el diseño de los botones y asegurar que la página sea responsive.

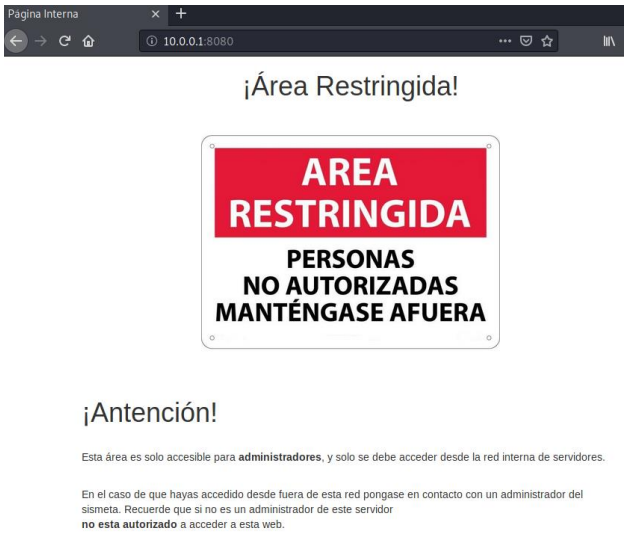

Ilustración 4-8: Área Restringida

El objetivo principal de este portal es que el usuario aplique técnicas de Fuzzing a la web. Es por ello por lo que tanto el panel de login (ilustración 4-9) como el fichero de texto que contiene las credenciales no se encuentran disponibles desde la página principal, obligando de esta forma al usuario a tener que encontrarlos.

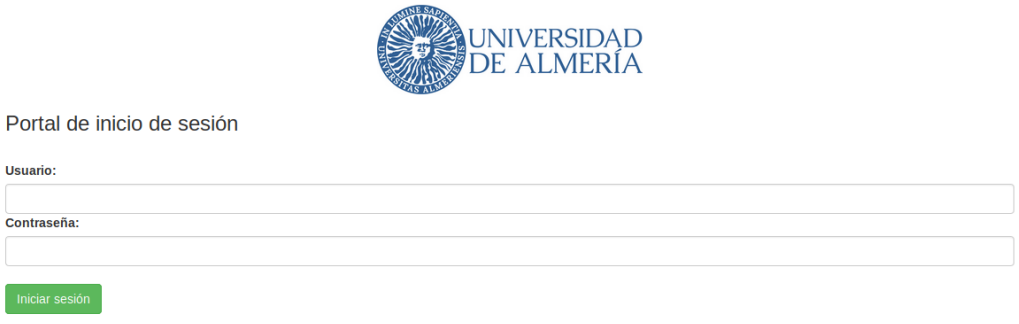

Ilustración 4-9: Panel de login

Una vez encontradas las credenciales y el panel de login, el usuario puede iniciar sesión, obteniendo acceso a una consola de administración, que se muestra en la ilustración 4-10, en la que se pueden ejecutar algunos comandos restringidos, mostrando el resultado correcto en el caso de que se utilice uno de los comandos permitidos o un mensaje de advertencia en el caso de introducir uno

no permitido. Además, se informa al administrador que para obtener una consola sin restricciones acceda mediante *ssh*.

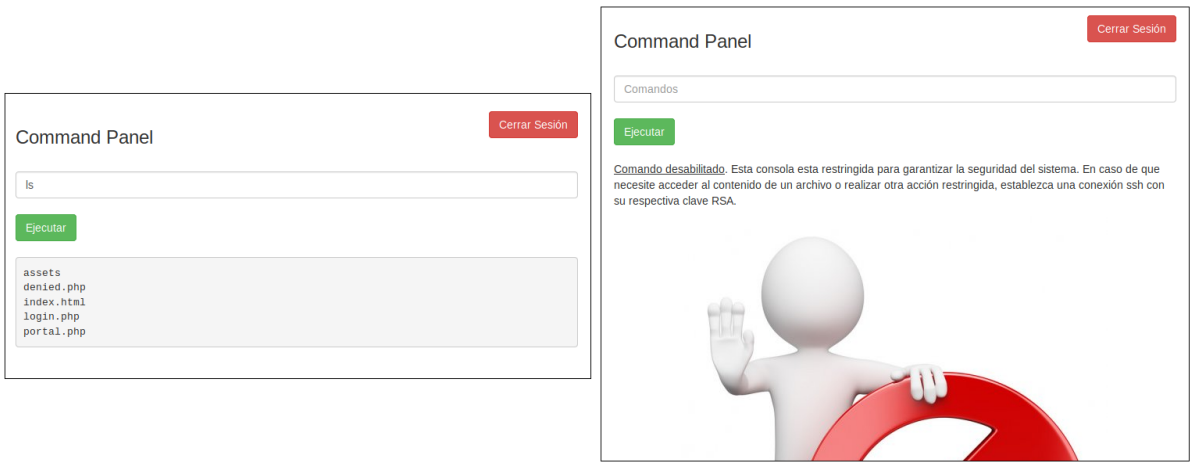

Ilustración 4-10: Consola administrativa

La vulnerabilidad de este portal web consiste en saltarse la restricción de comandos impuesta en la consola administrativa, con el objetivo de conseguir una *revershell*.

4.4 Vulnerabilidades a nivel de servicios y configuración

4.4.1 Servicios

Entre las máquinas del laboratorio se encuentran las máquinas Red Hat 7.1 y Windows Server 2003, que cuentan con vulnerabilidades a nivel de servicios. Estas vulnerabilidades se consiguen instalando versiones de sistemas operativos o versiones de servicios sin actualizar.

En el caso de Red Hat 7.1, se ha instalado la versión *wu-2.6.1-16*, la cual se corresponde con una versión vulnerable (CVE-2001-0550) de un servicio FTP que se encuentra en ejecución en el puerto 21. En Windows Server 2003 hay dos vulnerabilidades. En primer lugar, se ha instalado una versión de sistema operativo anterior a la actualización propuesta en el "Microsoft Security Bulletin MS03-026", consiguiendo de esta forma que el servicio RPC del puerto 135 sea vulnerable (CVE-2003-0352). En segundo lugar, se ha instalado la versión RealVNC 4.0 (CVE-2006-2369) la cual se encuentra activa en el puerto 5800.

4.4.2 Malas configuraciones

La mayoría de las formas de escalar privilegios disponibles en el laboratorio, vienen dadas por malas configuraciones. A continuación, se explica cómo se han creado tres de estas vulnerabilidades:

- **SUID.** Los permisos SUID permiten a cualquier usuario ejecutar el archivo que cuente con este permiso como si fuera propietario. Utilizando este concepto se ha otorgado dicho permiso al archivo binario *python3.6*, el cual tiene a root como propietario y su uso puede permitir la ejecución de comandos.
- **Sudoers.** El archivo */etc/sudoers* contiene una lista de los usuarios que pueden usar el comando sudo, así como el alcance de los privilegios de estos. Para crear la vulnerabilidad se ha añadido un usuario del sistema a este archivo, permitiéndole ejecutar el comando *nano* como usuario privilegiado sin contraseña, el cual permite abrir una Shell.
- **Capabilities.** El uso de capacidades permite otorgar privilegios de root a procesos para que estos puedan realizar una operación privilegiada. Utilizando este concepto se ha asignado la

capacidad cap_setuid+ep al archivo binario *perl*, permitiendo de esta forma que se puedan realizar cambios en el uid del usuario como administrador.

4.5 Web de seguimiento

Aparte de los portales web vulnerables que se han desarrollado en las máquinas que componen el laboratorio, se ha desarrollado una web de seguimiento en la que el usuario puede medir el progreso del laboratorio, así como obtener información y pistas según el nivel de dificultad seleccionado.

Esta web de seguimiento se ha desarrollado en la MV Atacante, con el fin de que los usuarios puedan acceder desde el navegador del sistema simplemente mediante la dirección *localhost*.

4.5.1 Base de datos

Para el desarrollo del portal, se ha creado una base de datos compuesta por siete tablas, tal y como se observa en su diagrama entidad-relación representado en la ilustración 4-11. Las tablas utilizadas en la base de datos son la siguientes:

- **sistemas_operativos_list.** Esta tabla sólo tiene la columna 'name' y será utilizada para almacenar una lista de sistemas operativos, los cuáles se usarán en el proceso de añadir máquinas virtuales a la web de seguimiento, tal y como se verá más adelante.
- **vulnerabilidades_list.** Este caso se asemeja a la tabla anterior, ya que únicamente existe la columna 'name', en la que se almacena una lista de vulnerabilidades, las cuáles se usarán en el proceso de añadir nuevas vulnerabilidades a la web de seguimiento, tal y como se verá más adelante.
- **jugador.** Al acceder por primera vez al entorno se solicita al usuario que introduzca su nombre y seleccione el nivel de dificultad con el que se quiere enfrentar el reto. Estos datos son almacenados en esta tabla.
- **mv.** Todas las máquinas virtuales disponibles en el laboratorio se almacenan en esta tabla, junto con todos los datos que podemos necesitar de las mismas, utilizando las columnas 'name', 'IP', 'sistemaOperativo' e 'imagen' para almacenar la información necesaria. Además, esta tabla cuenta con dos relaciones, una con la tabla *sistemas_operativos* (1-n) y otra con la tabla *jugador* (n-n).
- **vulnerabilidades.** Esta tabla contiene todas las vulnerabilidades disponibles en el laboratorio, las cuáles disponen de las columnas "descripción", "pista" y "flag", para la identificación de cada vulnerabilidad. Existen tres relaciones con esta tabla, la primera con la tabla *vulnerabilidades_list* (1-n), la segunda con la tabla *mv* (1-n) y la última con la tabla *jugador* (n-n).
- **jugador_descubre_mv.** Para la relación n-n entre las tablas *jugador* y *mv*, se ha creado esta tabla, la cual además de contener las claves necesarias para que se produzcan la relación, incluye las columnas "mostrar" y "descubierta", que se usarán para medir el progreso del usuario y saber si mostrar dicha máquina en el esquema de red que tendrá a disposición el usuario, el cual se verá más adelante.
- **jugador_descubre_vulnerabilidades.** Para la relación n-n entre las tablas *jugador* y *vulnerabilidades*, se ha creado esta tabla, formada por las claves necesarias para que se produzcan la relación, y las columnas "mostrar" y "explotada", que se usarán para medir el progreso del usuario y determinar si mostrar dicha vulnerabilidad en la tabla de *vulnerabilidades* a la que tendrá acceso el usuario, la cual se muestra más adelante.

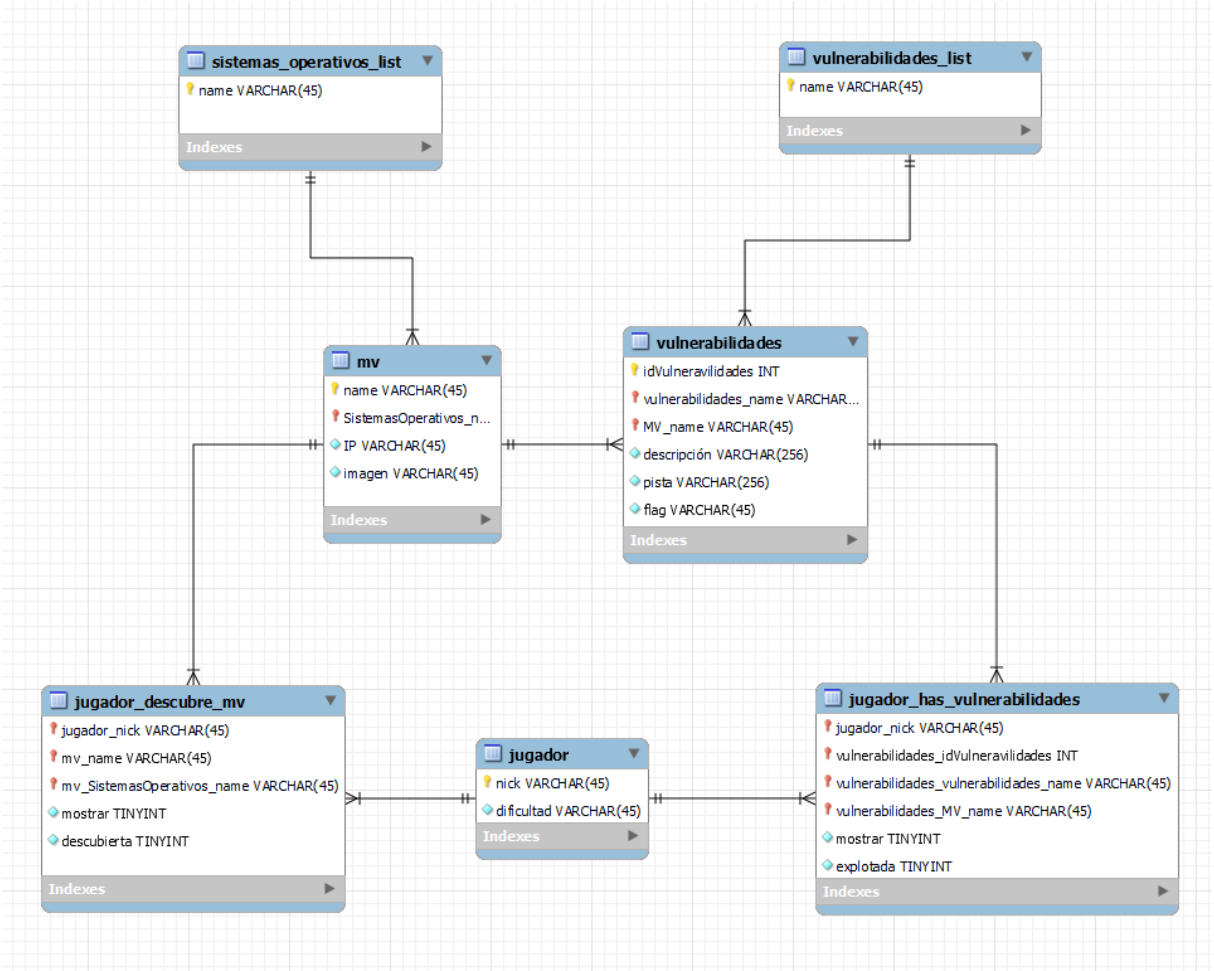

Ilustración 4-11: Diagrama entidad-relación

4.5.2 Página inicial

A partir de la base de datos se ha desarrollado el portal web, comenzando por la página de bienvenida, ilustración 4-12, en la cual tal y como se ha mencionado anteriormente, se solicita un nombre de usuario y dificultad para enfrentar el desafío.

Según el nivel de dificultad seleccionado se modifica los valores de la columna 'mostrar' de las tablas *jugador_descubre_mv* y *jugador_descubre_vulnerabilidades*, de la siguiente forma:

- **Fácil.** Este nivel de dificultad marca todas las MVs y vulnerabilidades con un "1" en la columna 'mostrar', permitiendo ver al usuario toda la información desde el comienzo.
- **Medio.** En este caso tan solo se mostrará la primera MV, la cual corresponderá con la del router e información básica sobre las vulnerabilidades más difíciles de encontrar.
- **Difícil.** No se proporciona ninguna información de ninguna clase.

Importante tener en cuenta que, en el momento de crear un usuario, independientemente del nivel de dificultad seleccionado, se añade todas las máquinas virtuales y vulnerabilidades a las tablas *jugador_descubre_mv* y *jugador_descubre_vulnerabilidades*, con el fin de llevar el progreso del usuario de forma controlada.

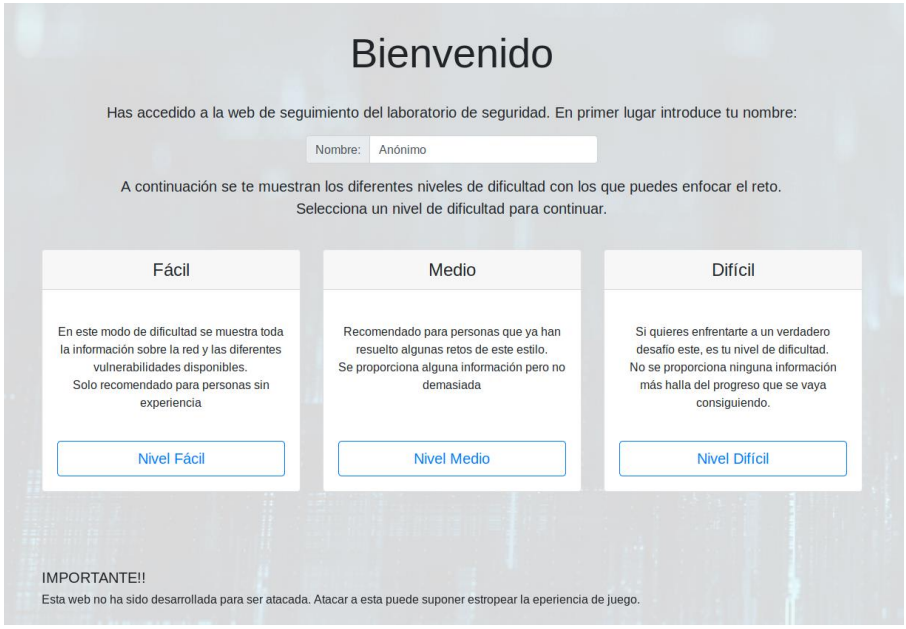

Ilustración 4-12: Página de bienvenida

4.5.3 Manual de uso

Tras seleccionar un nombre de usuario y una dificultad para comenzar el desafío, se realiza una redirección a la página 'Manual de uso', en la cual se han documentado todas las acciones que se pueden llevar a cabo y la forma de mostrar la información de este portal de seguimiento, consiguiendo de esta forma guiar al usuario entre las distintas interfaces del portal.

Ilustración 4-13: Manual de uso

4.5.4 Esquema de red

Tal y como se muestra en la primera imagen del 'Manual de uso', ilustración 4-14, el usuario tiene un esquema de red a su disposición con la información disponible hasta ese momento. En esta página hay cuatro elementos que se deben tener en cuenta.

1. Al presionar sobre el botón "Añadir Máquina Virtual", se abre una ventana (ilustración 4-15) en la que se solicita la IP y el sistema operativo de la máquina que se quiera añadir al esquema de red. La lista de los sistemas operativos es obtenida de la tabla *sistemas_operativos_list*. En el caso de que los datos sean correctos y dicha máquina no aparezca ya en el esquema de red, este se actualizará mostrando la nueva máquina.

2. Se puede pulsar sobre cualquier máquina descubierta en el esquema de red y se abre una página 'Resumen MV' en la que se muestra los detalles de esa máquina y una tabla con las vulnerabilidades descubiertas. En esta página se pueden añadir vulnerabilidades descubiertas mediante el botón "Añadir Vulnerabilidad", en el que se muestra una lista con todas las vulnerabilidades disponibles en la tabla *vulnerabilidades_list*.

3 y 4. Son barras de progreso, las cuáles muestran el avance del usuario en el laboratorio. Ambas barras cambian el color según el avance del usuario, mostrándose de un color verde en el caso de conseguir completarlas.

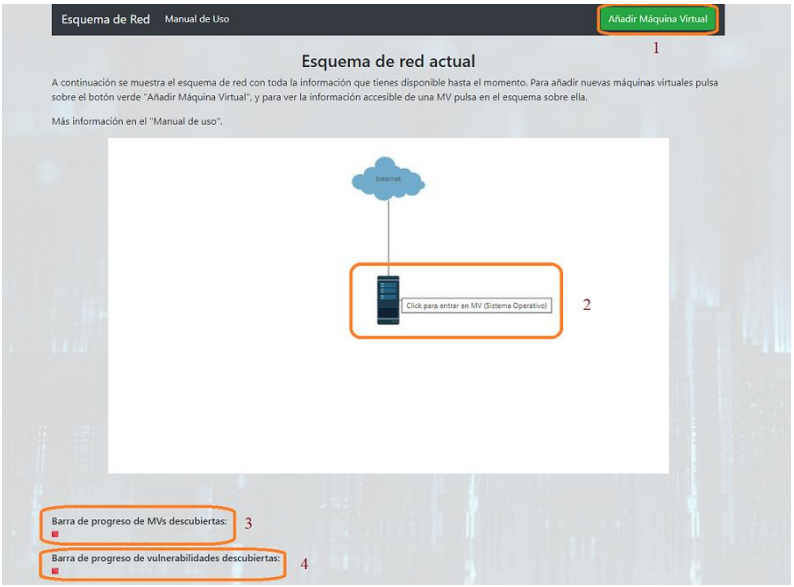

Ilustración 4-14: Esquema de red

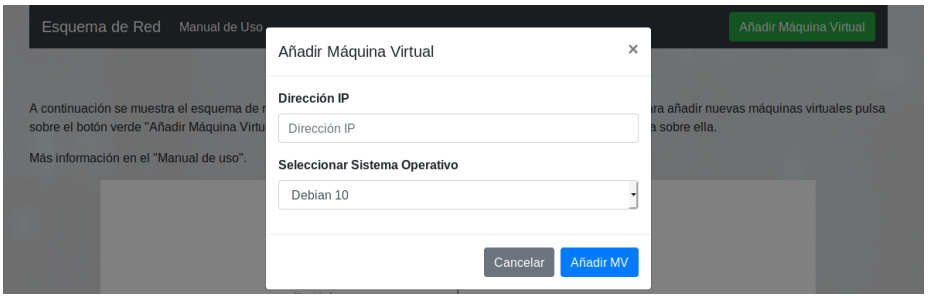

Ilustración 4-15: Añadir MV

4.5.5 Resumen MV

Tal y como se ha mencionado en el apartado anterior, al seleccionar una de las máquinas virtuales que aparecen en la página 'Esquema de Red', el usuario es redireccionado a una web en la que se muestra una tabla con todas las vulnerabilidades descubiertas, siendo visualizadas las vulnerabilidades que contengan la columna 'mostrar' habilitada en la tabla *jugador_descubre_vulnerabilidades* y correspondan a la máquina con la que se ha seleccionado.

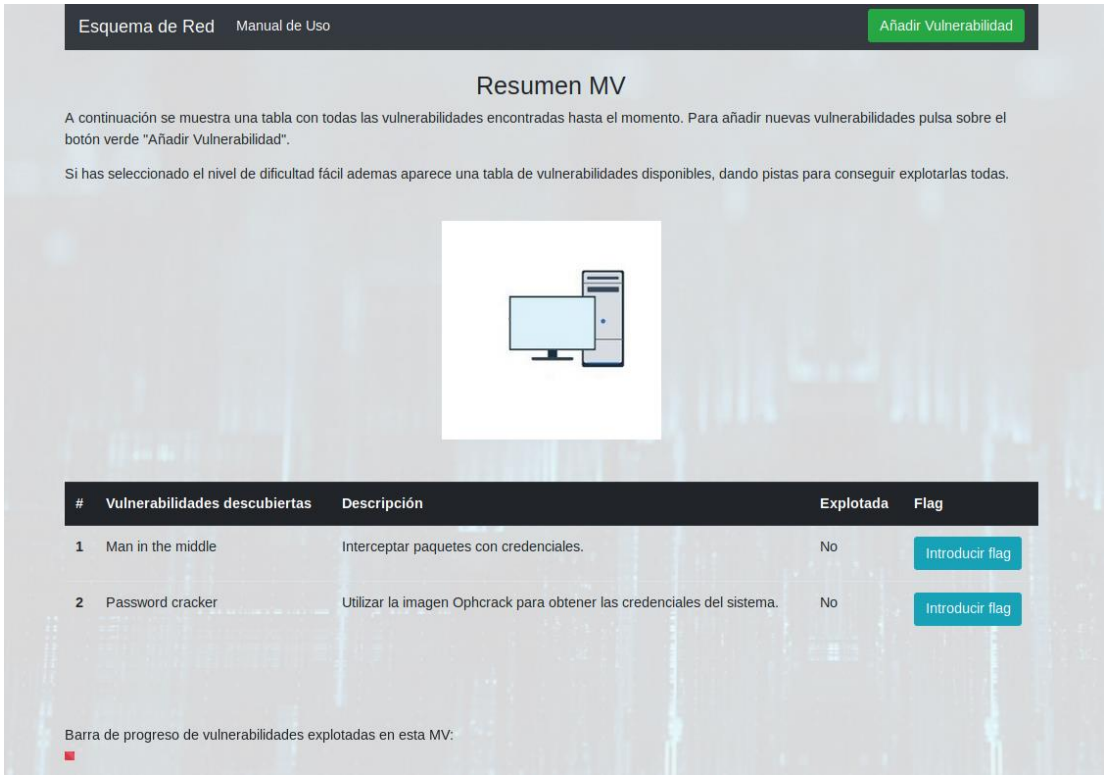

Ilustración 4-16: Resumen MV

En esta página el usuario tendrá oportunidad de añadir nuevas vulnerabilidades (parte izquierda de la ilustración 4-18) y verificar que ha conseguido explotarlas mediante el botón "Introducir flag", el cual se muestra para cada una de las vulnerabilidades descubiertas (parte derecha de la ilustración 4-18) y nos solicitará la flag específica para cada vulnerabilidad. Dicha flag se corresponde con la almacenada en la tabla *vulnerabilidades* de la base de datos. Además, esta página cuenta con su propia barra de progreso para cada MV, la cual se va completando a medida que se verifique la explotación de las vulnerabilidades descubiertas.

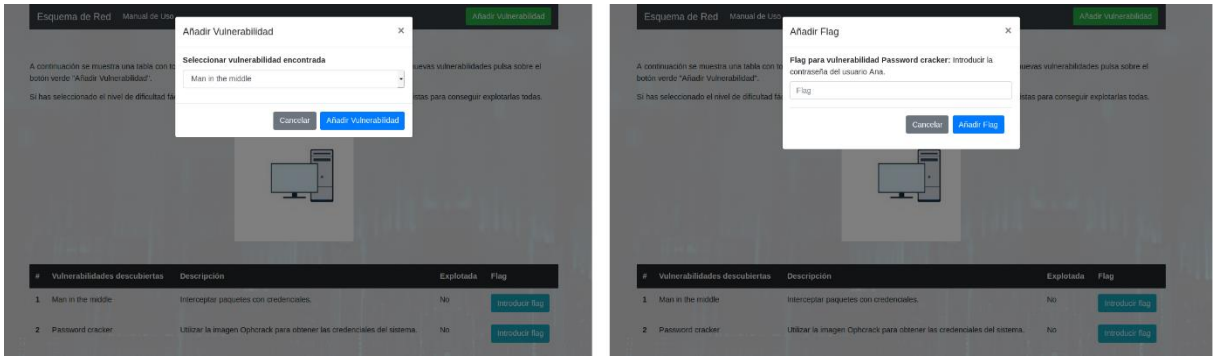

Ilustración 4-17: Añadir vulnerabilidad y Añadir Flag

Capítulo 5
Conclusiones y trabajo futuro

5. Conclusiones y trabajo futuro

5.1 Conclusiones

El objetivo principal de este Trabajo Fin de Grado ha sido la creación de un entorno virtual centrado en el área de la seguridad informática, donde usuarios de todos los niveles puedan practicar y poner a prueba sus conocimientos en seguridad informática.

Si bien es cierto que se han diseñado retos de bastante dificultad en el entorno, también se ha creado una web de seguimiento con el fin de guiar a aquellos usuarios inexpertos durante su progreso durante todo el laboratorio, consiguiendo de esta manera evitar el abandono de las personas que se están iniciando en el mundo de la ciberseguridad a través de este proyecto.

La realización de este entorno ha supuesto un reto desde el momento en el que se comenzó a trabajar en él, ya que, para cubrir las necesidades que existen actualmente en las plataformas de entrenamiento más conocidas actualmente, se han tenido que probar todas ellas, lo que ha llevado consigo una labor de investigación minuciosa. El hecho de que se haya invertido una gran cantidad de tiempo en este proceso de poner a prueba las distintas plataformas de entrenamiento y a la labor de investigación en el área de la seguridad informática, han dado lugar a los pilares de este proyecto, siendo estos los motivos principales de la calidad final del laboratorio.

Una de las cosas más importante de este Trabajo Fin de Grado ha sido la cantidad de conocimientos solidos que se han adquirido durante la realización del mismo, y es que se ha visto un claro avance desde el comienzo hasta ahora. Pero realmente lo más destacable ha sido el resultado final obtenido, ya que, realmente ha quedado un proyecto útil, con el que se puede aprender de una forma divertida y dinámica independientemente del nivel con el que se parta.

Finalmente comentar el alto grado de compromiso que ha existido entre las personas implicadas en este proyecto, que han invertido una gran cantidad de tiempo en este laboratorio con el fin de conseguir el mejor resultado posible.

5.2 Trabajo futuro

Ha medida que se ha ido realizando este trabajo, han ido surgiendo muchas ideas de como ampliar este proyecto, dando lugar a posibles Trabajos Fin de Grado para los estudiantes de los próximos años.

A raíz de estas ideas se ha creado este capítulo en el que se resumen las mejores ideas que se pueden llevar a cabo partiendo desde el proyecto realizado.

5.2.1 Evaluación automática

Aunque este proyecto no tenía como objetivo principal ser utilizado como método de evaluación, se ha detectado lo útil que podría ser el mismo para profesores del área de la seguridad informática que quieran evaluar a sus estudiantes mediante este laboratorio.

Con esto en mente, surge la idea de migrar la web de seguimiento ubicada actualmente en la MV Atacante a un servidor externo, donde se pueda almacenar el progreso de todos los estudiantes y facilitar su seguimiento por parte del profesorado. Además, se podría crear una serie de scripts básicos de generación de códigos aleatorios a partir del DNI o cualquier otro identificador único de los estudiantes, e introducir dichos códigos en las MVs del entorno, siendo estos las soluciones que se deben otorgar para verificar que una máquina ha sido superada y evitar de esta forma el plagio entre estudiantes.

Con esto se pretende ayudar a los docentes en sus labores de evaluación, así como proporcionar a dichos estudiantes un entorno de aprendizaje que cuente con retroalimentación.

5.2.2 Corregir las vulnerabilidades

Al igual que es importante conocer como los atacantes llevan a cabo sus ataques, es aún más importante aprender a protegerse de ellos y saber cómo arreglar aquellas vulnerabilidades que se encuentren en los sistemas.

Aunque solucionar las vulnerabilidades existentes se pueden llevar a cabo en el estado actual del proyecto, se ha pensado que sería una buena idea realizar un proyecto en el que se analicen todas las vulnerabilidades disponibles del entorno y se propongan la solución para arreglar cada una de ellas, suponiendo esto un apoyo a aquellas personas que quizás no sepan cómo solucionar determinados problemas.

5.2.3 Ampliar el entorno

Si bien es cierto que el laboratorio cuenta con bastantes tipos de vulnerabilidades, siendo todas diferentes entre ellas, también es cierto que existen muchos vectores de ataque que no se encuentran contemplados en el mismo.

Con el fin de ampliar el entorno de prácticas, se podrían crear nuevas máquinas virtuales con sistemas operativos que no hayan sido usados, creando de esta forma nuevos escenarios, así como introducir nuevas vulnerabilidades que no estén siendo contempladas en el entorno actual.

Bibliografía

Bibliografía

1. VMware Workstation. (s. f.). vmware. Recuperado 8 de junio de 2021, de https://www.vmware.com/es/products/workstation-player.html
2. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. (2021, 1 junio). Kali Linux. https://www.kali.org/
3. Dr., H. (2019, 6 febrero). Cómo ha evolucionado la ciberseguridad en los últimos 25 años y cómo ha sido la evolución de seguridad en las empresas | Hard2bit CyberSecurity. Hard2bit CyberSecurity | Nuestro Blog de Seguridad Informática, Informática Forense y Noticias de Tecnología. https://hard2bit.com/blog/como-ha-evolucionado-la-ciberseguridad-en-los-ultimos-25-anos-y-como-ha-sido-la-evolucion-de-seguridad-en-las-empresas/
4. Blog. (s. f.). INCIBE-CERT. Recuperado 8 de junio de 2021, de https://www.incibe-cert.es/blog
5. S. (2020, 6 julio). Malware - Concepto, tipos de malware y de dónde proviene. Concepto. https://concepto.de/malware/
6. Bahillo, L. (2021, 18 mayo). Historia de Internet: ¿cómo nació y cuál fue su evolución? Marketing 4 Ecommerce - Tu revista de marketing online para e-commerce. https://marketing4ecommerce.net/historia-de-internet/
7. ¿Qué es un ataque de dia cero? Los 5 ejemplos principales. (s. f.). SoftwareLab. Recuperado 19 de junio de 2021, de https://softwarelab.org/es/que-es-un-ataque-de-dia-cero/
8. S. (2017, 13 mayo). Ciberataque masivo afecta a 99 países. CNN. https://cnnespanol.cnn.com/2017/05/12/ciberataque-masivo-golpea-74-paises/
9. El SEPE comienza a recuperar sus servicios después de sufrir un ciberataque. (2021, 16 marzo). INCIBE-CERT. https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/el-sepe-comienza-recuperar-sus-servicios-despues-sufrir
10. Gómez López, J. (2014). Hackers: aprende a atacar y a defenderte / Julio Gómez López (2a ed. act.). Ra-Ma.
11. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? (2021, 12 abril). INCIBE. https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
12. Rain, Ottis and Lorents Peeter. «Cyberspace: Definitions and Implications», Cooperativa Cyber Defence Centre of Excellence, Tallinn, Estonia. 2010.
13. Urcuqui L. C. C. García P. M. y Osorio Q. J. L. (2018). Ciberseguridad: un enfoque desde la ciencia de datos. Editorial Universidad Icesi. Recuperado de https://elibro--net.ual.debiblio.com/es/lc/ual/titulos/120435.
14. elEconomista. (2021, 18 marzo). Las empresas demandan más inversión en ciberseguridad ante las amenazas crecientes. elEconomista.es. https://www.eleconomista.es/empresas-finanzas/noticias/11111681/03/21/Las-empresas-demandan-mas-inversion-en-ciberseguridad-ante-las-amenazas-crecientes.html
15. I. (2018, 19 febrero). ¡Pésima tendencia! El Malware aumentará con los años. Ciberseguridad para Empresas. https://www.iniseg.es/blog/ciberseguridad/pesima-tendencia-el-malware-aumentara-con-los-anos/
16. World Economic Forum. (2021, enero). The Global Risks Report 2021 (N.o 16). http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
17. colaboradores de Wikipedia. (2021, 18 mayo). Guerra informática. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Guerra_inform%C3%A1tica
18. HYPR. (2021, 19 marzo). What is EternalBlue? | Security Encyclopedia. https://www.hypr.com/eternalblue/
19. TryHackMe. (s. f.). TryHackMe | Cyber Security Training. https://tryhackme.com/

20. Hacking Training For The Best. (s. f.). Hack The Box. https://www.hackthebox.eu/
21. My OSCP Journey. (s. f.). Hack The Box OSCP Preparation. https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/my-oscp-journey-a-review
22. CVE-2001-0550. (2019, 20 septiembre). INCIBE-CERT. https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2001-0550
23. B. (2017, 11 octubre). Microsoft Security Bulletin MS03-026 - Critical. Microsoft Docs. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2003/ms03-026
24. A. (2019, 5 septiembre). Rainbow tables, creación y uso (cracking hash). Auditoría de código. https://auditoriadecodigo.com/rainbow-tables-como-se-crean-y-usan-las-tablas-de-cracking-de-hash-mas-potentes-explicado-facil-o-casi-facil/
25. H. (2021, 25 abril). How to Brute Force Websites & Online Forms Using Hydra. Infinite Logins. https://infinitelogins.com/2020/02/22/how-to-brute-force-websites-using-hydra/

Apéndice I
Manual de juego

I. Manual del juego

I.1 Introducción

Bienvenido al laboratorio de ciberseguridad virtual, este manual te permitirá desplegar el entorno virtualizado según el nivel de dificultad (fácil, medio o difícil) que creas más conveniente, teniendo en cuenta tus conocimientos en el área de la seguridad informática, ya que, este entorno se ha desarrollado con el fin de que pueda servir a usuarios de todos los niveles.

Además, servirá de guía durante todo el proceso de resolución de los distintos retos planteados, facilitando pistas especialmente a aquellos usuarios que escojan los niveles fácil o medio.

Con el fin de guiar al usuario en la selección del nivel de dificultad, a continuación, se explican brevemente los distintos modos disponibles:

- **Fácil:** Este modo de dificulta está destinado a personas que se estén iniciando en el mundo de la seguridad informática y tengan poco o casi ninguna experiencia con este tipo de retos, ya que en este nivel se proporcionará la mayor cantidad de pistas para conseguir completar todos los retos.
- **Medio:** El nivel de dificultad medio, está orientado a aquellas personas que ya han realizado algunos retos de este estilo y cuentan con cierta soltura a la hora de realizarlos. En este caso, se contará con información sobre el entorno, aunque dicha información será más reducida que la proporcionada en el nivel fácil.
- **Difícil:** Finalmente el nivel difícil está orientado a aquellas personas que quieran enfrentarse a un reto de verdad, y cuenten con conocimientos amplios sobre el sector, ya que no se proporcionará ninguna información sobre el laboratorio o pistas sobre la resolución de los retos.

I.2 Iniciar el juego

I.2.1 Material del juego

Antes de comenzar con el proceso de montaje del laboratorio, se debe disponer de todas las máquinas necesarias para la resolución del mismo. Dichas MVs se encuentran en la carpeta “Reto Laboratorio Ciberseguridad”, en la que se incluyen las siguientes máquinas:

- **MV 1**
- **MV 2**
- **MV 3**
- **MV 4**
- **MV 5**
- **MV Atacante.** Esta máquina contiene el sistema operativo Kali Linux instalado, el cual dispone de todas las herramientas necesarias para superar el laboratorio. Además, dispone de un portal web desplegado localmente que se usará como guía en la resolución del entorno.

También se necesitará disponer de un ordenador con al menos 8GB de RAM, para poder virtualizar todas las máquinas virtuales necesarias al mismo tiempo.

I.2.2 Herramienta de despliegue

Para desplegar el entorno de virtualización se recomienda utilizar la herramienta VMware, ya que el proyecto ha sido desarrollado utilizando dicho software. Es por ello, por lo que el uso de esta herramienta garantiza la mejor experiencia durante la realización del laboratorio.

I.2.3 Iniciar el entorno de trabajo

Para iniciar el entorno de trabajo se debe iniciar el programa VMware, una vez abierta la herramienta, se selecciona la opción de "Abrir Máquina Virtual" y se inician todas las máquinas virtuales disponibles según su orden numérico, siendo la última la MV Atacante.

La primera vez que se inicien las máquinas, el programa preguntará si dichas máquinas han sido copiadas o desplazadas. Es importante seleccionar la opción de copiadas.

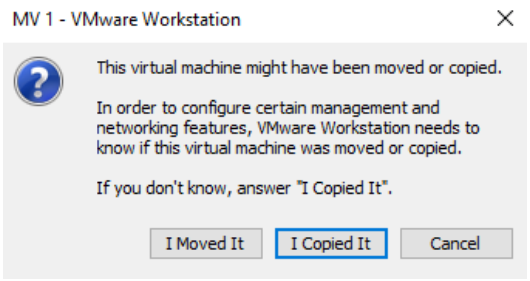

Ilustración I-1: Primer arranque

Una vez desplegadas todas las máquinas del laboratorio se debe configurar la IP de la MV Atacante según el nivel de dificultad seleccionado. En el caso del **nivel fácil** se deja tal y como está configurada por defecto, correspondiéndose esta configuración con la IP 10.0.0.4/24 y la puerta de enlace 10.0.0.1, mientras que, para los **niveles medio y difícil**, se debe configurar la IP 192.168.99.4/24, con la puerta de enlace 192.168.99.1.

Finalmente se recomienda comprobar que desde la MV Atacante se tiene comunicación tanto con la puerta de enlace como con el exterior.

I.3. Web de seguimiento del juego

La máquina MV Atacante cuenta con un portal web activo (Ilustración I-2), al cual se puede acceder introduciendo la dirección *localhost* en el navegador predeterminado del sistema. Dentro de este portal, se solicita un nombre y el nivel de dificultad con el que se quiere enfrentar al reto. A partir de que se indiquen los campos mencionados, esta web sirve como guía para la resolución del laboratorio y muestra el grado de progreso del mismo.

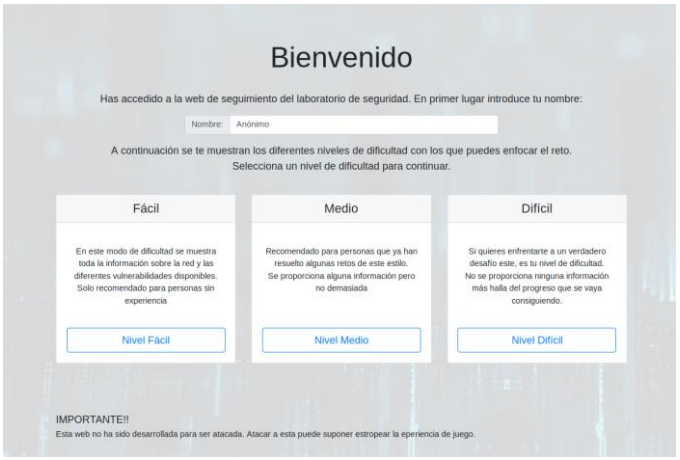

Ilustración I-2: Web de seguimiento

Esto significa que toda la información extra que necesites según el nivel de dificultad que hayas escogido será proporcionada a través de esa web.

I.4 Consejo

Con la información proporcionada por este manual y la web de seguimiento se pueden conseguir superar todos los retos del laboratorio independientemente del grado de dificultad escogido.

Dicho esto, no te rindas, tú puedes. ¡Mucha suerte!

Apéndice II
Fichas técnicas de vulnerabilidades

II Fichas técnicas de vulnerabilidades

II.1 Ficha técnica Red Hat 7.1

wu-ftpd.2.6.1	
Tipo	CVE-2001-0550 (Fácil) La versión de servicio ftp wu-ftpd 2.6.1, instalada en este servidor, permite a atacantes remotos ejecutar comandos arbitrarios mediante el argumento "~{" para comando como CWD, que no se maneja correctamente con la función glob (ftpglob).
MV donde se encuentra la vulnerabilidad	MV Red Hat 7.1
Material necesario	**MV necesarias:** • MV Red Hat 7.1 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	Esta vulnerabilidad se explota mediante el uso de un exploit que se utilizará mediante terminal, teniendo que especificar el SO y dirección IP del servidor para utilizarlo. Esto es así, ya que este exploit está disponible para varios sistemas operativos y los valores en hexadecimal utilizados para realizar este ataque varían según este.
Objetivo a conseguir	• Captura de pantalla para demostrar que se ha ejecutado el exploit • Fichero: /root/texto_muy_importante.txt
Próximos pasos	• Crear una cuenta de root • Explorar los retos del servidor web • Comprobar los equipos a los que puedes acceder • Indagar dentro del equipo para ver si ves información útil o vías de acceso a otros equipos

Fuerza bruta	
Tipo	Fuerza bruta (Medio) El ataque de fuerza bruta consiste en la recuperación de una clave mediante la prueba de todas las combinaciones posibles hasta hallar aquella que permite el acceso.
MV donde se encuentra la vulnerabilidad	MV Red Hat 7.1
Material necesario	**MV necesarias:** • MV Red Hat 7.1 • MV router (Ubuntu)

	Herramientas para aprovechar la vulnerabilidad: • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	Esta vulnerabilidad se explota mediante el desarrollo de un script propio, creado en cualquier lenguaje de programación, con el fin de realizar peticiones POST con todos los números posibles hasta dar con la solución requerida. Hay que destacar que esta vulnerabilidad también se puede explotar con herramientas ya desarrolladas, como puede ser el caso de hydra [25].
Objetivo a conseguir	• Captura de pantalla demostrando que se ha obtenido un serial válido
Próximos pasos	• Buscar vías de acceso a la máquina • Explorar el resto de los retos

XSS (Cross-site scripting)	
Tipo	XSS (★ Fácil) El Cross Site Scripting es un tipo de vulnerabilidad, usualmente encontradas en aplicaciones Web, la cual permite a un atacante inyectar código malicioso en una página web, con el fin de atacar a otros usuarios que se conecten a dicha página, consiguiendo de esta manera secuestrar su sesión, robar contraseñas o conseguir cualquier tipo de información de interés.
MV donde se encuentra la vulnerabilidad	MV Red Hat 7.1
Material necesario	**MV necesarias:** • MV Red Hat 7.1 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	Para aprovechar esta vulnerabilidad se requiere inyectar un código en la página web del reto correspondiente, consiguiendo de esta manera ejecutar su código cuando acceda a dicha web. Esto se puede realizar mediante la creación de un script en java que muestre una alerta.
Objetivo a conseguir	• Captura de pantalla demostrando la inyección de código realizada
Próximos pasos	• Buscar vías de acceso a la máquina • Explorar el resto de los retos

SQL Inyection	
Tipo	SQL Inyection (Medio) El ataque de inyección de SQL consiste en aprovechar una entrada del usuario no tratada, la cual vaya a ser utilizada en una consulta SQL, para inyectar código SQL, con el fin de realizar un bypass de un formulario de login, obtener información de la base de datos atacada e incluso destruir la base de datos.
MV donde se encuentra la vulnerabilidad	MV Red Hat 7.1
Material necesario	**MV necesarias:** • MV Red Hat 7.1 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	Para aprovechar esta vulnerabilidad, se debe realizar una inyección SQL al panel de login encontrado en el reto 3 del servicio web de esta MV, con el fin de realizar un bypass y conseguir acceso como un usuario válido.
Objetivo a conseguir	• Captura de pantalla de la inyección de código SQL realizada
Próximos pasos	• Buscar vías de acceso a la máquina • Explorar el resto de los retos

LFI (Local File Inclusion)	
Tipo	LFI (Medio) El ataque conocido en español como inclusión local de archivos, permite al atacante visualizar archivos locales del sistema atacado. Esto se realiza con la modificación de un parámetro vulnerable que sea utilizado para cargar archivos en la página web.
MV donde se encuentra la vulnerabilidad	MV Red Hat 7.1
Material necesario	**MV necesarias:** • MV Red Hat 7.1 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	Esta vulnerabilidad se aprovecha mediante la modificación de un parámetro de tipo GET que el servidor utiliza para determinar qué archivo mostrar en base a una selección del usuario. Gracias a dicho parámetro el usuario podrá acceder a cualquier archivo del

	servidor que cuente con permisos de lectura para el usuario que está ejecutando el servicio web.
Objetivo a conseguir	• Fichero: /etc/passwd
Próximos pasos	• Crackear hashes encontrados • Conseguir acceso al sistema • Explorar el resto de los retos

RFI (Remote File Inclusion)	
Tipo	RFI (★ Medio) El ataque conocido en español como inclusión remota de archivos, permite al atacante visualizar archivos remotos al sistema atacado. Esto permite al atacante montarse un servidor web con archivos php maliciosos y conseguir que el servidor objetivo acceda a dichos archivos, consiguiendo de esta manera comprometer el servidor atacado
MV donde se encuentra la vulnerabilidad	MV Red Hat 7.1
Material necesario	**MV necesarias:** • MV Red Hat 7.1 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	Esta vulnerabilidad se aprovecha mediante la modificación de un parámetro de tipo GET que el servidor utiliza para determinar qué archivo mostrar en base a una selección del usuario. Gracias a dicho parámetro el usuario podrá introducir la url del archivo remoto que quiera incluir, y el servidor los ejecutará.
Objetivo a conseguir	• Conseguir revershell a partir de la vulnerabilidad • Fichero: /etc/passwd
Próximos pasos	• Crackear hashes encontrados • Conseguir acceso al sistema • Explorar el resto de los retos

Modificación de parámetros GET	
Tipo	Modificación de parámetros GET (★ Fácil) Este tipo de vulnerabilidad permite al atacante modificar el comportamiento normal de una web, modificando los datos que viajan entre las distintas páginas del servidor.
MV donde se encuentra la vulnerabilidad	MV Red Hat 7.1
Material necesario	**MV necesarias:** • MV Red Hat 7.1

	• MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	Esta vulnerabilidad consiste en la modificación de los parámetros pasado por GET en una web de venta de coches, con el objetivo de conseguir comprar un coche por 1 €.
Objetivo a conseguir	• Captura de pantalla demostrando el reto superado
Próximos pasos	• Buscar vías de acceso a la máquina • Explorar el resto de los retos

Crackear contraseñas	
Tipo	Crackear contraseñas (★ Fácil) Debido a una mala configuración del sistema, los hashes de las contraseñas pueden verse expuestos, situación que puede ser aprovechada por un atacante para descifrar dichos hashes, generalmente mediante ataques de fuerza bruta, y obtener las contraseñas.
MV donde se encuentra la vulnerabilidad	MV Red Hat 7.1
Material necesario	**MV necesarias:** • MV Red Hat 7.1 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Acceso al archivo /etc/passwd de la MV vulnerable • Herramienta hashid • Herramienta hashcat • Diccionario de palabras para ataque de fuerza bruta
Aprovechar la vulnerabilidad (BÁSICO)	Una vez obtenido acceso a los archivos del sistema y conseguidos los hashes de los usuarios, se utilizará la herramienta hashid para determinar el tipo de hash encontrado, tras determinar el tipo de hash, se hará uso de la herramienta hashcat, especificando el tipo de hash y un diccionario para realizar un ataque de fuerza bruta contra dichos hashes.
Objetivo a conseguir	• Capturas del proceso de crackeo • Credenciales de los usuarios del sistema
Próximos pasos	• Conseguir acceso al sistema • Explorar los retos del servidor web

II.2 Ficha técnica Windows Server 2003

Remote Overflow (MS03-026)	
Tipo	CVE-2003-0352 (Medio) Esta vulnerabilidad del tipo buffer overflow (desbordamiento del búfer), afecta a una interfaz DCOM para RPC en Microsoft Windows NT 4.0, 2000, XP y Server 2003, permitiendo a los atacantes ejecutar códigos arbitrarios a través de un mensaje mal formado.
MV donde se encuentra la vulnerabilidad	Windows Server 2003
Material necesario	**MV necesarias:** • MV Windows Server 2003 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores • Metasploit
Aprovechar la vulnerabilidad (BÁSICO)	Para explotar dicha vulnerabilidad se necesitará un exploit, que puede ser encontrado en la herramienta Metasploit con un nombre de módulo “MS03-026”.
Objetivo a conseguir	• Captura de pantalla con la ejecución del exploit
Próximos pasos	• Crear una cuenta de root • Comprobar los equipos a los que puedes acceder • Explorar otras vulnerabilidades

RealVNC 4.0	
Tipo	CVE 2006-2369 (Medio) RealVNC 4.1.1 y otros productos que utilizan RealVNC, como AdderLink IP y Cisco CallManager, permiten a los atacantes remotos eludir la autenticación mediante una solicitud en la que el cliente especifica un tipo de seguridad inseguro, como "Tipo 1 - Ninguno", que se acepta incluso si no lo ofrece el servidor, como se demostró originalmente con una contraseña larga.
MV donde se encuentra la vulnerabilidad	Windows Server 2003

Material necesario	**MV necesarias:** • MV Windows Server 2003 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores • Metasploit
Aprovechar la vulnerabilidad (BÁSICO)	Para explotar dicha vulnerabilidad se necesitará un exploit, que se puede encontrar tanto en Metasploit con un nombre de módulo "realvnc_41_bypass" o en la web exploit-db con el número de su correspondiente CVE.
Objetivo a conseguir	• Captura de pantalla con la ejecución del sistema
Próximos pasos	• Iniciar sesión si dispones de credenciales • Explorar otras vulnerabilidades

II.3 Ficha técnica Debian 10

Copia de seguridad desprotegida	
Tipo	Copia de seguridad desprotegida (★ Medio) Este servidor exporta copias de seguridad de su directorio /home a la carpeta del servicio FTP del servidor Red Hat 7.1. Como dichas copias no están protegidas, cualquier persona con acceso a ellas puede acceder al contenido de estas.
MV donde se encuentra la vulnerabilidad	Debian 10
Material necesario	**MV necesarias:** • MV Debian 10 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • MV Red Hat 7.1 • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	Para explotar dicha vulnerabilidad ajena al sistema, se necesitará tener acceso a las copias de seguridad almacenadas en el servicio de la MV Red Hat 7.1. Con este acceso conseguiremos las copias de seguridad del sistema Debian 10 y podremos obtener una clave rsa con la que realizar una conexión ssh.
Objetivo a conseguir	• Clave rsa

Próximos pasos	• Iniciar sesión con la clave rsa obtenida • Comenzar escalada de privilegios

Subida de archivos	
Tipo	Subida de archivos (Difícil) Actualmente la mayoría de páginas webs dinámicas permiten a sus usuarios subir archivos al servidor, ya sea para almacenar un curriculum, una foto de perfil, etc. Pero en el caso de que esta subida de archivos no se encuentre correctamente tratada, puede ser utilizada por atacantes externos con el fin de conseguir información del sistema, e incluso una revershell con el servidor.
MV donde se encuentra la vulnerabilidad	Debian 10
Material necesario	**MV necesarias:** • MV Debian 10 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores • Burp Suite
Aprovechar la vulnerabilidad (BÁSICO)	En este caso, el servidor cuenta con un servicio web que permite a sus usuarios modificar sus fotos de perfil, aunque esta subida de archivos cuenta con bastantes restricciones, el objetivo es encontrar la forma de conseguir subir una revershell, obteniendo de esta forma acceso al sistema.
Objetivo a conseguir	• Conseguir revershell a partir de la vulnerabilidad • Comenzar escala de privilegios
Próximos pasos	• Escalar privilegios • Comprobar los equipos a los que puedes acceder

Escalada de privilegios mediante Cron	
Tipo	Cron (Difícil) Cron es una utilidad de los sistemas basados en Unix, que permite a los usuarios programar tareas para que se ejecuten periódicamente. Estas tareas se ejecutan con los privilegios del usuario que se especifique. Es por ello que, si un atacante encuentra una tarea que se está ejecutando periódicamente y es capaz de interactuar de alguna forma con la ejecución de la misma, puede llegar a conseguir los privilegios del usuario que está ejecutando dicha tarea.
MV donde se encuentra la vulnerabilidad	Debian 10

Material necesario	**MV necesarias:** • MV Debian 10 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	El objetivo de esta vulnerabilidad consiste en que el usuario sea capaz de detectar una tarea del sistema que se está ejecutando periódicamente y conseguir modificar dicha tarea para conseguir acceso como usuario root.
Objetivo a conseguir	• Permisos de usuario privilegiado • Captura con las modificaciones realizadas
Próximos pasos	• Buscar otras vías de escalada de privilegios • Comprueba los equipos a los que puedes acceder

Escalada de privilegios mediante Capabilities	
Tipo	Capabilities (Medio) Las capabilities consisten en una división de los privilegios asociados al usuario root en distintas unidades llamadas capacidades. Estas capacidades se tienen en cuenta a nivel de subprocesos y por lo tanto, permiten un mayor control sobre los privilegios asignados a distintas utilidades. Dichas capabilities pueden ser aprovechadas por atacantes para conseguir una escalada de privilegios
MV donde se encuentra la vulnerabilidad	Debian 10
Material necesario	**MV necesarias:** • MV Debian 10 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	El objetivo de esta vulnerabilidad consiste en que el usuario sea capaz de encontrar una capability en el sistema y la utilice con el fin de escalar privilegios en el sistema
Objetivo a conseguir	• Permisos de usuario privilegiado • Captura de la explotación de la vulnerabilidad
Próximos pasos	• Buscar otras vías de escalada de privilegios • Comprobar los equipos a los que puedes acceder

Sudoers	
Tipo	Sudoers (Fácil) Los sudoers permiten otorgar privilegios determinados a un usuario del sistema. Algunos de estos privilegios pueden ser utilizados por atacantes para realizar una escalada de privilegios y conseguir acceso como usuario root al sistema
MV donde se encuentra la vulnerabilidad	Debian 10
Material necesario	**MV necesarias:** • MV Debian 10 • MV router (Ubuntu) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet • Conexión a la Red de servidores
Aprovechar la vulnerabilidad (BÁSICO)	El objetivo de esta vulnerabilidad consiste en que el usuario sea capaz de encontrar los permisos sudo que tiene asignados su usuario, y aprovechar los mismo para escalar privilegios.
Objetivo a conseguir	• Permisos de usuario privilegiado • Captura de la explotación de la vulnerabilidad
Próximos pasos	• Buscar otras vías de escalada de privilegios • Comprobar los equipos a los que puedes acceder

II.4 Ficha técnica Ubuntu 18.04

Bypass de ejecución de comandos	
Tipo	Bypass (Medio) Este tipo de vulnerabilidad consiste en sobrepasar las restricciones impuestas por un servidor, como puede ser la necesidad de iniciar sesión con un usuario válido para acceder a determinadas webs, que sólo se puedan ejecutar ciertos comandos, etc.
MV donde se encuentra la vulnerabilidad	Ubuntu 18.04
Material necesario	**MV necesarias:** • MV Ubuntu 18.04 **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet
Aprovechar la vulnerabilidad (BÁSICO)	Esta vulnerabilidad se encuentra en el servicio web alojado en el servidor, el cual dispone de un portal en el que se pueden ejecutar comandos en el sistema según una serie de restricciones. El objetivo consiste en saltarse dichas restricciones, y conseguir una revershell con el sistema.
Objetivo a conseguir	• Ejecución de comandos sin restricciones • Captura de pantalla mostrando el bypass realizado

Próximos pasos	• Escalar privilegios • Comprobar los equipos a los que puedes acceder

Escalada de privilegios mediante SUID	
Tipo	SUID (★ Medio) Los permisos SUID permiten a un usuario ejecutar una utilidad del sistema como super usuario. Esto puede ser aprovechado por los atacantes con el fin de escalar privilegios en el sistema.
MV donde se encuentra la vulnerabilidad	Ubuntu 18.04
Material necesario	**MV necesarias:** • MV Ubuntu 18.04 **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • Conexión a Internet
Aprovechar la vulnerabilidad (BÁSICO)	El objetivo de esta vulnerabilidad consiste en que el usuario sea capaz de encontrar un binario con permisos SUID en el sistema y aprovechar el mismo para escalar privilegios
Objetivo a conseguir	• Permisos de usuario privilegiado • Captura de la explotación de la vulnerabilidad
Próximos pasos	• Comprobar los equipos a los que puedes acceder

II.5 Ficha técnica Windows XP

Man in the middle	
Tipo	Man in the middle (★ Medio) Este tipo de ataque consiste en la interceptación de los paquetes correspondientes a la comunicación entre dos o más dispositivos. Para ello, el atacante se sitúa en medio de la comunicación capturando los paquetes que circulan en ambas direcciones, y dejando que estos continúen su camino.
MV donde se encuentra la vulnerabilidad	Windows XP
Material necesario	**MV necesarias:** • MV Router (Ubuntu) • MV Windows XP • MV Servidor web (Debian) **Herramientas para aprovechar la vulnerabilidad:** • MV Kali o similar • MV Debian 10 • Conexión a Internet • Conexión a la Red Interna

	• Ettercap
Aprovechar la vulnerabilidad (BÁSICO)	Esta vulnerabilidad se llevará a cabo desde la red interna del laboratorio y consistirá en la interceptación de paquetes entre las MVs Windows XP y Debian 10 con el fin de obtener unas credenciales de acceso de administrador.
Objetivo a conseguir	• Credenciales de administrador • Captura del proceso para obtener las credenciales
Próximos pasos	• Utilizar las credenciales obtenidas

Password cracker	
Tipo	Fuerza bruta mediante tablas Rainbow (★ Medio) Los ataques de fuerza bruta mediante tablas Rainbow son utilizados generalmente para descifrar contraseñas, que previamente han sido cifradas por un determinado hash. Estas tablas contienen la información de una gran cantidad de posibles contraseñas y sus respectivos hashes, llegando a ocupar incluso cientos de gigas, permitiendo al atacante realizar una búsqueda entre los distintos hashes de la tabla hasta encontrar el hash necesario.
MV donde se encuentra la vulnerabilidad	Windows XP
Material necesario	**MV necesarias:** • MV Windows XP **Herramientas para aprovechar la vulnerabilidad:** • Imagen OphCrack (ISO)
Aprovechar la vulnerabilidad (BÁSICO)	Para explotar esta vulnerabilidad utilizaremos la herramienta OphCrack con el fin de obtener las contraseñas almacenadas en los hashes de los archivos del sistema operativo Windows.
Objetivo a conseguir	• Credenciales de los usuarios del sistema
Próximos pasos	• Probar credenciales • Buscar información en los archivos del sistema

UNIVERSIDAD DE ALMERÍA

Resumen/Abstract

In the last decades there has been a great technological development, which has led to an increasing number of devices capable of connecting to the Internet. If we add to this situation the little importance that has been given to computer security until a few years ago, it is possible to understand how cyber threats have become in a real problem in our society. This has led to an increase in the hiring of professionals in this area, reaching the point where the demand is higher than offer.

In order to help those interested people in training in the field of computer security and covering the current situation of personnel needs, this project appears, which consists of the creation of a network in a virtual environment, from scratch, which will have different vulnerable virtual machines. The project is oriented in the form of a challenge, thus managing to broaden the knowledge of the users who carry it out, as well as testing those previously in a dynamic and fun way.

The project has a monitoring web portal which is very useful for users, providing clues and information according to the level of difficulty to approach the challenge. This portal is the continuation of the game manual, which explains how to deploy the laboratory and start the challenges.

During this End of Degree project, the complete development of the practical laboratory is covered, starting from the state of the art, design and implementation. In addition, the manuals available to the end user are shown, both to deploy the network throughout the process.