AGRADECIMIENTOS

A Dios Todopoderoso, colegas y, por encima de todo, a la comunidad de investigación de seguridad informática, los verdaderos *hackers* de la tecnología de información que, han aportado sus conocimientos a través del *Open Source* y el *Free Software*, con fines de formación técnica en ciberseguridad.

Arturo Enrique Mata García

ACERCA DEL AUTOR

Arturo Mata es Hacker Ético, con más de dos décadas de carrera profesional en Petróleos de Venezuela, en proyectos de automatizados control de acceso y video vigilancia IP, pentesting empresarial, gestión de incidentes de ciberseguridad, tecnología de mantenimiento de plataformas de seguridad en tecnologías de información, monitoreo de redes informáticas, evaluación de riesgos y amenazas persistentes avanzadas (APTs).

Certified Network Security Specialist (CNSS), con Diplomaturas en Seguridad Informática, Enfoque Ágil de la Ciberseguridad y en Sistemas Informáticos, Técnico en Ciberseguridad, Máster en Marketing Digital y Analítica Web.

Entusiasta del software libre y del código abierto, programador e investigador de la seguridad ofensiva, centrado en la privacidad de los usuarios, autor del libro 'Curso de Programación Bash Shell' orientado al Hacking Ético, publicado por Grupo Editorial RA-MA en España y Alfaomega Grupo Editor Argentino.

Él cree firmemente en un mundo donde la ciberseguridad juegue un papel central en la preservación de la privacidad digital de todos los internautas.

PREFACIO

Este libro proporcionará al lector los conocimientos y habilidades necesarias para realizar pruebas de penetración (*pentesting* en inglés) y auditorias de seguridad informática, utilizando el sistema operativo <Kali Linux>, una distribución basada en Debian, que actualmente cuenta con una extensa recopilación de los mejores paquetes de herramientas de seguridad de código abierto orientadas al *Ethical Hacking*.

Hay dos tipos de hackers éticos, los que solo leen lo que dicen los *frameworks* que supuestamente hacen y aquellos que interpretan las herramientas, usando su ingenio para generar un informe que realmente agrega valor a sus clientes. Una empresa u organización necesita saber cómo mejorar la protección de la información y la infraestructura.

Aunque esta obra beneficiará tanto a principiantes como expertos, definitivamente será una ventaja, si el lector está familiarizado con GNU/Linux. En el transcurso de cada capítulo, se obtendrá progresivamente una comprensión completa de <Kali Linux>, explicando cómo usarlo, paso a paso, con una variedad de ejemplos prácticos.

También se proveerán los fundamentos teóricos-prácticos de seguridad informática ofensiva, que pueda llevarte a un nivel moderado de experiencia, que le permita a usted amigo lector a desempeñarse en puestos como Especialista *Red Team*, *Hacker* Ético, Técnico de Ciberseguridad, *Pentester*, o Auditor de Seguridad Informática.

1

UNA INTRODUCCIÓN A KALI LINUX

«Es crítico tomar el punto de vista del atacante para ver si sus defensas están funcionando.» .

Mati Aharoni

1.1 ¿QUE ES KALI LINUX?

Kali Linux es una distribución de seguridad ofensiva basada en Debian, diseñada bajo licencia GNU GLP, para pruebas de penetración (Pentesting en inglés) y análisis de redes de datos. Los creadores de Kali Linux son Devon Kearns y Mati Aharoni en 2013, como sucesora de BackTrack, basada en Ubuntu 10.04 LTS, destinada a la auditoría del *kernel*.

En realidad constituye uno de los sistemas operativos más populares utilizados por expertos en seguridad informática y *hackers*. Básicamente cuenta con las mejores funcionalidades y herramientas para el desarrollo pleno de *Ethical Hacking*, que no requiere de licencia para su uso (Sistema Operativo Libre), por la cual se podrá aprovechar sin necesidad de pago por cada una de las utilidades que necesitaremos para cualquier pruebas de conceptos o demo, ya que sus fuentes no son propietarias y está disponible a través de Git.

Se utiliza principalmente para seguridad de redes, computo forense, auditorias de seguridad y también criptografía, en búsqueda de posibles vulnerabilidades informáticas, evaluarlas y explotarlas en consecuencia. Dado que estas características también se pueden utilizar con fines ilegales, la distribución no está exenta de controversia.

Está dirigido mayormente a usuarios experimentados, permitiéndoles identificar y corregir agujeros de seguridad antes de que, los ciberdelincuentes o *crackers* puedan acceder a los equipos y dispositivos de los usuarios finales, con el objeto de descifrar contraseñas, sobrecargar y espiar los sistemas.

1.1.1 Organización de los directorios

Como cualquier distribución GNU Linux organiza la información en archivos que se encuentran en carpetas. Un directorio puede contener subdirectorios y, por lo tanto, tener una jerarquía, como en cualquier otro sistema operativo. Los nuevos lanzamientos de Linux (incluido Red Hat) siguen a FSSTND (Linux sistema de archivos estándar) que define los nombres, ubicaciones y funciones de la mayoría de ellos

Conociendo esta infraestructura básica de archivos y carpetas del sistema., los usuarios/administradores podrán moverse más fácilmente a través de directorios, ya que la mayoría de ellos tienen alguna utilidad.

Directorio	Descripción
/	Raíz (root), forma la base del sistema de archivos.
/boot	Archivos del kernel (compilados).
/bin	Archivos ejecutables esenciales para todos los usuarios.
/dev	Archivos de dispositivos.
/etc	Archivos de configuración.
/etc/rc.d	Archivos de inicialización.
/home	Generalmente, directorios de los usuarios.
/home/ftp	Contenido del servidor FTP.
/home/httpd	Contenido del servidor WWW.
/lib	Librerías esenciales y módulos del kernel.
/mnt	Directorios donde ``montar'' diversos dispositivos temporalmente.
/mnt/cdrom	Directorio donde se ``monta'' el CD-ROM.
/proc	Información sobre partes del sistema.
/root	Directorio del usuario principal del sistema.
/sbin	Archivos ejecutables para tareas de administración.
/tmp	Temporal.
/usr	Programas, documentación, fuentes,...compartidos por todo el sistema.
/var	Archivos variables del sistema, bitácoras, temporales, etc.

1.2 NUEVAS CARATERISTICAS EN 2022

1.2.1 ¿Qué entorno de escritorio usa Kali Linux?

Kali Linux usa el entorno de escritorio XFCE por defecto. Los usuarios pueden cambiar a GNOME Shell o KDE Plasma durante la instalación.

Los desarrolladores de la distribución Kali Linux han publicado a la fecha la versión 2022.3, que presenta diez nuevas herramientas y mejoras para usar VirtualBox, así como las versiones actuales de GNOME y escritorio para la mesa Plasma. Linux 5.16 se utiliza como kernel.

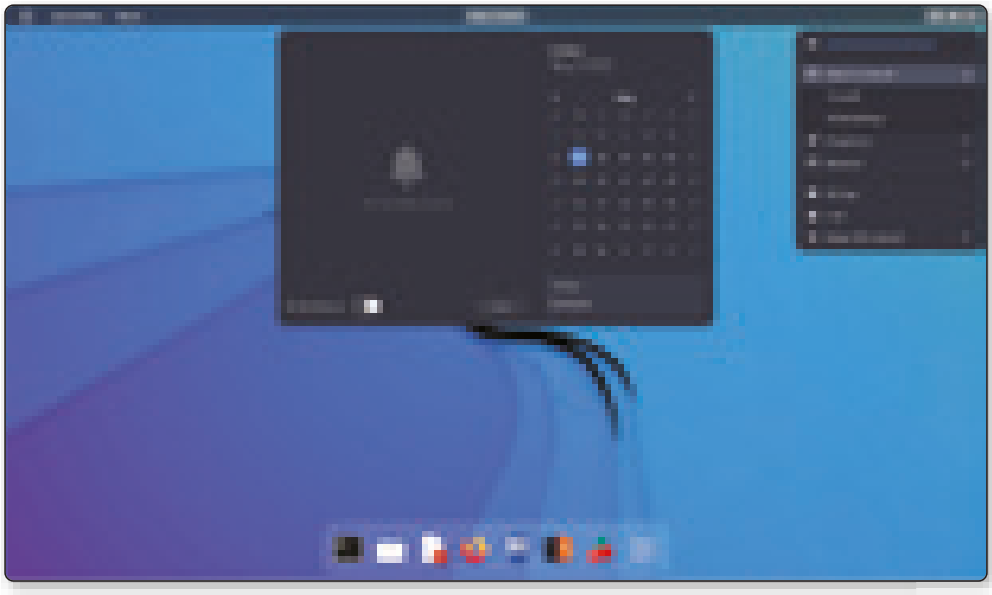

Figura 1.1. Tema - Kali-Dark

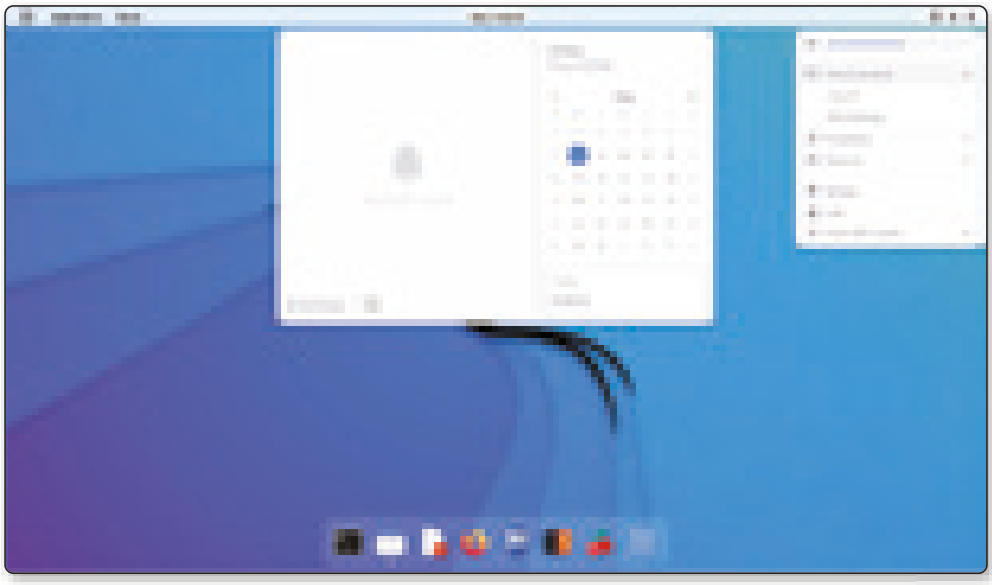

Figura 1.2. Tema - Kali-Light

Con GNOME 42, KDE Plasma 5.24 y Xfce 4.16, la distribución basada en Debian se actualiza con escritorios compatibles. Los usuarios de Kali Linux en VirtualBox ahora tienen un acceso más fácil a la función de carpetas compartidas, donde las cuentas de usuario se autorizan automáticamente con los permisos de grupo correctos para el grupo **vboxsf**.

Como es habitual, el repertorio de herramientas suministrado con Kali Linux 2022.3 se ha ampliado para incluir nuevas herramientas del campo de las pruebas de penetración:

Brute Shark: Herramienta de análisis forense de red (NFAT)

Este paquete contiene la Herramienta de análisis forense de red (NFAT) que realiza un procesamiento y análisis profundos del tráfico de red (principalmente archivos PCAP, pero también tiene la capacidad de capturar directamente desde la interfaz de red). Incluyen: Extracción de contraseñas, generación de mapas de red, reconstrucción de sesiones TCP, extracción de hash de contraseñas cifradas e incluso conversión al formato *Hashcat* para ataques fuera de línea.

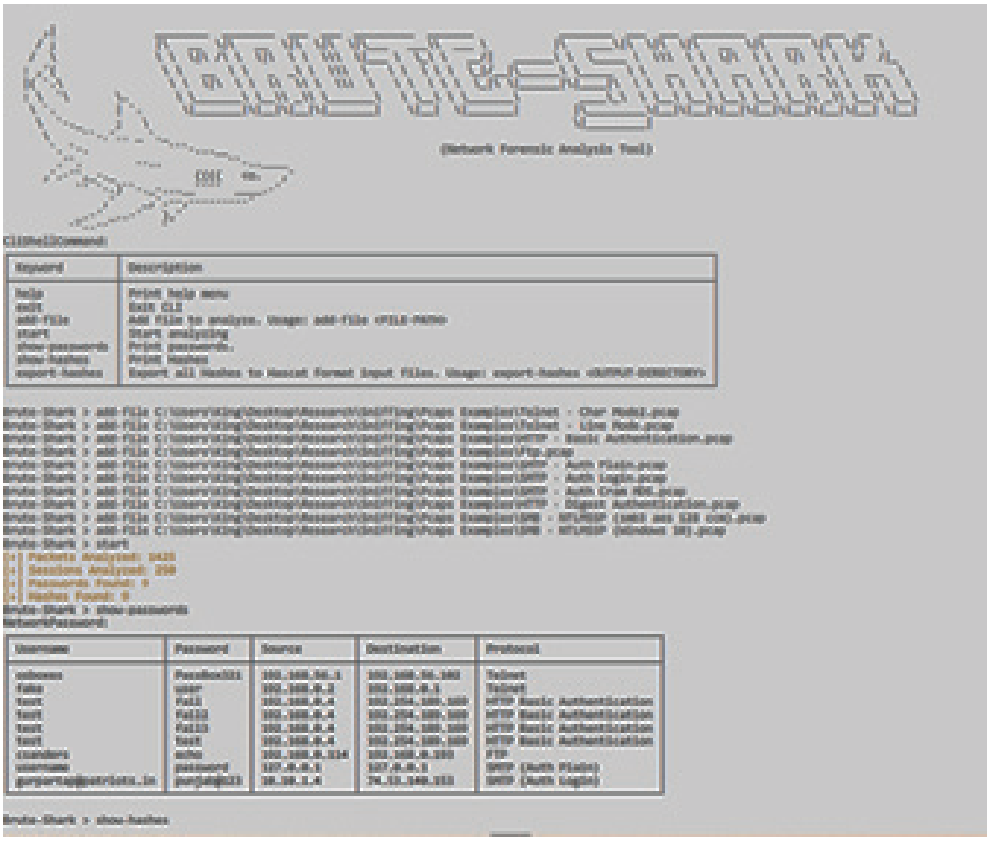

Figura 1.3. Brute Shark

Evil-WinRM: Shell de WinRM

WinRM (administración remota de Windows) es una implementación del protocolo Microsoft WS-Management. Un protocolo estándar basado en SOAP que permite la interoperabilidad de dispositivos y sistemas operativos de diferentes proveedores. Microsoft lo ha incluido en sus sistemas operativos para que sea más fácil para los administradores del sistema.

Este programa se puede usar en cualquier servidor de Microsoft Windows con esta función habilitada (generalmente en el puerto 5985), por supuesto, solo si tiene las credenciales y el permiso para usarlo. Por lo tanto, se puede utilizar en la explotación/post-explotación. El propósito de este software es proporcionar funciones buenas y fáciles de usar para piratear. Los administradores del sistema

también pueden utilizarlo con fines legítimos, pero la mayor parte de su funcionalidad se centra en la piratería/pentesting.

Figura 1.4. Evil-WinRM

Hakrawler: Rastreador web diseñado para el descubrimiento rápido y fácil de puntos finales URL activos

La URL se extrae rastreando la aplicación, consultando Wayback Machine, analizando el archivo robots.txt y analizando el archivo sitemap.xml.

La herramienta también recopila los subdominios que encuentra en el camino. Hasta donde yo sé, este método de enumeración de subdominios no es utilizado actualmente por ninguna otra herramienta popular de listado de subdominios, por lo que puede ayudar a revelar objetivos adicionales.

```
hakrawler$ echo https://google.com | ./hakrawler
[href] https://www.google.com.au/imghp?hl=en&tab=wi
[href] https://maps.google.com.au/maps?hl=en&tab=wl
[href] https://play.google.com/?hl=en&tab=w8
[href] https://www.youtube.com/?gl=AU&tab=w1
[href] https://news.google.com/?tab=wn
[href] https://mail.google.com/mail/?tab=wm
[href] https://drive.google.com/?tab=wo
[href] https://www.google.com.au/intl/en/about/products?tab=wh
[href] http://www.google.com.au/history/optout?hl=en
[href] https://www.google.com/preferences?hl=en
[href] https://accounts.google.com/ServiceLogin?hl=en&passive=true&continue=h
[href] https://www.google.com/advanced_search?hl=en-AU&authuser=0
[href] https://www.google.com/intl/en/ads/
[href] https://www.google.com/services/
```

Figura 1.5. Evil-WinRM

Httpx: Kit de herramientas HTTP rápido y versátil

Este paquete contiene el kit de herramientas httpX desarrollado por 'ProjectDiscovery'. Este es un conjunto de herramientas http rápido y flexible que le permite ejecutar múltiples pulidores con una biblioteca http reintentable y está diseñado para mantener la confiabilidad de los resultados con más subprocesos.

Figura 1.6. Httpx

LAPSDumper: Vuelca las contraseñas de LAPS

Una herramienta que descarga todas las contraseñas de LAPS (*Microsoft Local Administrator Password Solution*) que una cuenta puede leer usando un dominio.

Esta herramienta extraerá todas las contraseñas de LAPS a las que puede acceder la cuenta para leerlas en todo el dominio. El uso es muy simple y la sintaxis refleja la sintaxis de otras herramientas comunes. También es compatible con la transferencia hash (PtH).

```
root@kali:~# lapsdumper -h
usage: lapsdumper [-h] -u USERNAME -p PASSWORD [-l LDAPSERVER] -d DOMAIN

Dump LAPS Passwords

options:
  -h, --help            show this help message and exit
  -u USERNAME, --username USERNAME
                        username for LDAP
  -p PASSWORD, --password PASSWORD
                        password for LDAP (or LM:NT hash)
  -l LDAPSERVER, --ldapserver LDAPSERVER
                        LDAP server (or domain)
  -d DOMAIN, --domain DOMAIN
                        Domain
```

Figura 1.7. LAPSDumper

PhpSploit: Marco de post-explotación Stealth

PhpSploit es un marco de telemetría, cuyo propósito es proporcionar una conexión interactiva similar a un shell a través de HTTP entre un cliente y un servidor web. Es una herramienta posterior a la explotación capaz de mantener el acceso a un servidor web pirateado para fines de informes privilegiados.

La comunicación ofuscada se realiza mediante encabezados HTTP de solicitud de cliente estándar y respuestas relativas del servidor web, que se comunican a través de una pequeña puerta trasera polimórfica.

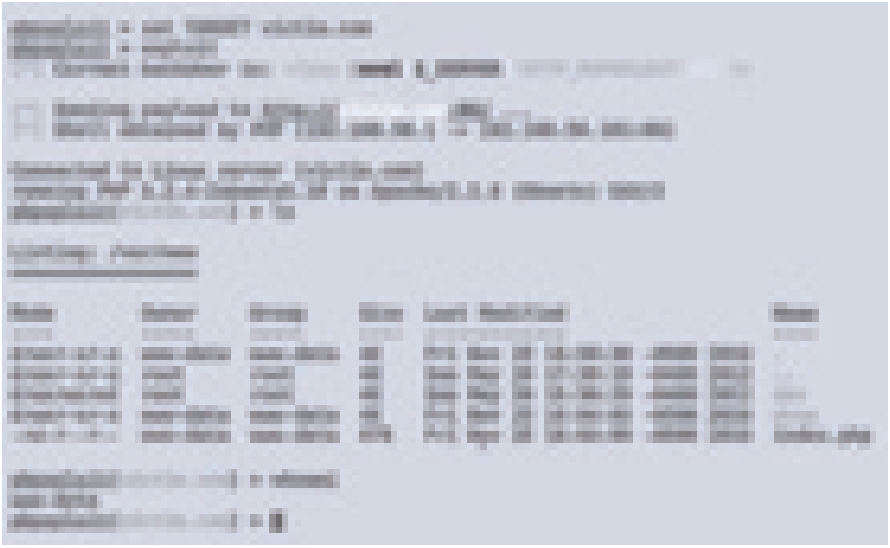

Figura 1.8. PhpSploit

PEDump: Vuelca los archivos ejecutables de Win32

Este paquete contiene un script para volcar encabezados y particiones, extraer recursos de win32 PE exe, dll y al final brinda una mirada rápida dentro del archivo PE sospechoso.

Figura 1.9. PEDump

SentryPeer: Honeypot SIP punto a punto para VoIP

Proyecto de código abierto relacionados con la seguridad que utilizan tecnología peer-to-peer. Analiza direcciones IP y números de teléfono de actores maliciosos.

SentryPeer es una herramienta de detección de fraude. Permite a los estafadores intentar hacer llamadas telefónicas y registrar la dirección IP de la que provienen y el número al que intentaron llamar.

Estos detalles se pueden utilizar para generar notificaciones en la red del operador, y la próxima vez que un usuario/cliente intente llamar a un número recopilado, puede actuar como mejor le parezca.

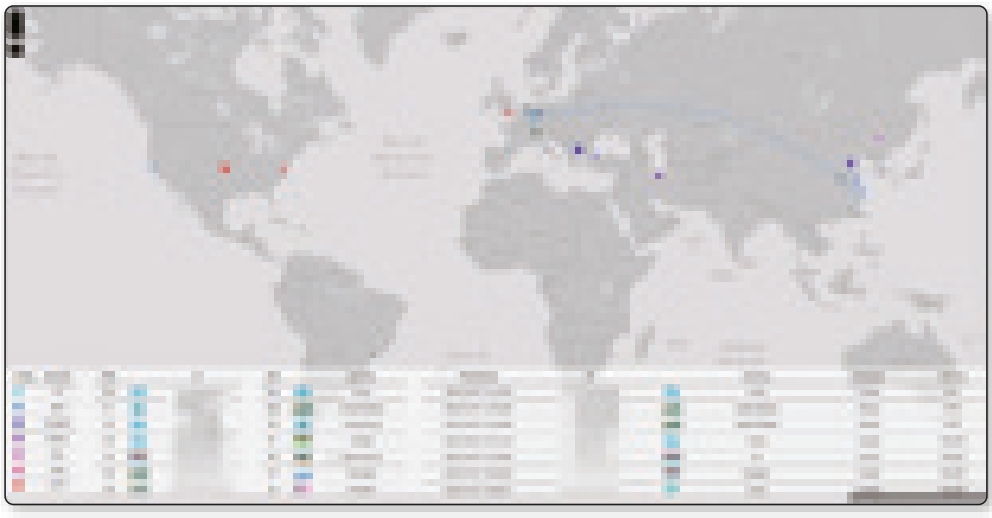

Figura 1.10. SentryPeer

Sparrow-wifi: Analizador gráfico Wi-Fi para Linux

Sparrow-wifi es la próxima generación de reconocedores de espectro Wi-Fi de 2,4 GHz y 5 GHz. En esencia, proporciona una alternativa basada en GUI más completa a herramientas como inSSIDer y linssid que se ejecutan específicamente en Linux.

Para casos de uso más extensos, Sparrow-wifi integra wifi, radio definida por software (hackrf), motor bluetooth avanzado (tradicional y Ubertooth), GPS tradicional (a través de GPS) y GPS móvil para pasajeros/drones a través de mavlink en una sola solución.

Figura 1.11. Sparrow-wifi

Wifipumpkin3: Potente marco para puntos de acceso no autorizados

Wifipumpkin3 es un marco creado en Python para proporcionar ataques de puntos de acceso maliciosos de equipo rojo e ingeniería inversa. Esta herramienta permite crear un punto de acceso Wi-Fi falso para que nuestra víctima se conecte y cómo explotar el sistema.

wifipumpkin3 es un poderoso framework de ataque de puntos de acceso, escrito en Python, que permite y proporciona a los investigadores de seguridad, equipos rojos e ingenieros inversos la instalación de redes inalámbricas para realizar ataques entre entornos.

Figura 1.12. Wifipumpkin3

Esta nueva versión incluye un nuevo protector de pantalla alternativo denominado *'Hollywood Activate'* que aparecen una y otra vez en las series de televisión y películas cuando se trata de hackear.

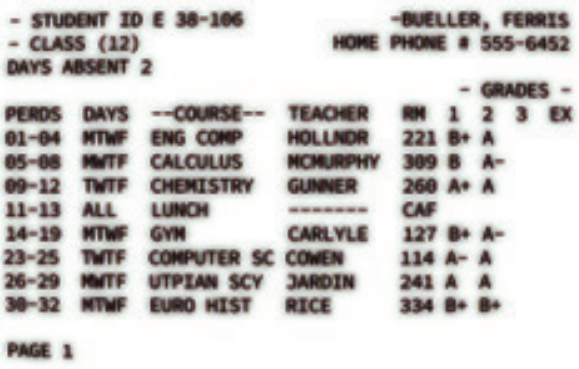

Figura 1.13. Salva pantalla - Hollywood Activate

Después de la instalación, se pueden instalar con el siguiente comando:

```
┌──(root@kali)-[~]
└─$ sudo apt -y install kali-screensaver
```

Para activar esta interfase usted deberá ejecutar el comando:

```
┌──(root@kali)-[~]
└─$ hollywood-activate
```

1.3 CATEGORÍAS DE HERRAMIENTAS

1.3.1 Recopilación de información

Esta es la primera categoría de la lista, alberga 57 herramientas, incluidos scripts, analizadores de protocolos de red y evaluadores de DNS, entre otros. Las más importantes incluyen Amap, que puede identificar las aplicaciones de puerto que se están ejecutando para comparar y determinar si este es el puerto correcto. Dnsmap, una herramienta diseñada para pruebas de penetración, ayuda a recopilar la mayor parte de la información de la infraestructura analizada, incluidos dominios, bloques de red y más.

1.3.2 Análisis de vulnerabilidad

Contiene herramientas de escaneo para encontrar vulnerabilidades en la mayoría de los sistemas de Cisco. Una de las herramientas que aparecen en la lista es Nmap, que es un poderoso escáner que permite explorar los equipos de la red con todas sus características para analizarlos y aprender más sobre ellos.

1.3.3 Aplicaciones web

El catálogo contiene todo lo necesario para iniciar un escaneo en línea, se compone principalmente de textos, también tienen la calidad de analizar bases de datos, ingresar código SQL, capturar elementos de páginas web y más. Entre las herramientas destacables se encuentra sqlmap, cuya función es detectar y explotar vulnerabilidades en aplicaciones web para realizar ataques de inyección SQL.

1.3.4 Ataques de contraseña

Ejecuta 36 herramientas de ataque de contraseña, algunas de las cuales utilizan la fuerza bruta para lograr su propósito, que es averiguar su información de inicio de sesión. Entre estos, John the Ripper se destaca por ser rápido y configurable para sus necesidades de investigación. Se diferencia de otras herramientas por tener sus propios módulos mejorados que utiliza para sus ataques.

1.3.5 Ataques a redes inalambricas

A continuación se muestra una lista de 32 herramientas, la mayoría de las cuales permiten monitorear el tráfico de la red. Incluye mecanismos que degradan los mecanismos que utilizan Bluetooth para transmitir datos. Tal como *BlueRanger*, que detecta este tipo de dispositivos con alta calidad de rastreo. Permite medir la distancia del dispositivo dependiendo de la calidad del enlace,

1.3.6 Herramientas de explotación

Lista de herramientas patentadas para tareas de explotación Esta lista incluye herramientas para realizar pruebas de penetración web, pruebas rápidas y avanzadas en dispositivos Cisco vulnerables, inyectar ataques SQL en aplicaciones web, etc.

1.3.7 Sniffing/Spoofing

Esta lista, que es necesaria para encontrar y explotar vulnerabilidades, contiene varias herramientas para el uso de esta tecnología, HexInject, mediante el uso de scripts, modifica el tráfico de la red a través de intercepciones. Otra herramienta importante en la lista es Mitmproxy, que le permite ver tanto el tráfico HTTPS como HTTP, y se usa para monitorear aplicaciones móviles para detectar transmisiones enviadas.

1.3.8 Herramientas para mantener el acceso

Las herramientas importantes de mantenimiento de acceso incluyen Polenum, que permite extraer información de la política de contraseñas de los dispositivos Windows, y Polenum, que permite realizar estas operaciones de forma remota. Otra herramienta importante es WebScarab, que permite a los profesionales de la seguridad encontrar vulnerabilidades en una aplicación basada en HTTP.

1.3.9 Reversing

El menú Herramientas permite la ingeniería inversa, la extracción del diseño en algunos casos para comprender cómo funciona el sistema. Una de las herramientas notables para hacer ingeniería inversa en la lista es javasnoop que, una vez en el código fuente, itera sobre el código modificando variables y recopilando toda la información del applet o la aplicación.

1.3.10 Stress Testing

Entre sus herramientas se encuentran FunkLoad, que permite realizar pruebas de rendimiento y regresión de proyectos web, Pruebas de recursos, pruebas de carga, entre otros. También en la lista está iaxflood, una herramienta para saturar el protocolo IAX2 que se usa en el PBX Asterisk.

Por último, pero no menos importante, está la llamada de inundación, que se utiliza en un ataque de denegación de servicio (DoS) contra dispositivos SIP, mediante el envío de múltiples solicitudes INVITE según la configuración aplicada.

1.3.11 Hacking de Hardware

Herramientas diseñadas para comprometer la parte física de un sistema con el fin de modificar el código de shell de un dispositivo para influir en su comportamiento o hacer que funcione según lo previsto por el atacante. La lista completa incluye 6 herramientas: Android- SDK, apktool, Arduino, dex2jar, Sakis3G, smali.

1.3.12 Computo forense

Un kit de herramientas para realizar tareas forenses en escenarios donde es importante conocer las acciones finales realizadas en el sistema. Entre el menú está chntpw, que le permite ver información y cambiar las contraseñas de los usuarios de la base de datos de Windows.

1.4 DESCARGAR KALI LINUX

1.4.1 ¿Kali Linux es ilegal?

Usar Kali Linux no es un delito. Es utilizado principalmente por hackers para pruebas de penetración o pentesting, para mejorar la seguridad de una empresa. Es ilegal usar las herramientas de Kali Linux con intenciones maliciosas.

1.4.2 ¿Puedo instalar Kali Linux en Windows 10?

Puede instalar Kali Linux desde Microsoft Store en Windows 10 después de activar el Subsistema de Windows para Linux. También es posible instalar Kali Linux en Windows utilizando un software de máquina virtual de terceros, como VMWare y Virtual Box.

VMWare es una plataforma ideal para realizar la instalación de máquinas virtuales, por lo que puede instalar Kali Linux sin restricciones. Si quieres saber los pasos necesarios para completar esta tarea, tendrás que seguir leyendo.

También en los siguientes párrafos encontrarás los requisitos del sistema para instalar Kali Linux y las mejores alternativas de VMWare.

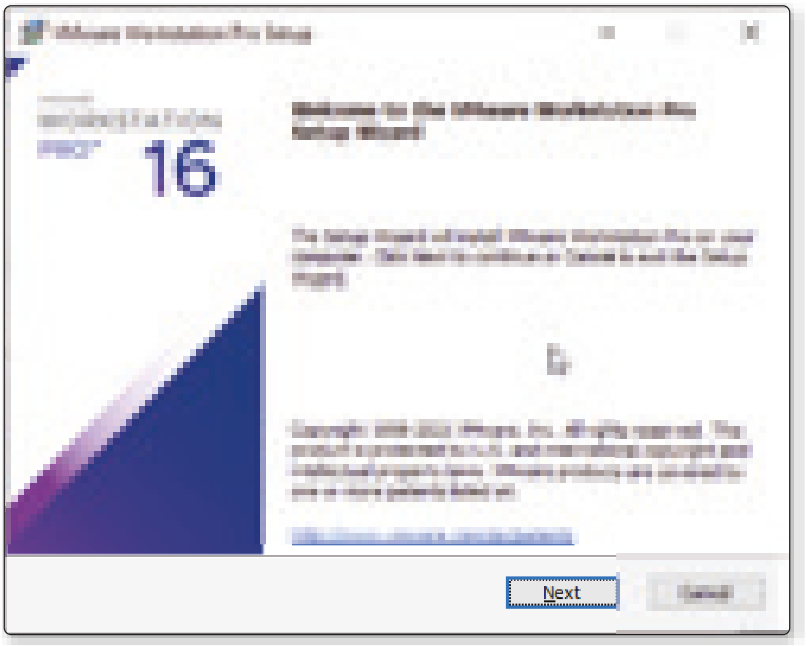

Figura 1.14. Imagen referencial – VMWare Workstation PRO

Para poder usar VMWare e instalar Kali Linux, primero debes conocer los requisitos, los requisitos mínimos para que funcione sin problemas.

He aquí por qué lo requerirás:

- 20 GB de espacio en disco duro.
- 2 GB de RAM solo para este programa.

Otro factor a tener en cuenta es la versión que estés utilizando en tu ordenador, ya que la arquitectura debe ser de 32 bits o de 64 bits.

1.4.3 Crear la máquina virtual

Lo primero que debe hacer es abrir VMware y presionar el botón para crear una nueva máquina virtual.

- Utiliza la combinación de teclas <Ctrl + N> para crear una nueva máquina.
- Luego dirígete al menú y selecciona las opciones Player, File y por último New Virtual Machine.

- A continuación, haz clic en <Create a New Virtual Machine>.

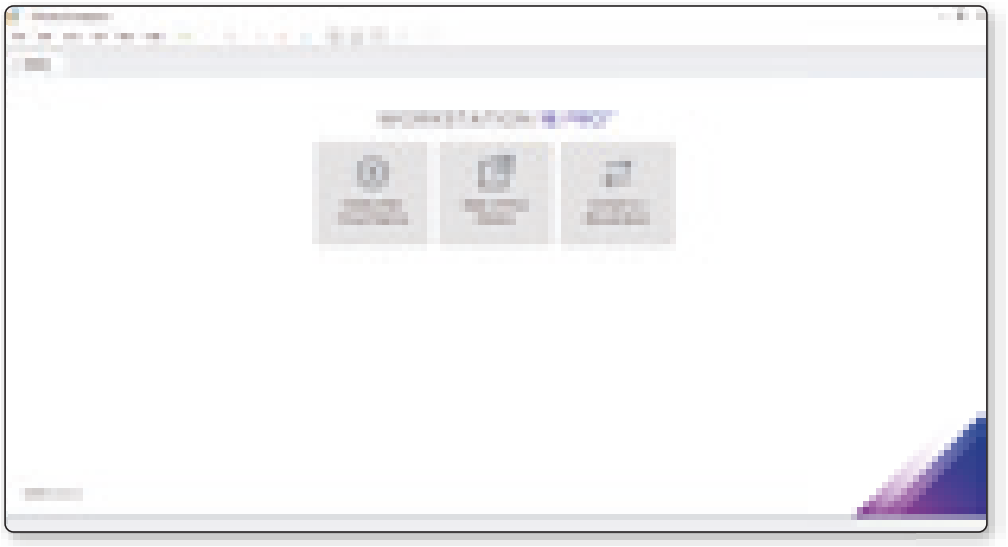

Figura 1.15. Imagen referencial – VMWare Workstation Player

Vista de creación de nueva máquina virtual.

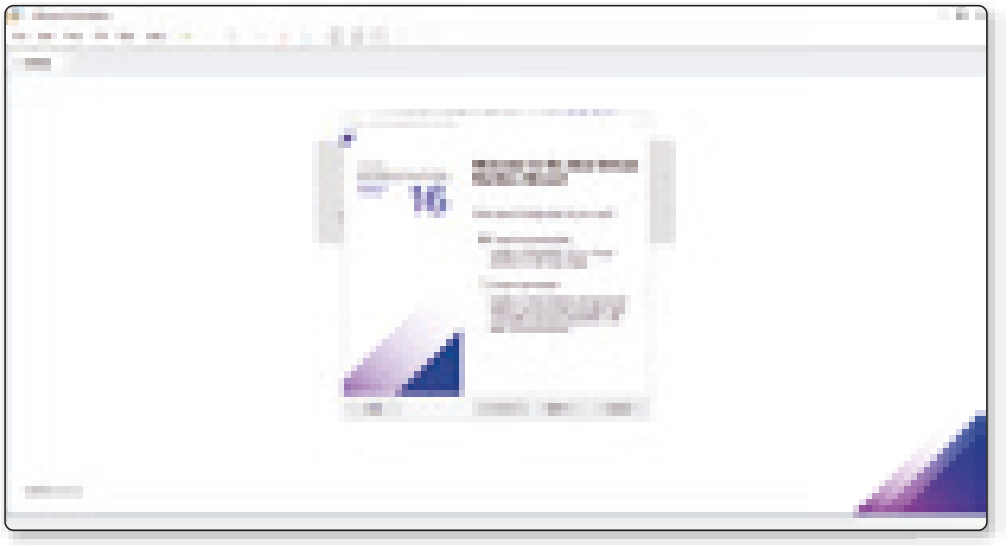

Figura 1.16. Imagen referencial – VMWare Workstation Player

Figura 1.17. Imagen referencial – Kali Linux instalada

1.4.4 ¿Puedo instalar Kali Linux desde cero?

Para iniciar este proceso tenemos que descargar la imagen ISO disponible en el repositorio de Kali desde el siguiente enlace: *https://www.kali.org/get-kali/*

Luego de grabar la imagen ISO en un DVD o en un dispositivo USB de arranque para disponer de ella, luego iniciamos el equipo con la imagen ISO de Kali Linux y veremos lo siguiente. Seleccionamos la opción "*Graphical Install*"

Figura 1.18. Imagen referencial – Instalación desde cero

Y esperamos que carguen los servicios, ahora seleccionamos el idioma de instalación:

Figura 1.19. Imagen referencial – Selección de idioma

Después de esto definimos la ubicación:

Figura 1.20. Imagen referencial – Elegir ubicación

Ahora seleccionamos el idioma del teclado:

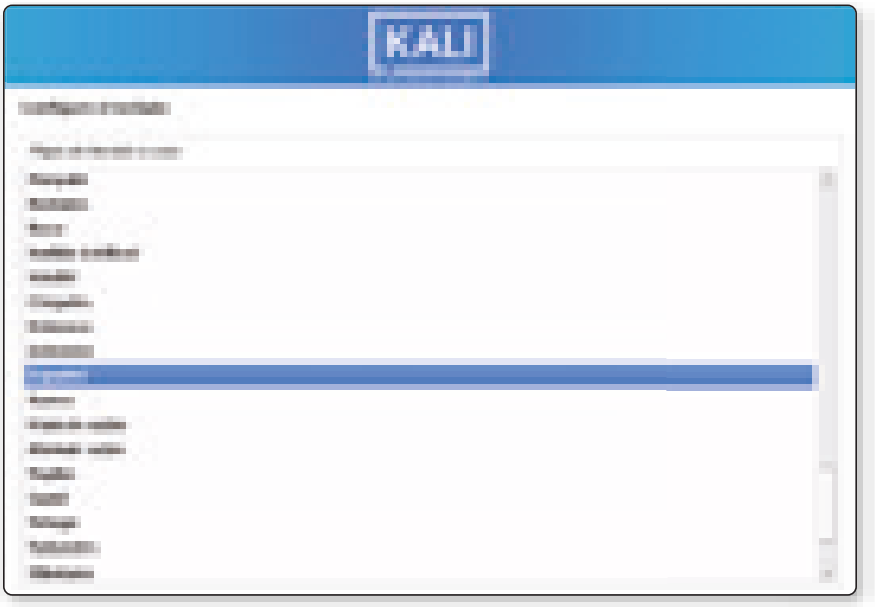

Figura 1.21. Imagen referencial – Elegir idioma del teclado

Damos clic en Continuar y se cargaran algunos componentes:

Figura 1.22. Imagen referencial – iniciando la carga de componentes

Se configurará la red:

Figura 1.23. Imagen referencial – iniciando reconocimiento de dispositivos de red

Asignamos el nombre al equipo:

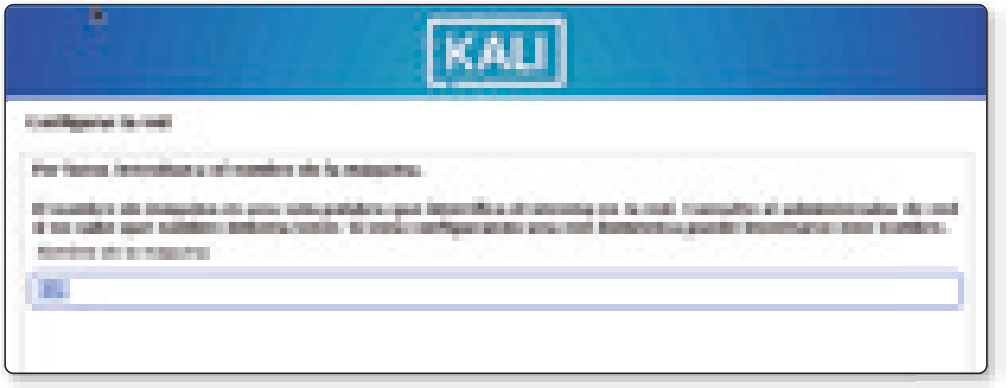

Figura 1.24. Imagen referencial – configurando el nombre de la maquina

Damos clic en Continuar y se cargaran algunos componentes:

Figura 1.25. Imagen referencial – configurando medios de instalación

Se configurará la red:

Figura 1.26. Imagen referencial – configurando medios de instalación

Asignamos el nombre al equipo:

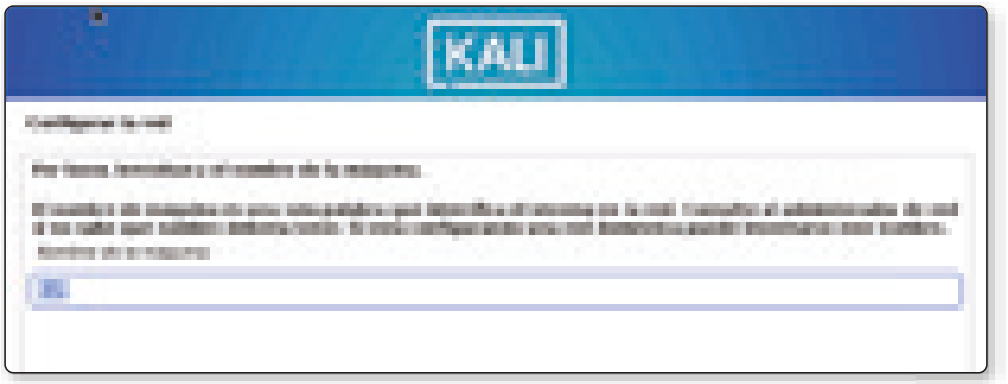

Figura 1.27. Imagen referencial – configurando medios de instalación

En la siguiente ventana es posible definir si se usará dominio o no:

Figura 1.28. Imagen referencial – configurando medios de instalación

Damos clic en Continuar para asignar el nombre de usuario. Damos clic en Continuar

Figura 1.29. Imagen referencial – configurando medios de instalación

y podemos dejar el valor por defecto del usuario o bien modificarlo:

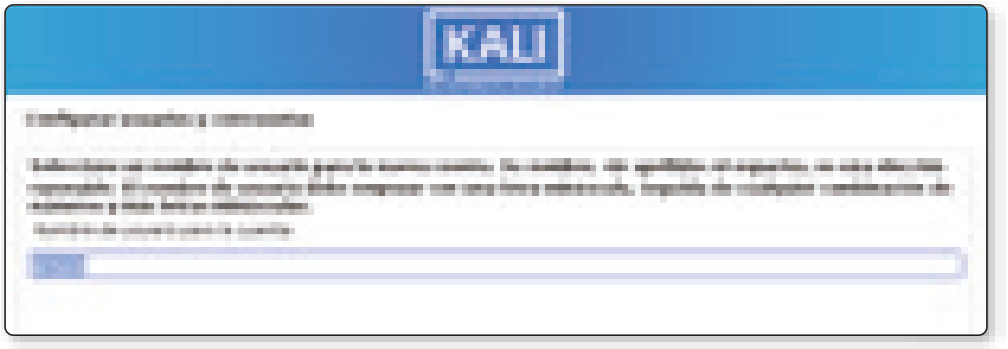

Figura 1.30. Imagen referencial – configurando medios de instalación

En la siguiente ventana es posible asignar la contraseña para el usuario administrador:

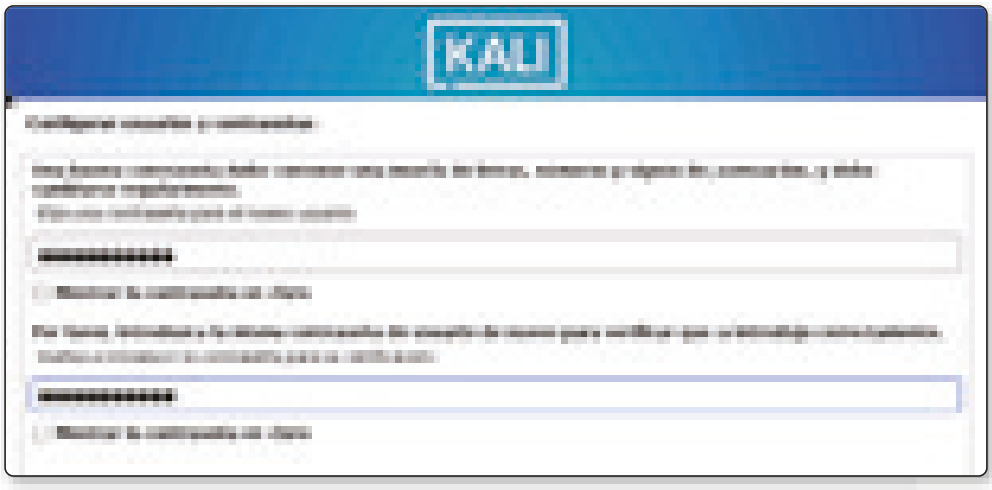

Figura 1.31. Imagen referencial – configurando medios de instalación

En base a la ubicación seleccionada podemos definir la zona donde nos encontramos geográficamente:

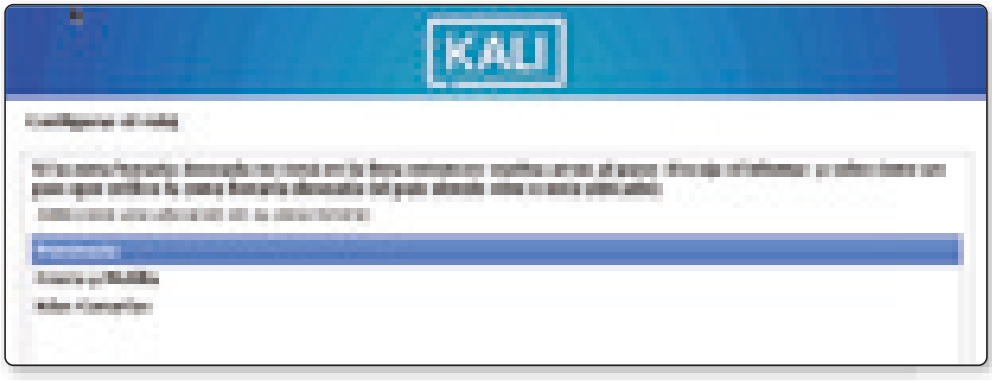

Figura 1.32. Imagen referencial – configurando medios de instalación

Accedemos ahora a la configuración del disco duro de Kali Linux:

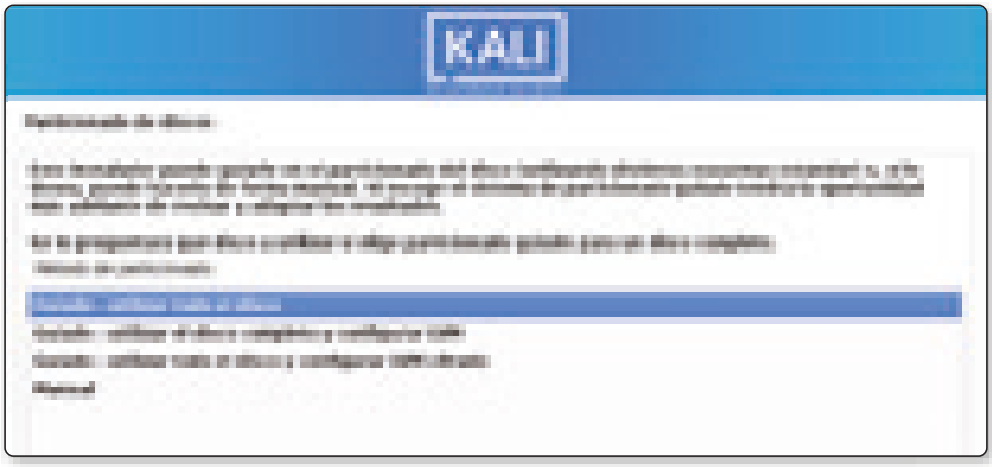

Figura 1.33. Imagen referencial – configurando medios de instalación

Veremos lo siguiente. Definimos la forma de particionado del disco, puede ser automático o asignando particiones.

Figura 1.34. Imagen referencial – configurando medios de instalación

En este caso vamos a asignar una partición especial para los temporales y para la carpeta de inicio de Kali Linux:

Figura 1.35. Imagen referencial – configurando medios de instalación

Damos clic en Continuar para ver la estructura que Kali Linux ha asignado al disco en base a la elección que hemos seleccionado:

Figura 1.36. Imagen referencial – particionado de directorios

Al dar clic en Continuar veremos lo siguiente. Confirmamos el proceso activando la casilla Si.

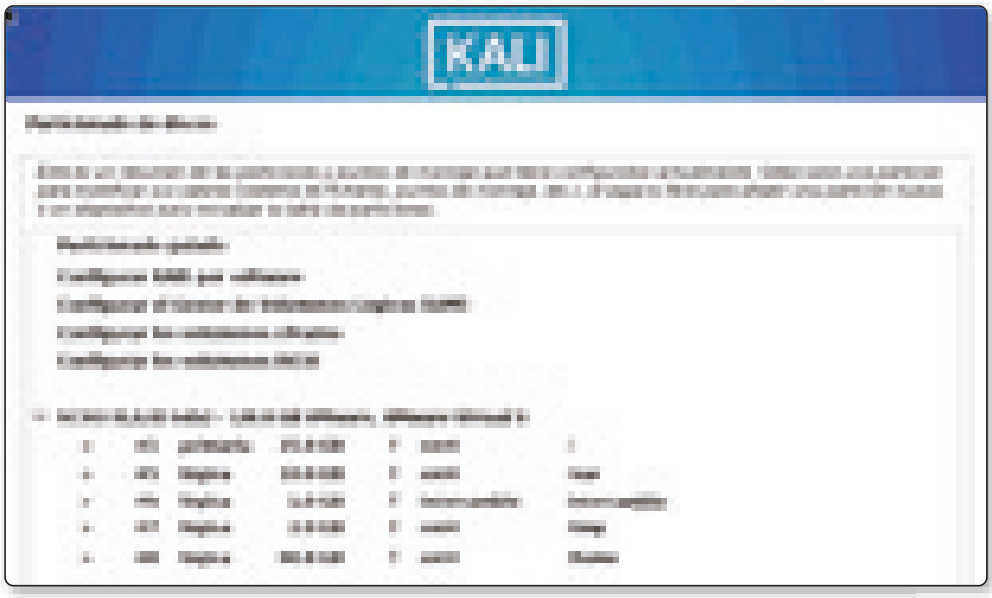

Figura 1.37. Imagen referencial – estructura definitiva de directorios

Hacer clic en la opción 'Finalizar el particionado y escribir los cambios en el disco'. Y se iniciará la instalación de Kali Linux 2022.3:

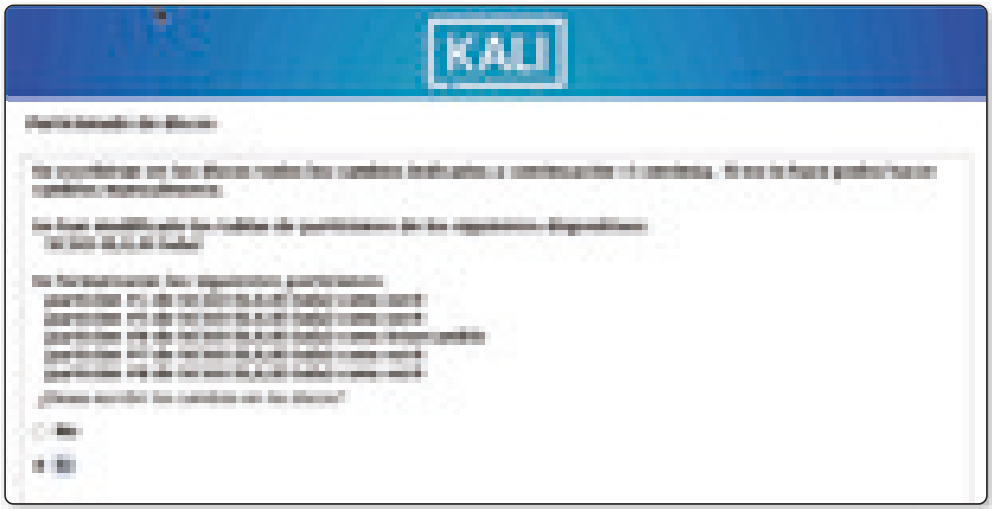

Figura 1.38. Imagen referencial – estructura definitiva de particionado

Podemos ver el paso a paso del proceso:

Figura 1.39. Imagen referencial – instalando sistema

Definimos si se usará una réplica de red o no:

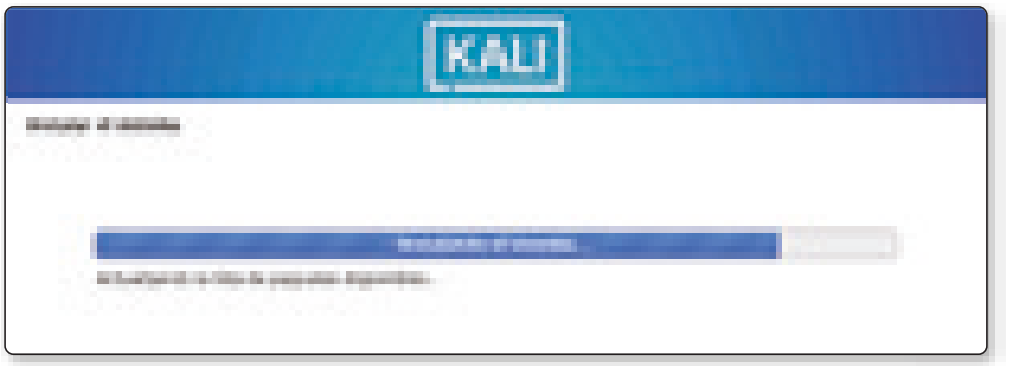

Figura 1.40. Imagen referencial – instalando paquetes disponibles

NOTA

La réplica de Kali Linux no nos permite tener acceso a un repositorio, ya sea local, nacional o internacional, donde podemos instalar programas y otras funciones de Kali.

Linux que no están en el medio original de instalación en este caso la imagen ISO. Después de esto se dará paso al gestor de arranque:

Figura 1.41. Imagen referencial – configurando réplicas de red

Confirmamos el uso del gestor de arranque GRUB:

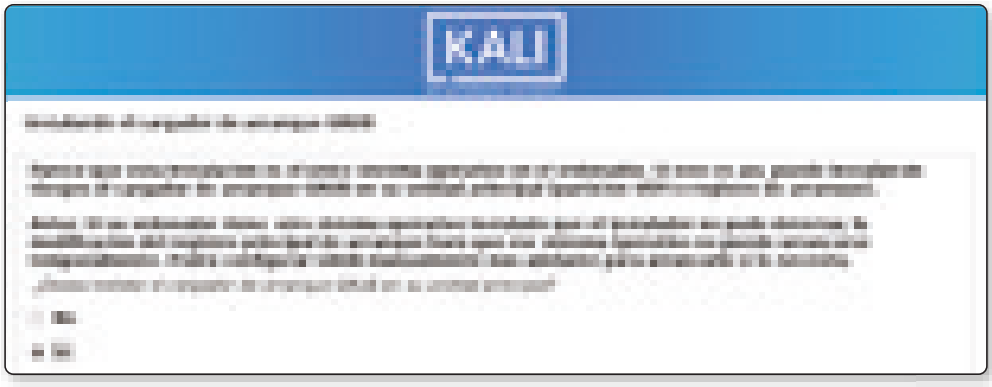

Figura 1.42. Imagen referencial – cargando arranque GRUB

Selecciona donde se instalará el gestor de arranque:

Figura 1.43. Imagen referencial – instalando arranque GRUB

Damos clic en Continuar para completar el proceso de instalación:

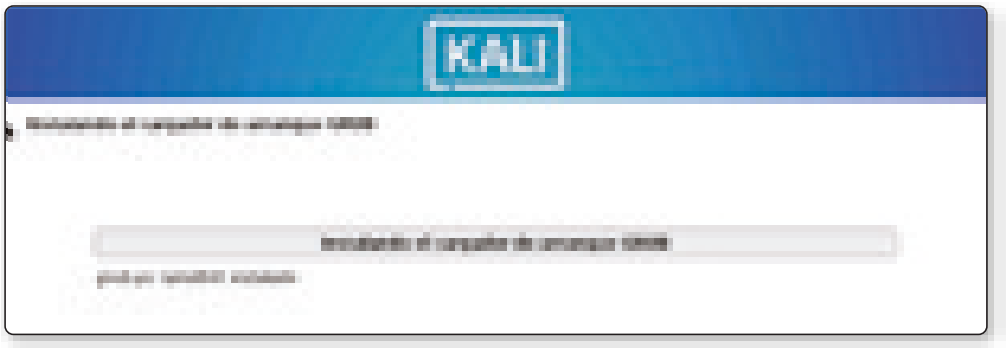

Figura 1.44. Imagen referencial – configurando partición donde se creará arranque GRUB.

Entramos en la recta final de la instalación:

Figura 1.45. Imagen referencial – actualizando GRUB.

Al finalizar veremos lo siguiente. Reiniciamos el equipo para completar la instalación:

Figura 1.46. Imagen referencial – finalizando instalación de replicas

y en la pantalla inicial seleccionamos el gestor:

Figura 1.47. Imagen referencial – finalizando instalación

Se cargarán los servicios:

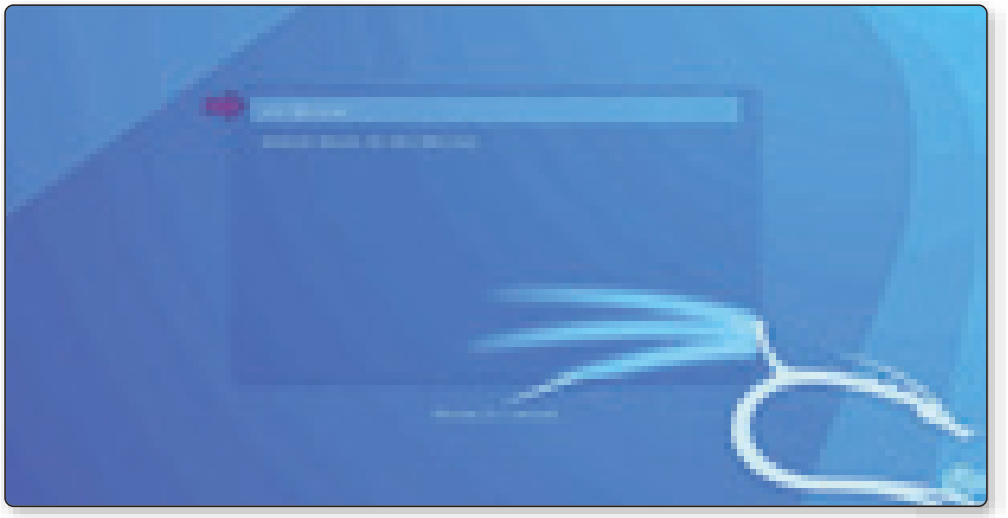

Figura 1.48. Imagen referencial – finalizando instalación

Inicia sesión:

Figura 1.49. Imagen referencial – iniciándose el sistema operativo

Al acceder veremos el entorno de Kali Linux 2022.3:

Figura 1.50. Imagen referencial – accediendo al sistema

1.5 UTILIZAR KALI LINUX

1.5.1 Posterior a la instalación

Ahora que ha terminado de instalar Kali Linux, es hora de personalizar su sistema.

> **NOTA**
>
> Para obtener más consejos sobre cómo aprovechar al máximo Kali Linux, visite el foro oficial de usuarios: *https://forums.kali.org/*

1.5.2 Actualizaciones, mejoras y actualizaciones de lanzamiento

Limpie, actualice, actualice y libere la actualización de su Kali instalado.

```
apt-get clean && apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y
```

1.5.3 Agregar usuarios estándar

Por defecto, Kali Linux solo tiene el usuario root. Aunque la mayoría de las aplicaciones requieren acceso raíz, se recomienda agregar un segundo usuario. Abra Terminal e ingrese el siguiente comando para crear un nuevo usuario (reemplace usuario1 con el nombre de usuario de su elección).

```
$ useradd -m user1
```

ⓘ NOTA

-m significa crear un directorio de inicio que generalmente es / home / username)

Ahora establezca una contraseña para este usuario:

```
$ passwd user1
```

Ingrese la contraseña requerida dos veces. Agregue el usuario al grupo sudo (permita que el usuario instale el programa, permita imprimir, use el modo privilegiado, etc).

```
usermod -a -G sudo user1
```

ⓘ NOTA

-a significa agregar o agregar, -G significa especificar un grupo / varios grupos).

Cambie el contenedor predeterminado para el usuario creado anteriormente para bash:

```
$ chsh -s /bin/bash user1
```

1.5.4 Instalar HTOP y NetHogs

HTOP es una herramienta especial que muestra los procesos en ejecución y la memoria utilizada, incluida información más detallada. (También puede usar el comando anterior, pero HTOP es más útil).

NetHogs también es útil porque muestra el tráfico que usa la aplicación en cada interfaz. El siguiente comando instalará estas herramientas:

```
$ apt-get install htop nethogs -y
```

Ahora puede ejecutarlos con los siguientes comandos:

```
# htop
$ nethogs eth0
$ nethogs wlan0
```

1.5.5 Instalar Terminator

Entre los terminales preferidos por los usuarios tenemos *Terminator*, emulador de terminal avanzado y personalizable que admite pestañas y accesos directos y nos permite guardar diferentes estilos o configuraciones que proporcionamos para el terminal Linux por defecto no tiene. Brinda la posibilidad de crear varias estaciones en una ventana para que puedan moverse más rápido entre ellas y así agilizar el trabajo en curso.

Para instalar Terminator en Kali Linux, por ejemplo (una distribución diseñada principalmente para pruebas y seguridad informática en general), abra Terminal e ingrese el comando:

```
$ sudo apt-get install terminator
```

De hecho, su uso es muy sencillo, para acceder al menú de opciones, haga clic derecho en el panel, las funciones más utilizadas como “Dividir horizontalmente”, “Dividir verticalmente” y “Abrir pestaña” estarán disponibles en el menú.

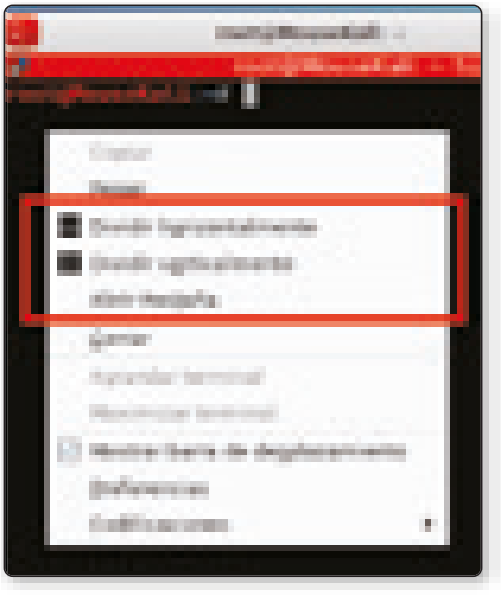

Figura 1.51. Imagen referencial – utilizando terminator

Comandos básicos

- F11: Activar pantalla completa
- Ctrl + Shift + O: Dividir terminal horizontalmente
- Ctrl + Shift + E: Dividir terminal verticalmente
- Ctrl + Shift + W: Cerrar el panel actual
- Ctrl + Shift + T: Abrir nueva pestaña
- Alt + ↑ Mover al terminal por encima del actual
- Alt + ↓ Mover al terminal debajo del actual
- Alt + ← Mover a la terminal izquierda de la actual.
- Alt + → Mover a la derecha de la terminal de la actual

Le encantará usar estas pequeñas herramientas de administración y, estoy seguro de que lo hará.

1.6 CONFIGURANDO ENTORNO DE PRUEBAS

La realización de pruebas de penetración es una tarea compleja, implica un proceso en el que se realizan diferentes tipos de tareas con el fin de identificar las vulnerabilidades que se pueden explotar en la infraestructura de destino y el daño que puede causar un atacante.

En otras palabras, existe un proceso de piratería ética para identificar problemas potenciales antes de que ocurran y luego reparar o mejorar el sistema para prevenir estos ataques.

Nada es totalmente libre de fallos de seguridad, ni siquiera el sistema de información. Ya sea un sistema informático, una aplicación móvil, un sitio web o un dispositivo de Internet de las cosas, todos están rodeados de riesgos inherentes.

Las vulnerabilidades aparecen a diario, ya que los expertos en seguridad están ocupados corrigiéndolas y los piratas informáticos las explotan. Los profesionales de la seguridad utilizan un software especializado llamado escáneres de vulnerabilidades para escanear los sistemas en busca de vulnerabilidades y agujeros de seguridad.

Para quienes quieran adentrarse de forma profesional en el mundo del hacking ético y las pruebas de penetración. En mi opinión, estas son las primeras herramientas que debes conocer, no solo para empezar a prepararte para esta tarea, sino también para empezar a entenderla:

1.6.1 Nessus

Una vez que haya identificado los servicios que se están ejecutando, puede comenzar a usar las herramientas utilizadas para identificar las debilidades en el servicio.

En este sentido, la mejor herramienta para adentrarse en este mundo es Nessus, otra aplicación gratuita (sólo para uso doméstico, suficiente para los fines de este artículo; en caso de uso profesional, debería ser necesario. Utilizar la versión de pago). Por su base de datos y facilidad de uso, es un privilegio en este sentido.

Aunque tiene una línea de comandos, considero que su interfaz gráfica completa e intuitiva es una manera fácil de comenzar a probar esta herramienta.

La lógica de Nessus es similar a la de Nmap: se debe especificar el destino, en este caso, las direcciones IP y los parámetros. Estos permiten limitar el campo de estudio, especialmente si se especifican servicios *upstream*.

Después del registro en el sitio de la empresa Tenable, recibirá un enlace en su correo electrónico para el código de activación. Este código de activación verificará que el producto está instalado. Ahora, haga clic en "Descargar" en la nueva página para continuar.

ⓘ NOTA

El código de activación anterior es un código de uso único provisto por el sitio tenable.com. Cada vez que instale Nessus, necesitará uno.

Luego dirigirse hacia la carpeta de descargas y abrirla desde la terminal. El siguiente comando para instalar el archivo .deb descargado.

El nombre del archivo será "Nessus-10.2.0-debian9_amd64.deb". Según la versión, podría ser un poco diferente.

Una vez ejecutado todo lo anterior, para instalar usar el comando:

```
$ sudo dpkg -i Nessus-10.0.1-debian6_amd64.deb
```

Ya instalado, se deberá iniciar el servicio Nessus. Simplemente ejecutando el comando "systemctl".

```
$ sudo systemctl start nessusd.service
```

Para permitir que el servicio se inicie automáticamente en el siguiente arranque, use el siguiente comando:

```
$ sudo systemctl enable nessusd
```

Ver estado del servicio Nessus:

```
$ sudo systemctl status nessusd
```

Bien, Nessus ahora está listo para configurar desde el navegador web. Necesitaremos el código de activación que recibimos de Tenable, así que téngalo respaldado en un archivo en local. Ahora, abra su navegador web y vaya a la URL:

```
https://kali:8834/
```

NOTA

El puerto de interfaz de usuario predeterminado en Nessus es 8834, asegúrese de que otros servicios no lo utilicen.

La siguiente página le solicitará ingresar algunos detalles para obtener el código de activación. Como ya lo tenemos, podemos saltarnos este paso con seguridad.

Después de enviar la información de su cuenta de usuario, comenzará a descargar varios complementos necesarios. Esperamos que la instalación haya sido exitosa, ahora podemos continuar. Ahora verá la ventana de inicio de sesión

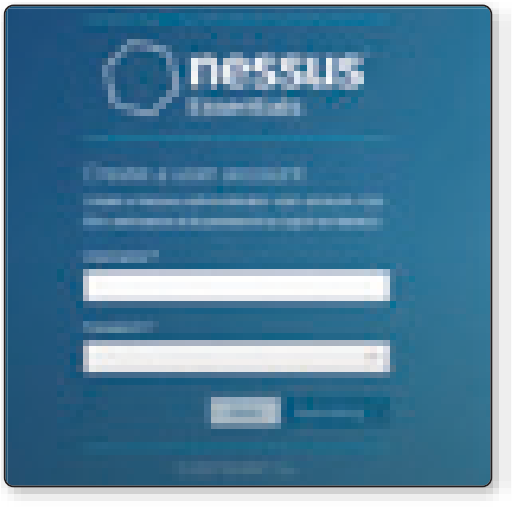

Figura 1.52. Imagen referencial – Inicio de sesión Nessus

NOTAS

- La ciberseguridad es un factor importante para que una organización proteja sus activos de TI. Con herramientas como Nessus, podemos identificar amenazas y vulnerabilidades antes de que los atacantes puedan explotarlas. Esto reduce la superficie de ataque y mejora la seguridad general de la red.
- Para usar esta herramienta de manera efectiva, recomiendo la revisión detallada de la documentación oficial del producto, antes de usarlas en un entorno real, en el siguiente enlace: *https://docs.tenable.com/*

1.6.2 Metasploit Framework

Una vez identificados los servicios y sus vulnerabilidades, el siguiente paso será explotar las vulnerabilidades. En otras palabras, primero debe verificar si las vulnerabilidades que se han identificado realmente permiten que un atacante cause daño. El marco Metasploit proporciona la infraestructura, el contenido y las herramientas para realizar pruebas integrales de seguridad y penetración.

A pesar de que en el caso anterior se identificó una vulnerabilidad, es posible que en el momento en que se intentó el exploit existieran otros controles que no se tuvieron en cuenta, otras capas de seguridad, u otras variables que pudieran hacer que los *exploits* fueran más complejos.

Asimismo, si se explota la vulnerabilidad, se puede verificar y determinar el alcance del daño a la organización, dependiendo de la información o los sistemas "detrás" de la vulnerabilidad en cuestión.

Para ello, Metasploit es la herramienta ideal para realizar estas pruebas. Mientras que Nessus tiene una base de datos de vulnerabilidades, Metasploit tiene una base de datos de *exploits* que puede aprovechar. En otras palabras, en lugar de buscar una vulnerabilidad en una computadora remota, el exploit se ejecuta directamente y los resultados posteriores, si se ejecutan con éxito, se simulan.

Al igual que Nessus, la versión de línea de comandos, msfconsole, es la versión tradicional, incluso recomendada para la automatización. Sin embargo, su interfaz gráfica es muy práctica para dar los primeros pasos y entenderlo mejor, con los siguientes pasos:

Iniciar el servidor de base de datos

La base de datos PostgreSQL viene instalada, pero, debe ejecutarse manualmente en Kali Linux. Inicie el servicio con el siguiente comando:

```
$ sudo systemctl enable --now postgresql
```

Configurar para que el servicio se ejecute en el arranque

```
$ systemctl status [email protected]*-main.service
```

Configurar la base de datos Metasploit PostgreSQL en Kali Linux

Una vez que el servidor de la base de datos PostgreSQL esté en funcionamiento, configure la base de datos Metasploit PostgreSQL.

```
$ sudo msfdb init
```

Ahora tenemos PostgreSQL ejecutándose y la base de datos configurada. El último paso requerido es ejecutar "msfconsole", pero, antes debe verificarse la conectividad de la base de datos con el siguiente comando:

```
$ sudo db_status
```

Y luego,

```
exit
```

Ahora que se inició satisfactoriamente la base de datos. Ejecute la siguiente prueba, usando la línea de comandos. En Kali, puede simplemente ejecutar un comando simple:

```
$ sudo msfconsole
```

Dado que el marco Metasploit es parte del sistema operativo Kali Linux, se actualiza a través del paquete apropiado APT.

```
$ sudo apt update
$ sudo apt install metasploit-framework
```

1.6.3 DVL – DVWA

Para probar las herramientas anteriores, es necesario definir el sistema de destino, que es el sistema sobre el que se realizarán las pruebas. Una de las malas costumbres de los recién llegados a este campo es dar los primeros pasos y experimentar en sistemas públicos de Internet, en un entorno real.

Esto puede generar problemas legales y no es la forma correcta (o ética) de hacerlo. Para aprender a usar estas herramientas, debe utilizar un entorno de prueba, es decir, un escenario de investigación donde puede tomar medidas sin riesgo de afectar el entorno de producción. Hay dos grandes herramientas para esto: *Damn Vulnerable Linux* (DVL) y *Damn Vulnerable Web Application* (DVWA) para Windows.

Damn Vulnerable Linux (DVL) es todo lo que una buena distribución de Linux no tiene. Sus desarrolladores pasaron horas llenándolo con software roto, mal configurado, obsoleto y frágil, dejándolo vulnerable.

DVL no está diseñado para ejecutarse en su escritorio, es una herramienta educativa para estudiantes de seguridad. DVL es un CD en vivo disponible en tamaño ISO de 150 MB. Se basa en la popular distribución de Linux Dam Small Linux (DSL), no solo por su tamaño mínimo, sino también porque DSL usa un kernel 2.4, lo que facilita la introducción de vulnerabilidades que pueden no funcionar con 2.6. esencia. Contiene versiones más antiguas y frágiles de Apache y MyS.

Figura 1.53. Imagen referencial – DVL

Aunque el primero está descatalogado, sigue disponible online para primeros pasos y primeras pruebas. Es un sistema operativo y aplicación web que tiene todo tipo de vulnerabilidades, por lo que las personas que lo utilizan pueden intentar explotarlas y probarlas.

ⓘ NOTA

Para descargar la imagen .ISO de DVL, ir al sitio vulhub, para ser utilizada en máquinas virtuales (recomendado).

https://www.vulnhub.com/entry/damn-vulnerable-linux-dvl-15-infectious-disease,1/

El objetivo de DVWA es ejercitar algunas de las vulnerabilidades más comunes de la web, con diversos grados de dificultad, con una interfaz simple y directa. Tenga en cuenta que existen vulnerabilidades documentadas y no documentadas en este software. es intencional. Le recomendamos que intente detectar tantos problemas como sea posible.

Este paquete contiene una aplicación web PHP/MySQL muy débil. Su objetivo principal es ayudar a los profesionales de la seguridad a probar sus habilidades y herramientas en un entorno legal, ayudar a los desarrolladores web a comprender mejor los procesos de protección de las aplicaciones web y ayudar a los estudiantes de magisterio y educadores a aprender sobre la seguridad de las aplicaciones web en un aula controlada. ambiente de la habitación.

Tampoco la idea es tardar mucho en la instalación y configuración de herramientas, hay muchas formas, sin embargo, recomiendo en este caso, descargar e instalar XAMPP si aún no tiene una configuración de servidor web, es la forma más fácil de instalar DVWA sin tantos pasos y a la vez tan complejos.

XAMPP es una distribución de Apache fácil de instalar para Linux, Solaris, Windows y Mac OS X. Este paquete incluye servidor web Apache, MySQL, PHP, Perl, servidor FTP y phpMyAdmin. XAMPP se puede descargar desde: *https://www.apachefriends.org/*

ⓘ ADVERTENCIA

No lo cargue en el directorio .html público de su proveedor de alojamiento o en servidores que tengan acceso a Internet, ya que usted será pirateado y, podría también enfrentar cargos penales por esta acción.

Figura 1.54. Imagen referencial – Configuración DVWA

NOTA

Asegúrese de que exista su archivo config/config.inc.php. Simplemente config.inc.php.dist no será suficiente y deberá modificarlo para adaptarlo a su entorno y cambiarle el nombre a config.inc.php.

Simplemente descomprima el archivo "dvwa.zip", coloque los archivos descomprimidos en la carpeta html pública y luego apunte el navegador a:

```
http://127.0.0.1/dvwa/setup.php
```

NOTA

Para más información sobre instalaciones en otros sistemas operativos, consultar el repositorio GitHub del desarrollador: *https://github.com/digininja/DVWA*

También es posible "construir" su propio sistema de prueba: simplemente instale cualquier sistema operativo (desactive las actualizaciones o instale versiones anteriores) y comience a instalar servicios en él en versiones anteriores. De esta manera tendrás tu sistema vulnerable para probar. Este entorno es el entorno adecuado para que dé sus primeros pasos en las pruebas de penetración.

Los atacantes no solo usan herramientas, sino que piensan en cómo atacar. Al realizar el *pentesting*, es imperativo que no perdamos de vista nuestra herramienta principal: La paciencia. No importa qué herramienta de software usemos, pensar constantemente como un atacante es clave, para un probador de penetración exitoso.

1.7 ACTUALIZAR KALI LINUX

1.7.1 ¿Cómo actualizar Kali Linux a la versión 2022.4?

Para realizar una actualización, primeo iniciar la terminal en Kali y validar la versión actual:

```
┌──(root@kali)-[~]
└─$ echo "deb http://http.kali.org/kali kali-rolling main non-free contrib"
| sudo tee /etc/apt/sources.list
```

Luego actualizar

```
┌──(root@kali)-[~]
└─$ sudo apt update && sudo apt -y full-upgrade
```

Luego

```
┌──(root@kali)-[~]
└─$ cp -vrbi /etc/skel/. ~
```

Finalmente

```
┌──(root@kali)-[~]
└─$ [ -f /var/run/reboot-required ] && sudo reboot -f
```

Podemos luego hacer una comprobación rápida de la versión instalada

```
┌──(root@kali)-[~]
└─$ grep VERSION /etc/os-release
VERSION="2022.4"
VERSION_ID="2022.4"
VERSION_CODENAME="kali-rolling"
```

```
┌──(root@kali)-[~]
└─$ uname -v
#1 SMP PREEMPT Debian 6.0.7-1kali1 (2022-11-07)
┌──(root㉿kali)-[~]
└─$ uname -r
6.0.0-kali3-amd64
```

1.8 COMANDOS AVANZADOS

Los comandos son los mismos que en cualquier sistema UNIX. De forma predeterminada, Kali Linux siempre usa "*bash*" (también conocido como "*Bourne-Again SHell*") como *shell* predeterminado, al abrir una terminal o consola. ¡Cualquier usuario experimentado de Kali estará muy familiarizado con el mensaje kali @kali: ~$ (o root@kali: ~# para usuarios avanzados!/).

Aquí hay una lista de todos los comandos UNIX/Linux más utilizados en Kali. Se presentan en orden alfabético para facilitar su estudio.

Comando	**Descripción**
A	
apropos	Sirve para buscar entre las páginas del manual y las descripciones
apt-get	Buscar e instalar paquetes de software (Debian)
aptitud	Buscar e instalar paquetes de software (Debian)
aspell	Corrector ortográfico
awk	Buscar y reemplazar texto
B	
basename	Listar directorio y el sufijo de nombres de archivo
bash	GNU Bourne-Again Shell
bc	Precisión arbitraria idioma calculadora
bg	Enviar a fondo
break	Salida de un bucle
builtin	Ejecutar una orden interna del shell
bzip2	Comprimir o descomprimir archivos
C	
cal	Mostrar un calendario
case	Ejecutar un comando condicionalmente
cat	Concatenar e imprimir (display) el contenido de los archivos
cd	Cambio de directorio

cfdisk	Administra de la tabla de particiones para Linux
chgrp	Cambia la propiedad grupo
chmod	Cambiar los permisos de acceso
chown	Cambia el propietario del archivo y el grupo
chroot	Ejecutar un comando con un directorio raíz diferente
chkconfig	Los servicios del sistema (nivel de ejecución)
cksum	Imprimir CRC checksum y bytes recuentos
clear	Borrar la pantalla
cmp	Compara dos archivos
comm	Comparación de dos archivos ordenadas por líneas
command	Ejecutar un comando - haciendo caso omiso de las funciones de shell
continue	Reanudar la siguiente iteración de un bucle
cp	Copiar archivos
cron	Ejecuta comandos programados
crontab	Programar un comando para ejecutar en un momento posterior
csplit	Dividir un archivo en trozos de contexto determinado
cut	Dividir un archivo en varias partes
D	
date	Visualizar o cambiar la hora y fecha
dc	Calculadora de Escritorio
dd	Convertir y copiar un archivo, escribir cabeceras de disco, los registros de arranque
ddrescue	Herramienta de recuperación de datos
declare	Declarar variables y darles atributos
df	Muestra el espacio libre en disco
diff	Muestra las diferencias entre dos archivos
diff3	Muestra diferencias entre los tres archivos
dig	Búsqueda de DNS
dir	Lista el resumen del contenido del directorio
dircolors	Configuración de color
dirname	Convertir una ruta completa a sólo una ruta
dirs	Mostrar la lista de directorios recordadas
dmesg	Imprime mensajes del Kernel y de los controladores
du	Estimar el uso del espacio de archivos
E	
echo	Mostrar Mensaje en la pantalla
egrep	Búsqueda de archivos (s) para las líneas que coincidan con una expresión extendida

eject	Expulsar medios extraíbles
enable	Activar y desactivar los comandos de shell
env	Las variables de entorno
ethtool	Configuración de la tarjeta Ethernet
eval	Evaluar varios comandos / argumentos
exec	Ejecuta un comando
exit	Salir de la shell
expect	Automatizar aplicaciones arbitrarias accedidos a través de un terminal
expand	Convierte pestañas a espacios
export	Establecer una variable de entorno
expr	Evaluar expresiones
F	
false	No hacer nada
fdformat	Formato de Bajo nivel de un disquete
fdisk	Administrar la tabla Partición para Linux
fg	Enviar trabajo a primer plano
fgrep	Búsqueda de archivos para las que líneas coincidan con una cadena fija
file	Determinar tipo de archivo
find	Búsqueda de archivos que cumplen unos criterios deseados
fmt	Cambiar el formato de texto de párrafo
fold	Ajustar texto para adaptarse a un ancho especificado
for	Ampliar las palabras y ejecutar comandos
format	Formatear discos
free	Uso de la memoria
fsck	Comprobación y reparación de archivos del sistema
ftp	Protocolo de trasferencia de archivos
function	Definir macros de función
fuser	Identificar/eliminar el proceso que está accediendo a un archivo
G	
gawk	Buscar y reemplazar texto dentro del archivo
getopts	Analizar parámetros posicionales
grep	Búsqueda de archivos que coincidan con las líneas de un patrón dado
groupadd	Añadir un grupo de seguridad de usuario
groupdel	Eliminar un grupo
groupmod	Modificar un grupo
groups	Imprimir nombres de grupo

gzip	Comprimir o descomprimir archivo con el nombre del archivo
H	
hash	Recuerda la ruta completa de un argumento de nombre ,
head	Salida de la primera parte del archivo
help	Muestra la ayuda para un comando
history	Historial de comandos
hostname	Imprimir el nombre del sistema
I	
iconv	Convertir un conjunto de caracteres de un archivo
id	Imprimir identificadores de usuario y de grupo
if	Mostrar condicionalmente un comando
ifconfig	Configurar una interfaz de red
ifdown	Detener una interfaz de red
ifup	Iniciar una interfaz de red
import	Captura de una pantalla de un servidor X y guardar la imagen en un archivo
install	Copia de archivos y establecer atributos
J	
jobs	Enumerar los trabajos activos
join	Une líneas en un campo común
K	
kill	Detener un proceso que se ejecuta
killall	Matar procesos por nombre
L	
less	Muestra la salida de la pantalla de una sola vez
let	Realizar operaciones aritméticas sobre variables de shell
ln	Crea un enlace simbólico a un archivo
local	Crear las variables
locate	Encontrar los archivos
logname	Muestra el nombre sesión actual
logout	Salir de un shell
look	Mostrar líneas que comienzan con una cadena dada
lpc	Programa de control de la impresora
lpr	Línea de impresión
lprint	Imprimir un archivo
lprintd	Abortar un trabajo de impresión

lprintq	Escribir la cola de impresión
lprm	Eliminar trabajos de la cola de impresión
ls	Lista información sobre archivos
lsof	Lista de archivos abiertos
M	
make	Vuelve a compilar un grupo de programas
man	Manual de Ayuda
mkdir	Crear nueva carpeta
mkfifo	Crear FIFO
mkisofs	Crear un Sistema de archivos híbridos ISO9660/JOLIET/HFS
mknod	Hacer de caracteres o bloques archivos especiales
more	La salida de visualización de una pantalla a la vez
mount	Montar un sistema de archivos
mtools	Manipular archivos de MS-DOS
mtr	Diagnóstico de la red (traceroute / ping)
mv	Mover o cambiar el nombre de archivos o directorios
mmv	Mover y renombrar (archivos)
N	
netstat	Información de Redes
nice	Establecer la prioridad de un comando o tarea
nl	Número de líneas escritas en un archivo
nohup	Ejecutar un comando inmune a bloqueos
notify-send	Enviar notificaciones de escritorio
nslookup	Consultas a los servidores de nombres de dominio de forma interactiva
O	
open	Abrir un archivo en su aplicación por defecto
op	Acceso del operador
P	
passwd	Modificar una contraseña de usuario
paste	Fusionar líneas de archivos
pathchk	Comprueba la portabilidad nombre del archivo
ping	Prueba de una conexión de red
pkill	Detener los procesos se están ejecutando
popd	Restaura el valor anterior del directorio actual
pr	Preparar archivos para impresión

printcap	Base de datos de la capacidad de la impresora
printenv	Variables de entorno de impresión
printf	Formato y datos de impresión
ps	Estado de Proceso
pushd	Guardar y luego cambie el directorio actual
pwd	Imprimir directorio de trabajo
Q	
quota	Visualizar el uso del disco y los límites
quotacheck	Escanear un sistema de archivos para el uso del disco
quotactl	Cuotas conjunto de discos
R	
ram	Memoria ram del dispositivo
rcp	Copiar archivos entre dos máquinas
read	Leer una línea de la entrada estándar
readarray	Leer de la entrada estándar en una variable de matriz
readonly	Marcar variables y funciones como solo de lectura
reboot	Reiniciar el sistema
rename	Cambiar el nombre de archivos
renice	Modificar la prioridad de los procesos en ejecución
remsync	Sincronizar archivos remotos vía e-mail
return	Salir de una función de shell
rev	Líneas inversas de un archivo
rm	Eliminar archivos
rmdir	Eliminar carpetas
rsync	Copia de archivos remotos (Sincronizar árboles de archivos)
S	
screen	Terminal de múltiple, ejecuta shell remota mediante SSH
scp	Copia de seguridad (copia de archivos remoto)
sdiff	Combinar dos archivos de forma interactiva
sed	Editor sencillo
select	Aceptar la entrada de teclado
seq	Imprimir secuencias numéricas
set	Manipular las variables y funciones de shell
sftp	Programa de transferencia de archivos seguro
shift	Shift parámetros posicionales

shopt	Opciones de Shell
shutdown	Apagar o reiniciar Linux
sleep	Retraso por un tiempo determinado
slocate	Encuentra archivos
sort	Ordenar archivos de texto
source	Ejecutar comandos desde un archivo
split	Dividir un archivo en fragmentos de tamaño fijo
ssh	Secure Shell client (programa de acceso remoto)
strace	Llamadas al sistema de seguimiento y señales
su	La identidad del usuario sustituto
sudo	Ejecutar un comando como otro usuario
sum	Imprime una suma de comprobación de un archivo
suspend	Suspender la ejecución de la Shell
symlink	Hacer un nuevo nombre para un archivo
sync	Sincronizar datos en el disco con la memoria
T	
tail	Salida de la última parte del archivo
tar	Archivador en cinta
tee	Redirigir la salida a varios archivos
test	Evaluar una expresión condicional
time	Medir Programa de tiempo de ejecución
times	Tiempos de usuario y del sistema
touch	Marcas de hora de modificación del archivo
top	Lista los proceso que se están ejecutando en el sistema
traceroute	Trace Route del Host
trap	Ejecutar un comando cuando se establece una señal (bourne)
tr	Traducir y/o eliminar caracteres
true	No hacer nada, con éxito
tsort	Clasificación topológica
tty	Imprimir nombre de archivo de la terminal en la entrada estándar
type	Describe un comando
U	
ulimit	Límites de recursos de usuario
umask	Archivo Usuarios máscara de creación
umount	Desmontar un dispositivo
unalias	Quitar un alias

uname	Imprimir la información del sistema
unexpand	Convertir espacios para pestañas
uniq	Permite remover o mostrar las líneas repetidas de un archivo
units	Convertir unidades de una escala a otra
unset	Quitar nombres de variables o funciones
unshar	Secuencias de comandos shell de desempaquetado de archivos
until	Ejecutar comandos (hasta error)
uptime	Mostrar el tiempo de actividad
useradd	Crear nueva cuenta de usuario
usermod	Modificar cuenta de usuario
users	Lista de usuarios logueado
uuencode	Codificar un archivo binario
uudecode	Decodificar un archivo creado por uuencode
V	
v	Lista el contenido del directorio más detallados (`ls -l -b ‘)
vdir	Lista más detallada del contenido del directorio (`ls -l -b ‘)
vi	Editor de texto
vmstat	Informe de estadísticas de memoria virtual
W	
wait	Esperar a que un proceso se complete
watch	Ejecutar / visualizar un programa periódicamente
wc	Imprimir byte, palabra y los recuentos de línea
whereis	Busca ruta del usuario, páginas del manual y archivos de código fuente de un programa
which	Busca la ruta del usuario para un archivo de programa
while	Ejecutar comandos
who	Imprimir todos los nombres de usuario actualmente logueados
whoami	Imprimir el ID de usuario actual y el nombre
wget	Recuperar páginas web o archivos a través de HTTP, HTTPS o FT
write	Enviar un mensaje a otro usuario
X	
xargs	Ejecutar utilidad, pasando lista de argumentos construidos
xdg-open	Abrir un archivo o URL en aplicación preferida del usuario
Y	
Yes	Imprimir una cadena hasta que se interrumpa

EJEMPLOS PRÁCTICOS

- **Escribir un mensaje con una salida estándar**

  echo [string]

```
echo ``Hola mundo''
```

- **Ver información general sobre usuario de la red**

  finger [usuario]

```
finger root@maquina.com
```

- **Terminar un proceso**

  kill [-señal] PID

```
kill 1234
```

- **Mostrar información de los usuarios conectados al sistema**

  who / rwho

```
who
```

- **Encontrar la diferencias entre registros**

  diff [-e] archivo1 archivo2

```
diff contrato-vigente.c nuevo-contrato.c
```

- **Buscar patrones en archivos**

  grep [-cilnv] expr archivos

```
grep root /etc/passwd
```

- **Crear directorios**

  mkdir [dir]

```
mkdir temp
```

- **Mover un archivo(s) a un directorio**

  mv [archivo1 ...archivoN] dir

```
mv a.out prog1
```

- **Cambiar los permisos de un archivo**

  chmod [permisos] [archivo]

```
chmod +x mibackup
```

- **Encontrar archivos**

  find [dir test] [acción]

```
find . -name ``.sh'' – print
```

- **Mostrar el final de un archivo**

  tail [-count] [archivo]

```
tail archivo1.txt
```

- **Programar la ejecución de un comando**

  at [-lr] hora [fecha]

```
at 6pm Friday script.py
```

- **Copiar un directorio en background**

  cp [-r] [ruta] [&]

```
cp -r /usr/src/linux /tmp &
#
[Done] cp -r /usr/src/linux /tmp
#
```

- **Definir una variable de entorno DISPLAY** (usado para acceder a un servidor X-Windows).

  export VARIABLE=Valor

```
export DISPLAY=10.0.0.0:0.0
```

- **"Montar" un determinado sistema de archivos de un dispositivo**

  mount -t [sistema_archivos dispositivo directorio] [-o opciones]

```
mount -t iso9660 /dev/cdrom /mnt/cdrom -o ro
```

- **"Desmontar" un determinado sistema de archivos de un dispositivo**

  umount [directorio]

```
umount /mnt/cdrom
```

Comandos útiles para configurar y administrar la red en un sistema GNU Linux:

- **Ver información de las interfaces de red disponibles**

  ifconfig [opción]

```
Ifconfig -a
```

- **Asignar una dirección IP**

  Ifconfig [interface] [dirección IP] [subnet]

```
ifconfig eth0 192.168.0.2 netmask 255.255.255.0
```

- **Habilitar una interfaz de red**

  ifup [interface]

```
ifup eth0
```

- **Deshabilitar una interfaz de red**

  ifdown [interface]

```
ifdown eth0
```

- **Acceder al root del equipo de destino**

  nslookup [usuario]

```
nslookup root
```

- **Definir el nombre del dominio**

  nslookup domain=NOMBRE

```
nslookup domain=MI_COMPAÑIA
```

- **Añadir una ruta**

  route add -net [segment de red] gw [IP del gateway]

```
route add -net 10.10.10.0/24 gw 192.168.0.1
```

- **Borrar una ruta**

  route del -net [segment de red] gw [IP del gateway]

```
route del -net 10.10.10.0/24 gw 192.168.0.1
```

- **Agregar el Gateway o puerta de enlace por defecto**

  route add default gw [IP del gateway]

```
route add default gw 192.168.0.1
```

- **Ver la caché ARP actual**

```
arp -a
```

- **Definir una interfaz a analizar**

  arp -i [Interfaz]

```
arp -i eth0
```

- **Ver el nombre completo incluido servidor DNS**

```
hostname -f
```

- **Ver la dirección IP del nodo**

```
hostname -i
```

- **Desplegar el nombre FQDN**

```
hostname –fqdn
```

- **Ver las conexiones activas**

```
netstat -a
```

- **Desplegar puertos de escucha**

```
netstat -l
```

- **Desplegar la tabla de ruteo:**

```
netstat -r
```

- **Ver el puerto en uso por un programa**

  netstat -ap | grep [Programa]

```
netstat -ap | grep ssh
```