# Análisis, diseño y desarrollo de una herramienta para la automatización del pentesting

**David Hervás Rodríguez**

**Directores: Rafael Pastor Vargas y Antonio Robles Gómez**

**Anteproyecto de Trabajo de Fin de Máster en Ciberseguridad**

**Universidad Nacional de Educación a Distancia**

**Curso 2022 / 2023**

# ÍNDICE

# 1. INTRODUCCIÓN

En esta sección se abordarán los conceptos más importantes para comprender el presente trabajo. Para ello en la sección 1.1. se presentan las causas que empujaron a la creación de la herramienta. En la sección 1.2. se exponen los objetivos que se propusieron cumplir, en la sección 1.3. se describirá la línea de trabajo y la planificación seguidas para llevar a cabo el proyecto. Por último, en la sección 1.4. se identificarán y explicarán las diferentes herramientas y entornos que se utilizarán para llevar a cabo el desarrollo.

## 1.1. Motivación

La realización de pruebas de penetración es un tema de la mayor relevancia y actualidad; son un requisito diario y crucial para garantizar la seguridad de los sistemas de información.

Unos de los principales trabajos diarios de los administradores de sistemas es la automatización de las tareas que realizan de manera frecuente y de forma manual. La automatización aumenta la producción y reduce la posibilidad de errores. Debido a la necesidad de automatizar las distintas etapas del pentesting utilizando herramientas Open Source ya disponibles y frecuentemente utilizadas de forma manual e independiente, nació el concepto de este trabajo. Como resultado, este trabajo propone diseñar y crear una aplicación que permita realizar todas las tareas de una prueba de penetración de forma automática e incluso periódica.

La utilidad y garantía de uso, que se basan en una necesidad real que tienen las organizaciones, sirven de base para la justificación de este proyecto, y la automatización de este tipo de pruebas de penetración ofrece una retroalimentación continua sobre el estado de seguridad de los sistemas en estudio.

La originalidad del concepto comienza con la integración de las etapas de pentesting y explotación utilizando herramientas de propósito general (Open Source) en el contexto de la seguridad informática y la auditoría, de modo que cada herramienta mantenga su funcionalidad de ejecución y ciclo de actualización mientras se pueden incorporar otras herramientas, como por ejemplo agregando las nuevas características que puedan proporcionar.

El análisis, diseño y desarrollo de una aplicación que permita la automatización de los distintos pasos presentes en las auditorías técnicas de seguridad o pentesting es el objetivo de este trabajo final de máster. Para implementar varias fases de pentesting de forma automática, la aplicación tomará como entrada datos relativos al objetivo, el dominio de la infraestructura y utilizará técnicas de auditoría activa y/o pasiva.

Este trabajo tiene aplicados los conocimientos de diversas asignaturas que se han estudiado como son: *Hacking Ético* para la realización de pruebas de pentesting pasando por todas las fases que las componen y *Auditoría y Monitorización de la Seguridad* la cual ha influido en la forma de representar la salida, mediante un informe que tenga efectos prácticos de cara a una posible auditoría de seguridad.

### 1.2. Objetivos

El objetivo principal del proyecto es desarrollar una plataforma automatizada para la realización de pruebas de penetración (pentesting) en sistemas informáticos. Los objetivos específicos incluyen:

- **Incrementar la eficiencia:** Automatizar las tareas repetitivas y manuales en el proceso de pentesting para liberar tiempo y recursos, permitiendo a los profesionales de seguridad enfocarse en análisis y soluciones.

- **Mejorar la precisión:** Minimizar errores humanos al realizar pruebas de penetración al eliminar la subjetividad y estandarizar las técnicas utilizadas.

- **Aumentar la cobertura:** Realizar pruebas más exhaustivas y sistemáticas al cubrir un amplio espectro de vulnerabilidades y escenarios de ataque.

### 1.3. Resumen de la metodología

La metodología se basará en un enfoque de ciclo de vida de pentesting, adaptado para la automatización. Esto incluirá las siguientes fases:

- **Planificación**: Definir los objetivos de la prueba, seleccionar los sistemas objetivo y establecer los límites y restricciones.

- **Recolección de Información**: Utilizar herramientas automatizadas para recopilar información sobre los sistemas, como escaneo de puertos, enumeración de servicios y análisis de configuraciones.

- **Análisis de Vulnerabilidades**: Aplicar técnicas automáticas para identificar vulnerabilidades conocidas y potenciales debilidades en el sistema.

- **Explotación**: Utilizar herramientas automatizadas para intentar explotar las vulnerabilidades descubiertas y obtener acceso a sistemas comprometidos.

- **Análisis de Resultados**: Evaluar los resultados de la prueba, generar informes detallados de las vulnerabilidades encontradas y proporcionar recomendaciones para la mitigación.

### 1.4. Arquitectura y desarrollo

Para abordar la realización de este proyecto, será requerido el despliegue de una infraestructura tecnológica, necesaria tanto para el desarrollo como para la ejecución, así como el uso de un conjunto de herramientas para la implementación y desarrollo. En las siguientes secciones describimos el sistema operativo, las herramientas para cada etapa, el lenguaje y las librerías empleadas para cubrir la penetración, la explotación y la generación del informe a implementar.

## 2. INFRAESTRUCTURA TECNOLÓGICA

Para llevar a cabo el proyecto se utilizará la distribución GNU Linux Kali, pionera en el campo de la seguridad informática. Esta distribución sobresale en análisis forense, así

como en pentesting. El lenguaje de programación empleado es Shell, escogido por ser el lenguaje empleado en la mayoría de las llamadas por la línea de comandos a las funcionalidades que se encuentran en la distribución Kali así como por su sencillez a la hora de probar y depurar comandos y scripts.

El editor de texto Sublime se utilizará en el entorno de desarrollo debido a su simplicidad para simplificar las condiciones de desarrollo. A continuación, se mostrarán las características de los sistemas operativos, el lenguaje, las bibliotecas y las herramientas utilizadas en el entorno de desarrollo y ejecución del proyecto.

## 2.1. Kali

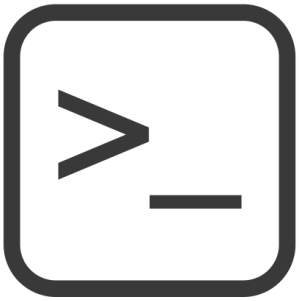
El sistema operativo que se empleará es un GNU/Linux, concretamente la distribución Kali, por ser una de distribuciones lideres en Pentest. Kali es la distribución sucesora de la distribución GNU/BackTrack, pero basado en el Core Debian, está diseñada básicamente para la seguridad y la auditoria informática y esta mantenida por la compañía Ofensive Security LTD.


La distribución Kali Linux trae preinstalados más de 600 programas, puede ser usada desde un Live CD, live-usb o como sistema operativo principal. Kali se distribuye en imágenes ISO compiladas para diferentes arquitecturas (32/64 bits y ARM), existen imágenes compatibles con los principales hipervisores de virtualización.

Para garantizar un entorno seguro de desarrollo, el equipo de Kali, está formado por un reducido número de personas que interactúan con los repositorios oficiales, todos los paquetes están firmados por los desarrolladores que los compilaron. Los paquetes también se firman en sus repositorios utilizando GNU Privacy Guard, para garantizar su autenticad.

## 2.2. Shell

El lenguaje shell, comúnmente conocido como "shell", es un tipo de lenguaje de programación que proporciona una interfaz de usuario para interactuar con el sistema operativo de una computadora. En esencia, es un intérprete de comandos que permite a los usuarios enviar instrucciones al sistema operativo para realizar diversas tareas.



La interacción con el shell se realiza a través de una línea de comandos, donde el usuario ingresa comandos y el shell los interpreta y ejecuta. Shell también se encarga de comunicar estas instrucciones al sistema operativo para realizar tareas como:

1. **Gestión de archivos y directorios**: Creación, eliminación, copia, movimiento, cambio de permisos, etc.

2. **Ejecución de programas**: Iniciar aplicaciones y procesos.

3. **Automatización de tareas**: Mediante secuencias de comandos (scripts) que pueden incluir lógica, bucles y condiciones.

4. **Manipulación de flujos de entrada/salida**: Redirección de la entrada/salida estándar para procesar datos.

5. **Configuración del entorno**: Establecer variables de entorno, definir alias, entre otras configuraciones.

6. **Gestión de usuarios y permisos**: Cambiar contraseñas, gestionar usuarios y grupos, establecer permisos.

Existen varios shells disponibles, siendo el "Bourne Shell" (sh) uno de los más antiguos, y el "Bash" (Bourne Again Shell) uno de los más utilizados en sistemas Unix y Linux. También hay otros shells populares como "Zsh" y "Fish", que ofrecen características adicionales y mejoras en la experiencia del usuario.

Los lenguajes shell son muy útiles para administradores de sistemas, desarrolladores y usuarios avanzados que necesitan realizar tareas en la línea de comandos, ya que permiten automatizar operaciones y aumentar la eficiencia en la gestión de sistemas y la ejecución de tareas repetitivas.

# 3. HERRAMIENTAS Y LIBRERÍAS

Las herramientas que se utilizarán constituyen el conjunto generador de la información en las distintas etapas que componen las pruebas de penetración y explotación mientras que las librerías son conjuntos de código y funciones que serán utilizadas por programas y aplicaciones. En Linux, las librerías son esenciales para el desarrollo de software ya que permiten reutilizar código y simplificar el proceso de creación de programas.

## 3.1. Pandoc

Pandoc es una herramienta de línea de comandos diseñada para la conversión de documentos entre diferentes formatos. Su objetivo principal es permitir la fácil migración de contenido entre diversas plataformas y formatos de documentos, lo que lo convierte en una herramienta valiosa para autores, escritores, programadores y cualquier persona que necesite transformar contenido de un formato a otro**.**

pandoc

A universal document converter

Pandoc admite una amplia variedad de formatos de entrada y salida, incluidos:

1. **Formatos de Documentos**: Markdown, reStructuredText, HTML, LaTeX, Microsoft Word (.docx), OpenDocument (.odt), EPUB, entre otros.

2. **Formatos de Marcado**: Markdown, HTML, reStructuredText, LaTeX.

3. **Formatos de Presentación**: PowerPoint (.pptx), PDF, Beamer.

4. **Formatos de Publicación Científica**: LaTeX, HTML, Markdown.

5. **Formatos de Ebooks**: EPUB, Kindle (.mobi).

Pandoc es especialmente útil para convertir documentos escritos en un formato simple y legible (como Markdown) en formatos más complejos y estructurados utilizados para la publicación o para generar presentaciones. Además, es capaz de aplicar plantillas para controlar el diseño y la apariencia de la salida.

Otra característica interesante de Pandoc es su extensibilidad. Puede admitir extensiones personalizadas y es posible escribir filtros personalizados en varios lenguajes de programación para manipular el proceso de conversión.

### 3.2. KaliTools

La distribución Kali contiene una amplia gama de herramientas de seguridad y pruebas de penetración que permiten a los profesionales de seguridad y a los investigadores evaluar la seguridad de sistemas, redes y aplicaciones.


Las KaliTools conforman la lista de herramientas y utilidades incluidas con la distribución Kali Linux; abordan desde la recopilación y explotación de datos hasta la creación de informes finales. Esto permite a los profesionales de la seguridad IT contar con múltiples funcionalidades necesarias, para cubrir su desempeño, las Kali Tools cubren las siguientes categorías:

- Recopilación de información
- Sniffing & Spoofing
- Análisis de vulnerabilidades
- Herramientas de explotación
- Ataques de contraseñas
- Ataques Wireless
- Herramientas forenses
- Herramientas de permanencia
- Hardware Hacking
- Aplicaciones web

- Técnicas de tes basadas en estrés
- Ingeniería inversa
- Herramientas de reporting

### 3.3. LaTeX

LaTeX es un sistema de composición de documentos muy utilizado, especialmente en el ámbito académico, científico y técnico para la creación de documentos de alta calidad tipográfica, como artículos científicos, tesis, informes, presentaciones, libros y otros tipos de publicaciones.

A diferencia de los procesadores de texto tradicionales, como Microsoft Word, que utilizan un enfoque de formato visual y WYSIWYG (lo que ves es lo que obtienes), LaTeX se basa en un sistema de marcado, lo que significa que los documentos se crean escribiendo texto plano en un editor de texto, pero incluyendo comandos especiales para estructurar el documento, definir estilos, crear fórmulas matemáticas, referenciar bibliografía, entre otras cosas.

Algunos aspectos clave de LaTeX son:

1. **Calidad Tipográfica**: LaTeX produce documentos con una calidad tipográfica excepcional. El sistema ajusta automáticamente el espaciado, las fuentes y otros elementos para obtener un diseño profesional.

2. **Fórmulas Matemáticas**: LaTeX es muy conocido por su capacidad para crear fórmulas matemáticas complejas con gran precisión y belleza. Es ampliamente utilizado en publicaciones matemáticas y científicas.

3. **Reutilización y Consistencia**: LaTeX permite crear plantillas y estilos personalizados, lo que facilita la reutilización de formatos y estilos coherentes en diferentes documentos.

4. **Gestión de Referencias**: LaTeX puede gestionar referencias bibliográficas y generar automáticamente listas de referencias y citas en diferentes estilos (por ejemplo, APA, IEEE).

5. **Portabilidad:** Los documentos LaTeX son archivos de texto plano, lo que facilita la colaboración y la portabilidad entre diferentes sistemas y plataformas.

Un editor popular para trabajar con LaTeX es TeXstudio, pero también hay otros como TeXmaker, Overleaf (plataforma en línea), LyX (orientado a WYSIWYM, what you see is what you mean) y varios editores de texto que tienen extensiones o complementos para admitir LaTeX.

# 4. BIBLIOGRAFÍA


https://www.kali.org/

https://www.gnu.org/software/bash/

https://pandoc.org/

https://www.kali.org/tools/

https://www.latex-project.org/