HACKEADO

MEJOR GUÍA DE KALI LINUX Y HACKING INALÁMBRICO CON HERRAMIENTAS DE SEGURIDAD Y PENETRACIÓN, LIBRO PASO A PASO

ALAN T. NORMAN

HACKEADO

Mejor Guía De Kali Linux Y Hacking Inalámbrico Con Herramientas De Seguridad Y Penetración, Libro Paso A Paso

Práctico De Hacking De Computadora

Alan T. Norman

Traductora: Enrique Laurentin

Aviso de exención de responsabilidad:

Tenga en cuenta que la información contenida en este documento es solo para fines educativos y de entretenimiento. Se ha hecho todo lo posible para proporcionar información completa precisa, actualizada y confiable. No hay garantías de ningún tipo expreso o implícito. Al leer este documento, el lector acepta que bajo ninguna circunstancia es el autor responsable de las pérdidas, directas o indirectas, que se incurran como resultado de la emisión de información contenida en este documento, incluidos, entre otros, errores, omisiones o inexactitudes.

TABLA DE CONTENIDO

Introducción

Este libro tiene la intención de servir como una guía de nivel intermedio sobre algunas herramientas y habilidades comunes de prueba de penetración, particularmente aquellas de hacking inalámbrico y para mantener el anonimato. El material se desprende de la información introductoria básica proporcionada en el libro ***Hacking para principiantes,*** por lo que se supone que el lector está familiarizado con los conceptos y la terminología de hacking para principiantes. A diferencia del ***hacking para principiantes***, este libro se concentra más en la ejecución práctica y proporciona algunos procedimientos paso a paso para instalar plataformas y herramientas esenciales, así como la teoría detrás de algunos ataques básicos.

Los “Cuatro Grandes"

Hay cuatro áreas de enfoque principales que todos los hackers deben considerar y perfeccionar, sin importar su nivel de competencia. Si quieres convertirte en un hacker maestro, deberías estar trabajando constantemente para mejorar en estas cuatro áreas. Estos "cuatro grandes" son conocimiento, herramientas, habilidades y juicio. Mientras lee este libro y pone en práctica sus ideas, debe preguntarse cuáles de estas áreas son relevantes para el concepto en cuestión. Esto le ayudará a crear un marco para sus habilidades y seguir su progreso a medida que avanza.

CONOCIMIENTO

El conocimiento profundo y amplio de conceptos relevantes es la base para cualquier hacker exitoso. Obtener conocimiento no es solo el comienzo de una carrera de hacking, sino que debe mantenerse constantemente debido a la rapidez con que crece y cambia la información en el mundo de la informática. Existe una oferta aparentemente interminable de fuentes de conocimiento y áreas de estudio, tanto que es probable que sea imposible saber todo lo que está disponible. Sin embargo, la dedicación a la búsqueda constante del conocimiento es esencial. Hay varias áreas en las que enfocarse que son críticas para una base de conocimiento funcional en seguridad y explotación de computadoras. En orden sucesivo, generalmente, son:

Estas áreas de conocimiento se solapan en algunos casos y el lector ciertamente no está limitado a la lista anterior (¡cuanto más conocimiento, mejor!), Sino que representa una buena lista de por "hacer" para que los auto estudiantes comiencen. La información en todas estas áreas se puede encontrar en libros, libros electrónicos, revistas, sitios web, cursos en línea y fuera de línea, mentores personales y conferencias, entre otras fuentes. Puede ser útil, si es asequible, graduarse o certificarse en redes, programación o seguridad de la información.

Herramientas

El conocimiento es inútil sin las herramientas para explotarlo. El hacker necesita un conjunto básico de herramientas de hardware y software que permanecen básicamente iguales, independientemente del nivel de habilidad. Sin embargo, estas herramientas se acumularán y evolucionarán con el tiempo, junto con los avances en tecnología y defensa. Las tres categorías básicas de herramientas que necesita un hacker exitoso son:

La mayoría de las herramientas no son particularmente sofisticadas, costosas o difíciles de obtener. Las computadoras pueden ser costosas, pero la mayoría de las operaciones de hackers no requieren la máquina más reciente y más rápida del mercado. Para la mayoría de los procedimientos, una computadora portátil que tenga una cantidad razonable de memoria y que pueda soportar sistemas operativos modernos suele ser suficiente. Aunque la mayoría de las computadoras vienen de serie con hardware de red, la penetración de Wi-Fi requiere un tipo especial de chipset inalámbrico (consulte el capítulo 10) que generalmente no viene con adaptadores estándar. Sin embargo, se puede obtener un adaptador USB externo con esta característica de manera relativamente económica.

Casi todo el software necesario para los procedimientos de hacking más comunes es gratuito, de código abierto y de fácil obtención. Estas herramientas están disponibles abiertamente para descargar y se actualizan con frecuencia. La mayoría de estas herramientas son compatibles con una rica comunidad de usuarios entusiastas que son un excelente recurso para obtener consejos y solucionar problemas. Es importante que los hackers mantengan actualizado su software con las últimas versiones y parches y que supervisen a la comunidad en busca de problemas, soluciones y casos de uso actuales.

HABILIDADES

Las habilidades de los hackers se obtienen cuando el conocimiento y las herramientas se combinan para lograr un propósito. Al final del día, las habilidades de un hacker determinan lo que puede o no puede lograr. Una vez que uno tiene el conocimiento y las herramientas, construir un buen conjunto de habilidades requiere una cosa... práctica.

Las habilidades se pueden practicar de forma segura en un entorno autónomo, como una red de área local o una red de área personal, o en un conjunto de máquinas virtuales en red dentro de un solo sistema. Además, hay varios sitios web, tanto gratuitos como de pago, donde los hackers y los profesionales de seguridad pueden practicar métodos ofensivos y defensivos en un espacio libre de consecuencias.

Al igual que cualquier otra habilidad, las habilidades de hacking disminuirán si no se usan, ya sea con práctica o aplicación, de manera regular. Además, nunca puede suponer que una vez que se aprende una habilidad, sigue siendo una habilidad utilizable para siempre. La naturaleza de la piratería y la seguridad es tal que evoluciona constante y rápidamente. Hubo un tiempo, por ejemplo, cuando la inyección de SQL era un ataque simple y común en los sitios web, pero ahora que los administradores se han dado cuenta (y el código del lado del servidor se ha vuelto más seguro) se considera anticuado. Se ha descubierto una vulnerabilidad reciente en las redes Wi-Fi (ver Capítulo 11) que ahora está a la vanguardia. Las habilidades deben actualizarse con los últimos conocimientos y herramientas para que sigan siendo efectivas.

Juicio

Finalmente, y quizás lo más importante, un hacker siempre debe poner en práctica un buen juicio. Mientras que las habilidades determinan lo que puede hacer un hacker, el juicio determina lo que debe hacer. Gran parte del conocimiento y las habilidades necesarias para el hacking implican la

comprensión de múltiples conceptos avanzados. Aunque la sociedad moderna es muy inteligente desde el punto de vista técnico, la mayoría de las personas con las que se encuentra en la vida diaria no tienen una fracción del conocimiento necesario para comprender, y mucho menos ejecutar, incluso los trucos más simples. Esto coloca a los hackers en un club bastante exclusivo, dándole al principiante una sensación embriagadora de poder e invencibilidad. Sin embargo, junto con todo el conocimiento técnico que viene con el estudio del hacking, también debe llegar a comprender los diversos riesgos y consecuencias. Es tentador querer saltar primero y practicar sus habilidades recién descubiertas, pero todas las acciones deben templarse primero con preguntas sobrias.

Un hacker debe tener objetivos claros en mente antes de embarcarse en cualquier esfuerzo, incluso aquellos destinados solo a la práctica. Todas las acciones deben llevarse a cabo con la debida consideración de los propios estándares éticos, las expectativas de la comunidad y las posibles consecuencias (ver el dilema en la Figura 1). Un error común para los principiantes es sobreestimar su nivel de anonimato. Un error aún más grave es sobreestimar su nivel de habilidad. Un ataque mal ejecutado puede revelar la identidad del hacker o causar daños involuntarios o pérdida de datos en un sistema objetivo. Se necesita tiempo para alcanzar un nivel adecuado de competencia y competencia para cualquier tarea, y la impaciencia puede arruinarlo todo.

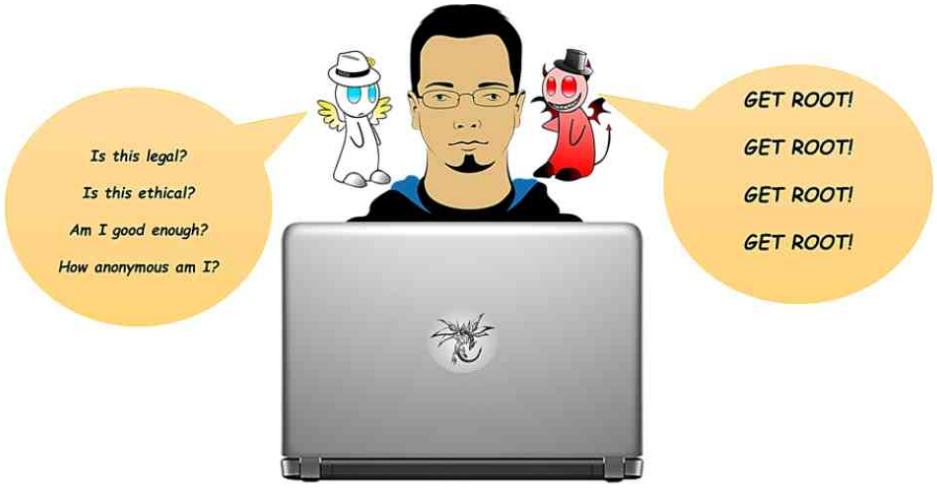


Figura 1 - El dilema del hacker

Algunas Palabras De Precaución

Antes de embarcarse en cualquier misión de prueba de penetración, o de otro modo implementar el conocimiento y las habilidades adquiridas de este libro, el lector debe tener en cuenta los siguientes consejos de precaución.

El Rápidamente Cambiante Paisaje

Más que cualquier otro tipo de industria o tecnología, el mundo de las computadoras y las redes de información (en términos de hardware y software) está cambiando rápidamente. Las nuevas versiones, a veces incluso varias versiones más adelante, siempre están en producción antes de que las más actuales lleguen al mercado. Por lo general, no es posible predecir cuándo se lanzará una nueva versión, subversión o parche para un paquete dado, o qué cambios vendrán con esa versión. El mundo del software de código abierto, de donde proviene la mayoría de las herramientas de hackers, es especialmente caótico. Las versiones, los parches y la documentación a menudo son realizados por la comunidad de usuarios y no necesariamente se mantienen de forma centralizada con ningún tipo de control de calidad riguroso. Hay varios tipos de distribuciones para sistemas operativos de código abierto y otras herramientas, y no siempre coordinan los cambios en su código fuente. Como resultado de este panorama rápidamente cambiante y a menudo impredecible, cualquier paso individual o sintaxis de comando para un procedimiento en particular está sujeto a cambios en cualquier momento. Además, la implementación de ciertos procedimientos puede diferir, a veces de manera sutil y a veces drásticamente, dependiendo de la naturaleza del hardware o sistema operativo en el que se ejecutan.

Este libro intenta esbozar la información más reciente, más común y más universal, y proporciona advertencias en las que se sabe que los procedimientos difieren. Sin embargo, el lector debe estar preparado para el hecho de que a menudo hay una gran cantidad de soluciones de problemas y refinamiento de pasos individuales que viene junto con la implementación de muchos de los procedimientos presentados en este libro. Cuando se producen errores o resultados inesperados, hay recursos disponibles de forma gratuita en Internet para obtener información actualizada. Los mejores lugares para

verificar son los sitios web anfitriones para el software en cuestión y varios hackers en línea o tableros de mensajes de software. En la mayoría de los casos, alguien más ya ha encontrado y publicado una solución al problema que usted tenga.

Los Límites Del Anonimato

Este libro discute varias herramientas y métodos diferentes para que los hackers (o incluso los usuarios casuales de Internet) mantengan un cierto grado de anonimato. Estos procedimientos van desde ocultar u ofuscar la dirección IP o MAC de uno hasta acceder a recursos a través de canales encriptados o de múltiples saltos. Sin embargo, es importante comprender que la naturaleza de la comunicación hace que sea prácticamente imposible para cualquier persona mantener el 100% de anonimato. Una parte motivada y bien financiada, ya sea un delincuente o una organización gubernamental (o ambas, en algunos casos) a menudo puede determinar la información que está buscando. En muchos casos, solo se necesita un único error menor por parte de la persona que desea permanecer en el anonimato para revelar su ubicación o identidad. La naturaleza de las actividades de esa persona generalmente determinará los recursos que otros están dispuestos a dedicar para encontrarlos. Todavía es posible mantener un alto grado de confianza en el anonimato implementando adecuadamente varios métodos simultáneamente. En muchos casos, esto hará que el tiempo que lleve localizar a alguien sea prohibitivo y costoso. La conclusión es que nunca debes asumir que estás completamente seguro o anónimo.

Ramificaciones Legales Y Éticas

Hacking para principiantes presenta un análisis detallado de los diversos problemas legales y éticos que deben considerarse antes de emprender la piratería informática como un pasatiempo o una carrera. Este libro presenta información de manera práctica y alienta al usuario a usar el conocimiento adquirido con cuidado y diligencia. Ninguna de las herramientas o procedimientos descritos en este libro son ilegales o incluso poco éticos cuando se usan en el contexto adecuado. De hecho, son cruciales para comprender la naturaleza de las amenazas modernas a la seguridad de la información y protegerse contra ellas. Además, es común y aconsejable realizar ataques contra los propios sistemas para identificar y corregir vulnerabilidades. Intentar acceder o comprometer un sistema sin el permiso del propietario no se recomienda, especialmente para principiantes sin experiencia, y podría tener graves consecuencias, incluido el enjuiciamiento penal. Asegúrese de comprender las leyes y sanciones, que pueden variar según el país y la localidad, y, como se mencionó anteriormente, no cuente con el anonimato para protegerlo.

Capítulo 1. Kali Linux

Para comenzar con el hacking inalámbrico, primero debe familiarizarse con las herramientas del oficio. Ninguna herramienta es más valiosa, especialmente para un hacker principiante, que Kali Linux. Kali, un conjunto de software de análisis y penetración gratuito, estable, bien mantenido y asombrosamente completo, evolucionó en el crisol de las distribuciones de Linux de código abierto y se ha convertido en el rey de todos los sistemas operativos de hackers. Este sucesor de la famosa distribución BackTrack tiene todo lo que un hacker necesita, desde novatos hasta expertos experimentados.

Breve Historia De Unix Y Linux

A principios de la década de 1970, el ***sistema operativo*** (SO) ***Unix***, abreviado de UNICS (Servicio de información y computación UNIplexado), evolucionó a partir de un proyecto difunto de AT&T Bell Labs para proporcionar acceso simultáneo de usuarios a servicios informáticos de mainframe. A medida que Unix se hizo más formal y creció en popularidad, comenzó a reemplazar los sistemas operativos nativos en algunas plataformas mainframe comunes. Originalmente escrito en ***lenguaje ensamblador***, la reescritura de Unix en el lenguaje de programación ***C*** mejoró su portabilidad. Finalmente, varias versiones de Unix, incluidas las destinadas a microcomputadoras, surgieron en el mercado comercial. Varios derivados de sistemas operativos populares, conocidos como ***"Unix-like"*** tomaron forma en las siguientes décadas, incluidos ***Mac OS*** de Apple, ***Solaris*** de Sun Microsystem y ***BSD*** (Berkeley Software Distribution).

Los esfuerzos para crear una versión gratuita de Unix comenzaron en la década de 1980 con el proyecto ***GNU*** ("GNU's No Unix") y General Public License (***GPL***), pero no lograron producir un sistema viable. Esto llevó al programador finlandés Linus Torvalds a abordar el desarrollo de un nuevo núcleo Unix (el módulo de control central de un sistema operativo) como un proyecto estudiantil. Utilizando el sistema operativo educativo similar a Unix ***Minix***, Torvalds codificó con éxito un núcleo del sistema operativo en 1991, haciendo que el código fuente esté disponible gratuitamente para su descarga y manipulación pública bajo la GPL de GNU. El proyecto finalmente se llamó ***Linux*** (una combinación del primer nombre de Torvalds, "Linus", con "Unix").

Aunque el término Linux inicialmente se refería únicamente al kernel desarrollado por Torvalds, eventualmente llegó a designar a cualquier paquete de sistema operativo que se basara en el kernel de Linux. Siendo un esfuerzo de

código abierto, varias distribuciones de Linux evolucionaron a lo largo de las décadas con conjuntos únicos de bibliotecas de software, controladores de hardware e interfaces de usuario. La flexibilidad y la eficiencia de Linux llevaron a la adopción generalizada por los entusiastas de la informática y algunas organizaciones grandes, tanto como una medida de ahorro de costos como para eludir el monopolio de los sistemas operativos por parte de Microsoft.

Dado que el software comercial y de consumo más popular está escrito para las plataformas Microsoft y Apple, Linux nunca ha tenido la ubicuidad o el atractivo comercial de los sistemas operativos de PC Windows y Macintosh.

Sin embargo, la flexibilidad, la portabilidad y la naturaleza de código abierto de Linux lo hacen ideal para la creación de distribuciones livianas y altamente personalizadas que sirven para propósitos muy específicos. Estas distribuciones generalmente se crean desde el núcleo hacia arriba, solo instalando las bibliotecas y los componentes mínimos necesarios para lograr los propósitos del hardware del host. Este enfoque produce paquetes de sistema operativo que utilizan recursos mínimos de memoria, almacenamiento y procesador y tienen menos vulnerabilidades de seguridad. Linux, y la sintaxis y estructura de Unix en las que se basa, es una parte esencial del kit de herramientas y la base de conocimiento de un hacker moderno.

Cientos de distribuciones individuales de Linux comerciales y de código abierto han surgido y actualmente se ejecutan en todo, desde pequeños dispositivos personales como teléfonos y relojes inteligentes, hasta computadoras personales, servidores mainframe y hardware militar. La mayoría de estas distribuciones se han ramificado de un puñado de paquetes anteriores de Linux, incluidos **Debian**, ***Red Hat*** y ***SLS***.

DEBIAN LINUX Y KNOPPIX

Debian, uno de los primeros proyectos abiertos de distribución de Linux, fue

creado conscientemente para permanecer libre y abierto sin dejar de mantener altos estándares de calidad. Debian ha tenido varios lanzamientos importantes por su cuenta, además de docenas de proyectos derivados que utilizan el núcleo de Debian y la base de la biblioteca. Cuando dos de estos proyectos, ***Linspire*** y ***Ubuntu*** (una distribución muy popular) estaban dirigidos principalmente a usuarios domésticos de PC, el proyecto ***Knoppix*** fue diseñado para ejecutarse en vivo desde un medio externo, como un CD-ROM. Esto, junto con su capacidad para interactuar con una gran variedad de hardware, convirtió a Knoppix en una herramienta ideal para la resolución de problemas, el rescate de datos, la recuperación de contraseñas y otras operaciones de servicios públicos. Knoppix fue una base natural desde la cual desarrollar las diversas subdistribuciones de seguridad, ***pruebas de penetración*** y subdistribuciones forenses que posteriormente se han generado.

BACKTRACK LINUX

Dos distribuciones basadas en Debian Knoppix que se centraron en las pruebas de penetración fueron ***WHAX*** (anteriormente ***Whoppix***) y ***Auditor Security Collection***. Ambos proyectos se ejecutaron en CD en vivo y presentaron un gran depósito de herramientas de prueba de penetración. WHAX y Auditor Security finalmente se fusionaron en la notoria distribución conocida como ***BackTrack***.

Kali Linux

El completo paquete de seguridad ofensiva y defensiva incluido en BackTrack Linux lo convirtió en la herramienta elegida por aficionados, profesionales de la seguridad, probadores de penetración legítimos y hackers. El desarrollador de BackTrack, Offensive Security, finalmente reescribió la distribución, renombrando el proyecto como ***Kali*** Linux. Los paquetes de instalación de Kali y las imágenes de máquinas virtuales están disponibles de forma gratuita. Offensive Security también ofrece cursos de pago de seguridad con Kali, así como certificaciones profesionales y un entorno de pruebas de penetración en línea.

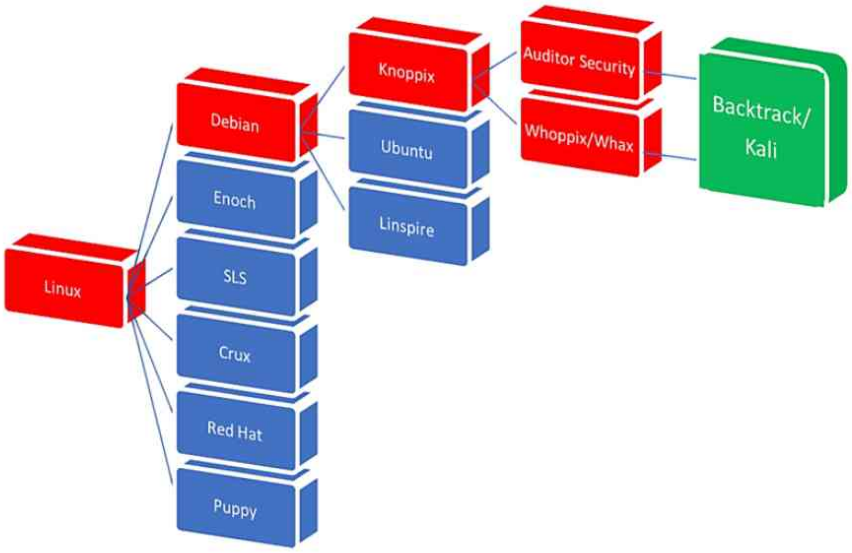


Figura 2 – Evolución de Kali Linux

HERRAMIENTAS KALI

La pieza central de Kali Linux, y la razón principal de su popularidad entre los hackers y los profesionales de seguridad, es su amplio y bien organizado conjunto de herramientas gratuitas. Kali actualmente cuenta con más de 300 herramientas que incluyen recopilación de información pasiva, evaluación de vulnerabilidad, análisis forense, descifrado de contraseñas, análisis de red, piratería inalámbrica y un poderoso conjunto de herramientas de explotación. Aunque todas las herramientas incluidas con Kali son gratuitas y de

código abierto y se pueden descargar y construir en la mayoría de los derivados de Linux (basados en Debian), tener un SO probado y examinado que viene nativo con una gran variedad de herramientas es un recurso invaluable.

Entre las herramientas más útiles que vienen con Kali están:

Metasploit Framework: Metasploit es una popular plataforma de explotación de vulnerabilidades que contiene varias herramientas de análisis y penetración. Cuenta con múltiples opciones para la interfaz de usuario y proporciona al usuario la capacidad de atacar casi cualquier sistema operativo. Kali también contiene ***Armitage***, una plataforma de gestión gráfica que ayuda al usuario a organizar las operaciones e interacciones entre múltiples herramientas de Metasploit durante un ataque.

Wireshark: Wireshark es una herramienta multiplataforma de análisis de tráfico de red en tiempo real. Todo el tráfico en un nodo de red elegido se captura y desglosa en metadatos de paquetes útiles, incluidos el encabezado, la información de enrutamiento y la carga útil. Wireshark se puede usar para detectar y analizar eventos de seguridad de red y para solucionar fallas de red.

John the Ripper: John the Ripper es una herramienta legendaria para descifrar contraseñas que contiene múltiples algoritmos de ataque de contraseña. Aunque originalmente fue escrito exclusivamente para Unix, John the Ripper ahora está disponible en varias plataformas de sistema operativo. Una de sus características más útiles es su capacidad de detectar automáticamente el tipo de ***"hash"*** de cifrado de contraseña. La versión gratuita de John the Ripper disponible en Kali admite el descifrado de muchos algoritmos de hash de contraseña, pero no tantos como su contraparte comercial.

Nmap: Nmap, abreviatura de mapa de red o mapeador de red, es una herramienta de hacking común que es esencial para las pruebas de penetración. Nmap permite al usuario escanear una red para todos los hosts y servicios de

red conectados, proporcionando una vista detallada de la estructura y los miembros de la red. Además, Nmap proporciona una lista del sistema operativo instalado de cada host, así como sus puertos abiertos. Esto permite al usuario concentrarse en vulnerabilidades conocidas durante la explotación.

Aircrack-ng: Aircrack-ng es el paquete de software por excelencia para el análisis inalámbrico y las pruebas de penetración, centrándose en los protocolos de encriptación Wi-Fi (***WEP***), acceso protegido Wi-Fi (***WPA***) y ***WPA2-PSK***. Esta herramienta presenta análisis de paquetes inalámbricos, inyección de paquetes, análisis de redes inalámbricas y herramientas de descifrado de contraseñas cifradas. Aircrack-ng requiere hardware de interfaz de red que admita la funcionalidad del modo monitor. Kali también presenta una herramienta de piratería inalámbrica basada en gráficos conocida como ***Fern***.

BurpSuite: BurpSuite es una colección de herramientas que se enfoca en la explotación de aplicaciones web. Estos programas interactúan no solo para probar las vulnerabilidades de las aplicaciones, sino también para lanzar ataques.

La lista anterior no es completa, pero es una muestra representativa del poder y la flexibilidad que Kali Linux proporciona como plataforma para pruebas de penetración y para la seguridad informática en general. Kali se puede ejecutar en vivo desde medios ópticos o USB, como un SO independiente en una estación de trabajo de escritorio o portátil, como alternativa en un sistema de arranque múltiple, o dentro de una máquina virtual dentro de otro SO host. El siguiente capítulo describe cómo instalar y configurar Kali en varios sistemas operativos para crear un entorno adecuado para el hacking y las pruebas de penetración.

Capítulo 2. Construyendo Un Entorno De Hacking

Para comenzar el hacking inalámbrico, primero se debe configurar un entorno adecuado para sus herramientas, comenzando, por supuesto, con la instalación de Kali Linux. Existen tres categorías principales para la instalación de Kali Linux, según las necesidades y el hardware del usuario:

- Standalone
- Arranque dual / múltiple

Cada tipo de instalación tiene sus propios pros y contras, y la mejor opción depende principalmente del uso previsto del software. Kali no fue escrito para ser un producto de consumo "cotidiano" con el software típico que disfrutan los usuarios ocasionales, por lo que instalarlo como un sistema operativo independiente en una computadora personal solo es práctico si esa máquina en particular se dedicará a actividades de pruebas de penetración. Alternativamente, Kali puede residir en el disco duro en un escenario de arranque dual o arranque múltiple con otras instalaciones del sistema operativo si el espacio lo permite. A menudo, Kali Linux se instala dentro del software de virtualización dentro de otro sistema operativo, ya sea Linux o no. Esta disposición consume más recursos, pero le da al hacker más flexibilidad y le permite practicar ataques en otras máquinas virtuales dentro del host. Kali también se puede utilizar como un sistema operativo "en vivo" de arranque cuando se instala en un medio externo extraíble, como un CD-ROM o una unidad flash USB. Dado que los lectores de discos ópticos se están volviendo extremadamente menos comunes, un medio USB es más práctico para instalaciones externas. Una ventaja de una distribución en vivo es que se puede usar en varias máquinas y algunas de las herramientas forenses digitales incluidas con Kali Linux se ejecutan mejor fuera de la estructura de arranque de una máquina de destino. Este capítulo se centrará en el hardware y los procedimientos de instalación virtual.

Instalación De Kali Linux En Un Disco Duro

Las últimas versiones de Kali Linux tienen los siguientes requisitos mínimos para una máquina host:

El usuario también necesitará un puerto USB o una unidad de CD-ROM para iniciar la instalación. Se recomienda que la máquina host tenga algún tipo de interfaz de red, por supuesto, para actualizaciones de software y conectividad en los esfuerzos de pruebas de penetración.

Ya sea que instale Kali Linux como un sistema operativo independiente o en un esquema de arranque múltiple, el primer paso en la instalación es obtener la última imagen de disco compatible con la Organización Internacional de Normalización (ISO) de Offensive Security y copiarla en un medio externo. Puede encontrar una lista de los últimos lanzamientos en www.kali.org/downloads/

Se recomienda que las imágenes ISO se obtengan del desarrollador, y no de un tercero o fuente de intercambio de archivos, para garantizar la integridad del código.

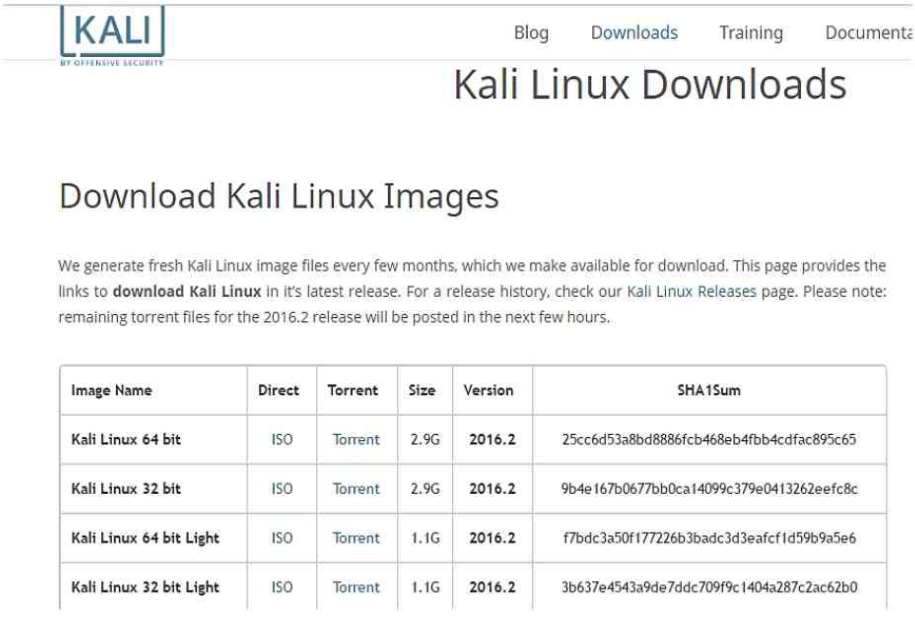


Figura 3 - Página de descarga ISO de Kali Linux (2/2/17)

El ISO está disponible en versiones de 32 bits y 64 bits, dependiendo de la arquitectura del procesador de la máquina host. Tenga en cuenta que la

versión de 64 bits no se ejecutará en un procesador de 32 bits. Puede descargar el ISO directamente desde el enlace correspondiente o mediante el enlace torrent si tiene un cliente torrent. Se proporciona un hash ***SHA1Sum*** para cada archivo ISO. Una vez que se ha descargado el archivo, se puede leer su hash utilizando el software de ***checksum*** y compararlo con la cadena dada. Si las cadenas no coinciden con precisión, entonces el archivo está comprometido y no debe usarse. Este procedimiento de checksum protege contra descargas corruptas o que han sido secuestradas (¡no hay honor entre los ladrones!).

Después de descargar la versión deseada de Kali Linux, grábela en un CD-ROM o cópiela en una unidad flash USB de arranque (siga las instrucciones en la sección X para crear una unidad flash de arranque).

INSTALACIÓN INDEPENDIENTE

Antes de comenzar una instalación independiente de Kali Linux, es importante comprender que el procedimiento **sobrescribirá todos los datos existentes en la unidad host**. Esto incluye el sistema operativo previamente existente, si lo hay, así como cualquier otro archivo o software.

Los pasos para una instalación independiente son los siguientes:

Verifique que su máquina host cumpla con los requisitos mínimos de hardware para Kali (actualmente 10 GB de almacenamiento y 512 MB de RAM) y que pueda admitir una instalación de 64 bits (si no, use la versión de 32 bits).

Dado que la instalación sobrescribirá los datos existentes en el disco duro del host, transfiera o realice una copia de seguridad de los archivos o configuraciones necesarios (es decir, a una unidad en la nube, unidad flash, CD, DVD o HDD externo).

Reinicie su máquina host e ingrese al menú del BIOS. Vaya a la sección de orden de arranque (los menús variarán de una computadora a otra) y asegúrese de que su unidad óptica (CD / DVD / BR) o los puertos USB, según el

medio elegido, estén primero en la lista. El orden de arranque se puede cambiar a otra configuración, si lo desea, después de la instalación. Asegúrese de guardar la configuración del BIOS al salir del menú del BIOS.

Después de alterar el BIOS, apague por completo la máquina host, inserte el medio óptico o USB que contiene el ISO, luego vuelva a encender la computadora. El menú de inicio de Kali puede demorar unos minutos en aparecer.

Cuando aparezca el menú de inicio de Kali, seleccione la opción **Instalación gráfica**.

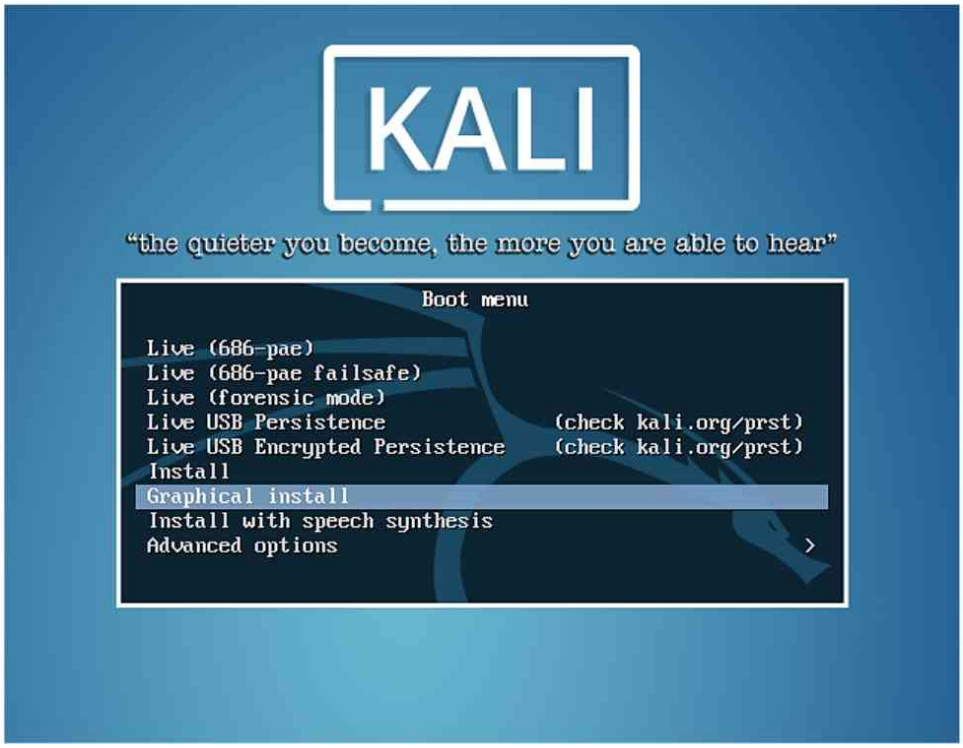


Figura 4 - Menú de arranque de Kali Linux

Los siguientes pasos de instalación incluyen opciones generales recomendadas para usuarios principiantes de Kali. En la mayoría de los casos, las opciones recomendadas ya están resaltadas de forma predeterminada en cada pantalla de menú. Estos pasos suponen que su máquina host tiene una conexión de red en vivo; puede aparecer un menú para la configuración de red inalámbrica o cableada. Si no tiene una conexión de red, puede haber ligeras diferencias en las opciones de su menú. Tenga en cuenta que esta parte del procedimiento será casi idéntica para las instalaciones virtuales y de arranque

múltiple.

- **Seleccione un idioma** >> [Seleccione su idioma deseado]
- **Seleccione su ubicación** >> [Seleccione su ubicación]
- **Configure el teclado** >> [Seleccione su teclado deseado]

(Kali configura la red, esto puede demorar unos minutos)

- **Configure la red** >> [use el nombre de host predeterminado "kali" o elija el suyo]
- o Nombre de dominio >> [esto puede dejarse en blanco si su red no lo requiere]
- **Configurar usuarios y contraseñas**
- **Contraseña de root** >> [elija una contraseña de "root" (administrador)]
- **Nombre real del usuario no root** >> [elija un nombre de identificación para su cuenta de usuario no privilegiado]
- **Nombre de usuario no root** >> [elija un nombre de usuario para su cuenta de usuario no privilegiada]
- **Contraseña no root** >> [elija una contraseña para su cuenta de usuario no privilegiada]
- **Configure el reloj** >> [elija su zona horaria]
- **Discos de partición** >> ["Guiado: use el disco completo"] >> [Elija el disco duro de instalación para su máquina host] >> ["Todos los archivos en una partición"] >> ["Finalice el particionamiento y escriba los cambios en el disco"]
- **Escribir los cambios en los discos?** [Si]

(Kali se instala... esto puede tomar varios minutos)

- **Configurar el administrador de paquetes**
- **Usar un espejo de red?** >> [Sí]
- **Información del proxy HTTP** >> [Ingrese su proxy o déjelo en

blanco]

(Kali configura... varios minutos)

- **Instale el cargador de arranque GRUB en el disco duro**
- **Instale el cargador de arranque GRUB en el registro maestro de arranque** >> [Sí]
- **Dispositivo para la instalación del cargador de arranque** >> [Elija el disco duro de instalación para su máquina host]

(Kali instala... varios minutos)

- **Finalice la instalación** >> [Continuar]

(Kali instala... varios minutos)

Después de la instalación, Kali reiniciará su máquina automáticamente. Si su computadora se inicia en la pantalla del menú de inicio original (Figura 4), apague la máquina, retire el CD de instalación o la unidad flash, luego enciéndala nuevamente.

INSTALACIÓN DE MÚLTIPLES ARRANQUES

Agregar Kali Linux como opción de arranque en una computadora con uno o más sistemas operativos existentes requiere la asignación de espacio separado en el disco duro. Tenga en cuenta que **manipular incorrectamente las particiones de la unidad puede provocar la pérdida de datos** y debe realizarse con cuidado. Se recomienda hacer una copia de seguridad de archivos y datos antes de manipular particiones. Dado que cada sistema operativo tiene su propia utilidad de administración de disco (además de algún software de terceros disponible), debe consultar las instrucciones para particionar el espacio en su sistema operativo nativo.

1. En el disco duro en el que instalará Kali Linux como opción de arranque, asigne una nueva partición de 20 GB (recomendada) utilizando la utilidad de administración de disco de su sistema operativo actual u otro software de utilidad de disco.

2. 2. Siga los pasos 1-4 de la sección anterior para comenzar la instalación de Kali en un medio externo.

3. 3. Comience el paso 5 de la sección anterior, deteniéndose antes del sub paso "Particionar discos" (5.VII).

4. 4. Elija la opción de partición "Manual" y continúe.

5. 5. En la lista de particiones en la siguiente pantalla, resalte la partición creada para Kali en el paso 1 anterior. **Asegúrese de seleccionar solo la partición destinada a Kali, o se borrarán otros datos.** Y continúe.

6. 6. En la lista "Configuración de partición", seleccione "Eliminar la partición" y continúe.

7. 7. La siguiente pantalla debería indicar ahora que la partición Kali prevista tiene "ESPACIO LIBRE". Seleccione esa partición nuevamente y continúe.

8. 8. En la pantalla "Cómo usar el espacio libre", seleccione "Particionar automáticamente el espacio libre" y continúe.

9. 9. Para “Esquema de particionamiento”, seleccione “Todos los archivos en una partición” y continúe.

10. 10. Finalmente, seleccione "Finalizar partición y escriba los cambios en el disco", continúe y seleccione "Sí" para confirmar los cambios escritos. Continúe y reanude la instalación en el paso 5.VIII.

Instalación De Kali Linux En Una Máquina Virtual

Los avances en la velocidad del procesador, el advenimiento de chips multinúcleo y multiprocesador, el mayor tamaño de la memoria y el mayor almacenamiento de datos han hecho de la virtualización de hardware un medio viable y práctico para ejecutar múltiples plataformas de software en un solo dispositivo informático. La ejecución de sistemas operativos dentro de una VM tiene ventajas porque elimina la necesidad de múltiples piezas de hardware costoso y hace práctico el uso de distribuciones altamente especializadas como Kali. Además, el uso de software de prueba de penetración dentro de un único host permite a los hackers practicar ataques en un entorno seguro de "caja de arena", apuntando a varias otras máquinas virtuales dentro del host. La desventaja de usar un sistema operativo dentro de una VM es que hay competencia por los recursos del host y las capacidades de hardware virtual se limitan a las de la máquina host.

El software de máquina virtual funcional y rico en características está disponible de forma gratuita. Las aplicaciones de VM gratuitas más comunes son ***Virtualbox*** y ***VMware Player*** (que tiene versiones comerciales con características adicionales). ***QEMU*** es una opción de código abierto que se ejecuta únicamente en Linux. Este libro usará Virtualbox para demostrar una instalación virtual de Kali porque está disponible para sistemas Windows, Macintosh, Linux e incluso Sun.

INSTALAR EL SOFTWARE DE VIRTUALIZACIÓN

Virtualbox es una popular aplicación de máquina virtual de código abierto multiplataforma. El procedimiento de instalación es el siguiente:

1. Garantizar especificaciones mínimas

Virtualbox está diseñado para ejecutarse en arquitecturas ***x86*** (chips Intel o AMD, et al) y se recomienda que la máquina host tenga al menos 1 GB de RAM. Además, la máquina host debería tener suficiente espacio libre en el

disco duro para acomodar cualquier sistema operativo de máquina virtual que desee instalar.

1. Habilite la virtualización de hardware

Si está utilizando una computadora host Windows o Linux, reinicie e ingrese al menú del BIOS. Navegue a la opción de virtualización (los menús variarán de una computadora a otra) y asegúrese de que esté habilitada. Asegúrese de guardar la configuración del BIOS al salir del menú del BIOS.

El hardware de Macintosh no usa BIOS de la misma manera que las computadoras "PC". La virtualización de hardware, si aún no está habilitada, debe establecerse mediante la línea de comandos en la aplicación de terminal. Este es un procedimiento avanzado que requiere acceso de root, y la sintaxis del comando puede variar entre las versiones de Mac OS. Consulte su documentación o al fabricante para habilitar la virtualización en hardware Macintosh.

1. Descargue los archivos de instalación

El último código fuente y las distribuciones binarias se pueden obtener en (Figura 5):

https://www.virtualbox.org/wiki/Downloads

Figura 5 - Página de descarga de Virtualbox

Windows

El enlace "hosts de Windows" proporciona un archivo binario de instalación

de Windows .exe. La documentación en el sitio web de Virtualbox enumera las versiones compatibles de Windows de la versión actual.

Macintosh OS X

El enlace "hosts OS X" proporciona un archivo de imagen de disco .dwg Mac OS X.

Linux

El enlace "Distribuciones de Linux" lanza una nueva página que enumera varios paquetes de Virtualbox para diferentes distribuciones de Linux. Sin embargo, se recomienda que descargue e instale Virtualbox a través de los repositorios de paquetes en su distribución individual de Linux (consulte el paso 4)

1. Instale Virtualbox

Windows

Al abrir el archivo de instalación ejecutable de Windows se abrirá un cuadro de diálogo típico de "asistente" de instalación de Windows. Siga las instrucciones de instalación. Las opciones de instalación y las opciones de aplicación adicionales dependen de sus preferencias individuales.

Macintosh OS X

Al abrir la imagen de disco .dwg se montará la imagen y se abrirá una ventana que contiene el archivo de instalación de OS X de Virtualbox ".mpkg". Inicie el archivo .mpkg para comenzar la instalación y siga las instrucciones. Las opciones de instalación y las opciones de aplicación adicionales dependen de sus preferencias individuales.

Linux (derivado de Debian)

La mayoría de las distribuciones modernas de Linux son derivados de los núcleos originales de Debian y Fedora (por ejemplo, Red Hat). Para ilustrar la instalación de Virtualbox en un sistema operativo Linux, los siguientes pasos describen la instalación tal como se aplica a un sistema Ubuntu Linux (un

derivado de Debian). La instalación para otras distribuciones de Linux puede variar en sintaxis y en ubicaciones de repositorio. Estos pasos deberían aplicarse a la mayoría de las versiones actualizadas de Debian.

Para instalar Virtualbox desde un repositorio de Ubuntu usando el centro de software:

- Abra la aplicación "Ubuntu Software" desde el menú del iniciador.
- Escriba "virtualbox" en la línea de búsqueda en la parte superior. VirtualBox debería aparecer en la lista de paquetes resultante (Figura 6).

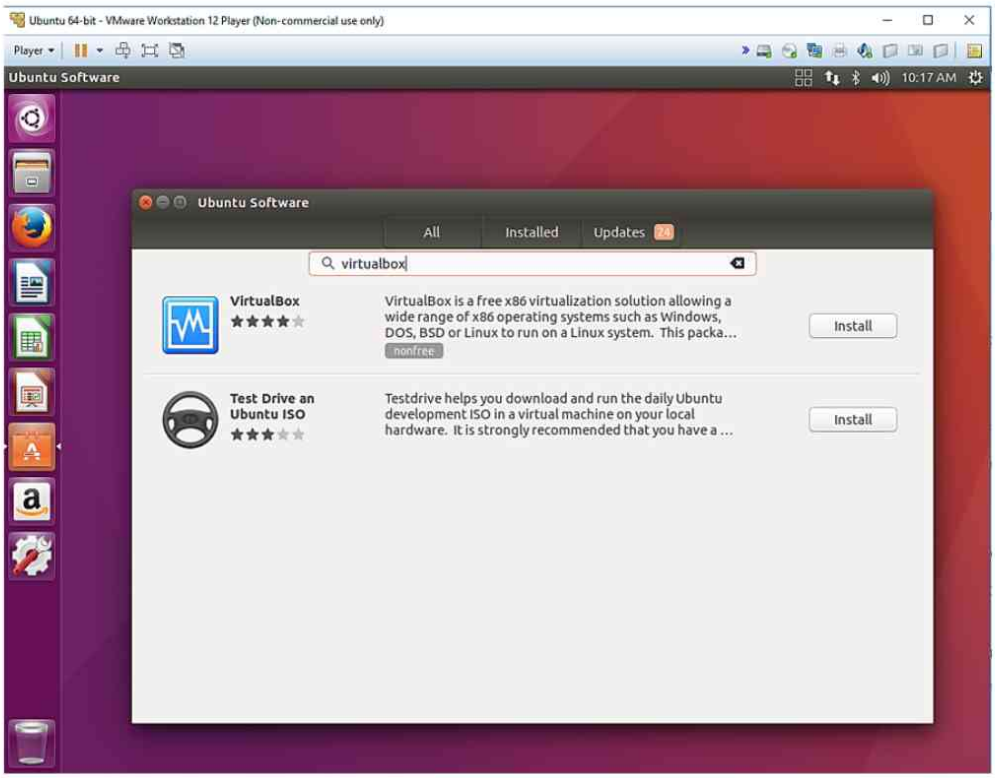


Figura 6: VirtualBox en el Centro de software de Ubuntu

- Haga clic en "Instalar" al lado del paquete VirtualBox.
- Si se le solicita, ingrese su contraseña para autenticar el acceso raíz.
- La instalación continuará automáticamente por un corto período.

Para instalar VirtualBox desde un repositorio de Ubuntu usando la línea de comando:

- Abra la consola de línea de comandos de Ubuntu, llamada "Terminal".
- Escriba lo siguiente para actualizar el repositorio de software (ingrese la contraseña de root si se le solicita):

```
# sudo apt-get update
# sudo apt-get install virtualbox
```

- La instalación continuará automáticamente durante un breve período.

INSTALACIÓN DE LA MÁQUINA VIRTUAL KALI LINUX DESDE UN DISCO O ISO

Una vez que se instala el software de virtualización, Kali Linux se puede instalar en el host como una máquina virtual. Este ejemplo volverá a presentar VirtualBox para ilustrar el procedimiento:

- Abra VirtualBox en su máquina host.
- Haga clic en "Nuevo" para crear una nueva máquina virtual.

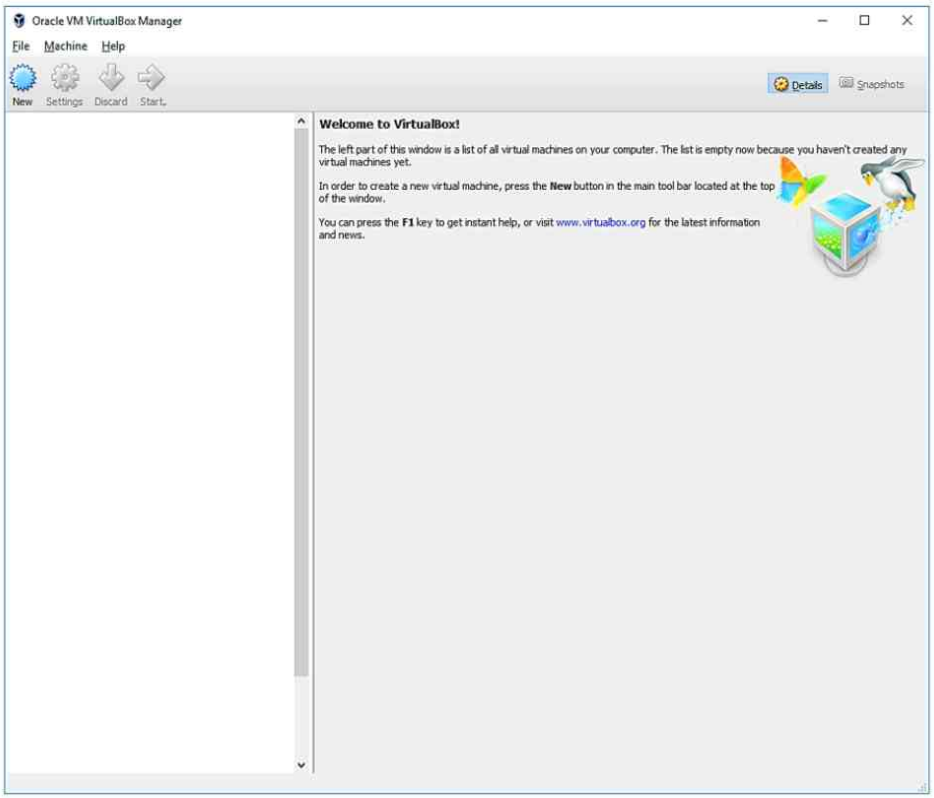


Figura 7 - Pantalla principal de Virtualbox

- Siga el cuadro de diálogo del asistente "Crear máquina virtual", utilizando los parámetros recomendados que se enumeran a continuación:
- **Nombre y sistema operativo**

Nombre >> [Kali Linux] (o lo que elijas)

Tipo >> [Linux]

Versión >> [Debian (64 bits)] (32 bits si corresponde)

- **Tamaño de memoria** >> [1024 MB]
- **Disco duro** >> [Cree un disco duro virtual ahora]
- **Tipo de archivo de disco duro** >> [VDI (VirtualBox Disk Image)]
- **Almacenamiento en disco duro físico** >> [Asignado dinámicamente]
- **Ubicación y tamaño del archivo:** use el nombre de archivo predeterminado del disco duro proporcionado. Se

recomienda asignar 10 GB - 20 GB para la unidad virtual.

- La máquina virtual Kali que creó ahora aparecerá en la lista de máquinas virtuales en la ventana principal de VirtualBox. Con la VM Kali resaltada, haga clic en el botón "Configuración" en la barra de herramientas para iniciar el diálogo de configuración.

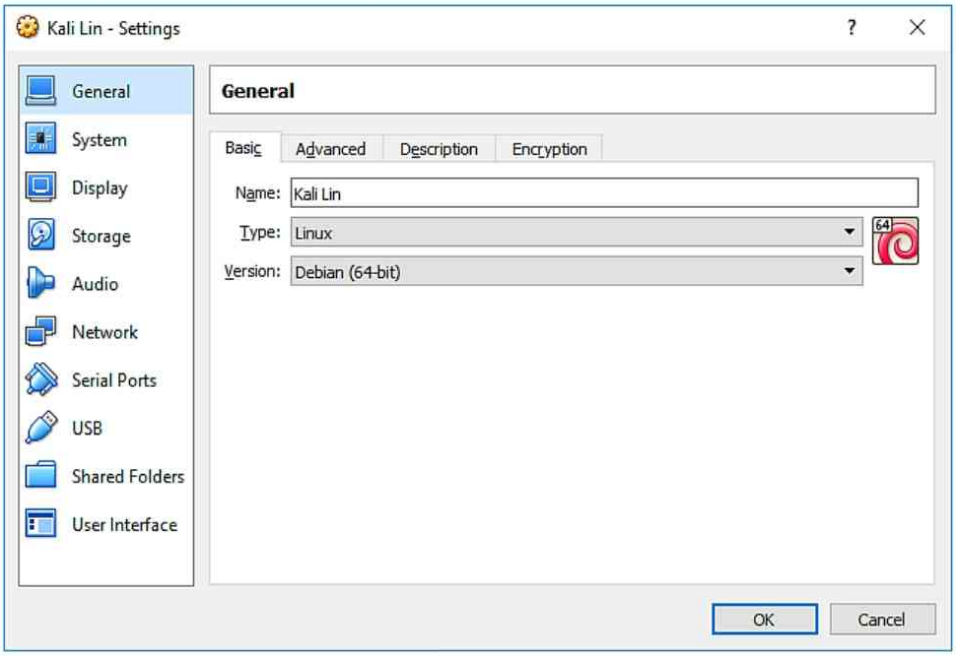


Figura 8 - Configuración general de Virtualbox

- Establezca la siguiente configuración recomendada navegando por las opciones y pestañas del menú de configuración (cambie otras opciones según lo desee):
- **Sistema** >> **Procesador** >> **Procesador(es)** >> [2 o más]
- **Sistema** >> **Procesador** >> **Funciones ampliadas** >> [Activar PAE/ NX]
- En la configuración de "Almacenamiento", resalte el icono de disco del controlador IDE "Vacío" en el Árbol de almacenamiento. En "Atributos", haga clic en el icono del disco "Unidad óptica" y navegue hasta la ubicación del archivo .iso de Kali Linux descargado al comienzo de este capítulo. Haga clic en

"Aceptar" para guardar y cerrar la configuración.

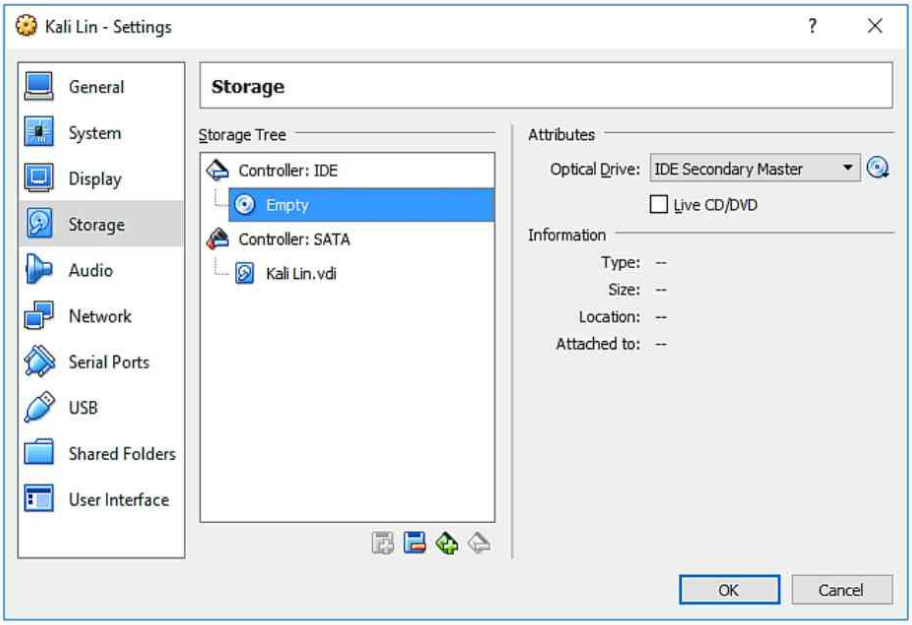


Figura 9 - Configuración de almacenamiento de Virtualbox

- En la ventana principal de VirtualBox, con la VM Kali resaltada, haga clic en iniciar para iniciar la VM.
- Se abrirá una nueva ventana que arrancará en la pantalla de arranque inicial de Kali. Siga las instrucciones gráficas de instalación que figuran en los pasos de instalación anteriores en este capítulo. En el paso 5.IX, "Instale el cargador de arranque GRUB en el disco duro", asegúrese de seleccionar la unidad virtual Kali Linux creada durante la instalación de VM. Complete el resto de los pasos de instalación.

INSTALACIÓN DE UNA MÁQUINA VIRTUAL KALI LINUX PRE CONFIGURADA

Algunas máquinas virtuales del **sistema operativo** están disponibles pre configuradas para una aplicación de virtualización particular. Estos se conocen como ***dispositivos*** y permiten al usuario evadir una gran cantidad de trabajo de configuración. Para instalar un dispositivo Kali en VirtualBox, siga estos pasos:

- Vaya a la página de descarga de Seguridad ofensiva:

www.kali.org/downloads/

y haga clic en "Kali Virtual Images".

Figura 10: descargas de VM de Kali Linux

- Descargue "Kali Linux 64 bit VM" (o 32 bits si es necesario para su hardware). Descomprima el contenido del archivo descargado en su directorio deseado.
- Abra VirtualBox y elija "Importar dispositivo" en el menú archivo.

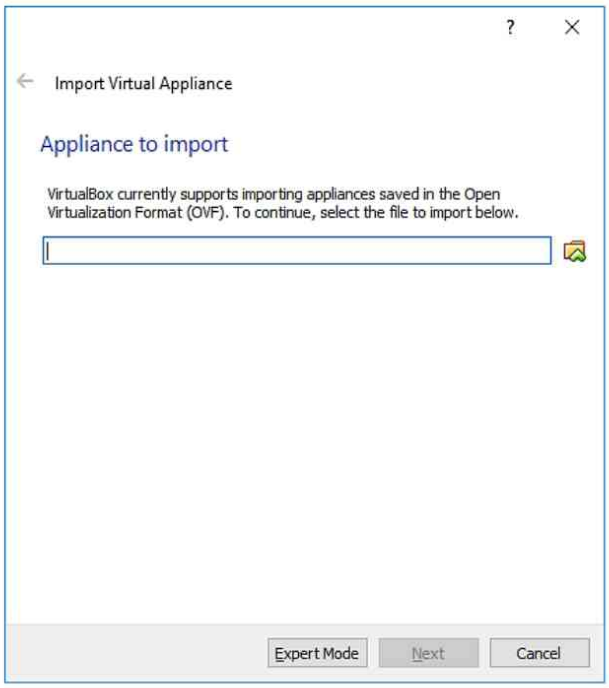


Figura 11 - Agregar dispositivo Virtualbox

- Navegue hasta el directorio que contiene el archivo ".vbox" y seleccione el dispositivo deseado.
- Haga clic en "Siguiente" para acceder a la página Configuración y realice los cambios que desee, luego haga clic en "Importar". Esto completará la instalación de VM.

Capítulo 3. Unidad De Arranque Externo Kali Linux

Una de las ventajas de los sistemas operativos Linux es que cada distribución se construye desde el núcleo con solo los paquetes y aplicaciones necesarias o deseadas para los propósitos de cada versión en particular. Esto ha resultado en distribuciones extremadamente "livianas" (es decir, de tamaño pequeño), pero completamente funcionales. El propósito original de desarrollar pequeñas distribuciones era satisfacer la necesidad de sistemas operativos "en vivo" que funcionen completamente para ejecutarse desde medios externos con espacio limitado, como CD-ROM y unidades flash USB, y hacer un uso eficiente de los recursos en algunas computadoras de plataformas antiguas. Desde entonces, las unidades flash han explotado en capacidad junto con la potencia de procesamiento, pero todavía se ha convertido en una especie de competencia y un punto de orgullo entre los desarrolladores de Linux, tanto aficionados como profesionales, para ver cuán pequeños pueden reducir una distribución funcional de Linux. Algunas distribuciones tienen un tamaño tan bajo como 12 MB.

Además de las consideraciones de capacidad y rendimiento del disco, sin embargo, a menudo se desea iniciar Linux desde medios externos por razones funcionales. Esto es particularmente cierto para las distribuciones derivadas de Debian / Knoppix cuyo propósito es proporcionar funciones de utilidad o seguridad para múltiples máquinas. La recuperación de datos, el restablecimiento de contraseñas y las funciones forenses a menudo deben realizarse fuera de los sectores de arranque de las máquinas en cuestión, por lo que es necesario arrancar las herramientas en medios separados. Además, las distribuciones especializadas como Kali no sirven necesariamente como sistemas operativos primarios e independientes para el uso diario, por lo que el arranque desde un medio externo según sea necesario desde una máquina deseada a menudo es más práctico. Este capítulo describe cómo crear una

unidad flash USB de arranque para Kali Linux. Esta unidad se puede utilizar como un sistema operativo en ejecución o como fuente de instalación.

Creando Una Unidad De Arranque Desde Windows

El sitio web de seguridad ofensiva contiene instrucciones detalladas sobre cómo crear una unidad de arranque Kali en vivo en varios sistemas operativos. Las instrucciones se pueden encontrar en:

http://docs.kali.org/downloading/kali-linux-live-usb-install

Esta sección resumirá las instrucciones para Windows y proporcionará algunas sugerencias adicionales.

IMAGEN DE DISCO WIN32

El programa Win32 Disk Imager incrusta una imagen de disco sin procesar en un dispositivo extraíble. Se puede descargar gratis desde el enlace de ***Sourceforge*** a continuación, así como desde otros repositorios de software libre en Internet.

https://sourceforge.net/projects/win32diskimager/

Para instalar una imagen de Kali con Win32 Disk Imager, siga estos pasos:

1. Descargue el archivo de instalación de Win32 Disk Imager y siga el procedimiento del asistente de instalación.
2. Inserte el USB o CD-ROM que desea utilizar como medio de arranque.
3. Inicie el programa Win32 Disk Imager. Tenga en cuenta que su máquina puede requerir privilegios administrativos para ejecutar este software.
4. En el cuadro "Archivo de imagen", navegue hasta la ubicación de su archivo .iso de Kali Linux.

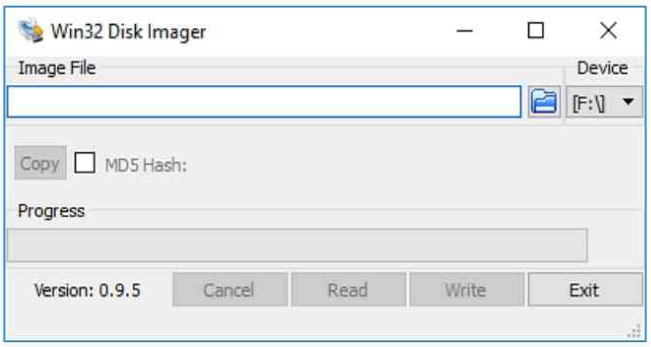


Figura 12 - Win32 Disk Imager

1. En "Dispositivo", seleccione la letra de unidad correspondiente al medio de destino. **¡Asegúrese de elegir el medio correcto, ya que los pasos posteriores sobrescribirán todos los datos!**
2. Haga clic en "Escribir" para completar el procedimiento.

YUMI

El Win32 Disk Imager es simple y útil. Sin embargo, para una mayor flexibilidad, el software Yumi Multi-boot es otra opción para crear una unidad USB Kali en vivo. Yumi está disponible gratuitamente, junto con las instrucciones, en el sitio web de Pendrivelinux:

https://www.pendrivelinux.com/yumi-multiboot-usb-creator/

Yumi se puede usar para crear dispositivos de arranque con una o varias opciones de distribución. Al arrancar, un medio Yumi mostrará las opciones de arranque en un menú.

Para instalar una imagen de Kali con Yumi, siga estos pasos:

1. Descargue el archivo de instalación de Yumi.
2. Inserte el USB o CD-ROM que desea utilizar como medio de arranque.
3. Inicie Yumi (no hay procedimiento de instalación, Yumi se ejecuta directamente como un .exe).
4. En "Seleccione la letra de unidad de su dispositivo USB", elija la letra de unidad correspondiente a la unidad USB de destino.

¡Asegúrese de elegir el medio correcto, ya que los pasos posteriores sobrescribirán todos los datos!

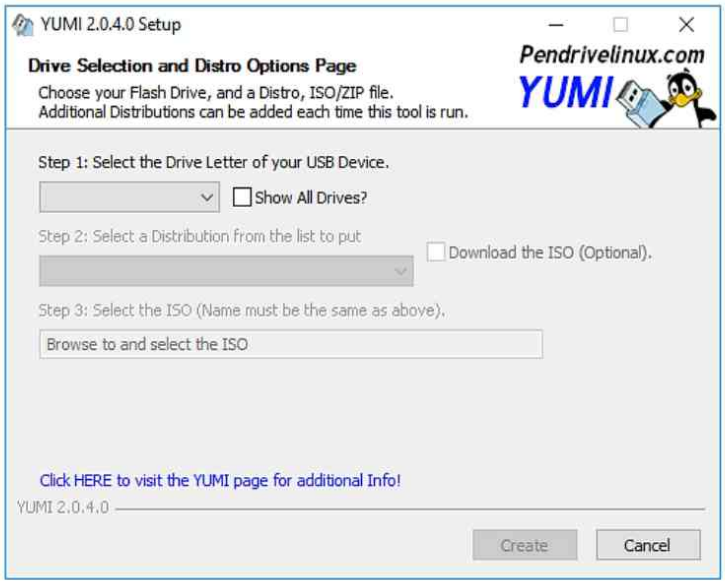


Figura 13 - Pantalla principal de Yumi

1. En el cuadro "Seleccione una distribución para poner en...", elija Kali (busque en "Herramientas del sistema"). Kali Linux .iso archivo.
2. En el cuadro "Examinar y seleccionar su kali * .iso", navegue hasta la ubicación de su archivo Kali Linux .iso.
3. Haga clic en "Crear" para completar el procedimiento.

Crear Una Unidad De Arranque Desde Os X O Linux

Crear un disco de arranque desde una plataforma Linux u OS X requiere instrucciones avanzadas de línea de comandos. Se recomienda que consulte el sitio web de seguridad ofensiva (a continuación) para obtener instrucciones actualizadas sobre cómo crear un medio Kali en vivo.

http://docs.kali.org/downloading/kali-linux-live-usb-install

Capítulo 4. Comandos Esenciales De Terminal De Linux

Antes de la aparición de las interfaces gráficas de usuario y los dispositivos de entrada ergonómicos, como los ratones, los usuarios de computadoras solo tenían su teclado y una pantalla monocromática con un aviso. Los comandos se ingresaron línea por línea y se interpretaron en el acto o se compilaron en masa en un programa. Para interactuar con el sistema de archivos o los periféricos (a través del núcleo), los usuarios tuvieron que emplear un léxico de comandos especiales para realizar las acciones deseadas. Los sistemas Unix originales, de hecho, se iniciaron directamente en un terminal de comando (generalmente una solicitud de inicio de sesión) para esperar la entrada. Aunque la mayoría de las distribuciones modernas de Linux ahora se inician en una GUI, el sistema de comando de terminal de Unix todavía subraya el sistema operativo. Se puede hacer que cualquier sistema Linux arranque directamente en la línea de comandos, pero la mayoría de los usuarios abren la aplicación ***Terminal*** desde el escritorio de la GUI principal si desean ingresar comandos directamente.

Aunque las interfaces gráficas de "apuntar y hacer clic" son convenientes y generalmente más intuitivas, los usuarios avanzados de Linux, especialmente los hackers, a menudo prefieren usar el terminal para ejecutar comandos. Escribir un comando de Linux manualmente no solo es, en muchos casos, más eficiente, sino que también le da al usuario un control más directo sobre las operaciones. Un solo comando de una línea, ingresado correctamente, puede reemplazar múltiples clics y ventanas anidadas. Además, al ingresar un comando directamente, el usuario puede rastrear más fácilmente la fuente de los errores. Los hackers tienden a ser individuos independientes y autosuficientes, y detestan ceder el control de su máquina a procesos automatizados escritos por otros.

Este capítulo discutirá cómo navegar en Linux a través de la Terminal e

introducirá algunos de los comandos de shell más críticos.

Anatomía Del Sistema Linux

Antes de ingresar a la lista de comandos, es importante comprender la estructura básica y el sistema de archivos de una distribución típica de Linux. La biblioteca de comandos es muy poderosa y puede controlar prácticamente cualquier aspecto de la operación o configuración de un sistema Linux.

Arquitectura

Todos los sistemas Linux están construidos hacia arriba desde el núcleo. El núcleo es el conjunto de instrucciones a nivel de máquina que se carga en la memoria cuando se inicia el sistema operativo. Las instrucciones del kernel interactúan directamente con el hardware de la máquina, incluidos los procesadores, la memoria, la interfaz de red y cualquier periférico.

El shell de Linux (Figura 14) es el medio por el cual un usuario interactúa con el núcleo. El shell puede ser un símbolo del sistema directo o una interfaz gráfica de usuario.

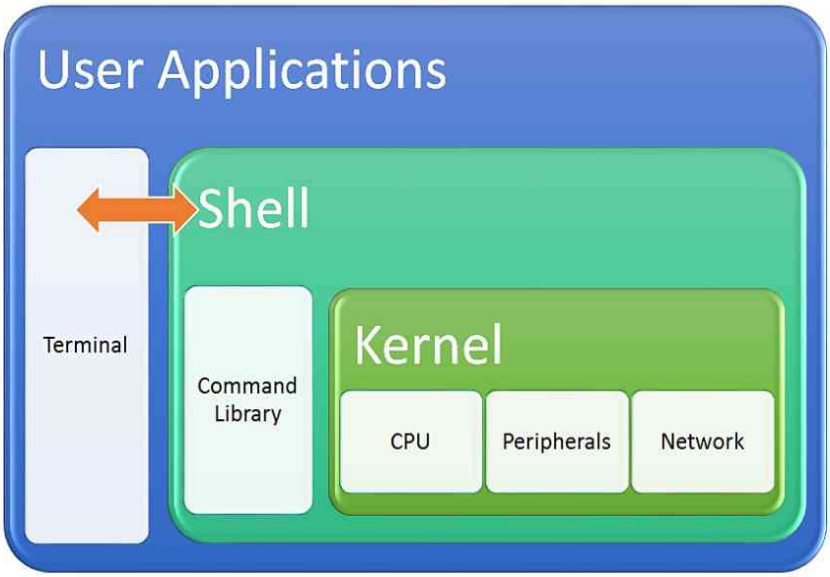


Figura 14 - Arquitectura del kernel de Linux

EL SISTEMA DE DIRECTORIO

Linux tiene una estructura de directorio organizada que está diseñada para compartimentar archivos para seguridad y estabilidad. Las rutas de directorio

usan la barra diagonal (/) para separar los nombres de directorio posteriores en la ruta, a diferencia de Windows que usa la barra invertida (\). El término "raíz" a veces puede ser confuso para los principiantes de Linux porque hay algunas ubicaciones que pueden denominarse directorio raíz. La verdadera "raíz" en un sistema de archivos de Linux, en la medida en que no hay directorios principales por encima, se designa simplemente con una barra diagonal, "/". Todos los demás directorios se encuentran debajo de esta ubicación. Los directorios bajo "/" varían ligeramente entre las distribuciones de Linux, pero la estructura general fue heredada del sistema Unix original y es en gran medida universal.

Figura 15 - Estructura del directorio de Linux

Comandos De Linux

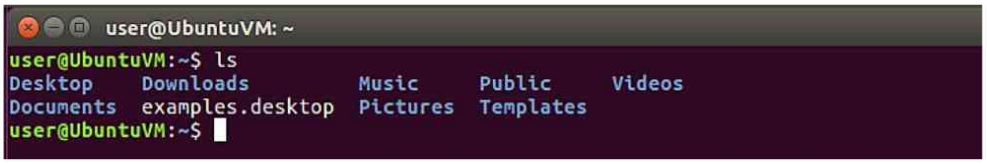
Linux tiene un rico conjunto de comandos de terminal, muchos de los cuales son iguales o similares a los del sistema operativo Unix original. Estos comandos permiten a los usuarios administrar y manipular archivos y carpetas, instalar software, interactuar con periféricos y, entre muchas otras tareas, realizar diversas operaciones de red. Aunque los comandos de Linux se introducirán en contexto en varias secciones a lo largo de este libro, los siguientes comandos básicos sirven como introducción al léxico básico de Linux y el formato general y el uso de comandos de terminal.

DIRECTORIOS Y ARCHIVOS

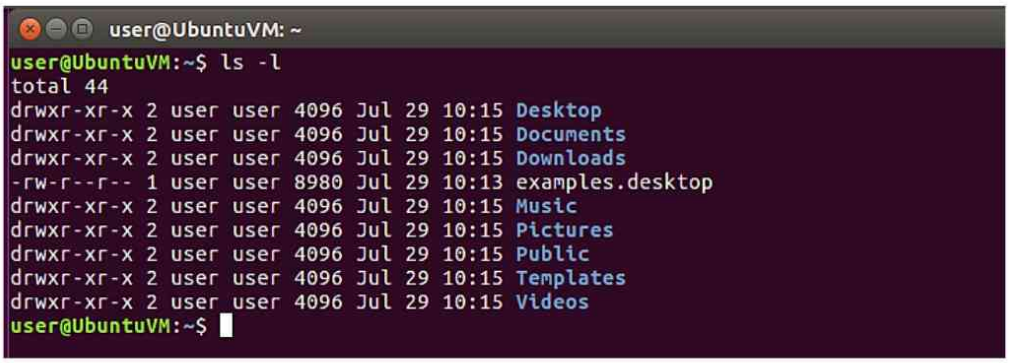
Los primeros comandos que un usuario de Linux debe aprender son los asociados con la navegación y manipulación de directorios. Una vez en el símbolo del sistema del terminal, el siguiente comando enumerará los archivos y el directorio presentes en el directorio raíz:

ls

En la mayoría de los casos, el directorio de terminal predeterminado será "/home/username", por lo que al escribir "ls" se enumerará el contenido de los archivos y carpetas del usuario actual.

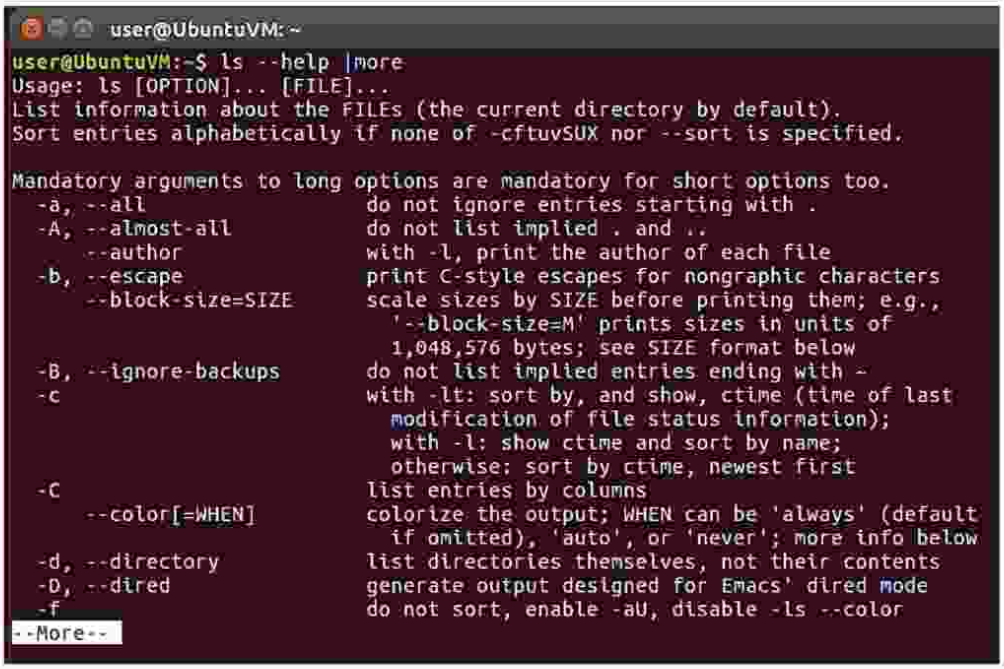


La mayoría de los comandos de Linux presentan opciones que se pueden agregar al formulario de comando predeterminado. Estas opciones varían para cada comando y van desde cambiar el formato de la salida hasta indicarle al comando que realice funciones específicas que no realiza de manera predeterminada. La opción "-l" para el comando ls es un ejemplo de una opción de comando que da como resultado una salida más detallada.



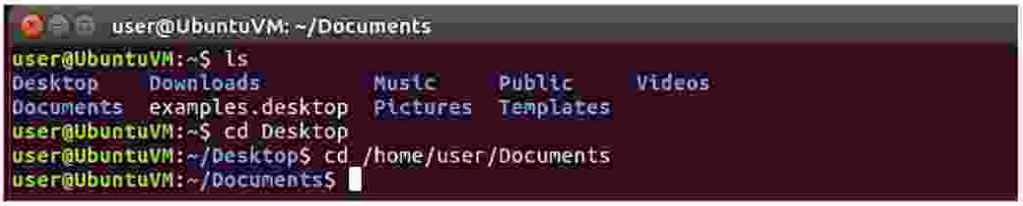
Tenga en cuenta que la lista del directorio ahora contiene detalles para cada archivo y carpeta en el directorio actual, incluidos los permisos de acceso, el tamaño y la fecha de creación. Las opciones están precedidas por varios símbolos (-, --, |, etc.) dependiendo de la naturaleza del comando ans y la opción. Muchas opciones se pueden encadenar en un solo comando, lo que las convierte en una forma poderosa de lograr muchas cosas en una sola línea de código eficiente.

Para mostrar las opciones de un comando en particular, junto con otra información útil, se puede agregar el comando con "--ayuda". Sin embargo, la salida de ayuda para los comandos mot tiene varias páginas y no se puede ver en una ventana de terminal sin desplazarse. Adjuntando el "| más" opción hará una pausa después de una sola página de salida, permitiendo al usuario avanzar página por página presionando la barra espaciadora hasta que se complete la salida.



El comando cd permite al usuario cambiar el directorio activo a una ubicación específica. Se supone que una ruta dada es relativa al directorio actual a menos que se construya de otra manera. Para cambiar a un directorio dentro de la ruta activa actual, simplemente agregue cd con ese nombre de directorio. Tenga en cuenta que los nombres de archivos y directorios de Linux distinguen entre mayúsculas y minúsculas.

Para cambiar a una ruta que no está en el directorio activo, se debe especificar la ruta absoluta.



La siguiente es una breve lista de directorios útiles de Linux y comandos de archivos. De ninguna manera es una lista completa, sino que representa algunos de los comandos más comunes. Se debe tener cuidado con algunos de estos comandos, ya que pueden cambiar o eliminar el contenido o la

ubicación de un archivo o carpeta.

Command	Action
pwd	Muestra la ruta del directorio activo
ls	Muestra el contenido del directorio activo
cd	Cambia el directorio activo
mkdir	crea un nuevo directorio
rmdir	elimina un directorio (si está vacío)
cp	Copiar un archivo
mv	Mover un archivo
rm	Eliminar un archivo

ACCESO "SUPERUSUARIO": EL COMANDO SUDO

Un comando más importante de Linux es el infame comando "sudo", uno que todo aspirante a hacker debería conocer. El término "sudo" es (según se informa) abreviatura de "superuser do" e indica al núcleo que el comando posterior se ejecutará con acceso root (o, a veces, como un usuario diferente del que está conectado actualmente).

Arriba, un usuario navegó a la carpeta Documentos de otro usuario, pero se le negó el permiso para eliminar un archivo llamado "contraseñas". Cuando el comando se volvió a emitir usando sudo, se le solicitó al usuario una contraseña y luego el comando rm se ejecutó con éxito.

Capítulo 5. Conceptos Básicos De La Red

La forma más directa, por supuesto, de obtener acceso a un sistema en particular sería directamente desde el terminal de interfaz del dispositivo objetivo. Esto presenta muchos obstáculos para el hacker porque requiere que obtenga acceso físico al sistema, exponiéndolo a ser descubierto o dejando rastros de su presencia. Sin embargo, la naturaleza en red de la mayoría de las computadoras y la tecnología de la información proporciona vías más seguras y menos visibles para la explotación: la red.

En general, una red es cualquier colección de partes interconectadas. Hay redes de personas, organizaciones, estados políticos, máquinas y casi cualquier grupo de entidades en el que la información pasa entre los miembros. Las redes informáticas y de TI han crecido y se han combinado para conectar miles de millones de nodos, desde pequeñas redes domésticas con uno o dos dispositivos informáticos personales hasta enormes granjas de servidores que requieren sus propios motores.

Ya sea enviando información de contacto de un teléfono inteligente a otro con una conexión Bluetooth, o transmitiendo una película a través de Internet desde Moscú a Buenos Aires, los conceptos básicos de redes y comunicación son los mismos. Comprender los protocolos de comunicación y redes de computadoras es esencial para convertirse en un hacker efectivo.

Componentes De Red Y Arquitectura

Todo lo que se necesita es un mínimo de dos dispositivos informáticos conectados de alguna manera para compartir información, y usted tiene una red informática (Figura 16). Cualquier dispositivo capaz de algún tipo de conectividad puede comprender un nodo en una red. Las plataformas de usuario tradicionales como servidores, PC de escritorio, computadoras portátiles, tabletas y dispositivos de mano personales como los teléfonos inteligentes son comunes en las redes. También hay un número cada vez mayor de periféricos en red y dispositivos inteligentes independientes como impresoras, televisores, plataformas de juegos, cámaras de red, consolas de entretenimiento, dispositivos de audio y relojes. Cada dispositivo generalmente puede conectarse a varios otros dispositivos a través de diversos medios de comunicación. Las conexiones físicas como el cableado de cobre y el cable de fibra óptica sirven como una red troncal para Internet global y conectan la mayoría de las redes hasta el punto de acceso principal de una red de área local. Dentro de una LAN, puede existir cualquier número de tipos de conexión, incluido el cableado físico y Wi-Fi. A distancias cortas, los dispositivos pueden conectarse a través de Bluetooth o tecnología de comunicación de campo cercano (NFC). Junto a esta arquitectura hay una creciente red celular de banda ancha que consiste en cualquier conjunto de torres de radiofrecuencia que están conectadas a la red troncal de Internet y a varios satélites. A medida que mejora la tecnología celular de banda ancha, el uso se expande más allá de los teléfonos y se está convirtiendo en la principal metodología de acceso a Internet para muchos dispositivos individuales y redes pequeñas.

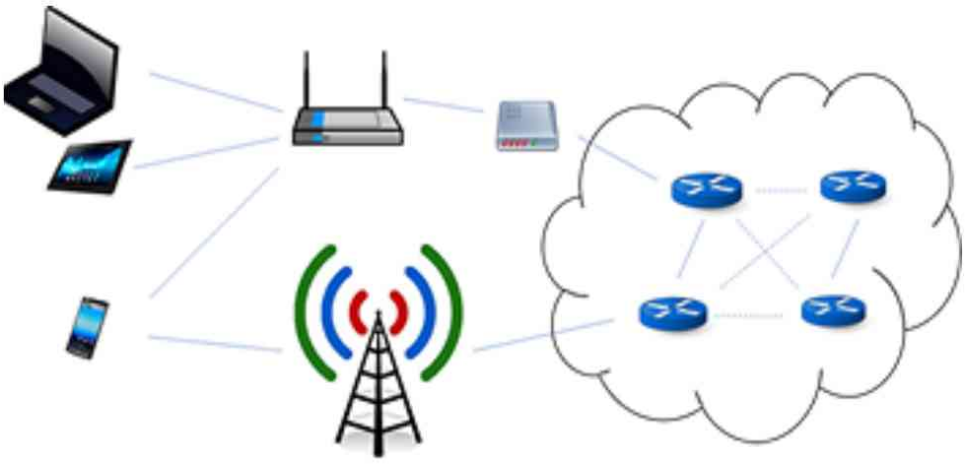


Figura 16 - Componentes de red

Modelos Y Protocolos De Red

Independientemente del tipo de nodo o medio de comunicación, dos dispositivos deben comunicarse utilizando algún tipo de protocolo común. Es necesario un protocolo estándar utilizado por todos los dispositivos a través de una red para evitar la falta de comunicación. El Protocolo de Internet (IP) existía desde los primeros días de la creación de redes. Aunque ha cambiado un poco en forma y función, sigue siendo el estándar de facto para la comunicación de red. IP, combinado con otro estándar conocido como Protocolo de Control de Transmisión (TCP) forma un paradigma de red en capas llamado TCP / IP. Este esquema divide una red en varias capas desde el hardware básico de la red hasta la aplicación del usuario. La colección de protocolos es un modelo conceptual de comunicación de red conocido como el modelo TCP / IP, o "pila" TCP / IP. Existe otro modelo conocido como el modelo de interconexión de sistemas abiertos (OSI), que es más granular con respecto al número de capas. El modelo OSI se puede aplicar de manera más general, pero describe los mismos principios esenciales que el modelo TCP / IP.

EL MODELO TCP / IP

El modelo TCP / IP consta de cuatro capas conceptuales apiladas que tienen un papel que desempeñar en la preparación y el transporte de datos de un punto en una red a otro. Estas son las capas de aplicación, transporte, red y enlace de datos (o enlace).

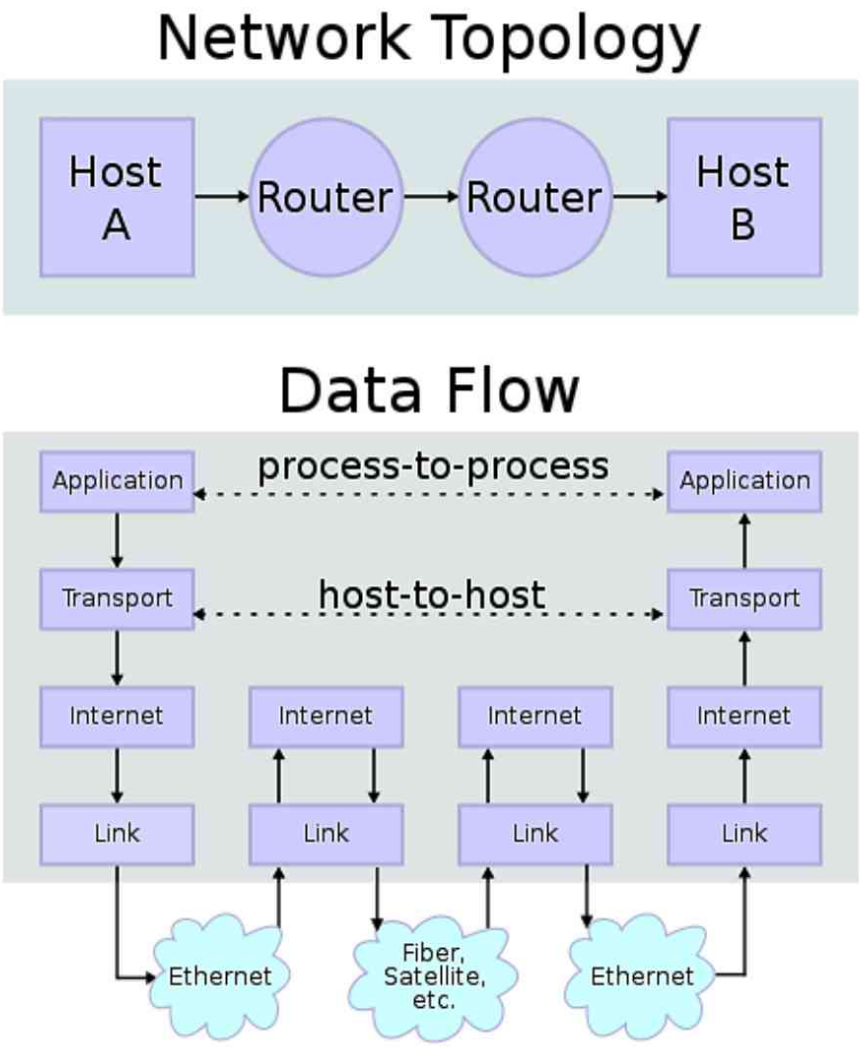


Figura 17 - Flujo de datos de red en capas (infosecinstitute.com)

La capa de aplicación de la pila TCP / IP (considerada la capa "superior") es la capa más visible y accesible para el usuario. Esta es la capa donde se crea el contenido o la carga útil de una comunicación antes de que se empaquete para su transporte. Los clientes de correo electrónico, navegadores web, software para compartir archivos, aplicaciones de transmisión de video y otras aplicaciones conectadas, todos operan en la capa de aplicación. Vale la pena señalar que la capa de aplicación ejecuta otros protocolos que residen dentro (o por encima) de TCP / IP. Esto incluye el protocolo de transferencia de hipertexto (HTTP) de aplicaciones web, smtp para correo electrónico y el Protocolo de transferencia de archivos (FTP), entre otros.

El funcionamiento en la capa de transporte es un concepto avanzado, pero basta con decir que esta capa ayuda a garantizar la calidad de la comunicación mediante la verificación de errores y otros medios. Además, la capa de transporte es donde la información pasada desde una aplicación se divide inicialmente en paquetes, que luego se agregan con encabezados apropiados. TCP funciona a este nivel, pero no es el único protocolo disponible. El protocolo de datagramas de usuario, o UDP, se usa cuando es necesario sacrificar la llegada exitosa de una pequeña cantidad de paquetes a cambio de la entrega de información en tiempo real. UDP es el protocolo de transporte elegido para la transmisión de audio y video.

La capa de red, a menudo llamada capa de Internet, es donde se realiza el trabajo de enrutamiento de paquetes. En esta capa, se determina la mejor ruta de red para un paquete, luego el encabezado del paquete se agrega con una dirección IP de origen y de destino antes de que se transmita al hardware de la interfaz de red. Existen otros protocolos que pueden operar en esta capa, pero la IP es, con mucho, la más frecuente y es la estructura subyacente para la mayoría de las comunicaciones de datos globales. La manipulación de encabezados IP en varias etapas de tránsito es la base de muchos ataques de hacking.

La capa inferior del modelo TCP / IP es la capa de enlace de datos o hardware. La capa de hardware es la última parada de un paquete de datos antes de abandonar su máquina de origen y llegar a su próximo destino a través del medio físico. Las direcciones MAC del hardware de redes involucradas en la retransmisión del paquete se agregan al encabezado del paquete en este nivel.

Protocolos De Red

Cuando un nodo en una red se comunica con otro, divide su mensaje en paquetes pequeños e independientes. Luego, cada paquete se agrega con un encabezado a medida que pasa a través de cada capa para que pueda volverse a ensamblar correctamente en un mensaje en su destino. La belleza de TCP / IP es que cada paquete individual puede tomar una ruta diferente y puede reenviarse si se pierde, asegurando un alto grado de eficiencia y fidelidad de mensaje.

En el corazón de TCP / IP está la dirección IP. Cada dispositivo en una red tiene una dirección única para identificar su ubicación dentro de la red y cualquier subred a la que pertenece. Comprender el direccionamiento IP porque les permite concentrarse en objetivos particulares. Además, los piratas informáticos pueden necesitar ocultar o manipular su propia dirección IP para permanecer visibles.

La versión estándar de IP ha sido IP v.4 durante muchos años y se usa en la mayoría de las redes y dispositivos. IP v.6 es un nuevo estándar que puede acomodar muchas más direcciones. Dentro de una LAN individual, el primer octeto en una dirección IP generalmente indica la designación de la red global, con octetos posteriores que designan subredes y máquinas individuales.

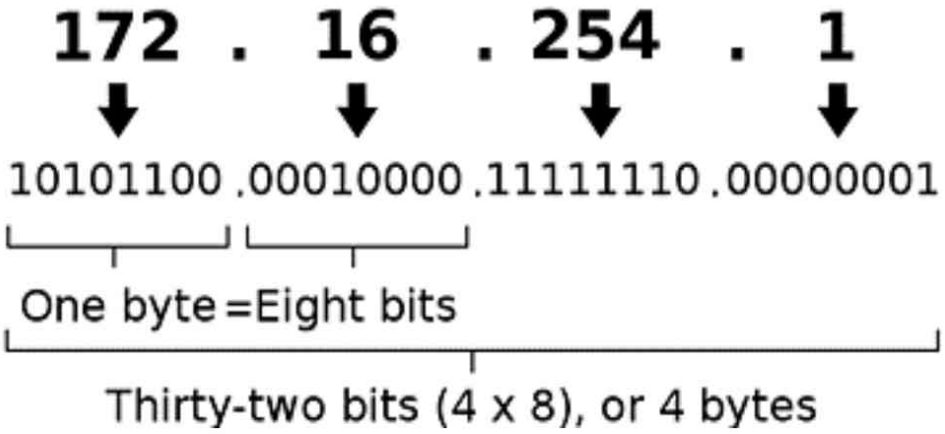


Figura 18 - Notación de dirección IP

Una de las cosas más importantes que debe comprender sobre el direccionamiento IP es que la dirección IP de un nodo dado dentro de una red local

es diferente de la que se le asigna cuando se comunica a través de Internet. Esto se debe a que es imposible controlar o evitar que dos máquinas individuales en redes separadas reciban accidentalmente o intencionalmente la misma dirección.

Desde la perspectiva del hacker, las direcciones IP proporcionan una hoja de ruta en cualquier red individual para identificar y distinguir máquinas individuales. Además, tanto impuesto implicó interceptar paquetes de datos individuales en tránsito en la red. La información del encabezado en el paquete contiene la dirección IP de nacimiento, el origen y el destino. Es la manipulación de estos encabezados lo que permite a los médicos conducir al hombre en el medio y los ataques de denegación de servicio. Es la manipulación de estos encabezados lo que permite a los golpeadores conducir al hombre en el medio y los ataques de denegación de servicio.

Las direcciones IP se consideran direcciones lógicas, lo que significa que se asignan mediante software, ya sea directamente por el usuario o automáticamente a través de algún tipo de proceso. Las direcciones IP residen en la capa de red. En muchos casos, las direcciones IP pueden ser falsificadas o falsificadas en un encabezado de paquete. Esto se puede hacer para ofuscar la fuente de un correo electrónico u otra carga útil de ataque, o para redirigir maliciosamente los paquetes.

Es importante comprender que la falsificación de IP no se puede utilizar para ocultar ninguna comunicación bidireccional. Para que dos máquinas intercambien información, sus direcciones deben ser válidas o los paquetes que se intercambian no pueden llegar a sus destinos. Esta es la razón por la cual es inútil tratar de ocultar o cambiar las direcciones IP cuando se opera en un servicio punto a punto, u ocultar la designación de un nodo de descarga. Lo mejor que se puede esperar en este escenario es enrutar la información a través de un gran número de servidores proxy geográficamente y lógicamente

distintos. La red TOR, que sirve de base para Dark Web, funciona creando múltiples capas a través de las cuales puede pasar la información.

Otro tipo importante de identificador de dispositivo es la dirección MAC (Control de acceso a medios). Las direcciones MAC se consideran direcciones físicas permanentes y se asignan a dispositivos de interfaz de red individuales. El esquema de direccionamiento MAC está diseñado para que no haya dos dispositivos que, en teoría, tengan la misma designación. La dirección se graba en la ROM del dispositivo para que no se pueda cambiar fácilmente. Las direcciones MAC son parte de la capa de enlace de datos.

Aunque las direcciones MAC están destinadas a ser permanentes, hay formas de "falsificar" una dirección escribiendo una dirección falsa en un encabezado de paquete. Esto no cambia la dirección permanente de un dispositivo, pero permite que un hacker evite ser identificado a través de su interfaz de red. Si un atacante con un MAC falsificado obtiene acceso local a una red, especialmente a través de medios inalámbricos, puede evitar ser rastreado a través de su hardware.

DETERMINAR LOS PARÁMETROS DE LA RED

Para buscar la dirección IP de una máquina Linux, así como las direcciones MAC de cualquier dispositivo de interfaz de red, escriba

```
# ifconfig
```

en una ventana de terminal. La dirección IPv4 de la máquina actual en la red local se proporciona en el campo "inet addr" en la sección del adaptador de red (en este caso, "enp0s3"). La dirección MAC del adaptador de red aparece (en este caso parcialmente oculta) en el campo "HWaddr".

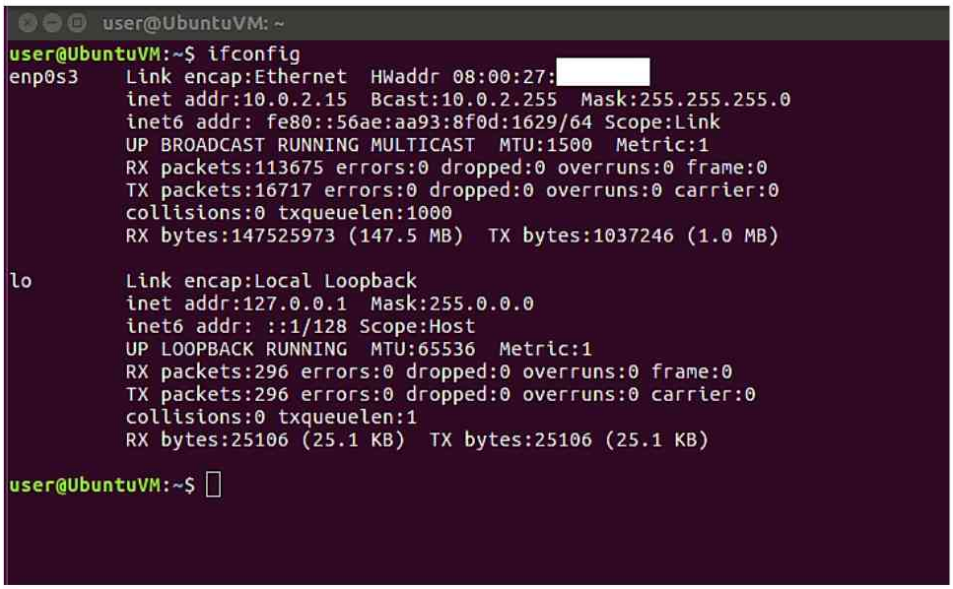


Figure 19 – Resultados de ifconfig

Un comando útil de Linux para ilustrar la ruta de un paquete a través de Internet es ***traceroute***. El comando traceroute muestra la dirección IP de cada ubicación, o "salto", que se utiliza para transmitir un mensaje desde su origen a su destino. También muestra medidas del tiempo (en milisegundos) de un viaje de ida y vuelta entre cada salto y el salto siguiente. Hay múltiples opciones para un comando traceroute, pero la demostración más simple es ejecutar traceroute a un destino común. El destino se puede ingresar como una URL web o una dirección IP conocida. (Tenga en cuenta que traceroute es nativo en Kali Linux, pero si el comando no funciona en su versión de Linux, es posible que deba instalarse con el comando:

sudo apt install traceroute

Además, si está utilizando Linux en una máquina virtual, debe configurarse para usar una conexión de ethernet con puente al adaptador de la máquina host, o el traceroute no funcionará correctamente.) Para rastrear un paquete desde la fuente del terminal a un común, estable destino como Google (el comando equivalente en un terminal de Windows es ***tracert***):

traceroute -q 1 google.com

La opción "-q 1" limita cada salto a una consulta para una salida más rápida y

simple.

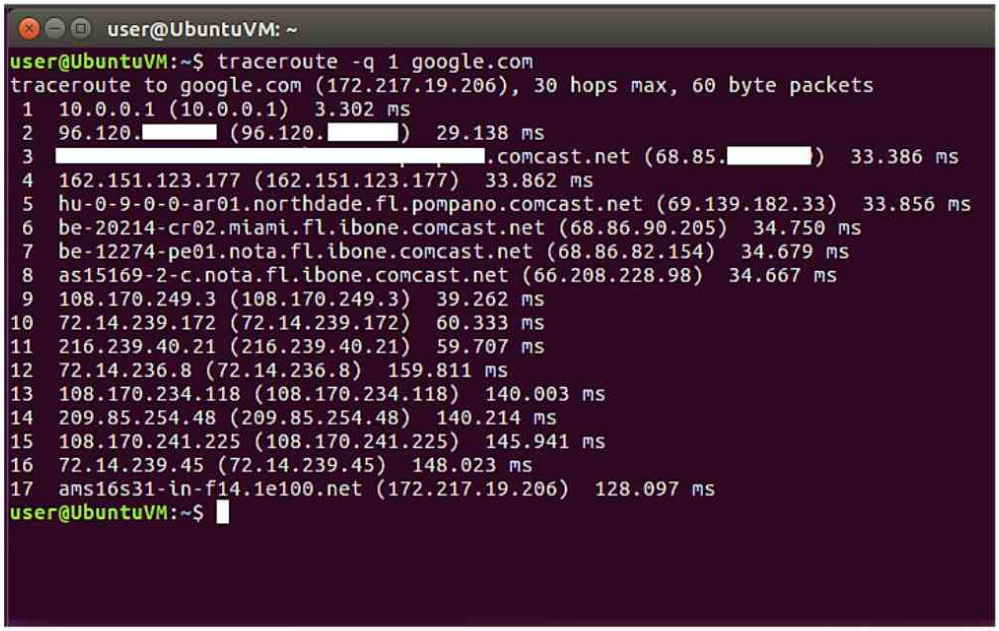


Figura 20 - resultados de traceroute

La primera ubicación, 10.0.0.1, es la dirección IP local del enrutador de red. La IP asignada públicamente del origen no aparece en una ruta de seguimiento. (Puede encontrar su dirección IPv4 o IPv6 a través de cualquier número de sitios web. Simplemente escribiendo algo como "cuál es mi ip" o "cuál es mi ipv4" en un motor de búsqueda mostrará múltiples sitios web que mostrarán libremente su información). En este ejemplo representa el primer punto de contacto con el proveedor de servicios de internet (ISP). Se puede ver cómo cada salto posterior viaja a través de la infraestructura del ISP hasta que llega a la red troncal de Internet y luego se mueve hacia su destino.

Es posible asignar cada dirección IP a una ubicación física utilizando algunos servicios en línea. Esto se puede usar para crear un mapa de saltos desde el origen hasta el destino. Estos pueden ser interesantes e ilustrativos, pero deben tratarse con cuidado porque no se garantiza que la información sea precisa o esté actualizada.

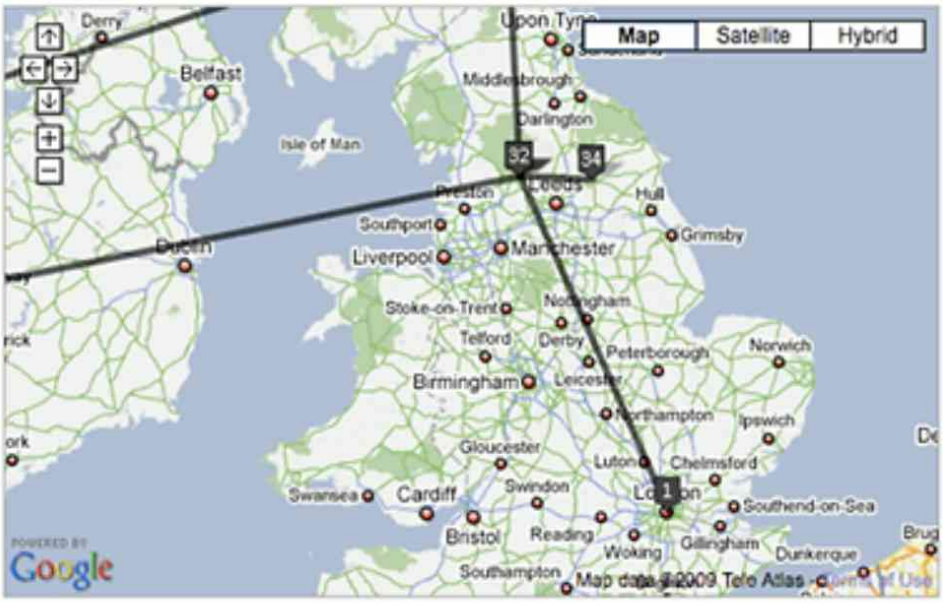


Figura 21 - Trazador de ruta visual

El comando ***ping*** también se puede usar para probar el tiempo entre el origen y el destino, pero sin incluir el tiempo entre saltos individuales. El comando ping se usa con mayor frecuencia para simplemente probar la conectividad entre nodos. La forma más simple de "hacer ping" es simplemente escribir el comando junto con la URL de destino o la dirección IP:

```
user@UbuntuVM: ~
File Edit View Search Terminal Help
user@UbuntuVM:~$ ping google.com
PING google.com (216.58.212.238) 56(84) bytes of data.
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=1 t
tl=48 time=128 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=2 t
tl=48 time=127 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=3 t
tl=48 time=131 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=4 t
tl=48 time=127 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=5 t
tl=48 time=138 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=6 t
tl=48 time=131 ms
64 bytes from ams16s22-in-f238.1e100.net (216.58.212.238): icmp_seq=7 t
tl=48 time=133 ms
^C
--- google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 127.199/131.226/138.841/3.748 ms
user@UbuntuVM:~$
```

Figura 22 – Resultados ping

El programa hará ping indefinidamente hasta que se agote el tiempo de espera o hasta que el usuario lo interrumpa (el interruptor "-c" limita el

número de intentos de ping a los especificados). Tenga en cuenta que la salida contiene la dirección IP de la URL marcada. El comando ***ping6*** se puede usar alternativamente para determinar la dirección IPv6 de una ubicación.

Capítulo 6. Tor Y La Red Oscura

El equilibrio entre la privacidad y la seguridad es una lucha perpetua, particularmente en un mundo que está floreciendo con la propagación de la democracia y las amenazas existenciales del terrorismo. Esto se complica aún más por el juego del gato y el ratón entre las autoridades, los delincuentes y aquellos que desean permanecer en el anonimato en línea. Ya sea para proteger simplemente la privacidad personal o para ocultar actividades nefastas, el deseo de comunicación anónima en Internet ha dado lugar a varios mecanismos que se están desarrollando para ese propósito. La red Tor es un sistema popular que consiste en personas de ideas afines que usan software de código abierto para crear una serie de conexiones virtuales entre usuarios. Utilizada correctamente, la red Tor puede frustrar significativamente los esfuerzos para rastrear las comunicaciones que viajan a través de ella.

El Sistema Tor

Tor es un acrónimo de "The Onion Router", que se refiere a la naturaleza en capas de la red (como las capas de una cebolla), por el cual un mensaje se envuelve dentro de múltiples niveles de cifrado. La función de Tor esencialmente se reduce a enrutar un mensaje a través de múltiples nodos de tal manera que resista los intentos de análisis de tráfico. Antes de enviar un mensaje, el cliente de origen crea una ruta prácticamente aleatoria, un salto a la vez, a través de otros nodos participantes. Cada nodo solo conoce la ubicación de los nodos inmediatamente anteriores y posteriores a él porque toda la otra información del encabezado está encriptada con su propia clave. Una vez que se establece una ruta, el tráfico seguro puede comenzar entre el origen y el destino. Sin embargo, para mantener la seguridad, se calcula una nueva ruta cada varios minutos. Los relés a través de los cuales pasan las comunicaciones en Tor son servidores gestionados por voluntarios de todo el mundo.

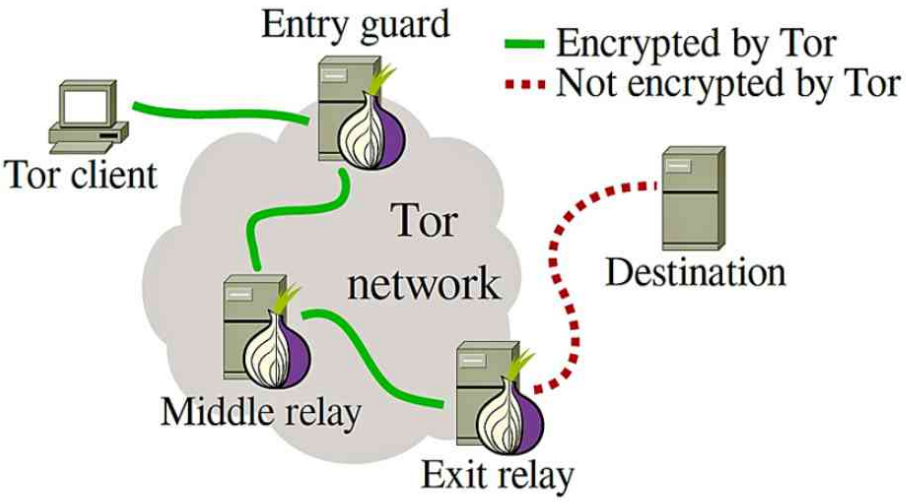


Figura 23 - La red Tor

EL NAVEGADOR TOR

El método más común para acceder a la red Tor es a través de un navegador Tor. El navegador Tor es una versión modificada del navegador web de

código abierto Mozilla Firefox (versión de soporte extendido). El navegador presenta varias extensiones de Firefox junto con el proxy Tor que establece una conexión con el enrutador Onion. También está configurado por defecto para no guardar cookies e historiales de navegación.

El navegador Tor es gratuito y se puede descargar e instalar para plataformas Windows, Mac y Linux. También hay una aplicación Tor móvil llamada Orbot que se ejecuta en dispositivos Android. El navegador se puede descargar desde el sitio web principal del Proyecto Tor.

https://www.torproject.org/projects/torbrowser.html.en

Hay versiones de 32 bits y 64 bits disponibles (solo una de 64 bits para Mac) en varios idiomas, incluida la última versión estable y algunas versiones experimentales/beta.

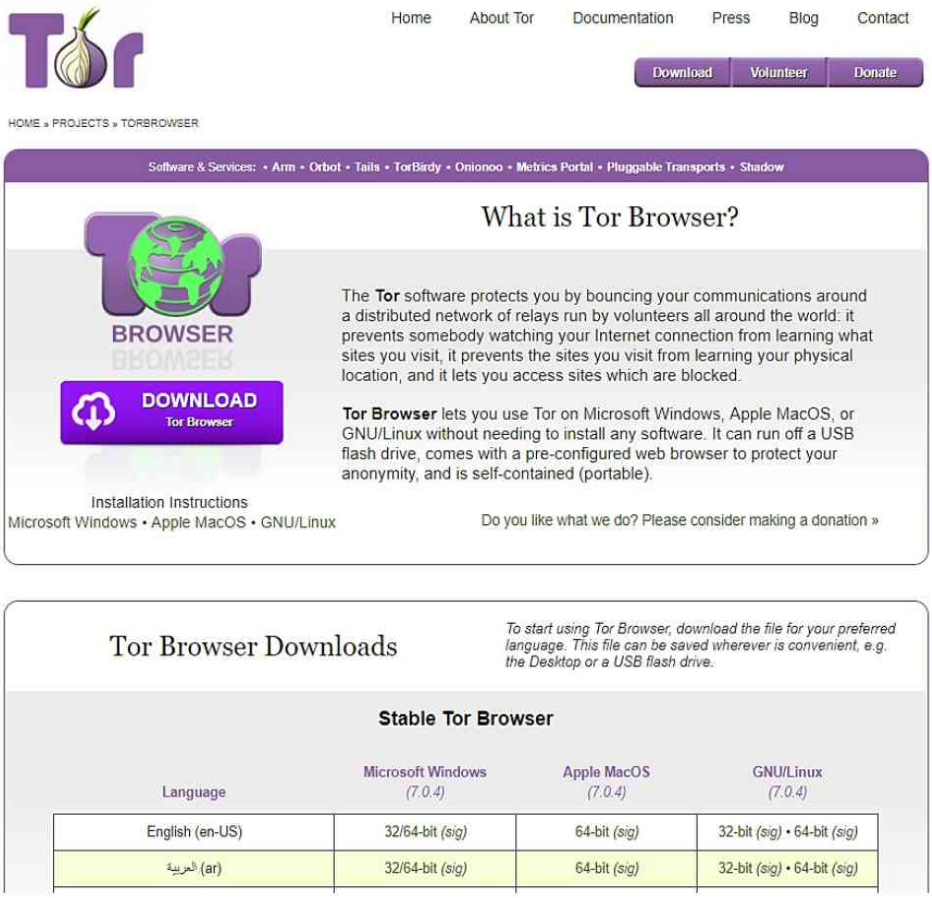


Figura 24 - Página de descarga de Tor

La versión de Windows se instala a través de un "asistente" típico. Sin

embargo, si la máquina host está detrás de un proxy o firewall, pueden ser necesarios pasos de configuración adicionales. Para Mac, simplemente haga clic en .dmg para extraer, luego arrastre la aplicación resultante a la carpeta Aplicaciones.

Las instrucciones para instalar el navegador Tor en plataformas Linux requieren algunos comandos de terminal y pasos de configuración que pueden variar entre las distribuciones. El sitio web de Tor tiene algunas instrucciones generales, pero hay pasos específicos (y, a menudo, algunas soluciones de problemas) para que el navegador funcione correctamente en ciertas plataformas, especialmente Kali Linux. Estos pasos adicionales generalmente se pueden encontrar fácilmente a través de una búsqueda en Internet o en la página de inicio de distribución. Algunas distribuciones también pueden tener el navegador Tor disponible en su repositorio de software que se puede instalar a través de la aplicación de instalación de software en la GUI del sistema operativo.

La Web Oscura

La "Web oscura" es un término que se refiere a los contenidos de Internet a los que solo se puede acceder mediante protocolos de anonimato y enrutamiento como la red Tor (es un error común pensar que la Web oscura y la "Web profunda" son términos intercambiables, pero "Deep Web" simplemente se refiere a los sitios en la World Wide Web que no están indexados por los motores de búsqueda.) La naturaleza anónima de la comunicación en la Dark Web es fuente de gran controversia en todo el mundo porque tal anonimato eventualmente lleva a proliferación de contenido objetable, y a veces peligroso. Además de servir como un posible canal de comunicación para terroristas, la Deep Web facilita la distribución abierta de narcóticos ilegales, armas, información financiera robada y pornografía ilícita, entre otras cosas. Sin embargo, el sistema también proporciona a las personas que viven bajo regímenes represivos su único acceso a ciertos tipos de información.

ACCEDIENDO A TOR

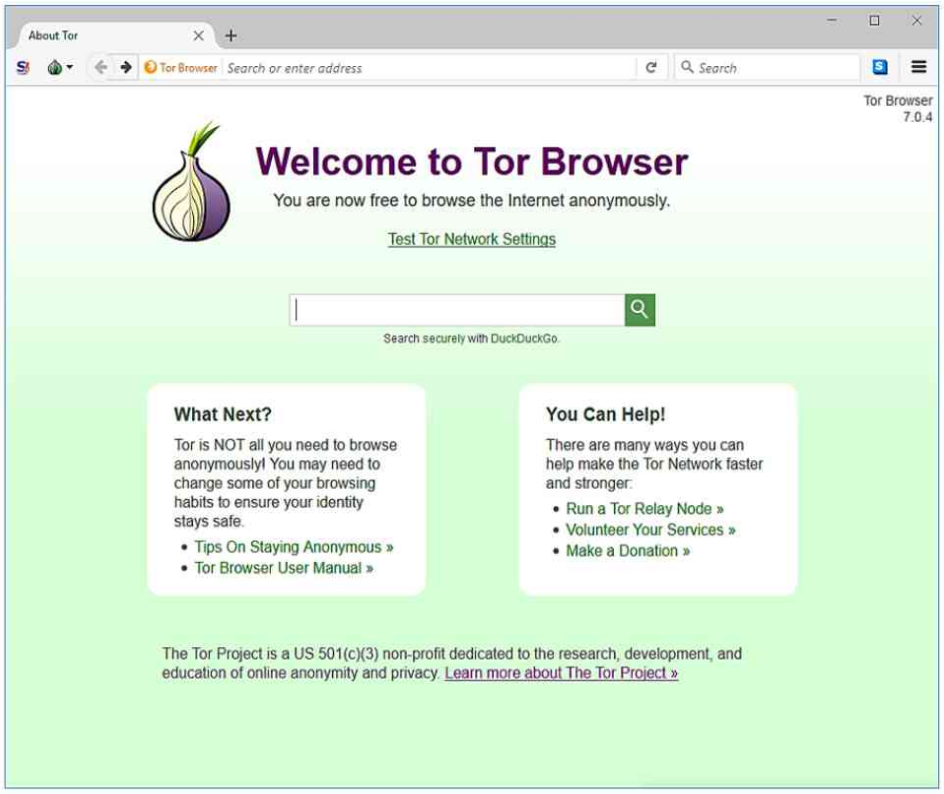


Figura 25 - Página de inicio del navegador Tor

Al iniciar el Navegador Tor por primera vez, es una buena idea familiarizarse un poco con el sistema antes de saltar directamente a la Dark Web. Es recomendable leer el manual proporcionado en la página de inicio del navegador Tor. Además, Tor proporciona un enlace a algunos consejos para usar correctamente el sistema para maximizar el anonimato.

Para verificar que el navegador esté conectado correctamente al enrutador Onion, haga clic en "Probar configuración de red Tor" en la página de inicio predeterminada. La página resultante informará la dirección IP que ven los sitios web cuando se conecta a ellos. Esta es la dirección del nodo final, o "nodo de salida" de su circuito Tor actual. Para ver los otros nodos en su circuito, haga clic en el ícono verde “cebolla” (etiquetado “Tor habilitado” al pasar el mouse) en la esquina superior izquierda de su navegador. Esto revelará los saltos en el circuito. De vez en cuando, esta ruta cambiará automáticamente, pero puede cambiarla manualmente haciendo clic en "Nuevo circuito Tor para este sitio" en el mismo panel.

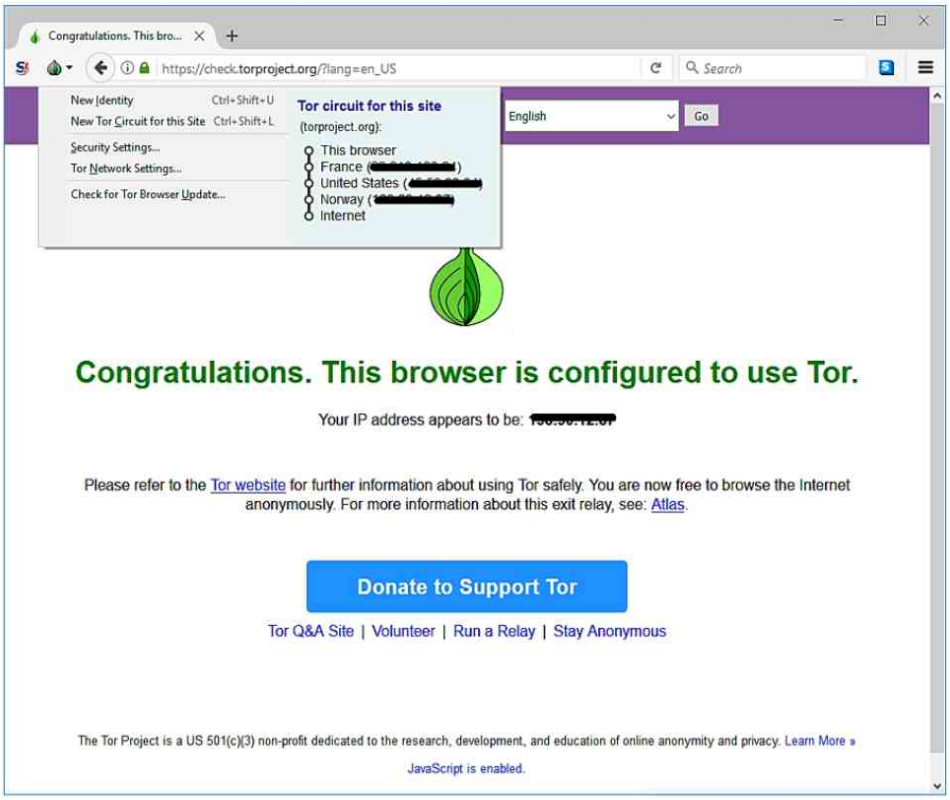


Figura 26 - Visualización del circuito Tor

La dirección IP del nodo de salida que los sitios web ven para su conexión es diferente de la dirección IP pública asignada a su máquina por su ISP. Así es como se logra el anonimato. Puede confirmar esto ingresando a un navegador web estándar (no en Tor) y verificando su dirección IP pública.

Una cosa a tener en cuenta al usar Tor es que muchos proveedores de servicios de Internet intentan detectar si sus clientes están usando Tor y bloquear el tráfico o informar la actividad a las fuerzas del orden público. Aunque en la mayoría de los casos no pueden rastrear acciones particulares hasta un usuario, el hecho de que se esté utilizando Tor puede atraer atención no deseada. La detección del tráfico Tor se puede eludir, aunque sea solo temporalmente, utilizando puentes Tor o relés de puente. Debido a la naturaleza de Tor, los nodos de cebolla son conocidos públicamente, por lo que un ISP puede ver si un cliente se está conectando a un punto de entrada de Tor. Los relés de puente son nodos de entrada alternativos que intentan permanecer ofuscados, pero debe tenerse en cuenta que generalmente son menos confiables que los nodos públicos de Tor. Además, algunos ISP todavía han encontrado formas de detectar conexiones puenteadas al examinar los paquetes. También existen puentes que admiten entidades conocidas como transportes conectables que ocultan la actividad Tor de los censores alternando el tráfico entre el usuario y el puente de entrada.

Para configurar el navegador Tor para usar relés de puente, haga clic en el icono del menú desplegable de Cebolla y abra el cuadro de diálogo "Configuración de red Tor".

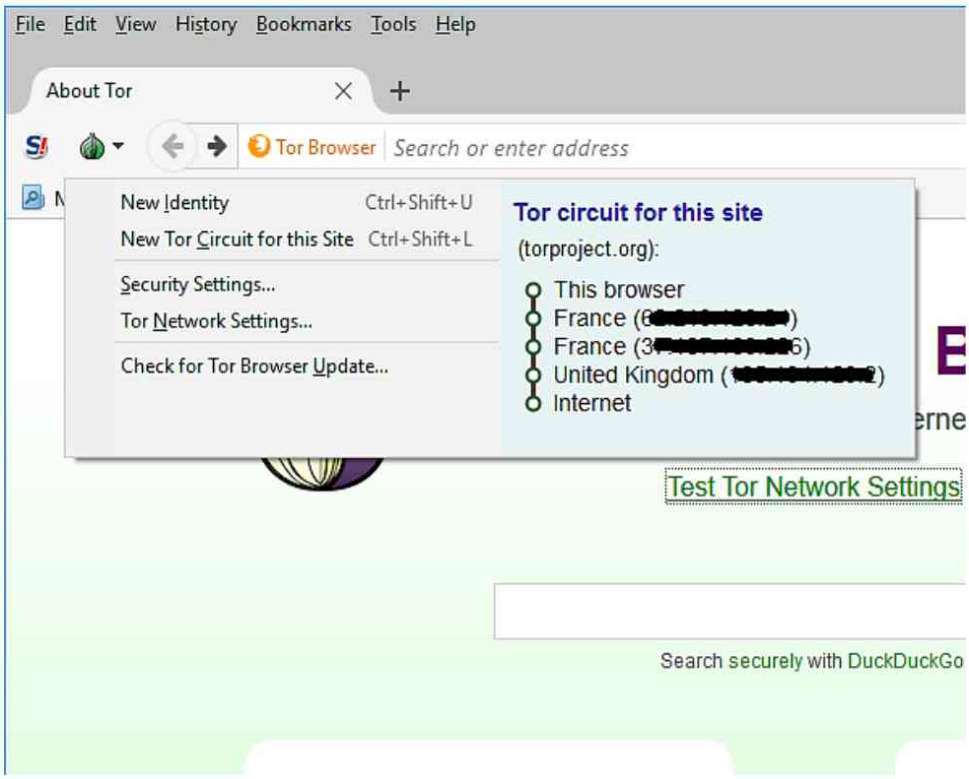


Figura 27 - Menú de configuración de Tor

Marque la casilla junto a "Mi proveedor de servicios de Internet (ISP) bloquea las conexiones a la red Tor" y elija el botón de opción "Conectar con puentes provistos". Elegir el tipo de transporte obs4 promulgará transportes enchufables.

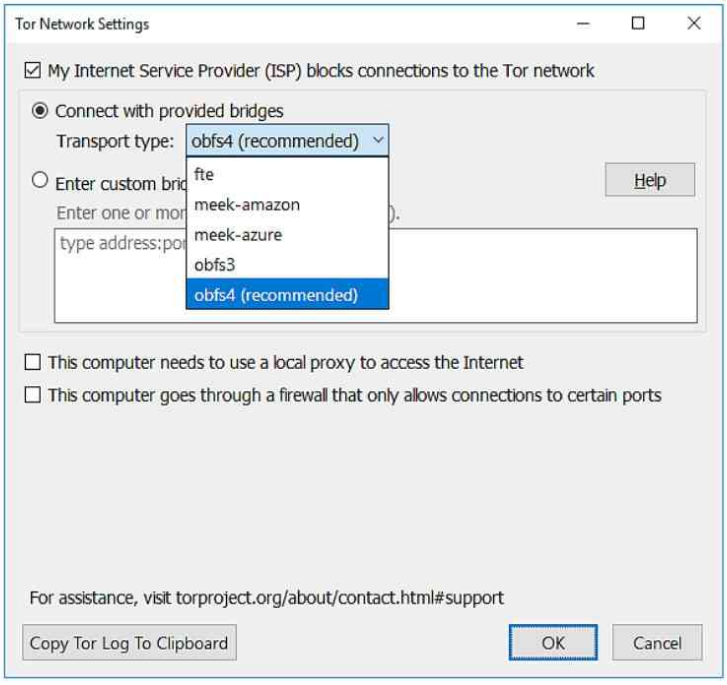


Figura 28 - Diálogo de configuración de Tor

Si tiene su propia lista de relés de puente que prefiere conectar, elija el botón de opción "Introducir puentes personalizados" y pegue las ubicaciones de los puentes en el cuadro de texto, uno por línea. Se puede encontrar una lista de puentes en el sitio web del Proyecto Tor en el siguiente enlace, pero los hackers siempre deben estar atentos a nuevos puentes de fuentes confiables.

Puentes estándar:

https://bridges.torproject.org/bridges

Puentes de transporte enchufables:

https://bridges.torproject.org/bridges?transport=obfs4

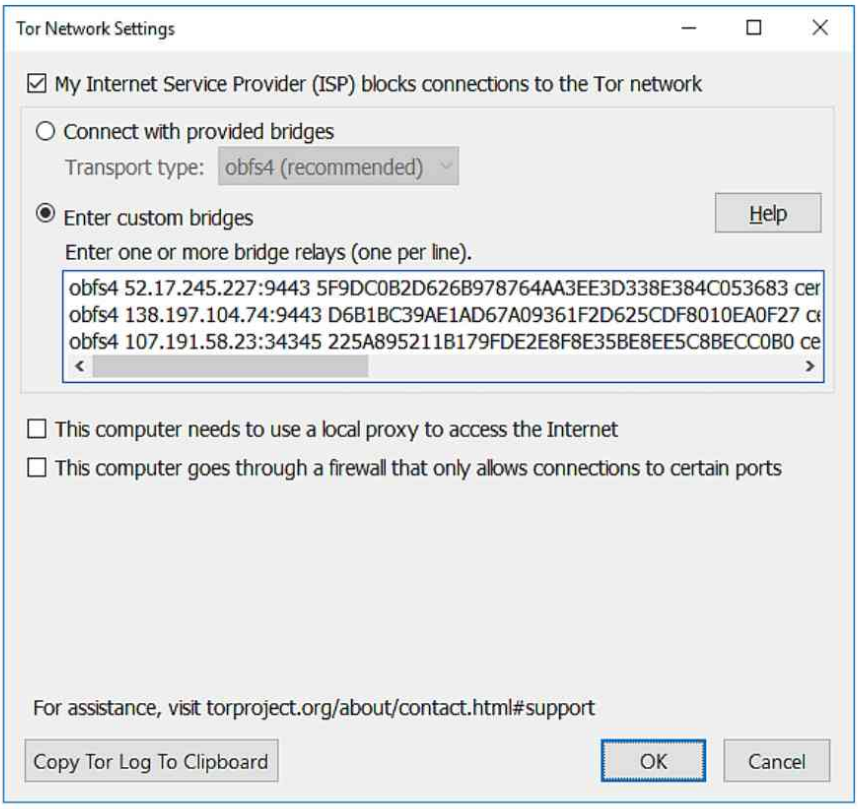


Figura 29 - Configuración del puente Tor

Tor es un proceso subyacente que el navegador Tor usa para acceder al enrutador Onion, pero también se puede usar con otras aplicaciones aparte de un navegador. Esto es especialmente importante cuando se ejecutan exploits. Para configurar Tor para usar relés de puente de transporte enchufables en Linux sin usar el Navegador Tor, se necesitan algunos comandos de terminal y configuración.

Suponiendo que Tor ya se haya instalado, ingrese los siguientes comandos para descargar e instalar los servicios de puente obsf (use sudo si es necesario):

service tor stop

apt-get update

apt-get install obsfproxy obsf4proxy

Ahora abra el archivo de configuración "torcc" (bajo /etc/tor/directory) en un editor de texto. Es una buena práctica hacer una copia de seguridad del archivo actual antes de realizar cualquier cambio. Inserte el siguiente texto (## es simplemente una línea de comentario), con las ubicaciones de puente deseadas después de cada línea que comienza con "Puente". Salve el archivo.

```
## Bridges
UseBridges 1
ClientTransportPlugin obfs3 exec /usr/bin/obfsproxy managed
ClientTransportPlugin obfs4 exec /usr/bin/obfs4proxy managed

Bridge obfs4 52[redacted]
Bridge obfs4 13[redacted]
Bridge obfs4 10[redacted]
```

Iniciar Tor desde una terminal:

service to start

Para confirmar que tor se está ejecutando, abra un navegador web estándar (no el navegador Tor). En la configuración de red, establezca la configuración manual del proxy en un host SOCKSv5 local de 127.0.0.1:9050.

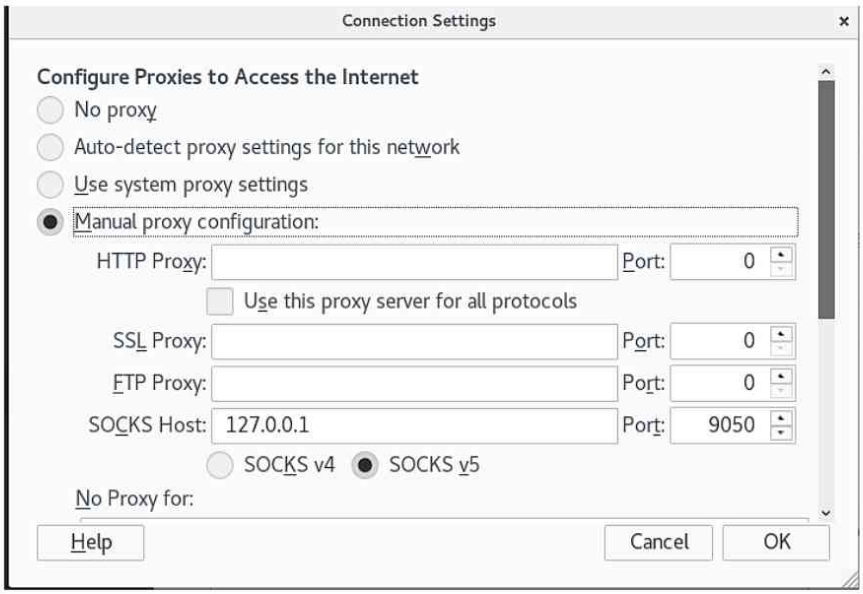


Figura 30 - Configuración del proxy del navegador Tor

Navegar a:

check.torproject.org

El sitio debe confirmar que Tor está conectado. Sin embargo, después de esta comprobación, restablezca la configuración de red del navegador a la normalidad y solo use el navegador Tor para acceder a la web. Ahora, cuando Tor se ejecuta desde el terminal, se pueden ejecutar otras aplicaciones con una conexión en puente a la red Onion.

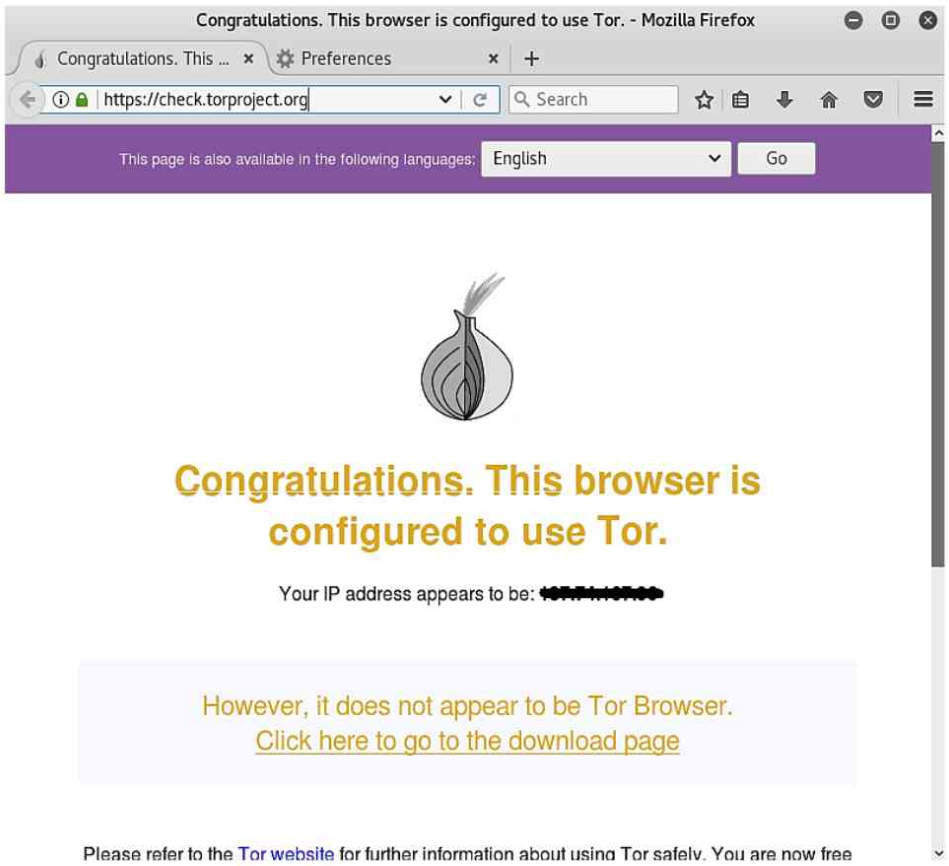


Figura 31 - Confirmación de conexión Tor

Recuerde que simplemente conectarse a la red Tor no garantiza la protección. Además de usar el navegador Tor (si usa Tor para la Web), la organización Tor recomienda ciertas prácticas para mejorar el anonimato:

1. No utilice aplicaciones de intercambio de archivos torrent sobre Tor
2. No instale complementos en el navegador Tor ni habilite ninguno que esté deshabilitado de forma predeterminada
3. Utilice siempre las URL HTTPS
4. No abra documentos descargados del navegador Tor
5. Use un relé de puente Tor cuando sea posible

SERVICIOS OCULTOS TOR

Algunas palabras de precaución antes de embarcarnos en un vistazo a la Deep Web. Gran parte del contenido disponible no está necesariamente

indexado, y los que sí a menudo caducan rápidamente. Los índices que existen contienen una mezcla ecléctica de sitios con diversos contenidos y servicios, muchos de los cuales son ilegales en la mayoría de los países. Asegúrese de comprender las leyes y sanciones asociadas con cualquier actividad que elija realizar en la Deep Web. Además, los hackers y las agencias gubernamentales muy poderosas están constantemente investigando a Tor en busca de debilidades, apagando servidores y comprometiendo nodos, por lo que el anonimato no es seguro.

Aunque se puede acceder a los sitios web en Internet estándar (conocido como "clearnet") bajo dominios tradicionales como ".com", ".net" y ".org" a través de Tor, existe un dominio virtual conocido como ".onion "Que solo se puede acceder de forma anónima a través de Tor. Estas ubicaciones, conocidas como "servicios ocultos" son la esencia de la Dark Web.

Un recurso que enumera varios servicios ocultos de Dark Web es el "Hidden Wiki". No existe un Wiki Oculto oficial, administrado centralmente, sino que se refiere a varios sitios independientes que intentan indexar los servicios ocultos actuales de interés. Un Wiki oculto típico consta de múltiples categorías de enlaces, algunos clearnet y otros ocultos, muchos de los cuales han existido durante mucho tiempo. Aunque los editores de Hidden Wiki intentan mantenerse actualizados, Dark Web es muy dinámico, por lo que los sitios van y vienen con frecuencia o cambian las URL. Las Wiki ocultas actualizadas generalmente se pueden encontrar usando un motor de búsqueda, y algunas existen en la red clara, pero las que tienen URL de .onion solo se pueden acceder a través de un enrutador Onion (Nota: hay formas de acceder a servicios ocultos sin Tor, pero no de forma anónima).

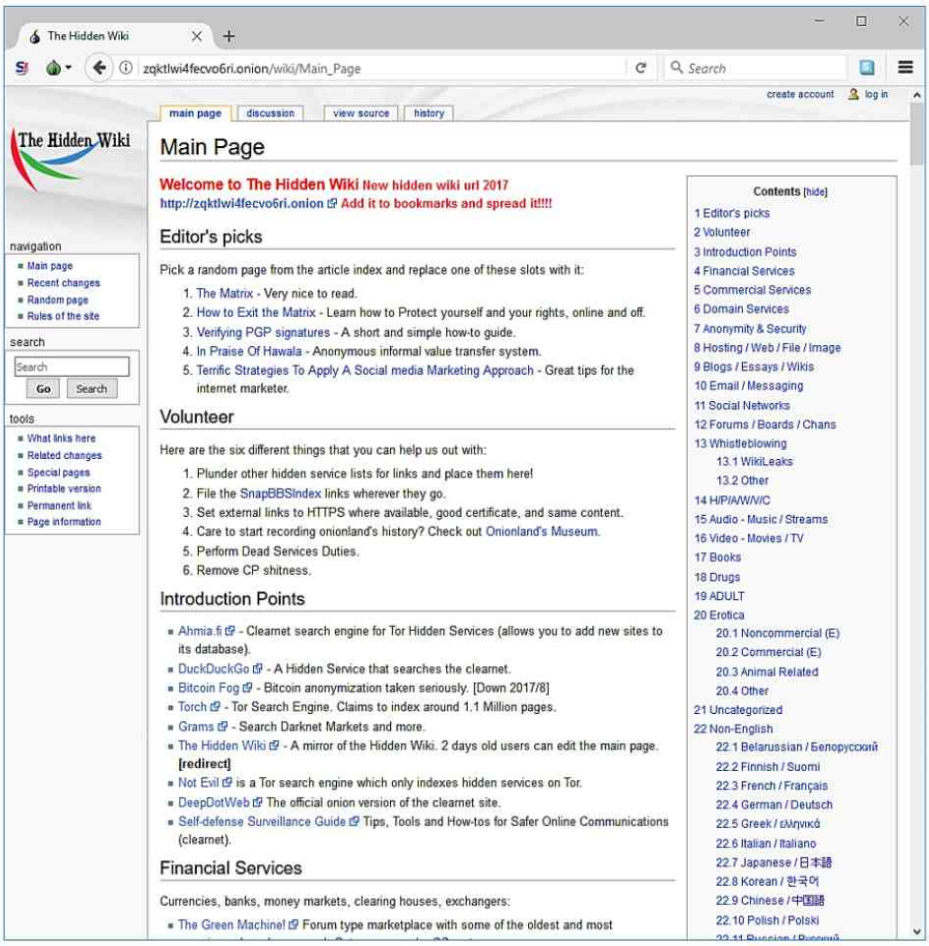


Figura 32 – Hidden Wiki de Tor

Hay tres tipos de motores de búsqueda a tener en cuenta con respecto a Tor:

1. **Motores ocultos basados en servicios que buscan en clearnet**: son buenos para realizar búsquedas anónimas en la Web. Un ejemplo es "DuckDuckGo" (que también tiene una versión clearnet), cuyo dominio .onion normalmente se puede encontrar en un Wiki Oculto.
2. **Motores basados en Clearnet que buscan en la red Onion**: Un ejemplo es Ahima.fi. No necesita estar en Tor para acceder a esto, pero no será anónimo.
3. **Motores basados en servicios ocultos que buscan en la red de Onion**: Un ejemplo es "Torch", cuyo dominio .onion generalmente aparece en un Wiki oculto.

Capítulo 7. Proxies Y Proxychains

Aunque el objetivo final de un ataque generalmente es obtener acceso (¡obtener root!), Entregar una carga útil o interrumpir un servicio, los hackers de todo tipo tienen poco interés en ser atrapados. En muchos casos, el desafío principal no es el pirateo en sí, sino el proceso de ocultar su identidad y cubrir sus huellas. Si un paquete llega a una máquina de destino con la dirección IP del originador todavía incrustada en el encabezado, el personal de seguridad requiere un esfuerzo mínimo para localizar al autor. Además, no sirve de nada falsificar la IP de origen (a menos que esté realizando algún tipo de ataque de denegación de servicio) porque también necesita recuperar paquetes en la mayoría de los casos. Para que sea más difícil para los investigadores rastrear la IP de origen de un usuario, es útil emplear un intermediario conocido como ***proxy***. Encadenar correctamente varios servidores proxy, de hecho, puede dificultar enormemente el seguimiento de cualquier persona sin un gran esfuerzo y gasto.

Servidores Proxy

La palabra "proxy" en el uso del inglés esencialmente significa "representante". Del mismo modo que alguien podría representarlo a usted y a sus intereses en una reunión o procedimiento legal, un servidor proxy transmite la comunicación de una fuente a un destino. Sin embargo, el nodo de destino verá la dirección IP del ***servidor proxy*** como agente de origen. Cuando el servidor proxy recibe paquetes del servicio solicitado, los devuelve a la parte solicitante. La dirección IP de origen, aunque se almacena en la ubicación del proxy, no se incluye en los encabezados de los paquetes que viajan entre el proxy y el destino. Esto sirve para ocultar la identidad de la parte de origen del servidor de destino.

Figura 33 - Configuración del servidor proxy

Sin embargo, los servidores proxy no solo se utilizan para el anonimato. Los proxies a menudo se emplean como una barrera protectora entre una red local e Internet en general. Tener un servidor como intermediario puede servir para filtrar la información en ambas direcciones, evitando tanto los ataques entrantes como el acceso a recursos externos no autorizados.

TIPOS DE IMPLEMENTACIONES DEL SERVIDOR PROXY

Un protocolo de Internet importante en la capa de aplicación de la pila TCP / IP es SOCKet Secure o ***SOCKS***. SOCKS, en general, maneja solicitudes de

conexión y transferencias de paquetes entre clientes, servidores proxy y servidores. La implementación de SOCKS5 admite medidas adicionales de seguridad y autenticación. Los servidores proxy ***HTTP*** utilizan los mismos encabezados y protocolos para conectarse a los servidores web a través del proxy como si fuera una conexión directa, lo que los hace más eficientes para el uso web. Sin embargo, la ventaja de las implementaciones de SOCKS es que admiten protocolos adicionales más allá de HTTP. Tenga en cuenta que Tor es en sí mismo un tipo de implementación de proxy SOCKS.

USOS DEL SERVIDOR PROXY

Las organizaciones con redes internas a menudo desean controlar el uso de conexiones externas a Internet por parte de su personal. Esto es tanto para evitar que usuarios individuales introduzcan involuntariamente scripts comprometedores en la red como para evitar que accedan a contenido no deseado o no relacionado con el trabajo, como correo electrónico personal, juegos, redes sociales, transmisión de video, comercio financiero o contenido para adultos . Un proxy web administrado internamente puede filtrar (ya sea mediante listas blancas o negras) contenido y bloquear el acceso a ubicaciones, dominios o servicios restringidos. Curiosamente, los empleados a menudo pueden eludir estas restricciones accediendo a un servidor proxy externo. De hecho, existen muchos proxies para este propósito específico. Si el cortafuegos de la organización no bloquea específicamente la dirección IP de un servidor proxy externo en particular (esta es la razón por la cual algunos eligen usar la lista blanca), entonces puede transmitir contenido a un usuario a través de su propia dirección IP no bloqueada, evitando así el filtro de contenidos.

Muchos usuarios se conectan a servidores proxy para acceder a sitios web o servidores de forma anónima. Esto podría ser solo por razones generales de privacidad o para ocultar actividades de hacking. A veces, los usuarios a los

que se les ha prohibido su dirección IP en un sitio web o un servicio en línea intentarán acceder a través de un proxy. Además, muchos países bloquean el acceso de sus habitantes a ciertos dominios, o bloquean el acceso de terceros a contenido local. Los proxies se pueden usar para presentar la impresión de que uno está en una ubicación geográfica particular para eludir estas restricciones.

Los hackers pueden configurar servidores proxy maliciosos para que se ubiquen entre un usuario objetivo y una ubicación legítima. Si el usuario objetivo desconoce el acuerdo, o tiene la impresión de que está utilizando un proxy seguro, el hacker puede leer y registrar el tráfico que pasa entre los nodos o realizar ataques de hombre en el medio.

ENCONTRAR Y CONECTARSE A SERVIDORES WEB PROXY ABIERTOS

La habilidad para utilizar un servidor proxy para el anonimato depende en gran medida del hecho de que el sistema al que se accede no es consciente de que está conectado a un proxy. Los servicios que no desean que los usuarios se conecten a ellos a través del proxy bloquearán las direcciones IP del servidor proxy conocido. Como resultado, las direcciones de los servidores proxy disponibles públicamente son en gran medida efímeras. Los usuarios pueden encontrar servidores proxy de pago (y algunos gratuitos) que usan software del lado del cliente para actualizar la dirección del proxy según sea necesario. Alternativamente, los usuarios pueden verificar cualquier número de sitios web que mantengan listas actualizadas regularmente de servidores proxy abiertos conocidos, para que puedan conectarse con un nuevo servidor si el anterior caduca o se bloquea. Estas listas a menudo contienen la velocidad, la confiabilidad, el país anfitrión, la última conexión exitosa conocida y otra información además de la dirección IP del servidor y el puerto de cada servidor en formato ordenable. Algunos sitios con listas de proxy abiertas son:

https://www.proxynova.com/proxy-server-list/

http://www.publicproxyservers.com/proxy/list1.html

http://list.proxylistplus.com/Fresh-HTTP-Proxy-List-1

Aunque algunos servidores proxy están basados en la web y lo conectarán a los servicios de destino dentro de su propia aplicación web, generalmente es necesario configurar un navegador web o sistema operativo para conectarse a la dirección proxy deseada.

En Windows 10, el servidor proxy se puede configurar en Panel de control> Opciones de Internet> Conexiones> Configuración de LAN.

En Linux, abra la aplicación Red y seleccione la sección Proxy de red. Elija la configuración Manual para ingresar la dirección del proxy.

En Windows, Linux y Mac, también se puede configurar un servidor proxy dentro de la configuración del navegador.

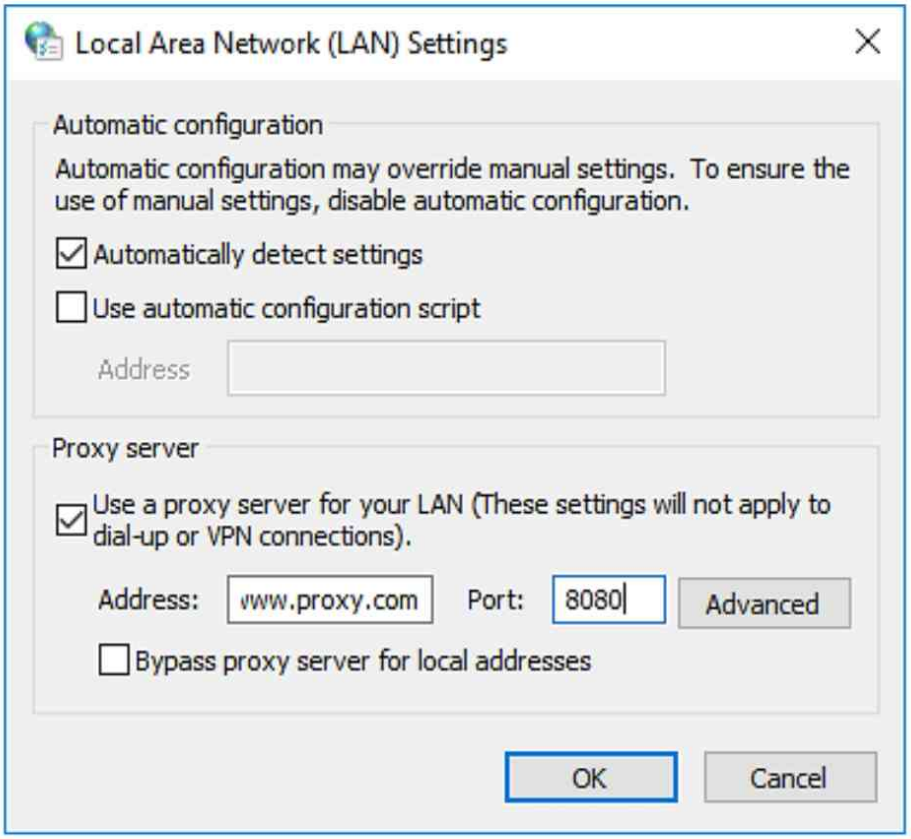


Figura 34 - Configuración del proxy del navegador

Proxichains

Aunque los servidores proxy hacen un trabajo suficiente en la mayoría de los casos para ocultar la dirección IP de un cliente de un servidor de destino, solo proporcionan una capa de protección. Dado que el servidor proxy conoce la dirección IP del cliente, aunque solo sea temporalmente, esa información se puede obtener accediendo a los registros del servidor proxy. El personal de seguridad o los hackers pueden intentar obtener estos registros mediante piratería propia o mediante citaciones judiciales. Sin embargo, cada servidor proxy solo tiene la dirección IP de la parte solicitante inmediatamente anterior. Por lo tanto, si se utilizan múltiples servidores proxy, se vuelve cada vez más difícil, costoso y lento rastrear el origen de un paquete.

Proxychains es un programa de Linux simple pero potente que enruta el tráfico de Internet a través de una serie de servidores proxy con el fin de ocultar la identidad de un cliente. Los hackers a menudo usan Proxychains junto con programas de recolección o explotación de información para mantener su ubicación e identidad en secreto. Debe reiterarse aquí que ninguna medida de anonimato es completamente infalible, y Proxychains no es una excepción. Las fuerzas del orden y la comunidad de piratas informáticos buscan constantemente formas de comprometer las herramientas comunes de piratería y anonimato.

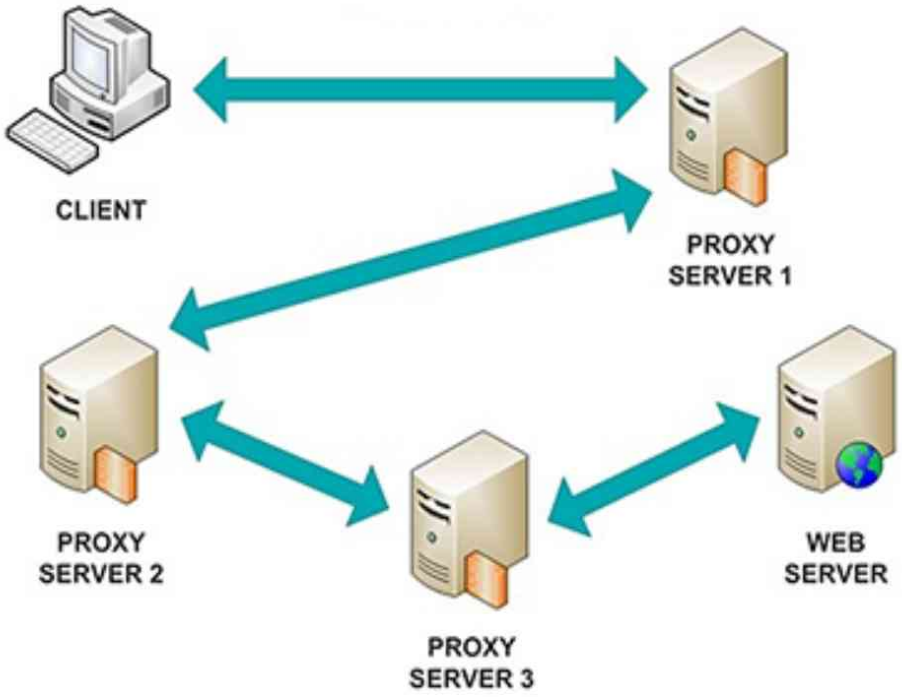


Figura 35 - Una cadena de proxy

INSTALANDO Y CONFIGURANDO PROXYCHAINS EN LINUX

Proxychains es una herramienta estándar en la suite Kali Linux. Para instalar en cualquier distribución de Linux:

sudo apt-get install proxychains

La configuración y las listas de servidores proxy para proxychains se pueden establecer en el archivo de configuración, proxychains.conf, generalmente ubicado en la ruta / etc. Una de las elecciones que un usuario debe hacer es establecer una cadena de proxy estricta o dinámica. Una cadena dinámica mantendrá la conectividad omitiendo un servidor en la lista de proxy si se cae. Por defecto, la opción dynamic_chain está habilitada y dynamic_chain está comentada. Para habilitar el encadenamiento dinámico, elimine el hash de comentario (#) de la línea dynamic_chain y escriba un nuevo hash antes de strict_chain.

La sección [ProxyList] del archivo de configuración es donde puede colocar

una lista línea por línea de servidores proxy para usar en la cadena. El archivo de configuración tendrá un ejemplo del formato requerido para cada línea de proxy, que consiste en el tipo de proxy (HTTP, SOCKS5, etc.), puerto de dirección, nombre de usuario (si es necesario) y contraseña (si es necesario), cada uno separado por un espacio o pestaña:

socks5 192.168.67.78 1080 lamer secret
http 192.168.89.3 8080 justu hidden
socks4 192.168.1.49 1080
http 192.168.39.93 8080

Una gran cosa sobre los proxychains es que puede usar Tor como fuente proxy. De hecho, de manera predeterminada, el archivo de configuración de proxychains está configurado para acceder al puerto Tor local. Sin embargo, debe verificar las líneas de configuración para asegurarse de que se incluyan todos los tipos de proxy correctos para Tor. Si la sección [ProxyList] solo contiene la siguiente línea,

socks4 127.0.0.1 9050

entonces está configurado para usar Tor, pero solo con el protocolo SOCKS4, que puede no funcionar. Agregue la siguiente línea para garantizar el uso de SOCKS5:

socks5 127.0.0.1 9050

Recuerde que para usar proxychains a través de Tor, el servicio Tor primero debe estar ejecutándose:

service tor start

Ahora, para usar un programa a través de cadenas de proxy simplemente escriba proxychains seguido del nombre del programa y las etiquetas de opción deseadas. Para probar la configuración, puede ejecutar un escaneo simple de nmap (discutido más adelante) en un sitio web seguro.

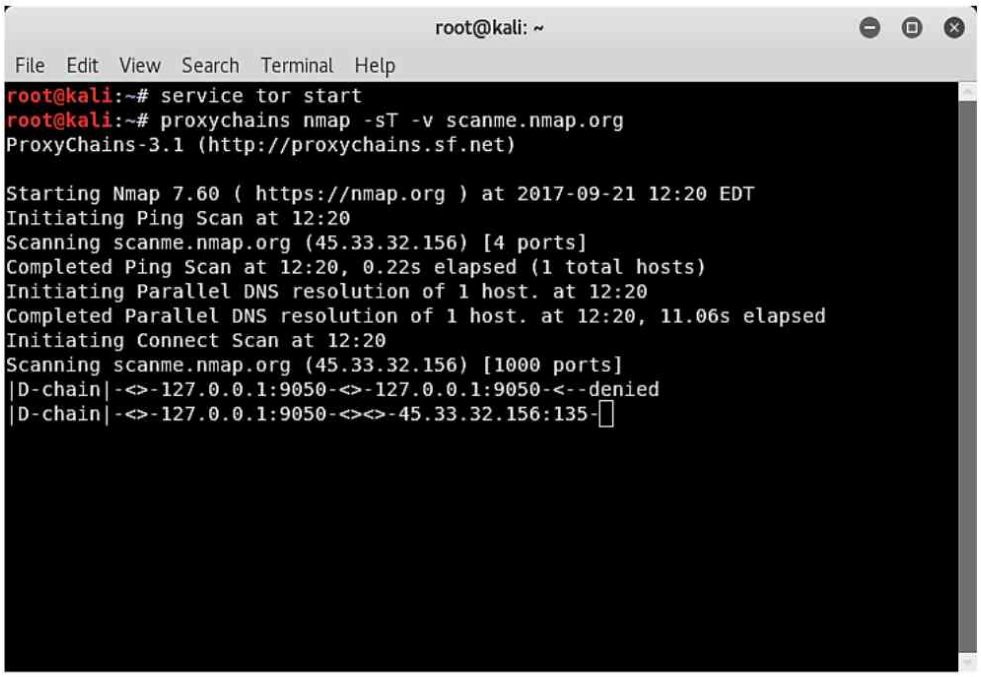


Figure 36 - Ejecutando proxychains

Capítulo 8. Redes Privadas Virtuales

Los mecanismos de retransmisión de los dos temas anteriores, los nodos Tor y los servidores proxy, pertenecen a un grupo particular de entidades conocidas como ***nodos de salida***. El propósito de un nodo de salida, independientemente de cómo funcione realmente, es enfrentar un servidor de destino en nombre de un usuario, ocultando tanto la identidad del usuario como cualquier ruta posterior. Otro tipo popular de nodo de salida es la ***red privada virtual*** (VPN). Una VPN es esencialmente un medio de extender una red local a nodos externos para que esos nodos se conviertan en parte de la red local. Esta práctica tiene muchos usos legítimos, incluido permitir que las redes corporativas en áreas geográficas dispares se conecten y compartan recursos de manera segura. Por supuesto, sería una gran ventaja para los piratas informáticos poder unirse a la red de un servidor de destino de esta manera.

VPN´s Y Túneles

El poder de una red privada virtual reside en la práctica del ***túnel***. En lugar de conectarse a un servidor de destino a través de Internet a través de un proveedor de servicios, el usuario establece una conexión cifrada a un servidor VPN que luego se conecta al destino. Aunque un ISP puede ver si un usuario está conectado a una dirección IP de un servidor VPN conocido, no puede leer el tráfico encriptado. Cuando se envía una solicitud del usuario al servidor VPN, el servicio VPN descifra la solicitud (que incluye los encabezados de destino) y la transmite a través de Internet. Cuando los paquetes se devuelven a la VPN, se vuelven a cifrar y se transmiten al usuario a través del túnel establecido.

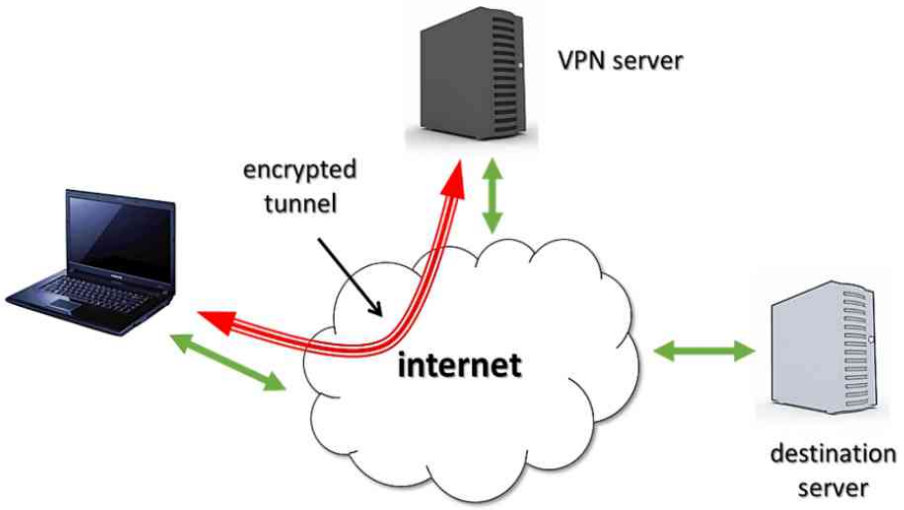


Figure 37 - Un túnel VPN

TIPOS Y USOS DE VPN

Hay dos tipos principales de servidores VPN en términos de su propósito, ***acceso remoto*** y de ***sitio a sitio***. Una VPN de acceso remoto es la más utilizada por usuarios domésticos o personales para proteger su anonimato o para evitar restricciones de acceso de ISP, corporativas o regionales. Los usuarios domésticos o corporativos también pueden usar este tipo de VPN para unirse a sus respectivas LAN desde una ubicación externa. Esta disposición puede ser deseable para organizaciones con múltiples ubicaciones o personal

remoto que necesitan acceder de forma segura a bases de datos o servicios centrales. Los usuarios domésticos pueden configurar una VPN de manera similar para acceder a sus archivos en casa o para controlar remotamente su computadora.

Aunque una VPN de acceso remoto puede crear una conexión encriptada, se realiza encapsulando paquetes que viajan a través de Internet como el tráfico estándar. Las VPN de sitio a sitio crean una conexión más segura mediante el uso de protocolos que mantienen la comunicación de enrutador a enrutador. Esta comunicación solo es posible después de la autenticación mutua del servidor y el cliente.

PROTOCOLOS DE VPN

El tipo de protocolo utilizado por un servicio VPN en particular depende en gran medida del propósito del servidor y las necesidades del usuario. Muchos servicios comerciales de VPN permitirán a los clientes seleccionar el tipo de protocolo de servidor que desean usar. Esta elección es a menudo una compensación entre seguridad, confiabilidad y velocidad. El cifrado, por naturaleza, ralentizará las velocidades de conexión hasta cierto punto, pero dado que varios usuarios suelen compartir el acceso a un servidor, la gran congestión puede reducir aún más las velocidades. El tipo de contenido al que se accede también afecta la elección del protocolo. La transmisión de video y audio requiere soporte de puerto UDP y mayor ancho de banda que la simple navegación HTTP. Ciertas conexiones corporativas pueden requerir el soporte de ciertos protocolos de transferencia de archivos.

OpenVPN es un protocolo VPN cada vez más popular que utiliza varias bibliotecas de código abierto para el cifrado y la comunicación. La mayor ventaja de OpenVPN es que se puede aplicar a prácticamente cualquier puerto o protocolo de subcapa. Para los ISP es difícil bloquear y se considera el protocolo más confiable, particularmente en términos de seguridad. Un

inconveniente es que la mayoría de los navegadores actualmente no son compatibles con OpenVPN de forma nativa. En la mayoría de los casos, es necesario utilizar software de terceros para conectar una computadora o un dispositivo móvil a un servidor VPN con este tipo de protocolo.

El ***protocolo de túnel punto a punto*** (PPTP) es un protocolo VPN más antiguo que, aunque todavía se usa ampliamente, generalmente no se recomienda cuando hay otras opciones disponibles. PPTP ofrece cifrado, pero está repleto de vulnerabilidades de seguridad y puede explotarse más fácilmente que otros protocolos. Sin embargo, debido a su soporte de plataformas antiguas y sistemas operativos heredados, además de su facilidad de uso, todavía se encuentra comúnmente. Muchos servicios VPN proporcionarán PPTP como una opción para los clientes que lo necesitan, pero les advertirán sobre los riesgos de seguridad. Este protocolo es el más adecuado para usuarios avanzados o en aplicaciones para las cuales la comunicación segura no es una prioridad principal.

El ***Protocolo de túnel de capa 2*** (L2TP) es otro protocolo VPN que a menudo se elige por su facilidad de uso y soporte nativo, pero no proporciona un canal altamente seguro. L2TP no realiza su propio cifrado de datos, por lo que debe combinarse con algún otro protocolo de cifrado (generalmente Internet Protocol Security o ***IPsec***). Otro inconveniente de L2TP es que está limitado a un puerto en particular, lo que hace que sea relativamente fácil para los firewalls o ISP bloquear su uso.

Existen otros protocolos con nuevos tipos de cifrado y soporte de plataforma diferente, pero OpenVPN, PPTP y L2TP son algunos de los más comunes para el uso del consumidor.

Eligiendo Una VPN

Un usuario doméstico que busca usar una VPN por libertad, seguridad y anonimato cuando se conecta a Internet tiene varias opciones, con las compensaciones habituales entre costo, velocidad, seguridad y confiabilidad (es decir, estabilidad). Aunque las VPN proporcionan cifrado y un nodo de salida para que los clientes ofusquen sus identidades, los usuarios pueden querer saber si su actividad se está registrando. Hay servicios VPN gratuitos disponibles, pero deben usarse con mucha precaución.

REGISTRO DE USUARIO

Una de las cosas más importantes a tener en cuenta al elegir un servicio VPN es si el proveedor mantiene o no la conexión del cliente y los registros de actividad. Si los registros de actividad de VPN son citados por la policía o comprometidos por hackers, entonces el anonimato relativo proporcionado por el nodo de salida ya no es una ventaja. Si un usuario desea una capa adicional de anonimato, debe elegir un servicio VPN "sin registro". Sin embargo, es importante tener en cuenta que "sin registro" realmente significa un registro mínimo. Hay un cierto grado de registro interno que debe ocurrir durante las operaciones de VPN para mantener la velocidad y la confiabilidad de la conexión, y para evitar ataques a los servidores. Los mejores servicios utilizan la cantidad mínima de registro necesaria para mantener operaciones estables, y no mantienen registros de esos registros por más tiempo del necesario.

Los usuarios deben ser escépticos con respecto a una VPN, especialmente una gratuita, que dice no registrar la actividad hasta que descubren exactamente lo que el servicio hace y no registra (a menudo hay advertencias y "letra pequeña" para las reclamaciones sin registro). Además, los servicios VPN gratuitos pueden no ser necesariamente confiables. La diligencia debida debe hacerse antes de usar una VPN gratuita. Es útil buscar comentarios de usuarios en línea para ver qué servicios (gratuitos y de pago) tienen buena

reputación.

CONSIDERACIONES ADICIONALES DE SEGURIDAD VPN

Si un usuario duda en comprar una suscripción a un servicio VPN de buena reputación por temor a perder su anonimato debido a la transacción, hay varias VPN comerciales que permiten a los clientes pagar con la moneda digital anónima de ***bitcoin***.

Si a un usuario le preocupa que se revele su identidad a través de registros de VPN, incluso a través de servidores "sin registro", es posible que los usuarios combinen conexiones VPN mediante un proceso llamado ***encadenamiento VPN***. Esto se puede lograr conectándose a una VPN en una máquina host, luego configurando un servicio VPN diferente en una máquina virtual dentro de ese mismo host. Si algún registro se ve comprometido en la VPN interna, la actividad se registrará como proveniente de la VPN externa. Por supuesto, no hay nada que impida que alguien intente obtener los registros de la VPN externa, pero agrega un obstáculo adicional y una capa de anonimato. En teoría, no hay nada que impida a un usuario crear múltiples máquinas virtuales dentro de máquinas virtuales, cada una con una VPN diferente, pero cada capa adicional disminuirá significativamente la velocidad de conexión. Incluso una cadena de dos VPN puede ser muy lenta. Algunos servicios de VPN comerciales tienen una opción para que los usuarios encadenen automáticamente dos de sus servidores (lo que no requiere configurar una máquina virtual).

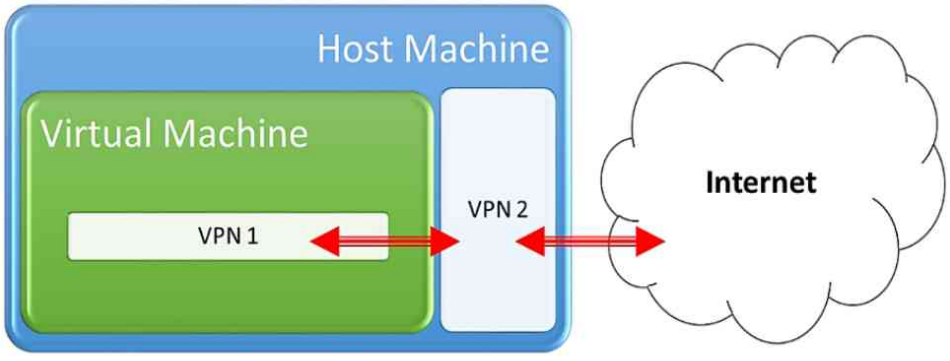


Figura 38 - Encadenamiento VPN

Tenga en cuenta que algunos servicios VPN también ofrecen a los usuarios la opción de conectarse desde el servidor VPN al destino a través de la red Onion. Aunque esto puede proporcionar ventajas de seguridad adicionales, también viene con una reducción en la velocidad de conexión.

Capítulo 9. Introducción A La Red Inalámbrica

Durante los primeros años de la red de computadoras, prácticamente todas las conexiones entre nodos se realizaron mediante cableado de cobre. El cable de cobre es eficiente, duradero y económico; además, fue el cobre que inicialmente comprendía la columna vertebral de Internet (que se implementó originalmente en el sistema de conmutación telefónica existente). A medida que aumentaron las necesidades de datos de banda ancha, los medios de fibra óptica reemplazaron el cobre para una gran parte de la red troncal de Internet, pero las redes locales se mantuvieron principalmente basadas en cobre. La explosión relativamente reciente de dispositivos móviles, junto con el hecho de que las computadoras portátiles comenzaron a reemplazar las unidades de escritorio menos portátiles como dispositivos informáticos primarios, requirieron la implementación generalizada de redes inalámbricas.

Aunque son más convenientes y flexibles que las redes cableadas, las redes inalámbricas son intrínsecamente menos seguras porque las señales se transmiten en todas las direcciones en lugar de limitarse a cables. El remedio para esta vulnerabilidad ha sido cifrar la comunicación entre nodos inalámbricos. Los piratas informáticos que pueden romper el algoritmo de cifrado en una red inalámbrica pueden acceder a su objetivo deseado.

Tecnologías Inalámbricas

Existen varios tipos de estándares de comunicación inalámbrica que generalmente se distinguen por su propósito, rango, ancho de banda y velocidad. Cada uno de estos estándares se rige por su propio conjunto de protocolos en las capas apropiadas, pero aún operan bajo TCP / IP para transmitir información como parte de una red. Debido a que las señales inalámbricas son omnidireccionales y se extienden al aire libre, la calidad de la señal disminuye rápidamente a medida que aumenta la distancia desde la fuente de la señal, por lo que las velocidades de datos solo se pueden mantener en un cierto rango. Además, las señales inalámbricas están sujetas a interferencias electromagnéticas que pueden degradar la calidad de la señal.

Wireless Fidelity (***Wi-Fi***) es un estándar de comunicación inalámbrica omnipresente que se usa comúnmente para implementar LAN locales y comerciales. El alcance efectivo de Wi-Fi es de hasta aproximadamente 100 metros sin obstrucción ni interferencia, pero para la mayoría de los entornos urbanos y residenciales, el alcance efectivo para una conexión confiable es de aproximadamente 10-30 metros. La tecnología Bluetooth generalmente se aplica a dispositivos y accesorios más pequeños dentro de los límites de una red de área personal (PAN) y puede extenderse a unos 10 metros. El Estándar de comunicación de campo cercano (NFC) de corto alcance normalmente está restringido a transferencias de datos a corto plazo dentro de un rango de 0.1 metros o menos (a veces requiere contacto físico entre dispositivos). La Figura 3 muestra los rangos relativos aproximados de estos estándares en una escala logarítmica.

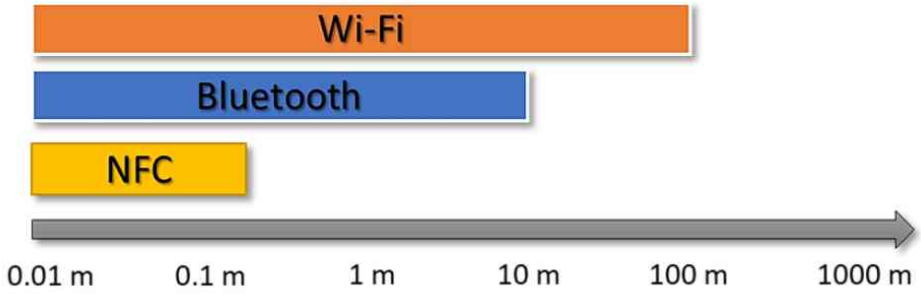


Figura 39 - Rangos comparativos de estándares de redes inalámbricas

Red Wi-Fi

El Wi-Fi es tan común ahora que es casi imposible encontrar un área en cualquier ciudad moderna donde no se detecte una señal de red pública o privada. Esto, por supuesto, es el corazón de la vulnerabilidad de Wi-Fi: el hecho de que cualquier persona dentro del alcance puede monitorear las señales sin estar físicamente conectado a la red o incluso, en algunos casos, en el sitio previsto de la LAN. De hecho, un método que los hackers han empleado es simplemente conducir o caminar por las calles de la ciudad (esto se llama ***conducción de guerra***) buscando redes Wi-Fi sin protección para explotar. A menudo, los piratas informáticos marcan estos lugares para que otros piratas informáticos los encuentren colocando símbolos en edificios o bordillos con tiza. Esta práctica se conoce como ***tiza de guerra***. Esta vulnerabilidad claramente hace que el cifrado de las redes Wi-Fi sea imprescindible.

El estándar 802.11

El estándar original para la comunicación W-Fi fue establecido por el estándar 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Este estándar se ha modificado a lo largo de los años con varias actualizaciones de velocidad, rango y seguridad. Los estándares 802.11gy 802.11n se mantuvieron posteriormente durante varios años hasta el reciente lanzamiento de 802.11ac (que probablemente alcanzará su propia obsolescencia en poco tiempo). Dado que las frecuencias más altas admiten más ancho de banda, las bandas de frecuencia compatibles con Wi-Fi incluyen 900 MHz, 2.4 GHz, 3.6 GHz, 5 GHz y 60 GHz (conocido como gigabit inalámbrico, destinado a aplicaciones de audio y video de alta velocidad). Las bandas que se usan actualmente en la mayoría de los sistemas son las bandas de 2.4 GHz y 5 GHz, que están segmentadas en varios canales. Aunque las frecuencias más bajas tienen menos ancho de banda, son menos susceptibles a la dispersión por paredes y otras obstrucciones.

Una red Wi-Fi, como se define en el estándar, consiste en dos o más estaciones inalámbricas cuya comunicación se rige por una función de coordinación (CF). Todas las estaciones gobernadas por un solo CF comprenden el conjunto de servicios básicos (BSS) de la LAN Wi-Fi (Ver Figura 4).

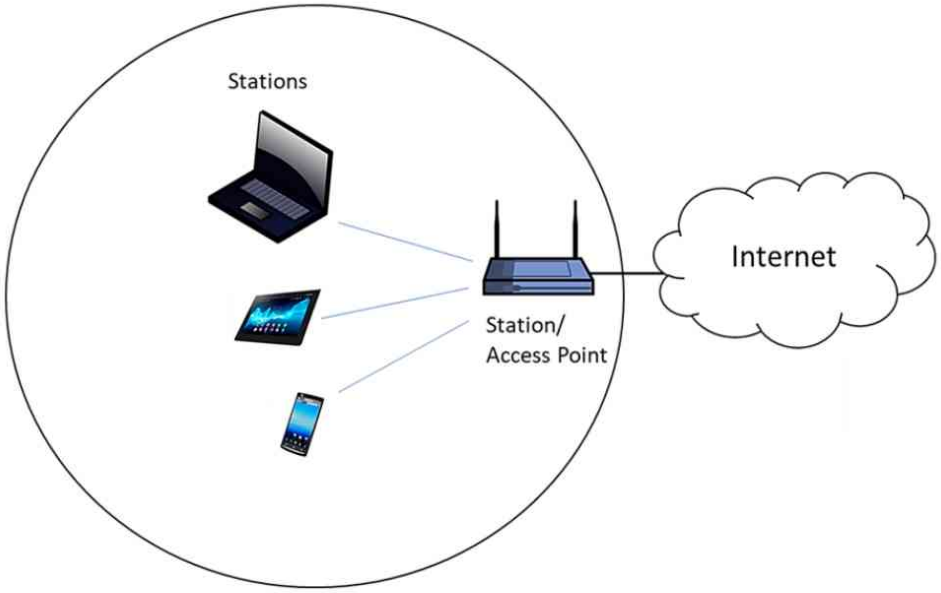


Figura 40 - LAN de Wi-Fi BSS

Se espera que cada estación brinde cuatro servicios básicos:

- ***Autenticación***: identificación adecuada de una estación en la red
- ***Desautenticación***: anular una estación previamente autenticada
- ***Privacidad***: cifrado de marcos de mensajes
- ***Entrega de unidad de datos de servicio MAC (MSDU)***: entrega de una trama de datos a su destino

Una estación que sirve como punto de acceso inalámbrico (que normalmente es un enrutador Wi-Fi) debe ofrecer cinco servicios adicionales:

- ***Asociación***: asignación de una estación autenticada al punto de acceso
- ***Desasociación***: anular una estación asociada previamente
- ***Reasociación***: reasignar una estación a otro punto de acceso
- ***Distribución***: manejo de la entrega de tramas MSDU dentro de la LAN

- ***Integración***: manejo de la entrega de tramas MSDU entre la LAN y una LAN cableada externa

OPERACIONES DE RED WI-FI

Parámetros

Una red Wi-Fi se define mediante tres parámetros básicos que la distinguen de otras redes cercanas: el nombre de la red, el modo operativo y el canal operativo.

El nombre de la red se conoce como el identificador del conjunto de servicios (***SSID***). Aunque los enrutadores vienen con un SSID predeterminado, la mayoría de los usuarios lo cambian al nombre de red deseado. Es posible suprimir la transmisión del SSID de una red para privacidad, pero los hackers expertos pueden encontrar fácilmente nombres de red ocultos.

Las redes Wi-Fi pueden funcionar en modos operativos ***ad-hoc*** o de ***infraestructura***. Las redes de infraestructura son las más comunes, ya que consisten en un punto de acceso central que da servicio a múltiples estaciones cliente. Así es como se configuran la mayoría de las LAN domésticas o comerciales. Una red Wi-Fi ad-hoc es simplemente una conexión bidireccional directa entre dos estaciones (por ejemplo, entre una computadora y una impresora inalámbrica).

Si hay varias redes de Wi-Fi dentro del alcance de la otra, es mejor que operen en sub frecuencias separadas (es decir, canales) dentro de una banda común. A cada red única se le puede asignar un canal manualmente, o se puede configurar para cambiar automáticamente los canales para evitar la superposición. Mantener canales de red no superpuestos puede mejorar el rendimiento de la red para todos los BSS en un área determinada.

Autenticación y apretones de manos

Para mantener la seguridad y la integridad de los datos entre dos nodos en

una LAN inalámbrica, primero debe llevarse a cabo la autenticación mutua. La autenticación es el proceso de confirmar la identidad de una estación (incluidos los clientes y los puntos de acceso). En el contexto de la autenticación, un cliente se conoce como un ***solicitante*** y el AP es un ***autenticador***.

Estas dos partes deben realizar un "***apretón de manos***" de cuatro vías para completar la autenticación mutua. El estándar IEEE 802.1X describe el establecimiento y el intercambio de ***claves criptográficas***. Un ejemplo de esto requiere el uso de una clave que se compartió por adelantado entre las dos partes y una clave concatenada conocida como clave transitoria por pares (PTK).

Otro concepto importante para que los hackers entiendan es el ***nonce criptográfico***. Un nonce (abreviatura de "**sin** sentido" usado "una ***vez***") es simplemente un valor aleatorio que se emite para usarse una vez y luego se descarta. El objetivo principal de un nonce es garantizar que las comunicaciones de protocolo de enlace no puedan ser capturadas y utilizadas posteriormente por hackers para forzar la autenticación (conocida como ***ataque de repetición***).

Con estas ideas en mente, un apretón de manos de cuatro vías procede de la siguiente manera (Figura 5):

1. El punto de acceso (AP) genera un nonce (ANonce) y lo envía a la estación (STA) para su autenticación.
2. El STA construye el PTK a partir de la clave previamente compartida, el ANonce recibido, su propio nonce (SNonce), su propia dirección MAC y la dirección MAC AP. Sin embargo, la única información que envía de vuelta al AP es su SNonce y un código de integridad de mensaje (MIC) generado algorítmicamente para verificar la autenticidad del mensaje.
3. Con el SNonce, el AP tiene toda la información que necesita para construir el mismo PTK que el STA construyó en el paso anterior. Luego, el AP construye una clave adicional llamada

clave temporal de grupo (GTK), necesaria para operaciones de multidifusión en la red, y la envía a la STA con un MIC.

4. Finalmente, la STA envía un acuse de recibo estándar (ACK) al AP, y se completa el protocolo de enlace.

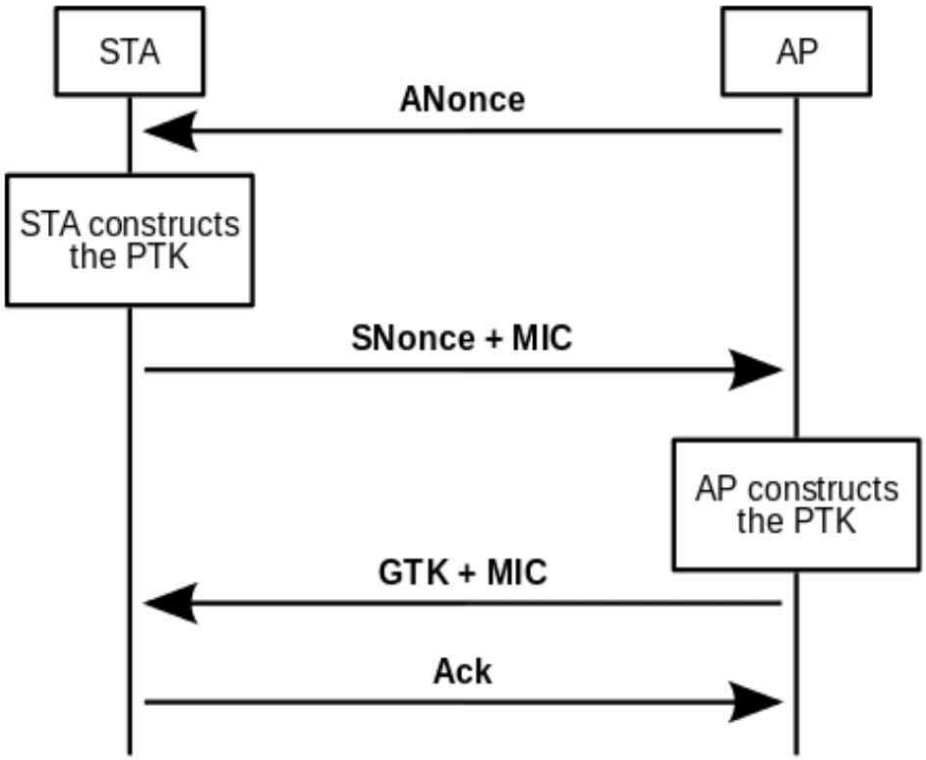


Figura 41 - Apretón de manos de cuatro vías

La importancia de los nonces criptográficos se hará evidente en el próximo capítulo, donde se muestra que pueden ser explotados para comprometer algunos protocolos de cifrado de Wi-Fi.

Capítulo 10. Configuración Y Herramientas De Hacking Inalámbrico

El hacking inalámbrico requiere herramientas de software y hardware especializadas debido a la naturaleza única de las redes inalámbricas y sus esquemas de cifrado estándar. Las herramientas de software son relativamente fáciles de obtener y usar, y vienen estándar con los paquetes de Kali Linux. Los adaptadores de red inalámbrica necesarios requieren un poco de investigación antes de la adquisición, pero generalmente son económicos y fáciles de encontrar.

Herramientas Kali Linux

La ***piratería para principiantes*** describe un procedimiento paso a paso para descifrar la contraseña de una red Wi-Fi cifrada con WEP usando Kali Linux. El Capítulo X de este libro sigue con un ataque WPA / WPA2 usando la misma colección de herramientas. Estas herramientas se describen con más detalle aquí, junto con el software adicional que se puede utilizar para ocultar la identidad del hacker.

LA SUITE AIRCRACK

El paquete ***aircrack*** es una colección de herramientas de código abierto basadas en Linux que se utilizan para el monitoreo de redes inalámbricas y las pruebas de penetración. Todos los programas en el paquete de aircrack se ejecutan en la línea de comando del terminal Linux. Aunque aircrack se usa como un término general para la suite actual, se ha titulado oficialmente ***aircrack-ng*** (un sufijo guión y "ng" significa "próxima generación" y se utiliza para denotar la ramificación de un proyecto de software con cambios significativos) desde 2007. Aircrack-ng es también el nombre de uno de los programas dentro de la suite. El paquete aircrack está disponible gratuitamente y se incluye de forma estándar en Kali Linux.

El paquete de aircrack está escrito para el estándar Wi-Fi 802.11 y puede monitorear o atacar el cifrado WEP y WPA / WPA2 con el equipo adecuado. Actualmente hay 16 programas en la suite que realizan varias tareas de rastreo, análisis, inyección, descifrado o descifrado de contraseñas, entre otras tareas.

El programa estrella de la suite es la herramienta de descifrado de clave de cifrado aircrack-ng. Este programa usa diferentes métodos dependiendo de si está descifrando una clave WEP o WPA / WPA2. El método de descifrado de claves WEP se basa en un ataque de cifrado de flujo que funciona juntando una gran cantidad de paquetes interceptados para formar la clave. Esto

explota una debilidad inherente en los vectores de inicialización para WEP. El ataque de cifrado de flujo se puede usar junto con un ataque de diccionario para explotar contraseñas débiles más rápidamente. Aircrack-ng también usa un ataque de diccionario para descifrar WPA / WPA2, pero esto solo funciona para claves significativamente débiles.

La herramienta ***airmon-ng*** se utiliza para poner el adaptador inalámbrico de la máquina atacante en un estado llamado ***modo monitor*** (consulte la siguiente sección). Este paso debe tomarse antes de que pueda llevarse a cabo un monitoreo útil de Wi-Fi.

Airodump-ng es un sniffer de paquetes de red inalámbrico o analizador de red. Intercepta tramas sin procesar del adaptador inalámbrico conectado. Aircrack utiliza estos marcos para extraer los vectores de inicialización necesarios para descifrar una clave WEP.

Aireplay-ng es una herramienta de inyección de paquetes que utiliza el adaptador inalámbrico conectado para transmitir en el canal del punto de acceso que está siendo atacado. Aireplay-ng se puede usar para eliminar la autenticación de clientes en una red para aumentar el tráfico de airodump-ng para capturar. Otros ataques que implican autenticación falsa e inyección de paquetes falsificados también se pueden lograr con aireplay-ng.

Los programas descritos anteriormente son las herramientas de aircrack más comunes y familiares. Se pueden usar para la mayoría de los ataques de craqueo, denegación de servicio o inyección WEP y WPA / WPA2. El resto de las herramientas de aircrack se enumeran en la tabla a continuación con una breve descripción de su propósito.

airbase-ng	Una herramienta para atacar clientes inalámbricos
airdecap-ng	Descifra los paquetes cifrados (cuando se conoce la clave)

airdecloak-ng	Filtra cualquier "encubrimiento" de los paquetes WEP capturados
airolib-ng	Mantiene una base de datos de contraseñas y claves para descifrar WPA / WPA2
airserv-ng	Permite que otras máquinas usen la interfaz inalámbrica conectada
airtun-ng	Crea una conexión de túnel virtual para monitorear o inyectar tráfico encriptado
buddy-ng	Un servidor remoto utilizado con easside-ng (ver más abajo)
easside-ng	Se comunica con un punto de acceso descifrado, conectado a Internet y encriptado WEP
ivstools	Extrae y combina vectores de inicialización de paquetes capturados
packetforge-ng	Falsifica paquetes cifrados personalizados para ser inyectados

MACCHANGER

Una de las vulnerabilidades de Wi-Fi es que las señales se transmiten en todas las direcciones para que cualquier persona dentro del alcance las detecte. Es por eso que el cifrado de datos es tan importante en las redes inalámbricas. Si alguien está recolectando u "olfateando" el tráfico de red que se transmite en un canal en particular, no hay forma de que el punto de acceso de esa red lo sepa porque el monitoreo es pasivo por naturaleza. Es importante que los hackers permanezcan discretos, por lo que siempre se prefieren los ataques pasivos cuando sea posible. Desafortunadamente (para el pirata

informático), muchas personas se están dando cuenta de los ataques pasivos de WEP y WEP se está eliminando gradualmente. Los ataques inalámbricos más valiosos eventualmente requerirán cierto grado de transmisión o inyección de paquetes en el canal.

Todos los paquetes IP deben contener información sobre los nodos de origen y destino en el encabezado, incluidas la dirección IP y la dirección MAC. Un pirata informático que realiza un ataque inalámbrico lo hace a través de su propio adaptador de red inalámbrica, no a través de Internet, por lo que cualquier información de dirección IP en un encabezado de paquete enviado por el pirata informático es ambigua (en cualquier caso, puede falsificarse fácilmente utilizando las herramientas de aircrack enumeradas en la sección anterior). Por lo tanto, el origen de un ataque inalámbrico no se puede rastrear a una máquina o ubicación a través de la IP de origen como puede hacerlo en Internet. Sin embargo, todas las tarjetas de interfaz de red vienen con una dirección MAC única que indica tanto el fabricante como el dispositivo individual. Los funcionarios encargados de hacer cumplir la ley decididos y bien financiados o el personal de seguridad pueden extraer este identificador de los encabezados de paquetes sospechosos y usarlo para intentar identificar al atacante. Si el pirata informático compró abiertamente la tarjeta de interfaz, el fabricante podría identificar de manera factible al comerciante que vendió la unidad con esa dirección MAC, la fecha y la hora de la compra, y la identidad del comprador de cualquier rastro financiero restante.

Es una buena práctica, y un asunto simple, por lo tanto, alterar la dirección MAC que se transmite en cualquier paquete durante un ataque. Aunque la dirección MAC es permanente en el hardware y no se puede cambiar, la dirección enviada a los encabezados de los paquetes se falsifica fácilmente con una herramienta Linux simple (y de código abierto) llamada ***macchanger***. Con una sola línea, el macchanger puede alterar la dirección MAC que está

asociada con una interfaz de red particular a una dirección aleatoria o arbitraria establecida por el usuario. Aunque una dirección MAC aleatoria o una falsificación simplista (como 00:00:00:00:00:00 o FF:FF:FF:FF:FF:FF) ciertamente ocultarán la identidad de un atacante, también puede hacer que aparezca un paquete sospechoso para sistemas de detección de intrusos o monitores de red. Si una red no reconoce el código del fabricante en la dirección MAC de un paquete entrante, podría diseñarse para descartar el paquete o señalar una alerta.

Para cambiar la dirección MAC de un adaptador en Kali Linux, primero debe estar fuera de servicio con el siguiente comando:

ifconfig etho down

Donde etho es el adaptador a alterar. Para cambiar la dirección MAC del adaptador a una dirección aleatoria, use macchanger con una etiqueta "-r":

macchanger -r etho

Un cambio exitoso producirá resultados similares a los siguientes:

Current MAC: 08:00:27:89:88:44

Faked MAC: 95:45:0c:ad:64:94

Donde el campo "Faked MAC " contiene la nueva dirección MAC hexadecimal aleatoria ahora asociada con el adaptador. Para cambiar a una dirección MAC especificada, use la etiqueta "-m":

macchanger -m 00:03:77:7d:8a:05 etho

Resultados:

MAC actual: 95:45:0c:ad:64:94

Fake MAC: 00:03:77:7d:8a:05

Finalmente, vuelva a conectar el adaptador para usar con la dirección MAC falsificada:

ifconfig etho up

Para falsificar la dirección MAC de un fabricante específico, se pueden

encontrar en línea listas de prefijos asociados con los fabricantes de dispositivos. Wireshark mantiene una lista en:
https://www.wireshark.org/tools/oui-lookup.html

Adaptadores Inalámbricos

La mayoría de los ataques informáticos no implican ningún equipo especial más allá de una computadora, las herramientas de software necesarias (la mayoría de las cuales son gratuitas) y algún tipo de interfaz de red. Sin embargo, la piratería inalámbrica, particularmente para el estándar Wi-Fi 802.11, generalmente requiere un adaptador de red inalámbrico especializado. Además de la compatibilidad con el modo de monitor (ver más abajo), un hacker puede necesitar un adaptador externo con alcance extendido o capacidad direccional para alcanzar un objetivo específico.

MODO DE MONITOR

Según el estándar 802.11 Wi-Fi, los adaptadores de red pueden funcionar en cualquier momento en uno de los siete modos, dependiendo del uso previsto del dispositivo.

- ***Modo maestro***: sirve como punto de acceso a la red
- ***Modo administrado***: un cliente en la red
- ***Modo ad-hoc***: nodo sin punto de acceso
- ***Modo de malla***: una topología ad-hoc alternativa
- ***Modo repetidor***: señales de retransmisión
- ***Modo promiscuo***: detección del tráfico asociado.
- ***Modo monitor***: olfatear todo el tráfico de Wi-Fi

Dos modos de interés para los hackers son el modo promiscuo y el modo monitor, los cuales se utilizan en el análisis de redes. El modo "promiscuo" es un poco inapropiado. A diferencia de la joven en la escuela secundaria que salió con todos los niños, un adaptador inalámbrico en modo promiscuo no aceptará todos los paquetes que detecte. Durante el modo promiscuo, los únicos paquetes capturados son aquellos con encabezados que indican que provienen de un punto de acceso al que el adaptador está asociado actualmente. Por el contrario, un dispositivo en modo monitor (Monitoreo de

radiofrecuencia o RFMON) simplemente está tomando cualquier paquete de Wi-Fi dentro de su rango detectable (una analogía sería la entrega de correo a su hogar. Idealmente, solo verá correo o paquetes que se dirigen a su hogar. Entonces, en ese caso, usted está operando en modo promiscuo. Sin embargo, en la oficina de correos, las personas y las máquinas que clasifican el correo pueden observar todo el correo que pasa y, por lo tanto, están operando en modo monitor) . Este modo es necesario para descifrar el cifrado WEP y WPA / WPA2 porque se deben capturar múltiples paquetes cifrados en la red protegida antes de poder intentar el descifrado. La herramienta airmon-ng se usa para poner un adaptador conectado en modo monitor. Este proceso de línea única se muestra en ***Hacking para principiantes***.

Por varias razones, no todos los adaptadores de red inalámbrica, controladores o sistemas operativos admiten los siete modos de funcionamiento de Wi-Fi. Para utilizar el paquete de aircrack a su máximo potencial, el hacker debe obtener un adaptador inalámbrico que admita el modo de monitor. La mayoría, si no todas, las radios inalámbricas internas en computadoras de escritorio, computadoras portátiles y dispositivos móviles no admiten el modo de monitor. Es necesario obtener un dispositivo (normalmente externo, USB) con esta capacidad antes de atacar una red inalámbrica. Este no siempre es un proceso sencillo, pero el equipo es generalmente asequible y fácil de obtener. El primer paso es encontrar una lista de los conjuntos de chips de controladores de adaptadores inalámbricos que son compatibles con su sistema operativo previsto. Esta lista cambiará periódicamente y los chips compatibles irán y vendrán: la mejor manera de encontrar una lista de trabajo es a través de búsquedas en Internet y foros. La siguiente es una lista parcial de conjuntos de chips inalámbricos que admiten el modo de monitor en Kali Linux a partir de 2017.

- Atheros AR9271

- Ralink RT3070 y RT3572
- Realtek 8187L Wireless G y RTL8812AU

Una vez que sepa qué conjuntos de chips son compatibles con su sistema operativo, resulta relativamente fácil buscar un adaptador de red que tenga uno de esos conjuntos de chips. Un fabricante común de adaptadores inalámbricos USB externos que cuentan con chipsets en modo monitor en Kali Linux es Alfa Network, Inc.

Capítulo 11. Hacking Encriptación WPA2 Wi-Fi

Comprender las operaciones básicas involucradas en la comunicación Wi-Fi, como se presenta en el Capítulo 9, es el primer paso para explotar sus vulnerabilidades. El libro ***Hacking para principiantes*** ofrece una buena introducción a los diversos protocolos de cifrado inalámbrico y herramientas de código abierto para atacar redes, y avanza a través de uno de los hacks más rudimentarios. Este capítulo sigue evaluando protocolos más avanzados y sus vulnerabilidades. Es importante recordar que una vez que un procedimiento de piratería se conoce bien y se pone en uso común, generalmente no pasa mucho tiempo hasta que se corrige la vulnerabilidad o se abandona por completo el objetivo en cuestión. Un gran hacker nunca debe ser complaciente y debe tratar de mantenerse informado sobre los últimos ataques.

El hacking de Wi-Fi se presta particularmente bien para practicar hacks de forma segura. La mejor manera de familiarizarse y dominar los diferentes ataques de Wi-Fi es simplemente explotar la propia red. Con acceso a un enrutador inalámbrico, el hacker puede configurar el protocolo de encriptación, cambiar la longitud y la complejidad de la contraseña, o hacer otros cambios que afecten la seguridad. Hackear la propia red Wi-Fi y luego ajustar varios parámetros para contrarrestar es la mejor manera de convertirse en un hacker experto en un entorno libre de consecuencias.

Protocolos De Encriptación Wi-Fi

Hacking para principiantes proporciona una breve historia y una descripción general de los protocolos de cifrado estándar desde el inicio de Wi-Fi. Este capítulo revisará parte de esa información a la luz de conceptos más avanzados, pero enfatizará los estándares y la tecnología más recientes, que proporcionan objetivos más desafiantes.

WEP

El primer protocolo de cifrado utilizado para redes inalámbricas fue Wired Equivalent Privacy (***WEP***). El nombre deriva del hecho de que los autores originales del estándar Wi-Fi reconocieron que se necesitaban medidas adicionales para asegurar las transmisiones inalámbricas de datos que se transmitían abiertamente, algo que no era un problema con las redes conectadas por cable. Se necesitaba un método para cerrar la brecha en la confidencialidad entre los medios alámbricos e inalámbricos.

Desafortunadamente (¡pero afortunadamente para los hackers!), No pasó mucho tiempo antes de que se descubrieran las debilidades inherentes en WEP. WEP utiliza un "vector de inicialización" de una sola vez, o ***IV*** (similar a un nonce) en sus protocolos de autenticación. Este vector se agrega a la clave compartida, pero se envía sin cifrar porque está destinado a usarse solo una vez. Sin embargo, debido a que la longitud IV es tan corta, reaparecerá naturalmente a intervalos aleatorios si hay suficiente tráfico. Por lo tanto, los hackers simplemente necesitan capturar pasivamente los paquetes de datos en el canal de destino y recuperar una parte de la clave cada vez que reaparece el IV. Cuanto más pesado sea el tráfico en la red de destino, más rápido se puede recuperar toda la clave (consulte la Figura 42).

Hacking para principiantes describe el procedimiento para explotar una red Wi-Fi cifrada con WEP. Se necesita un adaptador inalámbrico especial para el procedimiento cuyo conjunto de chips admite el "modo monitor". Este

equipo es relativamente económico y fácil de encontrar. Kali Linux presenta todo el software necesario para realizar el hack, incluidos ***airmon-ng***, ***airodump-ng*** y ***aircrack-ng***. Las mejoras a WEP, incluido un tamaño IV más grande, han aumentado el tiempo que lleva piratear una red encriptada WEP, pero la vulnerabilidad continúa. Muchos enrutadores inalámbricos más nuevos ya no incluyen WEP como una configuración de cifrado debido a su inseguridad, y generalmente se recomienda no usarlo para proteger una red a menos que sea necesario para el soporte de algunos clientes heredados. Sin embargo, piratear WEP es una buena manera para que los piratas informáticos se mojen y se familiaricen con algunas de las herramientas comunes utilizadas para la explotación inalámbrica.

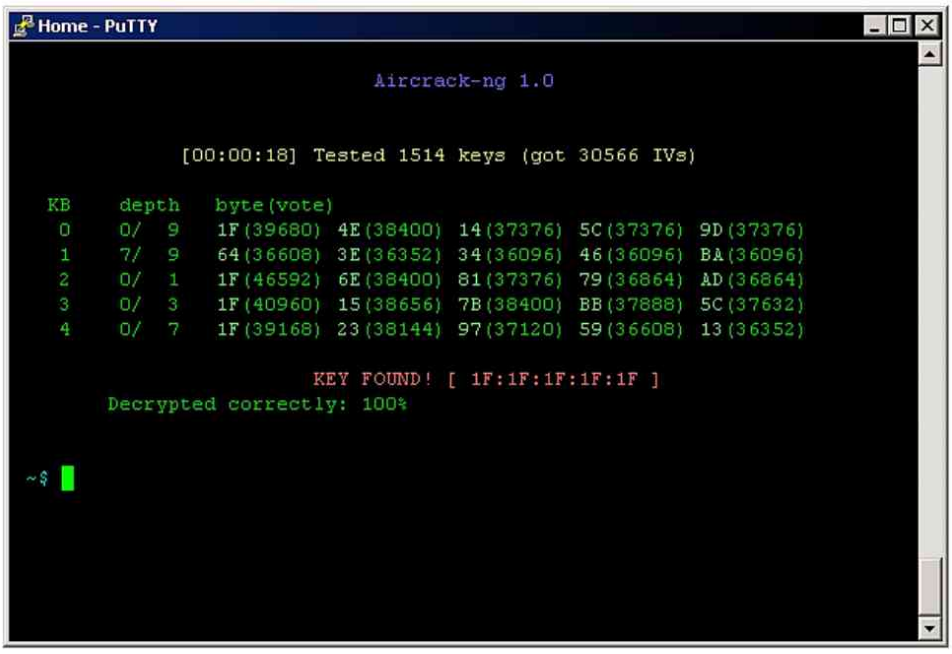


Figura 42 - Una clave Wi-Fi descifrada con éxito (aircrack-ng.org)

WPA

La respuesta a las vulnerabilidades de seguridad de WEP fue el desarrollo de un protocolo de cifrado completamente nuevo llamado WPA2, que se describirá a continuación. Sin embargo, la implementación de WPA2 requirió la fabricación y distribución de nuevo hardware de enrutador. Para los equipos que no pueden soportar WPA2, la medida provisional de WPA podría

implementarse como una mejora significativa, aunque temporal, respecto de WEP. Wi-Fi Protected Access (***WPA***) fue una implementación de software que mejoró la seguridad de la comunicación inalámbrica mediante el uso de una actualización de firmware para tarjetas de interfaz inalámbrica habilitadas para WEP.

En lugar de utilizar un vector de inicialización único agregado a una clave compartida, WPA cambia dinámicamente la clave de cifrado de 128 bits por paquete. Además, WPA comenzó a implementar el código de autenticación de mensajes (MAC), descrito en el capítulo anterior, para evitar la reutilización de paquetes antiguos. Estos procedimientos se denominan colectivamente Protocolo de integridad de clave temporal (***TKIP***).

A pesar de las mejoras que WPA proporcionó sobre WEP, los piratas informáticos lo comprometieron inevitablemente, aunque por medios más avanzados que el de WEP. Los ataques WPA, en contraste con la pasividad de la explotación WEP, requerían que los piratas informáticos transmitieran paquetes al canal de red de destino en lo que se conoce como inyección de paquetes. La ***inyección de paquetes*** se puede lograr usando otra herramienta en la suite de aircrack llamada ***aireplay-ng***. Dado que WPA2 ha estado disponible durante más de una década y se considera el protocolo más seguro, WPA ya no es compatible ni se recomienda su uso.

WPA2

Wi-Fi Protected Access II (***WPA2***) es el protocolo de cifrado estándar actual para redes Wi-Fi. Existen tres tipos de métodos de distribución de claves para WPA2, según el tipo y el tamaño de la red:

1. Clave precompartida (***WPA-PSK***): para redes domésticas y de oficinas pequeñas
2. Enterprise: para redes grandes y corporativas (requiere un servidor de autenticación)

3. Configuración protegida de Wi-Fi (***WPS***): un método simplificado pero inseguro

El libro limitará la discusión a WPA-PSK y se refiere a ese sistema al mencionar WPA2.

WPA2 mejoró el débil cifrado TKIP de WPA al adoptar el Estándar de cifrado avanzado (***AES***).

Hacking WPA2

A pesar de las tremendas mejoras en seguridad ofrecidas por WPA2 sobre WEP y WPA, tiene su parte de vulnerabilidades explotables. Si los usuarios emplean contraseñas débiles, sus redes son susceptibles a ataques de diccionario y otros métodos de fuerza bruta, incluso bajo WPA2. Aunque WPA2 todavía no puede verse comprometido por exploraciones triviales y pasivas como WEP, los piratas informáticos han estado ocupados investigando las debilidades. Varios ataques han surgido en los años de complejidad variable. A menudo, los estándares de Wi-Fi se han contrarrestado con actualizaciones y varios parches.

AIRCRACK

El procedimiento descrito aquí está diseñado para desarrollar las habilidades aprendidas en el ataque pasivo WEP explicado en ***Hacking para principiantes***, y utiliza el paquete de aircrack incluido en Kali Linux. Este ataque asume que el sistema de destino tiene una contraseña débil (usando palabras comunes) o relativamente corta, de lo contrario tomaría un tiempo prohibitivo de ejecución. Al igual que con cualquier ataque, no todo el equipo y el software son iguales y no todo irá siempre según lo planeado, por lo que se recomienda al lector que consulte múltiples fuentes para obtener información y solucionar problemas. Para atacar WPA / WPA2

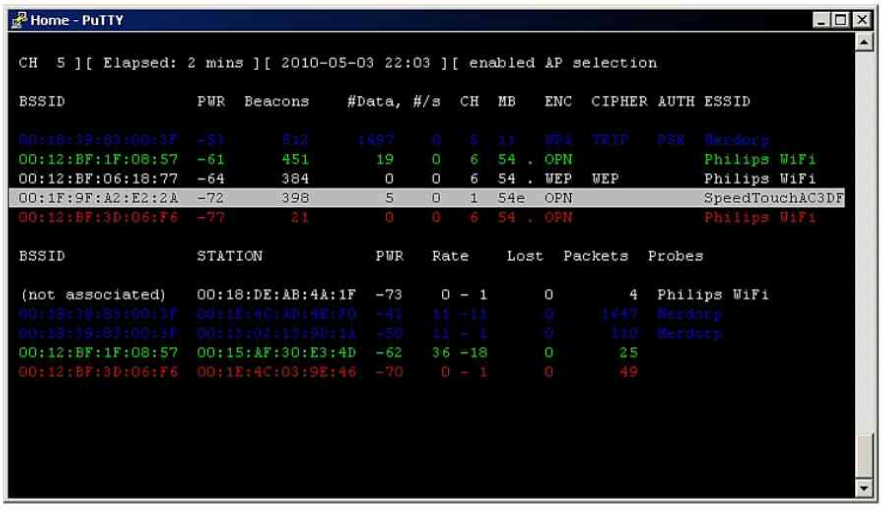


Figura 43 - resultados de airodump-ng

Tráfico Wi-Fi en vivo en varios enrutadores (.aircrack-ng.org)

~ $ airodump-ng -c CH --bssid **xx:xx:xx:xx:xx:xx** -w psk atho

donde CH es el canal para la dirección MAC de BSSID de destino XX:XX:XX:XX:XX:XX y atho es el adaptador habilitado para el modo de monitor.

aireplay-ng -o 1 -a XX:XX:XX:XX:XX:XX -c CC:CC:CC:CC:CC:CC atho

donde CC: CC: CC: CC: CC: CC Dirección MAC del objetivo de autenticación.

aircrack-ng -w contraseña.lst -b XX:XX:XX:XX:XX:XX psk * .cap

donde password.lst es un archivo de diccionario en la ruta local.

¡Un ataque de diccionario WPA / WPA2 exitoso producirá la salida de la clave pre compartida (Figura 7) y la contraseña resultante!

Figura 44 - Una contraseña WPA2 descifrada (itfellover.com)

EL NONCE "KRACK"

Aunque la desautenticación a través de la inyección de paquetes puede acelerar significativamente el descifrado de una clave WPA / WPA2, se puede frustrar fácilmente simplemente usando una mayor complejidad de contraseña. Los ataques de diccionario son efectivamente inútiles contra cadenas de caracteres largas y aleatorias. Se necesitan métodos más avanzados para romper una red WPA2 bien implementada.

Recientemente, los investigadores descubrieron una vulnerabilidad en el proceso de protocolo de enlace WPA2 de 4 vías y presentaron un documento de sus hallazgos en una conferencia técnica. El procedimiento se conoce como Key Reinstallation AttaCK (***KRACK***). Este ataque explota el uso del nonce criptográfico (introducido en el capítulo anterior) que se emite durante la autenticación. Aunque por su propia naturaleza, se supone que los nonces solo se usan una vez y se descartan, no hay ningún mecanismo en el protocolo WPA2 para garantizar esto. Por lo tanto, si el proceso de apretón de manos se puede manipular de tal manera que fuerce la reemisión de un nonce, los piratas informáticos pueden obtener información sobre la clave.

Recuerde que en el paso 3 del protocolo de enlace de 4 vías, el punto de acceso envía un mensaje final al cliente y espera el reconocimiento. No es inusual, especialmente en la comunicación inalámbrica donde la interferencia de la señal es significativa, que los paquetes se pierdan en la transmisión. Si el AP no recibe un ACK del cliente, por lo tanto reenviará el mensaje de saludo número 3 hasta que sea reconocido o agote el tiempo de espera. ¡Cada vez que el cliente recibe este mensaje, está reutilizando el nonce hasta que se completa el apretón de manos! KRACK funciona interceptando las transmisiones del mensaje 3 desde el AP y falsificando la pérdida de paquetes retransmitiéndolos al cliente para forzar la reutilización del Snonce.

Lo importante para recordar acerca de este ataque es que simplemente le permite al hacker descifrar el contenido de los paquetes del cliente, revelando información potencialmente confidencial. Sin embargo, no descifra la contraseña de la red misma. El procedimiento es avanzado y multifacético, lo que requiere que se escriban algunos scripts para llevar a cabo el ataque. Se puede encontrar una demostración en el siguiente video:

https://youtu.be/Oh4WURZoR98

La Figura 8 muestra el contenido de un paquete que se descifró con éxito

utilizando los procedimientos KRACK. En esta demostración, el paquete (es decir, "marco") contenía datos de formulario de usuario enviados a un sitio web.

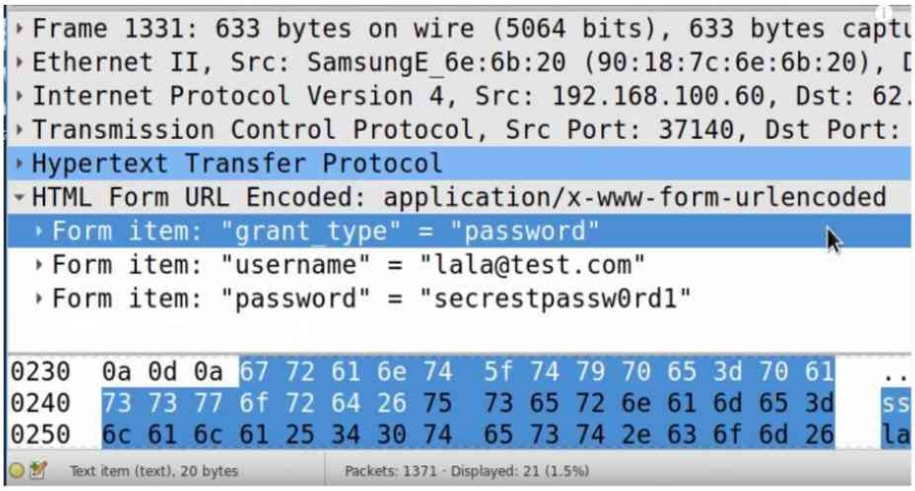


Figura 45 - Un ataque exitoso de KRACK (www.krackattacks.com)

Capítulo 12. Enrutadores Inalámbricos Y Explotación De Red

Obtener acceso a una red inalámbrica es un logro (uno que será más difícil a medida que mejore la seguridad de Wi-Fi), pero es solo el primer paso hacia objetivos más productivos. Al atacar una red inalámbrica, un pirata informático suele tener en cuenta cualquiera de estos tres objetivos:

1. Obtener acceso a un cliente en la red
2. Obtener acceso al punto de acceso
3. Ejecutando denegación de servicio

El último objetivo, la denegación de servicio, no necesariamente requiere acceso a la red, pero se puede lograr utilizando el mismo conjunto de herramientas. Este capítulo discutirá algunos aspectos de la seguridad del enrutador inalámbrico y describirá las herramientas que se utilizan para analizar y explotar a los miembros de una red.

Seguridad Del Enrutador

Romper el cifrado de una red inalámbrica le da acceso a la red en sí, pero no necesariamente a los nodos conectados. Los clientes y los puntos de acceso tendrán sus propias medidas de seguridad con las que el hacker debe lidiar. Los enrutadores inalámbricos que generalmente se usan como puntos de acceso en una LAN Wi-Fi están destinados solo para acceso administrativo y tienen seguridad incorporada. Los enrutadores también tienen ciertas vulnerabilidades que, cuando se explotan, pueden dar a los piratas informáticos un dominio libre sobre la red. Tener acceso al enrutador brinda a los piratas informáticos la posibilidad de cambiar los protocolos de cifrado, interceptar datos privilegiados o negar el acceso a usuarios legítimos.

CONTRASEÑAS ADMINISTRATIVAS

El software de configuración de un enrutador inalámbrico generalmente tiene la forma de firmware integrado en el dispositivo. Se accede a este programa, llamado puerta de enlace, a través de una interfaz web del cliente directamente a la dirección IP del enrutador. Un usuario autenticado accede a la interfaz cuando está conectado a la red (independientemente de cualquier conexión a Internet) escribiendo la dirección IP del enrutador en la barra de direcciones de su navegador web. La dirección del enrutador suele ser un formato estándar, que puede variar según la edad del dispositivo, y se incluirá en la documentación del producto o en una etiqueta adherida al dispositivo. Dos formatos comunes de dirección IPv4 del enrutador son:

192.168.X.X

10.0.X.X

La aplicación web saludará a los usuarios con un mensaje de nombre de usuario y contraseña en la pantalla de inicio (consulte la figura X), pero algunas puertas de enlace también pueden incluir información general sobre la red y los clientes conectados.

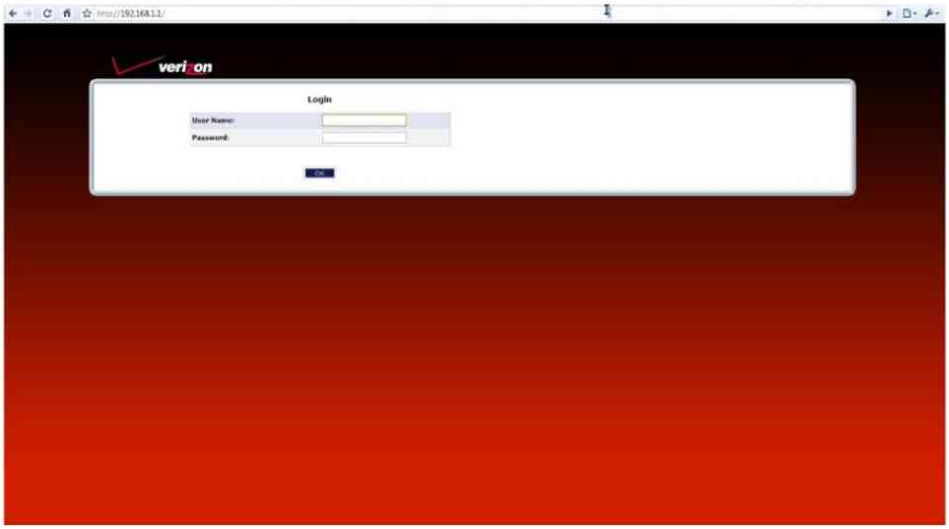


Figura 46 - Inicio de sesión del enrutador Wi-Fi

El nombre de usuario administrativo y la contraseña predeterminados para acceder al enrutador se incluyen en la documentación del producto o en el dispositivo. Muchos enrutadores, especialmente los más antiguos, tienen un nombre de usuario y una contraseña estándar en todos los modelos para que los administradores puedan restablecer el dispositivo a una contraseña fácilmente conocida si olvidan la que configuraron. Esta es una vulnerabilidad si el hacker tiene acceso físico al enrutador. Además, si el usuario no cambia la contraseña predeterminada, el acceso predeterminado para ese modelo de enrutador está disponible gratuitamente para los piratas informáticos en línea. En muchos casos, los inicios de sesión predeterminados son tan comunes y uniformes que se adivinan rápidamente. Algunas combinaciones comunes han sido tradicionalmente:

nombre de usuario: admin

contraseña: <en blanco>

nombre de usuario: admin

contraseña: admin

nombre de usuario: <en blanco>

contraseña: admin

nombre de usuario: admin

contraseña: contraseña

Existen bases de datos completas en línea con inicios de sesión de enrutadores ordenados por marca y modelo. Uno de esos sitios web es:

http://www.routerpasswords.com/

CRACKING WPS CON AIRCRACK Y BULLY

Un modo de funcionamiento que se ha agregado al estándar de Wi-Fi en los últimos años es la configuración inalámbrica protegida (WPS). El propósito de WPS es facilitar el inicio de sesión por parte de clientes inalámbricos mediante el uso de un botón WPS en el enrutador que empareja el dispositivo cliente con el enrutador, o alternativamente a través de un código PIN de 8 dígitos. El cifrado WPA / WPA2 subyacente (WPS no está disponible con WEP) todavía se está utilizando, pero los clientes usan WPA para conectarse sin necesitar la clave de cifrado. Esto presenta algunas vulnerabilidades claras en la seguridad del enrutador. Incluso si un enrutador está utilizando una clave de cifrado que es lo suficientemente fuerte como para frustrar los métodos de craqueo conocidos, si WPS está habilitado, un pirata informático solo necesita usar métodos básicos de fuerza bruta para obtener el pin WPS en un período de tiempo razonable. Además, en algunos dispositivos, incluso si el enrutador está configurado para conectarse con un botón WPS, la red puede ser hackeada con el pin WPS predeterminado del enrutador.

Los fabricantes de enrutadores se han dado cuenta de esta vulnerabilidad y han intentado solucionarla en nuevas actualizaciones de hardware y firmware, pero el problema persiste en muchos puntos de acceso antiguos y sin parches. Kali Linux presenta un script de ataque WPS de fuerza bruta conocido como ***bully*** que funciona con el paquete de aircrack y un adaptador inalámbrico con capacidad de modo monitor para romper el pin WPS, revelando posteriormente la contraseña de cifrado. A veces esto se puede hacer en cuestión de horas.

Después de colocar el adaptador Wi-Fi conectado de la máquina atacante en modo monitor, inicie airodump-ng para comenzar a recolectar paquetes, utilizando el procedimiento descrito en este libro y en ***Hacking para principiantes.***

Después de seleccionar una red de destino desde la pantalla de airodump (debe ser una que sepa que es vulnerable o este procedimiento no producirá resultados), ejecute bully para atacar el PIN:

bully mono -b <XX: XX: XX: XX: XX: XX> -e <ESSID> -c <CH>

donde <XX: XX: XX: XX: XX: XX>, <ESSID> y <CH> son la dirección MAC de la red de destino (BSSID), ESSID y canal, respectivamente. Después de ejecutarse durante el tiempo necesario, el acosador simplemente enviará el PIN WPS y la clave de cifrado WPA / WPA2 al terminal de comando.

Mapeo De Red Con NMAP

Después de obtener acceso a una red inalámbrica, el siguiente paso importante para el hacker es investigar cualquier vulnerabilidad de cliente explotable. En primer lugar, sin embargo, una vista panorámica de la red y sus clientes conectados es útil para identificar posibles objetivos. No debería sorprendernos que Kali Linux venga con una aplicación gratuita de mapeo de red de código abierto. Network Mapper, o ***nmap***, escanea una red conectada al "hacer ping" a los nodos en la red con paquetes especiales que están diseñados para obtener una respuesta de los hosts. Nmap analiza los paquetes de respuesta y construye metódicamente un "mapa" de la red descubriendo los hosts, escaneando sus puertos y determinando el tipo y las versiones de los sistemas operativos que se ejecutan en cada dispositivo.

Una forma sencilla de familiarizarse con nmap y practicar el mapeo de red es usarlo en la propia red. Al igual que otros comandos de Linux, nmap tiene una serie de opciones que se pueden agregar al comando para especificar las funciones deseadas. La opción "-sn" realiza un escaneo simple para los hosts abiertos en la red. El siguiente ejemplo:

```
# nmap -sn 10.0.0. *
```

Recorre todas las direcciones IP en el dominio proporcionado e informa las direcciones MAC de cualquier host abierto, incluidos los fabricantes asociados con direcciones MAC conocidas. La Figura 47 muestra los resultados en una red doméstica inalámbrica.

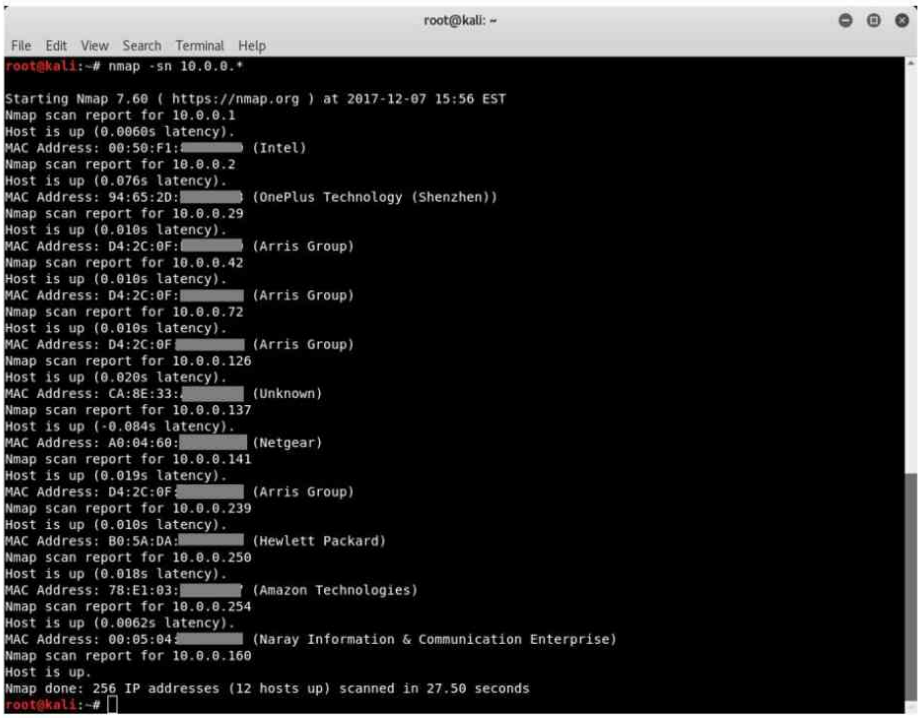


Figura 47 - resultados de nmap

Una mirada rápida a la salida revela que los dispositivos que se pueden suponer son teléfonos inteligentes, tabletas, enrutadores, impresoras y dispositivos conectados. Algunos de los nombres de los fabricantes se refieren a los adaptadores de red de lo que posiblemente sean computadoras.

Aunque nmap en sí mismo es una aplicación de línea de comando y produce salida de texto, sus resultados pueden ser analizados por aplicaciones complementarias que proporcionan una representación más visual de la red. La aplicación ***zenmap*** incluida en Kali Linux puede producir una topología de red gráfica (Figura 48) usando nmap como back-end.

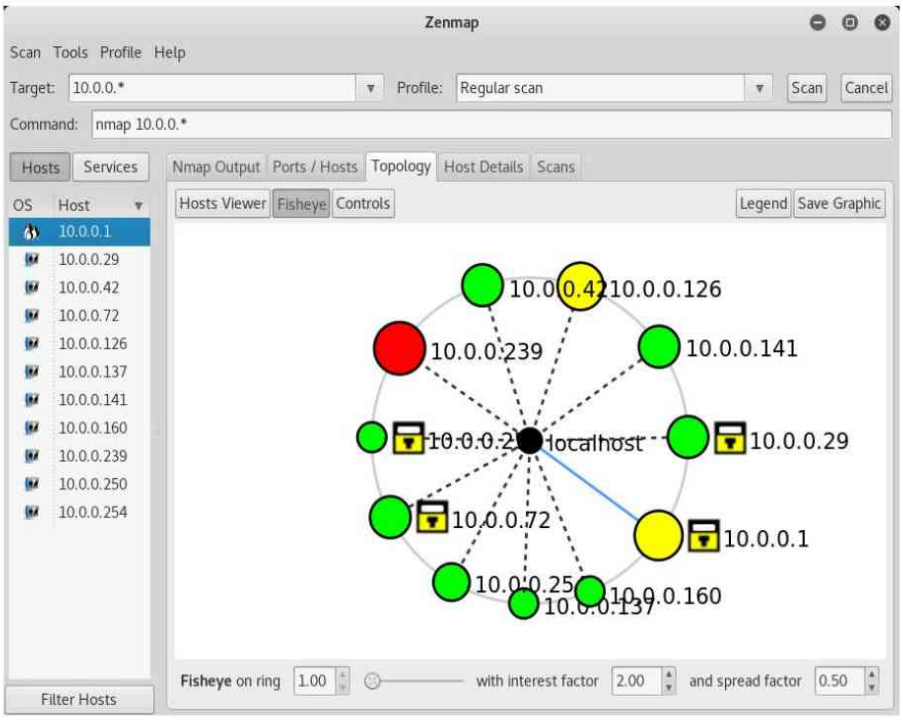


Figura 48 - resultados de zenmap

La opción "-O" (letra mayúscula O) en nmap se puede usar para determinar el sistema operativo que se ejecuta en un host de destino. Esta información es útil para planificar un exploit. La ejecución de un análisis del sistema operativo en el destino 10.0.0.1 revela sus puertos abiertos y un sistema operativo basado en Linux.

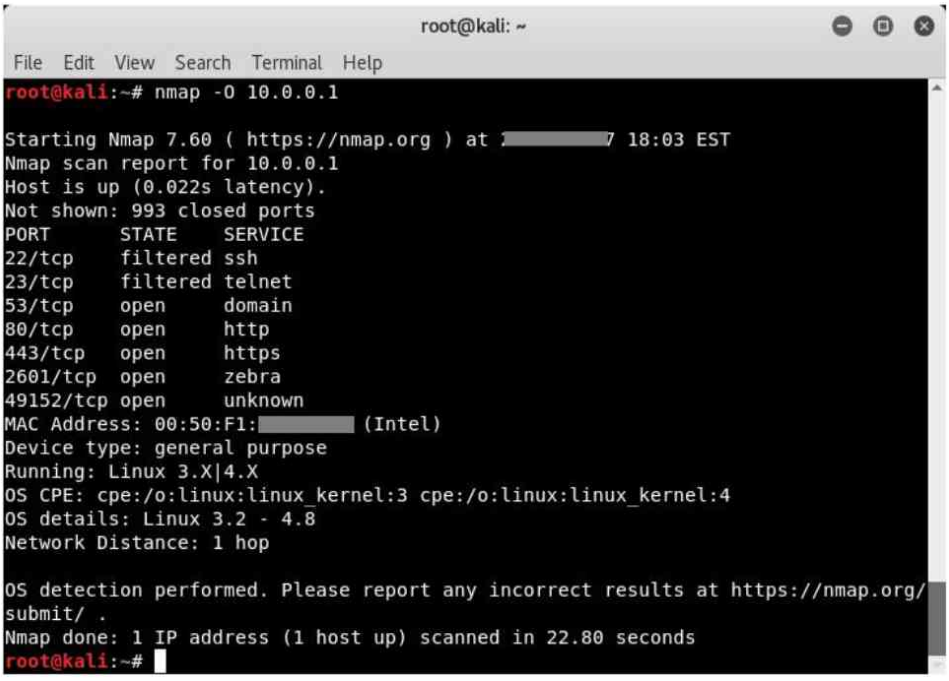


Figura 49 - Escaneo del sistema operativo en nmap

Una amplia gama de opciones de nmap le permite al usuario controlar cuánta o poca información recopilar y revelar en un escaneo.

Es importante recordar que usar nmap no es una actividad pasiva, funciona intercambiando paquetes con nodos de destino. Algunas máquinas están equipadas para detectar cuándo se están escaneando y generar una alerta, recopilar información de encabezado de los paquetes entrantes o bloquear la dirección IP de origen sospechosa.

Metasploit

Metasploit es una de las herramientas más poderosas en el arsenal de hackers serios. Metasploit proporciona un marco para detectar y explotar vulnerabilidades en los puertos de destino. Utiliza una base de datos constantemente actualizada de vulnerabilidades conocidas del sistema y sus vulnerabilidades asociadas. A partir de 2017, Metasploit presenta más de 1600 exploits (y sigue creciendo).

Metasploit requiere una interfaz externa para ejecutarse. Hay varias opciones de interfaces que pueden ejecutar Metasploit, algunas de las cuales también administran otras aplicaciones. La aplicación ***msfconsole*** (Metasploit Framework Console), disponible en Kali Linux, es una interfaz estándar para ejecutar Metasploit. Para iniciarla:

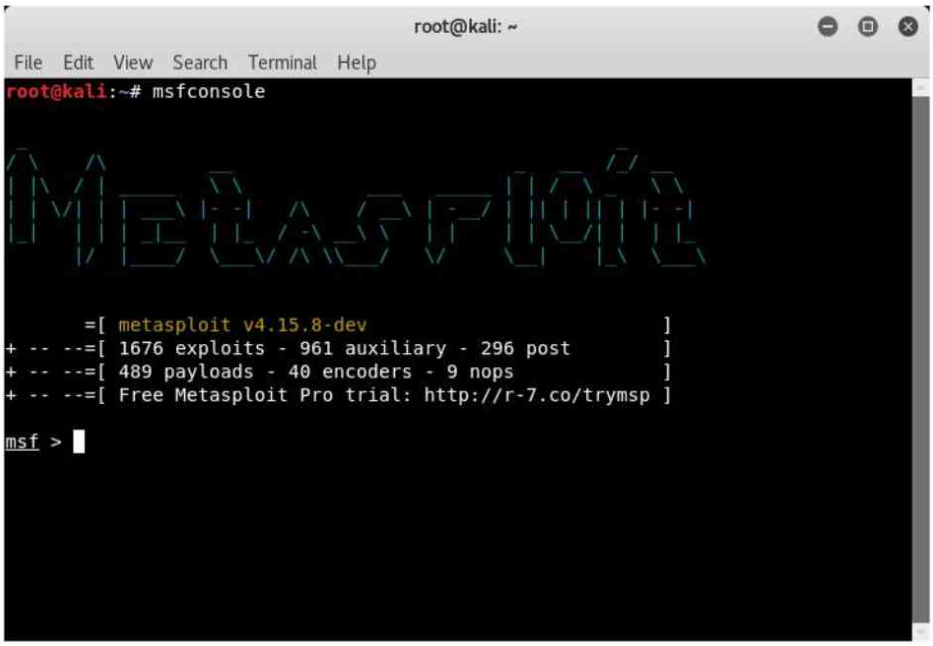


Figura 50 - msfconsole

Una característica útil de msfconsole es que otras herramientas, como nmap, se pueden ejecutar dentro de la interfaz, aunque a veces con una sintaxis diferente que en el terminal de comando de Linux. Para ejecutar nmap en un objetivo seleccionado:

msf> db_nmap <opciones> <ip de destino>

Después de identificar un objetivo, puede buscar en la base de datos de metasploit vulnerabilidades en el sistema operativo o abrir el servicio identificado en sus escaneos:

msf> buscar <palabra clave>

donde <palabra clave> identifica el servicio o aplicación de destino:

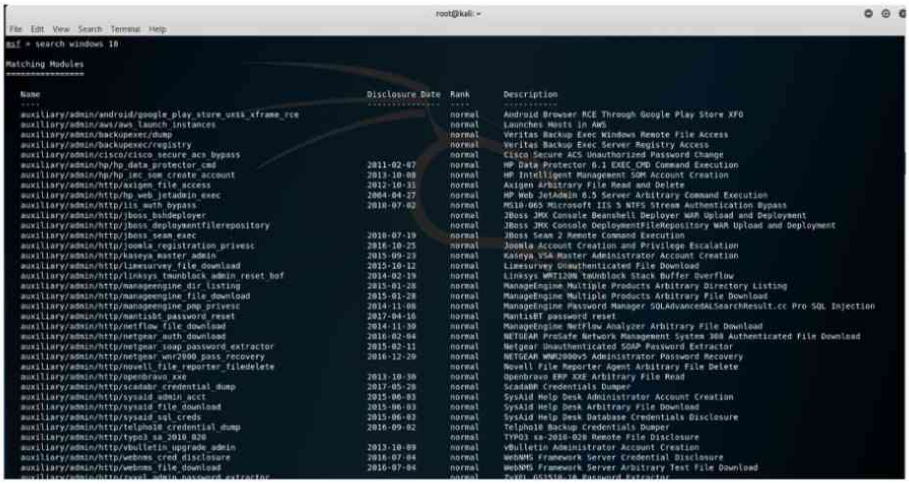


Figura 51 - Búsqueda de vulnerabilidad de metasploit

Las vulnerabilidades conocidas se enumeran y describen junto con sus respectivas fechas de descubrimiento.

Capítulo 13. Denegación Inalámbrica Del Servicio

Los ataques de denegación de servicio (DoS), introducidos en principio en ***Hacking para principiantes***, son intentos de evitar que los usuarios legítimos accedan a servicios o recursos en un host determinado. Las razones de los ataques DoS van desde la travesura general y el activismo social o político hasta las actividades más serias de chantaje o guerra electrónica patrocinada por el estado. Los ataques DoS son relativamente fáciles de ejecutar porque no necesariamente requieren acceso al sistema de destino y, por lo tanto, no implican un descifrado complicado o la inyección de cargas útiles. Como resultado, estos ataques se pueden lanzar a través de Internet desde múltiples ubicaciones anónimas, muchos de los cuales pueden ser secuestrados anfitriones que se han convertido en participantes involuntarios. Esto se conoce como denegación de servicio distribuida (DDoS) y es muy difícil y costoso de prevenir.

La denegación inalámbrica de servicio difiere de los ataques DoS tradicionales de "línea de cable" en que el atacante (al menos, el host atacante del punto final) debe estar dentro del rango de radiofrecuencia del punto de acceso objetivo. Los ataques DoS inalámbricos se pueden ejecutar interfiriendo la señal de Wi-Fi en el canal de destino o forzando el punto de acceso para desacreditar repetidamente clientes legítimos asociados. Estos no son ataques pasivos y pueden requerir cuidado para ofuscar la fuente de los paquetes ofensivos.

Existe cierto desacuerdo sobre si la denegación de servicio es técnicamente "hacking", ya que el atacante no está realmente accediendo a los recursos. En cualquier caso, los ataques DoS implican el mismo conjunto de habilidades y herramientas que otros tipos de hacking y dan como resultado un comportamiento involuntario del sistema. Tanto como cualquier otro tipo de ataque, los profesionales de seguridad deben comprender cómo se llevan a cabo para

protegerse contra ellos. Además, los ataques de deauth suelen ser precursores de actividades más intrusivas y se utilizan para obligar a los clientes a acceder a puntos de acceso comprometidos.

Ataques De Desautenticación

El Capítulo 9 discute el proceso de reconocimiento con el que las redes Wi-Fi autentican a los clientes. Este proceso implica un intercambio de paquetes de varios pasos entre el agente de autenticación (generalmente un punto de acceso o enrutador) y el cliente. Una de las responsabilidades del punto de acceso (AP) es volver a autenticar a los clientes que han sido desconectados temporalmente (una ocurrencia común en las redes inalámbricas), lo que hace al pedirle al cliente que acuse recibo (ACK) del paquete de saludo inicial. Un ataque de desautenticación (deauth) funciona enviando un flujo de paquetes tanto al AP como al cliente. El AP y el cliente responden con paquetes ACK que están fuera de contexto para un procedimiento de protocolo de enlace estándar (Figura 9). Mientras este ataque sea sostenido, el cliente bajo ataque no podrá autenticarse adecuadamente en la red. Este es un ejemplo de un ataque de hombre en el medio (ver ***Hacking para principiantes***). Solo requiere paquetes falsificados y no requiere que la máquina atacante sea parte de la red o tenga la clave de cifrado.

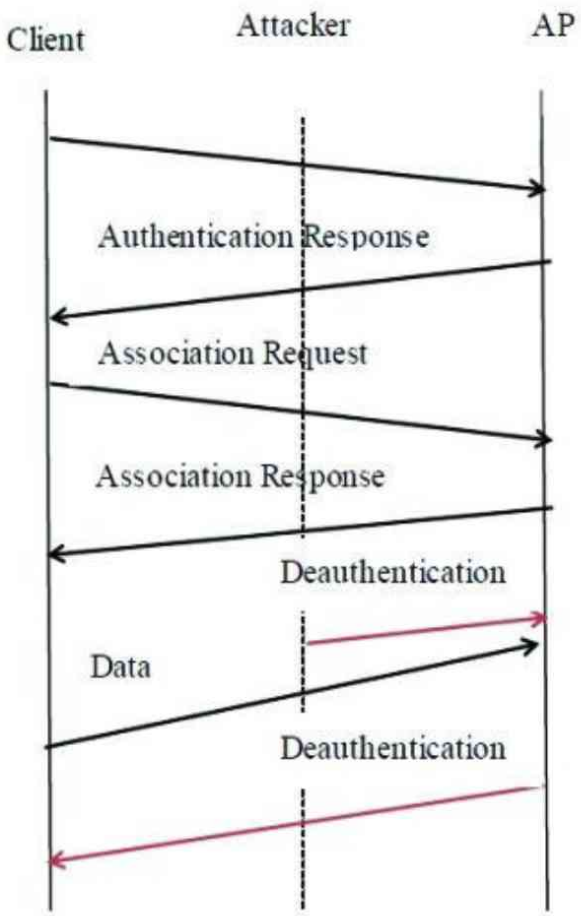


Figura 52 - Ataque de desautenticación (opensourceforu.com)

ATAQUES "MUERTOS" CON AIRCRACK

Se puede lanzar un simple ataque de eliminación de Wi-Fi usando el paquete de aircrack y un adaptador inalámbrico adecuado que admita el modo de monitor.

Utilizando el procedimiento descrito en los capítulos anteriores, coloque el adaptador de Wi-Fi conectado de la máquina atacante en modo monitor y comience airodump-ng para comenzar a recolectar paquetes. También puede falsificar su dirección MAC con macchanger para mantener el anonimato. Elija un cliente en la lista de airodump que desee denegar el servicio. Para este ataque necesitará el BSSID (dirección MAC) tanto del cliente como del AP asociado. El comando de inyección de paquetes aireplay-ng se usa para la desautenticación:

aireplay-ng -0 1 -a 00: 14: 6C:XX:XX:XX -c 00:0F:B5:XX:XX:XX atho

Donde -0 le dice al programa que inyecte paquetes de deauth. El "1" es el número de veces que se debe ejecutar el procedimiento, enviando 64 paquetes a cada nodo. Cuanto mayor sea el número, más durará el ataque. Un "0" hará que el ataque se repita hasta que se detenga manualmente. La opción -a es seguida por el BSSID del AP y el -c por el BSSID del cliente. "Atho" es el adaptador wifi de ataque.

Capítulo 14. Conclusión

Ética

Hacking para principiantes analiza los diferentes "sombreros" del hacking: el negro, el blanco y el gris. El sombrero negro es la idea estereotipada de cómo la mayoría de la sociedad concibe a los hackers: el que quiere acceso no autorizado a la propiedad o información de otro. El sombrero blanco es el "buen chico": el que aprende los trucos del oficio para evitar la explotación de activos o localizar a los delincuentes. El sombrero gris es un poco híbrido, usan sus habilidades de hacking (aunque sin el conocimiento previo o la autorización de los propietarios) para exponer las debilidades en los sistemas para que esos sistemas puedan fortalecerse. Independientemente de las motivaciones de cualquier individuo, la base de conocimientos y el conjunto de herramientas generales siguen siendo los mismos. El hacking requiere una comprensión de cómo los equipos informáticos se comunican en varios niveles, qué vulnerabilidades se encuentran tanto en las máquinas como en las redes, y cómo se explotan esas vulnerabilidades. Este conocimiento requiere tiempo, práctica, estudio y disciplina para alcanzarlo, y no es algo con lo que la gente común esté familiarizada. Como resultado, los hackers expertos tienen la capacidad de infligir o prevenir un daño considerable en individuos, organizaciones y la sociedad.

Cada hacker debería adoptar un código de ética para guiarlos. Incluso los sombreros negros tendrán alguna línea que no cruzarán para llevar a cabo sus ataques. La aplicación de la ley se está volviendo muy seria sobre la seguridad de la información y la prevención de ataques generalizados a las identidades individuales, el comercio y las instituciones gubernamentales. Las leyes y la aplicación varían según la ubicación, pero cualquier hacker (negro, blanco o gris) debe tener una comprensión completa de los riesgos que están asumiendo. Esto es especialmente cierto para los hackers principiantes que no tienen la experiencia de ocultar sus huellas o evitar daños colaterales. Un

ataque que se realiza incorrectamente podría borrar o corromper la información, o causar otras consecuencias no deseadas. Es por eso que es importante practicar habilidades en los sistemas de uno en un "sandbox" aislado hasta ganar la suficiente confianza para atacar a otro sistema.

Manteniendo El Borde Del Hacker

Hay una carrera perpetua entre la comunidad de hackers y la comunidad de seguridad de la información. Cuando se descubre la vulnerabilidad, tiende a extenderse sabia y rápidamente como lo demuestra el ataque WPA Krack descrito en el Capítulo X. El personal de seguridad intenta mantenerse al día constantemente haciendo parches o actualizaciones para proteger los sistemas. Los hackers deben perfeccionar constantemente su oficio y superar los límites para mantener una ventaja. Como cualquier habilidad, las habilidades de los hackers disminuyen si no se usan regularmente. Además, el panorama en seguridad informática está en constante cambio. La naturaleza de código abierto de la mayoría de las herramientas de hacking significa que hay cambios frecuentes en la funcionalidad y la sintaxis que deben mantenerse al día. Las vulnerabilidades se publican y se revisan casi a diario, y los estándares de cifrado se están presionando muy duro para proporcionar una mejor seguridad contra los ataques. Entonces, para mantener una ventaja y tener una posibilidad razonable de convertirse en un hacker exitoso, uno debe hacer lo siguiente:

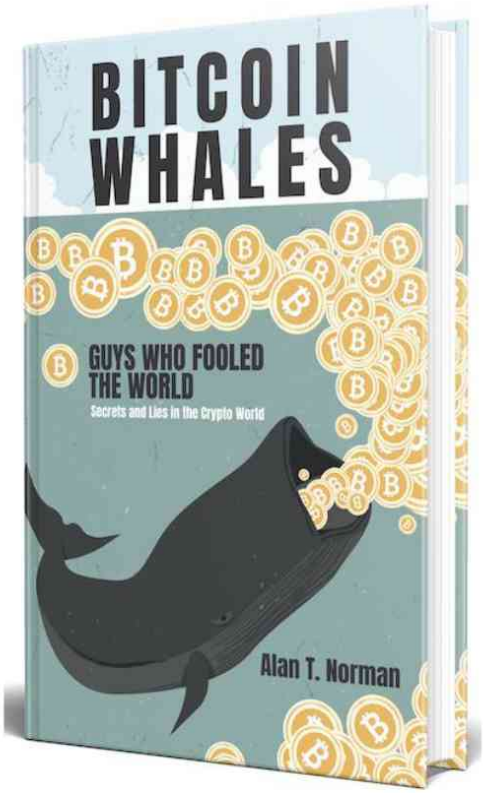
1. Mantener las versiones actuales de todos los sistemas operativos, scripts, herramientas y entornos de programación.
2. Practique las habilidades de forma regular, en un entorno de espacio aislado, con énfasis en mejorar tanto la velocidad como el anonimato.
3. Investigue periódicamente su propio sistema y adopte las medidas de seguridad apropiadas.
4. Tenga un ciclo de lectura diario o semanal sobre desarrollos de seguridad tanto ofensivos como defensivos (revistas, diarios, artículos web, tableros de mensajes, comunidades de hackers web oscuros, etc.) Texto del capítulo.

Acerca Del Autor

Alan T. Norman es un hacker orgulloso, inteligente y ético de la ciudad de San Francisco. Después de recibir una Licenciatura en Ciencias en la Universidad de Stanford. Alan ahora trabaja para una empresa de tecnología de la información de tamaño medio en el corazón de SFC. Aspira a trabajar para el gobierno de los Estados Unidos como hacker de seguridad, pero también le encanta enseñar a otros sobre el futuro de la tecnología. Alan cree firmemente que el futuro dependerá en gran medida de los "geeks" informáticos tanto para la seguridad como para el éxito de las empresas y los futuros trabajos por igual. En su tiempo libre, le encanta analizar y escrutar todo sobre el juego de baloncesto.

Bitcoin Whales Libro Bono

Encuentre El Enlace Al Libro De Bonificación A Continuación



Enlace al Libro: http://bit.ly/2LprwpV

Una última Cosa...

¿DISFRUTÓ EL LIBRO?

¡SI ES ASÍ, ENTONCES HÁGALO SABER DEJANDO UNA RESEÑA EN AMAZON! Las reseñas son el alma de los autores independientes. Agradecería incluso unas pocas palabras y calificación si solo para eso tiene tiempo

SI NO LE GUSTA ESTE LIBRO, ¡POR FAVOR DÍGAMELO! Envíeme un correo electrónico a alannormanit@gmail.com y hágame saber lo que no le gustó! Quizás pueda cambiarlo. En el mundo de hoy, un libro no tiene que estar estancado, puede mejorar con el tiempo y los comentarios de lectores como usted pueden impactar este libro, y agradezco sus comentarios. ¡Ayuda a mejorar este libro para todos!