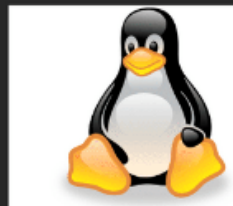
Machine Translated by Google

Kali Linux Tutorial

Cameron Wyatt PH.D

LUNES



Linux

MARTES

MIÉRCOLES

Ciberseguridad

JUEVES

Hacking

VIERNES

Pentesting

SÁBADO

Python

LIBROS DE INFORMÁTICA

EN APRECKING

LIBROS POR SEMANA

HTTPS://T.ME/LIBROSDEHACKING

APRECKING

Machine Translated by Google

Tabla de contenido

Machine Translated by Google

Introducción

La mayoría de las veces, los sistemas operativos específicos quedan vinculados a ciertas tareas. Cualquier cosa relacionada con gráficos o creación de contenido trae macOS en nuestro mente. Del mismo modo, cualquier instancia de piratería o simplemente juguetear en general con utilidades de red también se asigna a un sistema operativo en particular y que es KaliLinux.

Kali Linux es una distribución de seguridad de Linux derivada de Debian y diseñado específicamente para informática forense y penetración avanzada pruebas. Fue desarrollado a través de la reescritura de BackTrack por Mati Aharoni y Devon Kearns de Seguridad Ofensiva. Kali Linux contiene varios cientos de herramientas que están bien diseñadas para diversas seguridad de la información tareas, tales como pruebas de penetración, investigación de seguridad, informática forense y Ingeniería inversa. BackTrack era su seguridad de la información anterior Sistema operativo. La primera iteración de Kali Linux fue Kali 1.0.0 fue presentado en marzo de 2013. Offensive Security actualmente financia y apoya Kalin Linux. Si visitara el sitio web de Kali hoy (www.kali.org), vería una pancarta grande que decía: "Nuestra prueba de penetración más avanzada Distribution, Ever." Una declaración muy audaz que, irónicamente, aún no se ha refutado Kali Linux tiene más de 600 pruebas de penetración preinstaladas

Machine Translated by Google

Aplicaciones por descubrir. Cada programa con su flexibilidad y uso únicos.

caso. Kali Linux hace un excelente trabajo separando estas utilidades útiles en el

siguientes categorías:

Recopilación de información

Análisis de vulnerabilidad

Ataques inalámbricos

Aplicaciones web

Herramientas de explotación

Pruebas de estrés

Herramientas forenses

Rastreo y suplantación de identidad

Ataques de contraseña

Mantenimiento del acceso

Ingeniería inversa

Herramientas de informes

Hackeo de hardware

Machine Translated by Google

¿Quién desarrolló Kali Linux? (Desarrollo de Kali Linux)

Mati Aharoni y Deavon Kearns son los principales desarrolladores de Kali Linux. Eso fue una reescritura de Backtrack Linux, que fue otra prueba de penetración Distribución Linux centrada. El desarrollo de Kali se establece de acuerdo con el Estándares de Debian ya que importa la mayoría de su código de Debian repositorios El desarrollo comenzó a principios de marzo de 2012, entre un pequeño grupo de desarrolladores. Solo a unos pocos desarrolladores seleccionados se les permitió cometer paquetes, eso también en un entorno protegido. Salió Kali Linux de desarrollo con su primer lanzamiento en 2013. Desde entonces, Kali Linux ha sido a través de una serie de actualizaciones importantes. El desarrollo de estas actualizaciones es manejado por Seguridad Ofensiva.

Machine Translated by Google

¿Quién usa Kali Linux y por qué?

Kali Linux es realmente un sistema operativo único, ya que es una de las pocas plataformas utilizado abiertamente tanto por los buenos como por los malos. Administradores de seguridad, y Ambos Black Hat Hackers usan este sistema operativo ampliamente. Uno para detectar y prevenir brechas de seguridad, y el otro para identificar y posiblemente explotar brechas de seguridad. El número de herramientas configuradas y preinstaladas en el sistema operativo, haga de Kali Linux la navaja suiza en cualquier seguridad caja de herramientas profesionales.

Machine Translated by Google

Kali Linux y su papel en la ciberseguridad

Una de las mejores características de Kali Linux es el hecho de que tiene preinstalado herramientas que se pueden utilizar para una gran cantidad de tareas relacionadas con la ciberseguridad. Tareas. Hay más de 600 herramientas incluidas en Kali Linux para penetración propósitos de prueba y ciberseguridad, y la distribución de Kali se actualiza continuamente y mejorado por Offensive Security.

Machine Translated by Google

¿Por qué los profesionales de la ciberseguridad prefieren Kali Linux?

Una de las principales razones por las que los profesionales cibernéticos usan y a menudo prefieren Kali Linux es el hecho de que todo el código fuente original es de código abierto, lo que significa que el sistema se puede modificar a gusto del profesional de la ciberseguridad eso es usarlo. Lo cual no se hace necesariamente a menudo, proporciona la opción de personalizar Kali para tareas específicas de ciberseguridad. Kali Linux también viene con soporte multi idioma. Curiosamente, hasta 2019 Kali Linux había sido diseñado para ser utilizado para el acceso de usuario raíz único, lo que significa que el el usuario tiene plenos derechos y acceso a todo. Esto fue cambiado recientemente para acomodar a los usuarios que usaban Kali Linux con más frecuencia que solo por fines de ciberseguridad.

Machine Translated by Google

Esos fueron solo algunos ejemplos de las aplicaciones populares que vienen antes instalado en Kali Linux. Si bien es cierto que todas las aplicaciones de Kali Linux son gratuitos y se pueden descargar en otros sistemas operativos, Kali Linux hace que sea mucho más fácil para el usuario al hacer todo el trabajo por usted y compilándolos en una distribución de sistema operativo.

¿Puedes descargar Kali como tu sistema operativo principal?

Si bien puede ser, y a veces se hace, usar Kali Linux como predeterminado El sistema operativo diario no es ideal ni recomendado por Offensive Seguridad, debido al enfoque de seguridad del sistema operativo y al hecho de que hay otros Versiones de Linux que se consideran más estables. La mayoría de las instalaciones de Kali Linux existe como un disco en vivo de arranque o como una máquina virtual alojada por otro sistema operativo.

Machine Translated by Google

Profesionales que usan Kali Linux

Administradores de seguridad: los administradores de seguridad son responsables de salvaguardar la información y los datos de su institución. Usan Kali Linux para revise su(s) entorno(s) y asegúrese de que no haya vulnerabilidades.

Administradores de red: los administradores de red son responsables de mantenimiento de una red eficiente y segura. Usan Kali Linux para auditar su red Por ejemplo, Kali Linux tiene la capacidad de detectar accesos no autorizados. puntos.

Network Architects – Network Architects, son los encargados de diseñar entornos de red seguros. Utilizan Kali Linux para auditar su inicial diseños y asegurarse de que no se haya pasado por alto ni configurado mal nada.

Pen Testers : Pen Testers, utilizan Kali Linux para auditar entornos y realizar reconocimientos en entornos corporativos que han sido contratado para revisar.

CISO: CISO o directores de seguridad de la información, use Kali Linux para auditar internamente su entorno y descubrir si hay nuevas aplicaciones o Se han puesto en marcha configuraciones de colorete.

Machine Translated by Google

Ingenieros forenses : Kali Linux posee un "Modo forense", que permite un Ingeniero forense para realizar descubrimiento y recuperación de datos en algunos casos.

Hackers de sombrero blanco: los hackers de sombrero blanco, similares a los Pen Testers, usan Kali Linux para auditar y descubrir vulnerabilidades que pueden estar presentes en un ambiente.

Black Hat Hackers : Black Hat Hackers, utilice Kali Linux para descubrir y explotar vulnerabilidades. Kali Linux también tiene numerosos ingenieros sociales aplicaciones, que pueden ser utilizadas por un Black Hat Hacker para comprometer un organización o individuo.

Grey Hat Hackers – Grey Hat Hackers, se encuentran entre White Hat y Black Hat Hackers de sombreros. Utilizarán Kali Linux de la misma manera que los dos listados arriba.

Entusiasta de la computadora : Entusiasta de la computadora es un término bastante genérico, pero cualquier persona interesada en aprender más sobre redes o computadoras, en en general, puede usar Kali Linux para aprender más sobre tecnología de la información, redes y vulnerabilidades comunes

Machine Translated by Google

¿Por qué los hackers usan Kali Linux?

Anteriormente conocido como Backtrack, Kali Linux se anuncia a sí mismo como un sucesor pulido con herramientas más centradas en las pruebas, a diferencia de Backtrack, que tenía múltiples herramientas que servirían para el mismo propósito, a su vez, haciéndolo repleto de utilidades innecesarias. Esto hace que el hacking ético use Kali Linux una tarea simplificada.

Machine Translated by Google

¿Kali Linux es ilegal?

Kali Linux no es ilegal por sí mismo. Después de todo, es solo un sistema operativo. sin embargo es un herramienta para hackear también y cuando alguien la usa especialmente para hackear, es ilegal. Es legal si lo instala para propósitos útiles como aprender o enseñanza, o usarlo en la forma de fortalecer su software o su red como si fuera no es ilegal instalar ningún sistema operativo que tenga licencia y esté disponible para descargar

Machine Translated by Google

¿Por qué usar Kali Linux?

Hay una amplia gama de razones por las que uno debería usar Kali Linux. Dejar
Yo enumero algunos de ellos:

Tan gratis como puede ser: Kali Linux ha sido y siempre será de uso gratuito.

Más herramientas de las que podría pensar: Kali Linux viene con más de 600
diferentes herramientas relacionadas con pruebas de penetración y análisis de seguridad.

Código abierto : Kali, al ser miembro de la familia Linux, sigue ampliamente
apreciado modelo de código abierto. Su árbol de desarrollo es visible públicamente
en Git y todo el código está disponible para tus ajustes.

Soporte multilingüe : aunque las herramientas de penetración tienden a estar escritas en
Inglés, se ha asegurado que Kali incluye verdadero soporte multilingüe,
permitiendo que más usuarios operen en su idioma nativo y ubiquen las herramientas
necesitan para el trabajo.

Completamente personalizable : los desarrolladores de la seguridad ofensiva entienden
que no todo el mundo estará de acuerdo con su modelo de diseño, por lo que lo han hecho como
fácil posible para el usuario más aventurero personalizar Kali Linux para
su gusto, hasta el núcleo.

Requisitos del sistema para Kali Linux- (¿Cuánta RAM necesita Kali Linux?
¿necesitar?)

Machine Translated by Google

Instalar Kali es pan comido. Todo lo que tiene que asegurarse es que tiene el hardware compatible. Kali es compatible con i386, amd64 y ARM (ambos plataformas ARMEL y ARMHF). Los requisitos de hardware son mínimos ya que se enumeran a continuación, aunque un mejor hardware, naturalmente, proporcionará una mejor rendimiento.

Un mínimo de 20 GB de espacio en disco para la instalación de Kali Linux.

RAM para arquitecturas i386 y amd64, mínimo: 1GB, recomendado: 2GB o más.

Unidad de CD-DVD/soporte de arranque USB/VirtualBox

Machine Translated by Google

¿Debo usar Kali Linux?

¿Qué tiene de diferente Kali Linux?

Kali Linux está diseñado específicamente para cumplir con los requisitos de los profesionales pruebas de penetración y auditorías de seguridad. Para lograr esto, varios núcleos Se han implementado cambios en Kali Linux que reflejan estas necesidades:

Servicios de red deshabilitados de forma predeterminada: Kali Linux contiene ganchos systemd que desactivan los servicios de red de forma predeterminada. Estos ganchos nos permiten instalar varios servicios en Kali Linux, al tiempo que garantiza que nuestra distribución permanezca seguro por defecto, sin importar qué paquetes estén instalados. Servicios adicionales como Bluetooth también están en la lista negra de forma predeterminada.

Kernel personalizado de Linux: Kali Linux usa un kernel upstream, parcheado para inyección inalámbrica.

Un conjunto mínimo y confiable de repositorios: dados los objetivos y metas de Kali Linux, mantener la integridad del sistema como un todo es absolutamente clave. Con ese objetivo en mente, el conjunto de fuentes de software upstream que utiliza Kali se mantiene en un mínimo absoluto. Muchos nuevos usuarios de Kali se sienten tentados a agregar repositorios adicionales a su lista de fuentes, pero al hacerlo se ejecuta una muy grave riesgo de romper su instalación de Kali Linux.

Machine Translated by Google

¿Kali Linux es adecuado para usted?

Como desarrolladores de la distribución, puede esperar que le recomendemos que
todos deberían usar Kali Linux. El hecho es, sin embargo, que
Kali es una distribución de Linux específicamente orientada a profesionales
probadores de penetración y especialistas en seguridad, y dada su naturaleza única, es
NO es una distribución recomendada si no está familiarizado con Linux o si
buscando una distribución de escritorio de Linux de uso general para el desarrollo,
diseño web, juegos, etc.

Incluso para usuarios experimentados de Linux, Kali puede plantear algunos desafíos. Aunque
Kali es un proyecto de código abierto, no es un proyecto de código abierto, por razones
de seguridad El equipo de desarrollo es pequeño y confiable, paquetes en el
los repositorios están firmados tanto por el autor del compromiso individual como por el equipo, y —
lo que es más importante: el conjunto de repositorios ascendentes desde los cuales se actualizan y
Los paquetes se dibujan es muy pequeño. Agregar repositorios a su software
fuentes que no han sido probadas por el equipo de desarrollo de Kali Linux es una
buena manera de causar problemas en su sistema.

Si bien Kali Linux está diseñado para ser altamente personalizable, no espere
ser capaz de agregar paquetes y repositorios aleatorios no relacionados que están "fuera de
band" de las fuentes de software regulares de Kali y haz que funcione. En
particular, no hay absolutamente ningún soporte para el apt-add-

Machine Translated by Google

comando de repositorio, LaunchPad o PPA. Intentando instalar Steam en tu
El escritorio Kali Linux es un experimento que no terminará bien. Incluso conseguir un
paquete tan convencional como NodeJS en una instalación de Kali Linux puede tomar un
poco esfuerzo extra y retoques.

Si no está familiarizado con Linux en general, si no tiene al menos un conocimiento básico
nivel de competencia en la administración de un sistema, si está buscando un Linux
distribución para usar como una herramienta de aprendizaje para familiarizarse con Linux,
o si desea una distribución que pueda usar como escritorio de uso general
instalación, Kali Linux probablemente no sea lo que está buscando.

Además, el uso indebido de herramientas de seguridad y pruebas de penetración dentro de una red,
particularmente sin autorización específica, puede causar daños irreparables y
resultar en consecuencias significativas, personales y/o legales. "No entendiendo
lo que estabas haciendo" no va a funcionar como una excusa.

Sin embargo, si eres un probador de penetración profesional o estás estudiando
pruebas de penetración con el objetivo de convertirse en un profesional certificado, hay
no hay mejor kit de herramientas, a cualquier precio, que Kali Linux.

Machine Translated by Google

¿Cuál es la mejor manera de aprender Kali Linux?

Si está listo para comenzar a aprender el sistema operativo Kali Linux y cómo se puede utilizar para la ciberseguridad, siga los pasos a continuación.

1. Comience con la construcción de una máquina virtual Kali Linux

Hay muchas formas gratuitas de configurar un hipervisor y comenzar a trabajar con él. máquinas virtuales, incluida una implementación de Kali Linux. una maquina virtual entorno le permitirá configurar y desmontar uno, incluso varios instancias de Kali Linux y tome instantáneas en el camino.

Machine Translated by Google

2. Comience por instalar un hipervisor gratuito, como Oracle'sVirtualBox.

Una vez instalado, puede descargar e instalar en una máquina virtual Kali
ISO de Linux. Si no está familiarizado con Linux en general, es posible que desee
también instale otras distribuciones gratuitas de Linux y constrúyalas en su propia
máquinas virtuales, como Ubuntu o CentOS. Ver videos en YouTube si
te quedas atascado o necesitas alguna dirección.

3. Explora las herramientas cibernéticas en Kali Linux

Una vez que haya instalado Kali Linux en una VM, eche un vistazo a los diversos
herramientas integradas en el sistema operativo. Notarás que están ordenados
por categoria. Una buena manera de comenzar es elegir una herramienta a la vez y aprender
ellos uno por uno. Elija una herramienta dentro de una categoría de interés y
comience a trabajar con él, utilizando tutoriales en línea según sea necesario para trabajar a su manera
a través de las opciones de la herramienta. Hay muchos tutoriales en YouTube que pueden
ayudarlo a navegar a través de las numerosas herramientas y utilidades de Kali. Intentar
concéntrese en aprender una herramienta a la vez porque aprender una herramienta a menudo hará
aprender otra herramienta más fácil sobre la marcha. Mientras trabaja con estos
herramientas, no las utilice contra ningún sistema que no sea de su propiedad o que no tenga
autorización de acceso, ya que el uso de estas herramientas de esta manera es ilegal.

Intente usar estas herramientas contra sitios de piratería legales

Si bien es ilegal intentar piratear cualquier sitio en el que no esté

Machine Translated by Google

autorizado para atacar, afortunadamente hay varios sitios en línea que están configurados exactamente para este propósito, ya que le permiten intentar explotarlos legalmente. Haga una búsqueda en Internet para ver qué sitios están disponibles y se pueden usar con la herramienta que está probando y lea cualquier descargo de responsabilidad. no debería ser difícil encontrar un sitio web en el que esté legalmente autorizado para intentar un exploit gratis.

Machine Translated by Google

Característica clave de Kali Linux

1. Más de 600 herramientas de prueba de penetración preinstaladas

Kali Linux viene con más de 600 herramientas útiles como Wireshark,

Crunch, Nmap y Aircrack-ng.

2. Soporte multilingüe

Las herramientas de Kali Linux incluyen soporte multilingüe para permitir a sus usuarios operar en

su idioma nativo.

3. Desarrollado en un entorno seguro

Solo un número limitado de personas de confianza pueden interactuar con Kali Linux

repositorios de código.

4. Cumplimiento del estándar de jerarquía del sistema de archivos (FHS)

Kali Linux se adhiere a FHS para localizar bibliotecas, archivos de soporte, etc. con

facilitar.

5. Sin costo

Kali Linux es de uso gratuito y sus desarrolladores prometen que seguirá siéndolo.

Machine Translated by Google

¿Qué herramientas vienen con Kali Linux? (Lista de herramientas)

A continuación se muestra una lista de herramientas que vienen preinstaladas para la piratería ética con Kali linux Esta lista no es extensa ya que Kali tiene una gran cantidad de herramientas, todas de los cuales no se pueden enumerar y explicar en un libro.

Machine Translated by Google

1. Aircrack-ng- Ethical Hacking usando Kali Linux- Edureka. Aircrack-ng es

un conjunto de herramientas utilizadas para evaluar la seguridad de la red WiFi. Se enfoca en áreas clave de seguridad Wi-Fi:

Supervisión: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por herramientas de terceros

Ataque: ataques de repetición, desautenticación, puntos de acceso falsos y otros mediante inyección de paquetes

Pruebas: Comprobación de las tarjetas WiFi y las capacidades del controlador (captura e inyección)

Craqueo: WEP y WPA PSK (WPA 1 y 2)

Todas las herramientas son de línea de comandos, lo que permite secuencias de comandos pesadas. Muchas GUI han aprovechado esta característica. Funciona principalmente Linux pero también Windows, OS X, FreeBSD, OpenBSD, NetBSD y Solaris.

2. **Nmap**

logo nmap - Hacking Ético usando Kali Linux - Edureka

Network Mapper, también conocido comúnmente como Nmap, es un código abierto y gratuito utilidad para el descubrimiento de redes y la auditoría de seguridad. Nmap usa paquetes IP sin procesar de manera sigilosa para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y versión) que ofrecen esos hosts, qué sistemas operativos que están ejecutando, qué tipo de filtros de paquetes/cortafuegos están en

Machine Translated by Google

uso, y decenas de otras características.

Machine Translated by Google

Curso curricular

Curso de Certificación en Ciberseguridad

Muchos administradores de sistemas y redes también lo encuentran útil para tareas como:

inventario de red

administrar los programas de actualización del servicio

Supervisar el tiempo de actividad del host o del servicio.

3. THC HydraTHC hydra logo - piratería ética usando kali linux -

edureka

Cuando necesite descifrar por fuerza bruta un servicio de autenticación remota, Hydra es
a menudo la herramienta de elección. Puede realizar rápidos ataques de diccionario contra más
de 50 protocolos, incluidos telnet, FTP, HTTP, HTTPs, SMB, varios
bases de datos y mucho más. se puede usar para acceder a escáneres web, inalámbricos
redes, creadores de paquetes, etc.

4. Logotipo de Nessus nessus - Hacking ético usando Kali Linux - Edureka

Nessus es una herramienta de escaneo remoto que puede usar para verificar las computadoras en busca de
vulnerabilidades de seguridad. No bloquea activamente ninguna vulnerabilidad que
sus computadoras tienen, pero podrá olfatearlas ejecutando rápidamente
Más de 1200 verificaciones de vulnerabilidades y alertas de lanzamiento cuando hay parches de seguridad
hay que hacer.

Machine Translated by Google

5. WireShark logo de wireshark - piratería ética usando kali linux - eduerka

WireShark es un analizador de paquetes de código abierto que puede utilizar de forma gratuita.
Con él, puedes ver las actividades en una red desde un nivel microscópico.
junto con acceso a archivos pcap, informes personalizables, disparadores avanzados, alertas,
etc. Según se informa, es el analizador de protocolo de red más utilizado en el mundo.
para Linux.

Demostración de poder: Aircrack-ng y Crunch

Paso 1: verifique el nombre de su interfaz inalámbrica y colóquelo en el monitor
modo.

ifconfig wlo1 abajo

monitor de modo iwconfig wlo1

ifconfig wlo1 arriba

Paso 2: elimine cualquier proceso que pueda interferir con el proceso de escaneo. Siempre
mata al administrador de la red primero. Es posible que deba ejecutar el comando que se muestra
mas de una vez.

Paso 3: después de haber eliminado con éxito todos los procesos, ejecute el comando:
airodump-ng <nombre-interfaz>. Debe producir una lista de puntos de acceso como
mostrado a continuación:

Paso 4: elija el punto de acceso y ejecútelo junto con el indicador -w para escribir el

Machine Translated by Google

resultintoafil p. El archivo ur se llama captur e.

Machine Translated by Google

Paso 5: ejecutar el comando anterior debería mostrarle la dirección MAC de los dispositivos conectados a ese punto de acceso en 'estaciones'.

Paso 6: este es el paso más importante en la piratería ética con Kali Linux. Aquí transmitiremos una señal de desautenticación al punto de acceso que tenemos elegido para atacar. Esto desconecta los dispositivos conectados al punto de acceso. Dado que estos dispositivos probablemente tendrán la contraseña almacenada, intentarán reconexión automática. Esto iniciará un protocolo de enlace de 4 vías entre el dispositivo y el punto de acceso y será capturado en el escaneo que continúa desde el paso 4 (sí, eso el análisis aún se está ejecutando en segundo plano).

Paso 7: Ahora usaremos crunch junto con aircrack-ng. Crunch es una lista de palabras generador. Este proceso para descifrar contraseñas asume que sabes un poco sobre la contraseña, por ejemplo, la longitud, algunos caracteres específicos, etc. Cuanto más ya sabes, más rápido es el proceso. Aquí he intentado generar una lista de palabras. que comienzan con 'dulce', ya que sé que la contraseña contiene esa frase. El resultado se canaliza al comando aircrack que toma los archivos de captura y compara los valores clave.

Paso 8: Los resultados del escaneo deberían verse así dependiendo del parámetros que ha ingresado.

Paso 9: Cuando la contraseña coincide. Lo muestra en el paréntesis siguiente

Machine Translated by Google

'Llave encontrada'.

Machine Translated by Google

Otras herramientas populares de Kali Linux

Las herramientas de ciberseguridad preinstaladas son el factor principal en la popularidad de KaliLinux. Dediquemos unos minutos a repasar algunos de los más populares.
y útil como ejemplo de lo que Kali Linux puede hacer por nosotros como ciberseguridad profesionales

metasploit

Metasploit es una herramienta de prueba de penetración que hace que la piratería sea mucho más fácil para los cibernéticos. profesionales Toma procesos que solían ser manuales, como la información recopilar, obtener acceso y evadir la detección y automatizarlos.
Metasploit es extremadamente popular y muy utilizado por profesionales en el campo de seguridad de la información, y es una gran manera de probar exploits y vulnerabilidades.

Juan el Destripador

John the Ripper es una herramienta para descifrar contraseñas que se puede personalizar y combina Numerosos modos de craqueo para adaptarse a las necesidades individuales. La mejor parte es que puede ser se ejecuta contra varios formatos de contraseña cifrada, y puede realizar técnicas de descifrado de contraseñas, como diccionario y ataques de fuerza bruta.

Netcat

Netcat es una herramienta de red que se utiliza para leer y escribir datos a través de la red.

Machine Translated by Google

conexiones Netcat incluye una lista de funciones, desde escaneo de puertos hasta transferir archivos al puerto de escucha. Netcat puede crear casi cualquier tipo de conexión que necesitaría y es una herramienta preferida para escanear puertos.

Tiburón alambre

Wireshark es un analizador de paquetes de código abierto y se utiliza para ver y evaluar el tráfico en una red, lo que lo hace esencial para cualquier seguridad profesional o administrador de sistemas. Cuando se ejecuta y analiza en vivo, es un indicador en tiempo real de qué tráfico está pasando a través de la red, e incluso puede utilizarse para la solución de problemas.

Machine Translated by Google

Métodos de instalación de Kali Linux

Kali Linux se puede instalar usando los siguientes métodos:

Formas de ejecutar Kali Linux:

Directamente en una PC, computadora portátil: utilizando una imagen ISO de Kali, Kali Linux puede ser instalado directamente en una PC o computadora portátil. Este método es mejor si tiene un repuesto PC y están familiarizados con Kali Linux. Además, si planea o está haciendo algún acceso pruebas puntuales, instalar Kali Linux directamente en una computadora portátil habilitada para Wi-Fi es recomendado.

Virtualizado (VMware, Hyper-V, Oracle VirtualBox, Citrix) – Kali Linux es compatible con la mayoría de los hipervisores conocidos y puede incorporarse fácilmente a los más populares unos. Las imágenes preconfiguradas están disponibles para su descarga desde https://www.kali.org/, o se puede usar un ISO para instalar el sistema operativo en el hipervisor preferido manualmente.

Nube (Amazon AWS, Microsoft Azure): dada la popularidad de Kali Linux, tanto AWS como Azure proporcionan imágenes para Kali Linux.

Disco de arranque USB: utilizando la ISO de Kali Linux, se puede crear un disco de arranque para ejecutar Kali Linux en una máquina sin instalarlo realmente o para Fines forenses.

Machine Translated by Google

Windows 10 (aplicación): Kali Linux ahora puede ejecutarse de forma nativa en Windows 10, a través de la línea de comandos. No todas las funciones funcionan todavía, ya que todavía está en modo beta.

Mac (arranque dual o único): Kali Linux se puede instalar en Mac, como sistema operativo secundario o como el principal. Arranque de Parallels o Mac La funcionalidad se puede utilizar para configurar esta configuración.

Machine Translated by Google

Cómo instalar Kali Linux usando Virtual Box

Aquí hay un proceso paso a paso sobre cómo instalar Kali Linux usando Vitual Box y cómo usar Kali Linux:

El método más fácil y posiblemente el más utilizado es instalar Kali Linux y ejecutándolo desde VirtualBox de Oracle.

Este método le permite continuar usando su hardware existente mientras experimentando con Kali Linux enriquecido destacado en un entorno completamente aislado ambiente. Lo mejor de todo es que todo es gratis. Tanto Kali Linux como Oracle VirtualBox son de uso gratuito. Este tutorial de Kali Linux asume que ya has instaló Oracle's VirtualBox en su sistema y ha habilitado 64 bits Virtualización a través de la Bios.

Paso 1) Vaya a https://www.kali.org/downloads/

Esto descargará una imagen OVA, que se puede importar a VirtualBox

Paso 2) Abra la aplicación Oracle VirtualBox y, desde Archivo, Menú seleccione Importar dispositivo

Menú Archivo -> Dispositivo de importación

Paso 3) En la siguiente pantalla "Aparato para importar" Busque la ubicación

Machine Translated by Google

del archivo OVA descargado y haga clic en Abrir

Paso 4) Una vez que haga clic en Abrir, volverá al "Dispositivo para

Importar" simplemente haga clic en Siguiente

Paso 5) La siguiente pantalla "Configuración del dispositivo" muestra un resumen de la

configuración del sistema, dejar la configuración predeterminada está bien. Como se muestra en el

captura de pantalla a continuación, tome nota de dónde se encuentra la máquina virtual y

luego haga clic en Importar.

Paso 6) VirtualBox ahora importará el dispositivo Kali Linux OVA. Esta

el proceso puede tardar entre 5 y 10 minutos en completarse.

Paso 7) Felicitaciones, Kali Linux se ha instalado con éxito en

VirtualBox. Ahora debería ver Kali Linux VM en VirtualBox

Consola. A continuación, veremos Kali Linux y algunos pasos iniciales para

llevar a cabo.

Paso 8) Haga clic en Kali Linux VM dentro del Tablero de VirtualBox y

haga clic en Inicio, esto iniciará el sistema operativo Kali Linux.

Paso 9) En la pantalla de inicio de sesión, ingrese "Root" como nombre de usuario y haga clic en Siguiente.

Paso 10) Como se mencionó anteriormente, ingrese "toor" como contraseña y haga clic en Iniciar sesión.

Ahora estará presente con Kali Linux GUI Desktop. Felicidades

Has iniciado sesión con éxito en Kali Linux.

Machine Translated by Google

Introducción a la interfaz gráfica de usuario de Kali Linux

Kali Desktop tiene algunas pestañas de las que inicialmente debe tomar nota y familiarizarse con. Pestaña Aplicaciones, Pestaña Lugares y Kali Linux Aunque.

Ficha Aplicaciones : proporciona una lista desplegable gráfica de todas las aplicaciones y herramientas preinstaladas en Kali Linux. Revisando el La pestaña Aplicaciones es una excelente manera de familiarizarse con las características enriquecidas Sistema operativo KaliLinux. Dos aplicaciones de las que hablaremos en este Kali Los tutoriales de Linux son Nmap y Metasploit. Las aplicaciones se colocan en diferentes categorías, lo que hace que la búsqueda de una aplicación sea mucho más fácil.

Acceso a aplicaciones

Paso 1) Haga clic en la pestaña Aplicaciones

Paso 2) Busque la categoría particular que le interesa explorar

Paso 3) Haga clic en la aplicación que desea iniciar.

Pestaña Lugares: similar a cualquier otro sistema operativo GUI, como Windows o Mac, el fácil acceso a sus Carpetas, Imágenes y Mis Documentos es un componente esencial. Places en Kali Linux proporciona esa accesibilidad que es vital para cualquier sistema operativo. Por defecto, el menú Lugares tiene lo siguiente

Machine Translated by Google

pestañas, Inicio, Escritorio, Documentos, Descargas, Música, Imágenes, Vídeos,

Computadora y navegar por la red.

Acceso a lugares

Paso 1) Haga clic en la pestaña Lugares

Paso 2) Seleccione la ubicación a la que desea acceder.

Kali Linux Dock: similar al Dock de Apple Mac o Microsoft Windows Task

Bar, el Kali Linux Dock proporciona acceso rápido a los favoritos/utilizados con frecuencia

aplicaciones Las aplicaciones se pueden agregar o eliminar fácilmente.

Para eliminar un elemento del Dock

Paso 1) Haga clic con el botón derecho en el elemento del Dock

Paso 2) Seleccione Eliminar de favoritos

Para agregar un elemento al muelle

Agregar un elemento al Dock es muy similar a eliminar un elemento del

Aunque

Paso 1) Haga clic en el botón Mostrar aplicaciones en la parte inferior del Dock

Paso 2) Haga clic derecho en la aplicación

Paso 3) Seleccione Agregar a favoritos

Una vez completado, el elemento se mostrará en el Dock.

Machine Translated by Google

Kali Linux tiene muchas otras características únicas, lo que hace que este sistema operativo
El sistema es la elección principal tanto de los ingenieros de seguridad como de los piratas informáticos.
Desafortunadamente, cubrirlos todos no es posible dentro de Kali Linux.
tutoriales de piratería; sin embargo, debe sentirse libre de explorar los diferentes
botones que aparecen en el escritorio.

¿Qué es Nmap?

Network Mapper, más conocido como Nmap para abreviar, es un programa gratuito y de código abierto
utilidad utilizada para el descubrimiento de redes y el escaneo de vulnerabilidades. Seguridad
los profesionales usan Nmap para descubrir dispositivos que se ejecutan en sus entornos.
Nmap también puede revelar los servicios y los puertos que cada host está sirviendo, exponiendo un
riesgo potencial de seguridad. En el nivel más básico, considere Nmap, haga ping en
esteroides Cuanto más avanzadas evolucionen sus habilidades técnicas, mayor será su utilidad
encontrarás en Nmap

Nmap ofrece la flexibilidad de monitorear un solo host o una gran red
que consta de cientos, si no miles, de dispositivos y subredes. los
flexibilidad que ofrece Nmap ha evolucionado a lo largo de los años, pero en esencia, es un puerto
herramienta de escaneo, que recopila información mediante el envío de paquetes sin procesar a un host
sistema. Nmap luego escucha las respuestas y determina si un puerto está abierto,
cerrado o filtrado.

El primer escaneo con el que debe estar familiarizado es el escaneo Nmap básico que escanea

Machine Translated by Google

los primeros 1000 puertos TCP. Si descubre un puerto escuchando, mostrará el puerto

como abierto, cerrado o filtrado. Filtrado, lo que significa que lo más probable es que haya un cortafuegos instalado

modificando el tráfico en ese puerto en particular. A continuación se muestra una lista de Nmap

comandos que se pueden utilizar para ejecutar el análisis predeterminado.

Machine Translated by Google

Selección de destino de Nmap

Escanear una sola IP

nmap 192.168.1.1

Escanear un host

nmap www.testnetwork.com

Escanea un rango de IPs

nmap 192.168.1.1-20

Escanear una subred

nmap 192.168.1.0/24

Escanear objetivos desde un archivo de texto

nmap -iL lista-de-direcciones-i.txt

Cómo realizar un escaneo básico de Nmap en Kali Linux

Para ejecutar un escaneo básico de Nmap en Kali Linux, siga los pasos a continuación. Con Nmap como se muestra arriba, tiene la capacidad de escanear una sola IP, un nombre DNS, un gama de direcciones IP, subredes e incluso escanear desde archivos de texto. Para esto ejemplo, escanearemos la dirección IP localhost.

Paso 1) Desde el menú Dock, haga clic en la segunda pestaña que es la Terminal

Machine Translated by Google

Paso 2) La ventana de Terminal debería abrirse, ingrese el comando ifconfig, esto
El comando devolverá la dirección IP local de su sistema Kali Linux. En esto
ejemplo, la dirección IP local es 10.0.2.15

Paso 3) Tome nota de la dirección IP local

Paso 4) En la misma ventana de terminal, ingrese nmap 10.0.2.15, esto escaneará el
primeros 1000 puertos en el localhost. Teniendo en cuenta que esta es la instalación base sin puertos
debería estar abierto.

Paso 5) Revisar los resultados

Por defecto, nmap solo escanea los primeros 1000 puertos. Si necesita escanear el
completar 65535 puertos, simplemente modificaría el comando anterior para
incluir -p-.

Nmap 10.0.2.15 -p

Exploración del sistema operativo Nmap

Otra característica básica pero útil de nmap es la capacidad de detectar el sistema operativo del
sistema anfitrión. Kali Linux por defecto es seguro, así que para este ejemplo, el host
El sistema, en el que está instalado VirtualBox de Oracle, se utilizará como un
ejemplo. El sistema host es una superficie de Windows 10. La IP del sistema host
la dirección es 10.28.2.26.

En la ventana Terminal ingrese el siguiente comando nmap:

Machine Translated by Google

nmap 10.28.2.26 – A

Revisar resultados

Agregar -A le dice a nmap que no solo realice un escaneo de puertos sino que también intente detectar El sistema operativo.

Nmap es una utilidad vital en cualquier caja de herramientas de Security Professional. Utilizar el comando nmap -h para explorar más opciones y comandos en Nmap.

Machine Translated by Google

¿Qué es Metasploit?

Metasploit Framework es un proyecto de código abierto que proporciona una
recurso para investigar vulnerabilidades y desarrollar código que permita
profesionales de la seguridad la capacidad de infiltrarse en su propia red e identificar
riesgos de seguridad y vulnerabilidades. Metasploit fue adquirido recientemente por Rapid
7 (https://www.metasploit.com). Sin embargo, la edición comunitaria de
Metasploit todavía está disponible en Kali Linux. Metasploit es, con mucho, el mundo
Utilidad de penetración más utilizada.

Es importante que tenga cuidado al usar Metasploit porque escanear un
red o entorno que no es suyo podría considerarse ilegal en algunos
instancias. En este tutorial de metasploit de Kali Linux, le mostraremos cómo comenzar
Metasploit y ejecute un escaneo básico en Kali Linux. Metasploit es considerado un
utilidad avanzada y requerirá algo de tiempo para convertirse en experto, pero una vez familiarizado
con la aplicación será un recurso invaluable.

Metasploit y Nmap

Dentro de Metasploit, podemos utilizar Nmap. En este caso, aprenderá
cómo escanear su subred VirtualBox local desde Metasploit usando Nmap
utilidad que acabamos de conocer.

Paso 1) En la pestaña Aplicaciones, desplácese hacia abajo hasta 08-Herramientas de explotación y
luego seleccione Metasploit

Machine Translated by Google

Paso 2) Se abrirá una caja de terminales, con MSF en el cuadro de diálogo, esto es Metasploit

Paso 3) Ingrese el siguiente comando

db_nmap -V -sV 10.0.2.15/24

(asegúrese de reemplazar 10.0.2.15 con su dirección IP local)

Aquí:

db_ significa base de datos

-V significa modo detallado

-sV significa detección de versión de servicio

Utilidad de explotación de Metasploit

Metasploit muy robusto con sus características y flexibilidad. Un uso común para Metasploit es la Explotación de Vulnerabilidades. A continuación vamos a pasar por el pasos para revisar algunos exploits e intentar explotar una máquina con Windows 7.

Paso 1) Suponiendo que Metasploit aún esté abierto, ingrese Hosts -R en la terminal ventana. Esto agrega los hosts descubiertos recientemente a la base de datos de Metasploit.

Paso 2) Ingrese "mostrar exploits", este comando proporcionará una completa mira todos los exploits disponibles para Metasploit.

Paso 3) Ahora, intente reducir la lista con este comando: nombre de búsqueda: Windows 7, este comando busca los exploits que incluyen específicamente

Machine Translated by Google

Windows 7, para el propósito de este ejemplo intentaremos explotar un Windows 7 Máquina. Dependiendo de su entorno, tendrá que cambiar el parámetros de búsqueda para cumplir con sus criterios. Por ejemplo, si tiene Mac o otra máquina Linux, tendrá que cambiar el parámetro de búsqueda a coincida con ese tipo de máquina.

Paso 4) Para los propósitos de este tutorial usaremos un Apple Itunes vulnerabilidad descubierta en la lista. Para utilizar el exploit, debemos ingresar al camino completo que es desplegado en los lista: utilizar explotar/windows/navegar/apple_itunes_playlist

Paso 5) Si el exploit tiene éxito, el símbolo del sistema cambiará a muestre el nombre del exploit seguido de > como se muestra en la siguiente captura de pantalla.

Paso 6) Ingrese mostrar opciones para revisar qué opciones están disponibles para el explotar. Cada exploit, por supuesto, tendrá diferentes opciones.

Machine Translated by Google

Reseña de Kali Linux: No es del agrado de todos

Breve: En esta revisión de Kali Linux, tratamos de responder algunas
preguntas: ¿qué es Kali Linux, cuáles son los usos de Kali Linux y debería
¿Los principiantes usan Kali Linux o no? Kali Linux ha ganado mucha popularidad
hace poco. Y hay una razón para eso. La piratería ha vuelto como lo mejor que se puede hacer
en la cultura popular y esto se puede atribuir significativamente a la serie de televisión Mr.
Robot. Kali es una de las pocas distribuciones de Linux enfocadas en piratería, y el Sr.
La popularidad de Robot obviamente ha ayudado a Kali Linux a atraer nuevos usuarios. los
El siguiente gráfico ilustra esto.

La popularidad de ali Linux aumenta con la serie de televisión Mr. Robot. Y con eso,
gente sin apenas conocimientos de Linux ni nada relacionado con la informática
security ahora están tratando de usar Kali como su principal distribución de Linux. pero Kali
Ciertamente, Linux no fue diseñado para propósitos generales. Mira el Kali
Herramientas de Linux y encontrará que muchas de ellas se relacionan con "piratería". Por supuesto,
Fácilmente podría escribir un artículo explicando por qué está mal usar Kali como primer
Distribución de Linux. De hecho, podrías encontrar grandes argumentos aquí y aquí para
disuadirlo de usar Kali a menos que realmente tenga necesidades específicas. Pero yo
quería hacer algo diferente. Así que instalé Kali Linux en VirtualBox y
Traté de ponerme en el lugar de un "nuevo usuario" que intenta algunas tareas básicas en su

Machine Translated by Google

Nuevo sistema Linux. ¿Encontraría algunos problemas o sería
¿simple? Quédate conmigo hasta el final de este artículo para leer mi
conclusiones.

Para citar el título de la página web oficial, Kali Linux es un "Prueba de Penetración y
Distribución de Linux de Hacking Ético". En pocas palabras, es una distribución de Linux.
repleto de herramientas relacionadas con la seguridad y dirigido a la red y la computadora
expertos en seguridad.

Una distribución de Linux no es más que un paquete que contiene el Linux
kernel, un conjunto de utilidades y aplicaciones principales y algunas configuraciones predeterminadas. Entonces
Kali Linux no ofrece algo único en el sentido de que la mayoría de las herramientas
proporciona podría instalarse en cualquier distribución de Linux.

La diferencia es que Kali viene preempaquetado con esas herramientas y el valor predeterminado
la configuración se eligió de acuerdo con los casos de uso previstos de esa distribución,
en lugar de, por ejemplo, adaptarse a las necesidades del usuario de escritorio típico. En otras palabras,
cualquiera que sea tu objetivo, no tienes que usar Kali. es solo un especial
distribución que facilita las tareas para las que está diseñado específicamente, mientras
en consecuencia, haciendo algunas otras tareas más difíciles.

Descargar Kali Linux y verificar la integridad de la imagen

Para descargar Kali Linux, fui a la página de descarga oficial y seguí
el primer enlace de descarga en esa página. Afortunadamente, mi computadora está equipada con un

Machine Translated by Google

CPU Intel de 64 bits, por lo que la imagen amd64 era la correcta para mi arquitectura.

Además, en la página de descarga, había un montón de hexadecimales

números. ¿Eso ya no se siente "hackish"? No, en serio, esos no son

allí para divertirse. Kali Linux está destinado a ser utilizado para tareas relacionadas con la seguridad. los

Lo último que desea es que las herramientas que utiliza se vean comprometidas de alguna manera. Entonces,

después de descargar la imagen de Kali, debe verificar la huella digital SHA-256

del archivo y compárelo con el proporcionado en la página de descarga. Tú

Puede leer este tutorial sobre cómo verificar las sumas de verificación en Linux. ahora puedo ser

confiado en instalar Kali Linux en mi VM desde esa imagen ISO.

Machine Translated by Google

Instalación y experiencia inicial de Kali Linux

Kali Linux está basado en Debian, el proceso de instalación es bastante
simple. Y esto está bien documentado en el sitio web de Kali. Para esto
prueba, me quedé lo más posible con las opciones predeterminadas. y solo unos pocos
Minutos más tarde, pude iniciar Kali Linux por primera vez y terminé
en esta pantalla:

Un usuario acostumbrado a los sistemas tipo Unix podría sorprenderse al saber que
“root” es el único usuario disponible después de una instalación predeterminada. pero eso es porque
muchas herramientas de prueba de penetración requieren permisos de superusuario.

Una vez más, esta es una opción específica de Kali dado su caso de uso previsto. Pero esto
no es la mejor opción para el uso diario de la computadora (navegar por Internet,
uso de aplicaciones ofimáticas, etc.). Y es posiblemente la peor elección si
tienes que compartir tu computadora con otra persona (más sobre eso más adelante).
Hablando de aplicaciones, las únicas instaladas en un Kali Linux predeterminado
están claramente orientados hacia la seguridad. Además de eso, hay un
un montón de herramientas de línea de comandos no visibles desde el menú, y algunas
utilidades como una calculadora, un visor de imágenes y un par de editores de texto. Pero
no encontrará aplicaciones de oficina pesadas ni herramientas de productividad.

Revisión de Kali Linux: menú de aplicaciones

Para dar un ejemplo concreto, no hay un lector de correo electrónico como parte del estándar

Machine Translated by Google

instalación. Por supuesto, Kali Linux está basado en Debian y muchos paquetes
fueron portados. Por lo tanto, puede instalar una gran cantidad de software adicional por su cuenta y
Deberia trabajar:

apt-get actualizar && apt-get instalar thunderbird

Thunderbird en Kali Linux

Y de hecho lo hará. Pero una vez más, ¿es realmente inteligente revisar su correo como root?
en una máquina que utilizará para la auditoría de seguridad?

¿Qué tiene de “malo” trabajar como root?

En un sistema tipo Unix típico, los usuarios trabajan como usuarios sin privilegios, con acceso
a sus propios archivos, pero sin la capacidad de alterar el sistema u otros
archivos de los usuarios. Para mantenimiento informático o para realizar tareas administrativas,
algunos usuarios pueden respaldar temporalmente la identidad privilegiada "raíz" que les da
ellos super-poderes en el anfitrión.

Por otro lado, en un sistema Kali Linux predeterminado, el único usuario instalado es
root y tienes que trabajar bajo esa identidad todo el tiempo. Tienes que
entienda que ser root significa que básicamente no hay verificaciones de permisos
en su máquina. Puedes hacer lo que quieras. E incluso cosas que no
querer. Por ejemplo, al explorar su sistema, puede editar sin darse cuenta
algunos archivos críticos como /etc/passwd o algún archivo en el directorio /etc/grub.d/ en
tal manera que su sistema se vuelva inutilizable. En algunos casos, puede

Machine Translated by Google

modifique su sistema sin notar ningún cambio obvio hasta el próximo reinicio
o la próxima actualización, cuando de repente se rompa. Y hay potencialmente
cientos de estos archivos críticos en un sistema Linux típico. Los permisos de archivo
están configurados de tal manera que un usuario "normal" no podría poner en peligro el sistema como
entero. Pero ser la raíz de su trabajo diario en Kali eliminará esa seguridad.
net (como lo haría en cualquier sistema Linux, por cierto).

Por supuesto, nada le impide crear nuevas cuentas sin privilegios en
tu sistema. Pero este es un trabajo extra que tienes que hacer en Kali que no harías
en otra distribución, simplemente porque está tratando de usar Kali para
algo para lo que no fue diseñado.

¡Sabe lo que haces!

Algo con el mismo espíritu, Kali Linux está repleto de pruebas de penetración.
herramientas: algunas de ellas son herramientas GUI, otras son herramientas CLI. En ambos casos, se
podría ser tentador "jugar" con ellos más o menos al azar. Pero algunos
Los comandos pueden ser potencialmente dañinos para su red doméstica. Además, por
sin comprender las implicaciones de lo que está haciendo, puede poner
usted mismo en una situación difícil utilizando esas herramientas en el trabajo o la escuela, o en
redes públicas. Y en ese caso, la ignorancia no será una excusa. Otra vez,
este no es un problema específico de Kali: si instala herramientas de prueba de penetración en
Fedora o Linux Mint, y prueba cosas al azar con ellos, puedes terminar en

Machine Translated by Google

el mismo problema Kali simplemente lo hace más fácil.

Kali está en silencio, y debería permanecer así.

Lo primero que puede ver en la pantalla de inicio de sesión de Kali es ese lema: "El
cuanto más callado te vuelves, más eres capaz de oír". ¿Que significa eso? Si
Escucho en la interfaz de red de mi sistema Debian, puedo ver que es
relativamente ruidoso, enviando paquetes de red a intervalos más o menos regulares.
Algunos de ellos son enviados por aplicaciones de usuario, otros por servicios en segundo plano.
Y si ejecuto nmap para realizar un escaneo de puertos en mi escritorio normal, puedo ver
varios puertos abiertos. Incluyendo un puerto vnc nunca utilizado y un olvidado hace mucho tiempo
¡Servidor HTTP! Todo eso porque tengo varios servicios y software de usuario
instalado. Algunos de ellos son parte de mi configuración predeterminada de Debian. algunos están aquí
porque un día instalé un paquete y simplemente no lo eliminé cuando no
ya lo necesitaba. Este es el caso, por ejemplo, del servidor HTTP que
no lo he necesitado durante semanas, pero que todavía se está ejecutando en mi
ordenador portátil.

Por otro lado, Kali está diseñado para ser lo más silencioso posible. Esto es requerido
tanto para ocultar su presencia en la red, como para endurecerse frente a potenciales
ataques Para lograr ese objetivo, la configuración predeterminada de Kali Linux deshabilita muchos
servicios que estarían habilitados en un sistema Debian genuino. Pero otra vez,
porque Kali Linux se basa en Debian, siempre que habilite el requerido

Machine Translated by Google

paquetes, debería poder instalar los servicios que desee. Por ejemplo, si
quieres practicar el desarrollo web, podrías tener la tentación de instalar una web
servidor en su host Kali:

apt-get install apache2

Servidor Apache en Kali Linux

Servidor Apache en Kali Linux

Si observa detenidamente la salida del comando, aunque tiene éxito, es posible que
Observe los mensajes de insserv que tienen algunas preocupaciones sobre los "niveles de ejecución de
script apache2".

Y de hecho,

rizo host local

curl: (7) No se pudo conectar al puerto localhost 80: Conexión rechazada

Una vez instalado, el servidor web no se inicia. Tienes que hacerlo de forma manual.

systemctl iniciar apache2

Y tendrás que hacerlo después de cada reinicio: “Kali Linux, como estándar
política, no permitirá que los servicios de red persistan a través de reinicios por
por defecto." (http://docs.kali.org/policy/kali-linux-network-service-policies)

Otra opción sería cambiar la política en el archivo /usr/sbin/update-rc.d

Machine Translated by Google

a la lista blanca de apache2 como un servicio de inicio. Pero en ese caso, al igual que con mi computadora portátil, hay posibilidades de que deje esa puerta abierta, incluso cuando no ya no lo necesita. Lo que podría ser una preocupación en mi sistema de escritorio sería mucho más grave el día que conecta su sistema Kali a un sistema comprometido la red.

No lo olvides, una cosa que hace que Kali sea "especial" es que fue específicamente diseñado para funcionar incluso cuando se utiliza en un entorno muy hostil. En eso contexto, ejecutar un servidor web al inicio en su host Kali derrota eso propósito. En resumen, has roto a Kali. Tal vez no visiblemente. Pero en espíritu en menos. ¡Necesito el software $prog pero no está en el repositorio de Kali!

No hay garantía de que todos los paquetes de Debian estén disponibles en Kali. Y de todos modos, no hay garantía de que todo el software posible esté disponible en Debian.

Por lo tanto, podría ser tentador agregar repositorios de fuentes adicionales a su sistema para descargar más software del que proporciona la distribución oficial. O para agregar un repositorio que proporcione la última versión de vanguardia de su favorito software. Aquí y allá, incluso puede ver "consejos" que sugieren que modifique el archivo /etc/apt/sources.list para ese propósito.

Seamos claros. Si considera hacer eso, una distribución compatible con PPA como Ubuntu probablemente se adaptará mejor a sus necesidades. No es que diga que no puedes agregar más repositorios fuente a Kali Linux. Pero no debería: Debian nos advierte

Machine Translated by Google

contra lo que llaman FrankenDebian ya que puede amenazar la estabilidad de su sistema. Y para Kali Linux es aún peor. No solo podría romper su sistema, pero agregar paquetes de una fuente no confiable a un sistema de seguridad es simplemente tonterías. Incluso si confía en la fuente, tenga en cuenta que los paquetes de Kali están endurecidos (¿recuerdas cuando instalé apache2 arriba?), Que no es el caso de la mayoría de los paquetes en la naturaleza.

Conclusión: ¿Deberías usar Kali Linux?

Y ahora es el momento de mi conclusión. Pero no quería terminar tanto tiempo artículo con una opinión simplista, en blanco y negro. Especialmente porque no sé usted. Así que aquí hay tres resultados posibles. Simplemente elija el que se adapte a su caso mejor:

1. Si llegaste directamente a esta conclusión sin leer el resto del artículo, o ya tienes una opinión sólida y no tengo ninguna posibilidad de hacerte cambiarlo, o Kali aún no es para ti. En ese caso, deberías primero considere una distribución más convencional como un sistema Debian simple o Ubuntu. Todavía habrá oportunidades más adelante para instalar las herramientas que necesita en caso por caso.

2. Si leyó el artículo pero se saltó las partes que contienen demasiada información técnica jerga, Kali no es para ti. Kali Linux podría ser una herramienta de enseñanza increíble. Pero si vas por ese camino, debes estar preparado para una curva de aprendizaje empinada. Si

Machine Translated by Google

eres un usuario muy nuevo de Linux comenzando desde cero o si solo quieres usar su computadora sin dolores de cabeza, hay un montón de propósito general y distribuciones fáciles de usar para empezar. ¿Por qué no probar Linux Mint o Zorin OS? ¿O tal vez otro derivado de Ubuntu?

3. Si leyó el artículo, probó los comandos que usé, siguió los enlaces y Miró los términos que no entendió, bueno, felicitaciones. Tu no eres solo otro "script kiddie". Por el contrario, aparentemente estás listo para pasar incontables horas y esfuerzos para hacer que su sistema funcione, entender el fundamentos de la informática y descubrir los aspectos internos de las redes. Que lo convierte en uno de los pocos nuevos usuarios de Linux que podría beneficiarse del uso Kali. Pero en lugar de usarlo directamente en su computadora, sugeriría que primero instala alguna otra distribución basada en Debian y ejecuta Kali Linux en un máquina virtual. De esa manera podrías practicar tus habilidades sin sacrificar sus otras actividades.

Como última palabra, tal vez no estés de acuerdo conmigo o no te reconociste en las tres categorías anteriores, así que no dude en utilizar la sección de comentarios para ¡Da tu opinion!

Machine Translated by Google

Conclusión

En resumen, Kali Linux es un sistema operativo increíble que es ampliamente utilizado por varios profesionales desde Administradores de Seguridad, hasta Black Hat Hackers. Dadas sus robustas utilidades, estabilidad y facilidad de uso, es un sistema operativo todo el mundo en la industria de TI y los entusiastas de la informática deben estar familiarizados. Utilizar solo las dos aplicaciones discutidas en este tutorial mejorará significativamente ayudar a una empresa a asegurar su infraestructura de tecnología de la información. Ambas cosas Nmap y Metasploit están disponibles en otras plataformas, pero su facilidad de uso y la configuración preinstalada en Kali Linux hace que Kali sea el sistema operativo sistema de elección al evaluar y probar la seguridad de una red. Como mencionado anteriormente, tenga cuidado al usar Kali Linux, ya que solo debe usarse en entornos de red que usted controla o tiene permiso para probar. Como algunas utilidades, pueden causar daños o pérdida de datos.

Tenga en cuenta que Kali Linux, aunque no es demasiado complicado, no es exactamente para principiantes, así que tómate tu tiempo mientras trabajas con las herramientas. Intenta aprender en menos una cosa nueva cada día.

Si eres nuevo en el mundo de Linux, considera comenzar con otro Linux sistema como Ubuntu para tener una idea de en qué se estaría metiendo.

Nunca intente usar las herramientas en Kali Linux contra cualquier sistema que no sea

Machine Translated by Google

autorizado para acceder. Existen muchos sistemas legalmente libres para
practica tus habilidades.

Tenga en cuenta que todas las herramientas que necesita son gratuitas. Desde virtuales gratis hipervisores de máquinas, a sistemas operativos libres, a herramientas de ciberseguridad y Kali Linux en sí mismo, aprender ciberseguridad es principalmente una inversión de su tiempo y esfuerzo.