MANUAL DE GUÍAS PARA EL APRENDIZAJE DE LINUX

RICARDO ENRIQUE ALVAREZ TÁMARA

UNIVERSIDAD PONTIFICIA BOLIVARIANA
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESCUELA DE INGENIERÍA
BUCARAMANGA
2016

MANUAL DE GUÍAS PARA EL APRENDIZAJE DE LINUX

RICARDO ENRIQUE ALVAREZ TÁMARA

PROYECTO DE GRADO PARA OPTAR POR EL TITULO DE INGENIERO ELECTRÓNICO

DIRECTOR
PH.D. JHON JAIRO PADILLA AGUILAR

UNIVERSIDAD PONTIFICIA BOLIVARIANA
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESCUELA DE INGENIERÍA
BUCARAMANGA
2016

Nota de aceptación

_____
_____
_____
_____
_____

_____
Firma del director de proyecto

_____
Firma del jurado

_____
Firma del jurado

Bucaramanga, febrero 12 de 2016

AGRADECIMIENTOS

Primero que todo darle gracias a Dios y a mis padres, los cuales fueron y son muy importantes para seguir siempre adelante con mis sueños y mis metas.
También a mis familiares, amigos y a los profesores los cuales aportaron en los conocimientos de la carrera y de la vida.

CONTENIDO

Pág

LISTA DE FIGURAS

Pág

RESUMEN GENERAL DEL TRABAJO DE GRADO

TITULO: MANUAL DE GUÍAS PARA EL APRENDIZAJE DE LINUX

AUTOR: RICARDO ENRIQUE ALVAREZ TÁMARA

FACULTAD: INGENIERÍA ELECTRÓNICA

DIRECTOR: Ph. D. JHON JAIRO PADILLA AGUILAR

RESUMEN:

El objetivo de este proyecto es crear guías de laboratorio que introduzcan al estudiante en las bases del manejo del sistema operativo Linux y el manejo de las redes de computadores en Linux. Esto permitirá capacitar al estudiante para que desarrolle proyectos en el área de redes de computadores.

La metodología usada es basada en el modelo pedagógico integrado de la Universidad Pontificia Bolivariana. El estudiante estará interesado en investigar más debido a que las guías se presentan de una forma dinámica que hará que desarrolle sus destrezas, habilidades, actitudes y valores en este campo; también hay un tema muy delicado que es el hackeo, en el cual se le explica al estudiante cómo poder hacerlo de una forma ética, ya que este modelo pedagógico se basa en principios éticos y responsabilidad social.

El principal resultado obtenido es que los alumnos aprenden rápidamente el manejo del sistema operativo Linux y el funcionamiento de las redes, además del aprendizaje sobre cómo crear sus programas personales de acuerdo a sus necesidades.

Las guías están muy bien distribuidas siguiendo un orden y proceso en aumento del conocimiento y complejidad, lo que permite al estudiante un aprendizaje paso a paso.

PALABRAS CLAVE: Comandos, redes, terminal, Wireshark, Kali Linux, Hacking ético.

GENERAL SUMMARY OF WORK OF GRADE

TITLE: LAB PRACTICES MANUAL FOR LINUX LEARNING

AUTHOR: RICARDO ENRIQUE ALVAREZ TÁMARA

FACULTY: ELECTRONIC ENGINEERING

DIRECTOR: Ph. D. JHON JAIRO PADILLA AGUILAR

ABSTRACT:

The main objective of this project is to create lab guides which introduce students to the basics of the Linux operating system management, and some aspects of management of computer networks in Linux. These guides enable students to develop projects in the area of computer networks.

The methodology is based on the integrated pedagogical model used in the Pontificia Bolivariana University. The student is interested in research more in depth because the guides are presented in a dynamic way that will develop their skills, abilities, attitudes and values in this field. There is also a very sensitive issue that is hacking. Some aspects of Hacking are explained to the student, such as how to do it in an ethical manner, because this educational model is based on ethics and social responsibility.

The main result is that students quickly learn the Linux operating system management and the operation of networks under Linux system, also, the student learns how to use the tasks programming under bash shell.

The guides are very well distributed following an increasing complexity order and process knowledge, which allows an easy step by step learning.

KEY WORDS: Commands, networks, terminal, Wireshark, Kali Linux, Ethical Hacking.

INTRODUCCIÓN

Dentro de la Facultad de Ingeniería Electrónica de la Universidad Pontificia Bolivariana se ha venido avanzando en el desarrollo de prácticas de laboratorio para la asignatura “Redes de datos”; en estas prácticas se ha requerido el manejo del sistema operativo Linux, también dentro de los proyectos de grado y proyectos de investigación desarrollados en el área de telecomunicaciones, se ha detectado la necesidad de que los estudiantes tengan ciertas bases del sistema operativo Linux.

Es por estas razones, que el proyecto que se plantea se enfocará en crear guías de laboratorio que introduzcan al estudiante en las bases del manejo del sistema operativo Linux y el manejo de las redes en Linux.
El proyecto a desarrollar, se basaría exclusivamente en el sistema operativo Linux versión Backtrack5r3, distribución de Linux que fue diseñada para aplicar auditoria de seguridad informática. La versión Backtrack caducó durante el desarrollo del proyecto, por tal motivo se trabajó con la versión actual llamada Kali Linux para trabajar con programas mejores y actualizados que nos brinda esta versión de Linux para la seguridad en las redes.

En este documento se presenta la justificación del por qué se desarrollará el proyecto, objetivos que se desean lograr, información más relevante para el desarrollo de este, al igual que la metodología que se llevará para la realización de las guías, el cronograma y los resultados esperados.
En las guías a desarrollar se encontrarán temas relacionados con redes de computadores como comandos básicos de Linux, comandos básicos para redes, manejo del bash Shell (script), instalación de programas, configuración básica de tarjetas de red (dirección IP, mascara, comando ifconfig, broadcast), instalación de máquinas virtuales, programas de escaneo de la red como el Wireshark y por último una introducción al mundo del hackeo ético.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Crear guías de laboratorio que introduzcan al estudiante en las bases del manejo del sistema operativo Linux y el manejo de las redes de computadores en Linux. Esto permitirá capacitar al estudiante para que desarrolle proyectos en el área de redes de computadores.

1.2 OBJETIVOS ESPECÍFICOS

- Investigar en diferentes fuentes el manejo de Linux en las áreas de capacitación del proyecto.
- Seleccionar los temas que deberán cubrirse en las diferentes guías de laboratorio.
- Investigar modelos pedagógicos para el diseño adecuado de las guías.
- Realizar pruebas de las guías con estudiantes para determinar el tiempo destinado para cada guía y comprobar la importancia de los temas planteados.

2. MARCO TEÓRICO

2.1 ¿QUÉ ES KALI LINUX?[1]

Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad.

Kali es una completa re-construcción de BackTrack Linux desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de Debian. Toda la nueva infraestructura ha sido puesta en el lugar, todas las herramientas fueron revisadas y fueron embaladas, y se ha cambiado a Git para el VCS.

- **Más de 300 herramientas de pruebas de penetración:** Después de revisar todas las herramientas que se incluyen en BackTrack, hemos eliminado una gran cantidad de herramientas que, o bien no funcionaban o tenían otras herramientas disponibles que proporcionan una funcionalidad similar.
- **Gratis y siempre lo será:** Kali Linux, al igual que su predecesor, es completamente gratis y siempre lo será. Nunca, jamás, tendrás que pagar por Kali Linux.
- **Git – árbol de código abierto:** Somos partidarios enormes de software de código abierto y nuestro árbol de desarrollo está disponible para todos y todas las fuentes están disponibles para aquellos que desean modificar y reconstruir paquetes.
- **Obediente a FHS:** Kali ha sido desarrollado para cumplir con el Estándar de jerarquía del sistema de ficheros, permitiendo que todos los usuarios de Linux puedan localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, etc.
- **Amplio apoyo a dispositivos inalámbricos:** Hemos construido Kali Linux para que soporte tantos dispositivos inalámbricos como sea posible, permitiendo que funcione correctamente en una amplia variedad de hardware y hacerlo compatible con varios USB y otros dispositivos inalámbricos.
- **Kernel personalizado con parches de inyección:** Como probadores de penetración, el equipo de desarrollo a menudo tiene que hacer evaluaciones inalámbricas para que nuestro kernel tenga los últimos parches de inyección incluidos.

[1] KALI LINUX Official Documentation, Introducción, ¿Qué es kali linux?, 2015, http://es.docs.kali.org/introduction-es/que-es-kali-linux [Consulta: Jueves, 10 de diciembre 2015]

- **Entorno de desarrollo seguro:** El equipo de Kali Linux está compuesto por un pequeño grupo de personas de confianza que sólo puede comprometer e interactuar con los paquetes de los repositorios, haciendo uso de múltiples protocolos seguros.
- **Paquetes firmados con PGP y repos**: Todos los paquetes de Kali son firmados por cada desarrollador individualmente cuando se construyen y son comprometidos. Los repositorios posteriormente firman los paquetes también.
- **Multi-lenguaje:** Aunque las herramientas de penetración tienden a ser escritas en inglés, nos hemos asegurado de que Kali tenga soporte multilingüe, lo que permite a más usuarios poder operar en su idioma nativo y encontrar las herramientas necesarias para el trabajo.
- **Totalmente personalizable:** Estamos completamente consiente de que no todo el mundo estará de acuerdo con nuestras decisiones de diseño por lo que hemos hecho lo más fácil posible para nuestros usuarios más aventureros puedan personalizar Kali Linux a su gusto, todo el camino hasta el núcleo.
- **Soporte ARMEL y ARMHF:** Dado a que los sistemas basados en ARM son cada vez más frecuentes y de bajo costo, sabíamos que el soporte de ARM de Kali tendrían que ser tan robusta como podríamos administrar, resultando en instalaciones que trabajan en sistemas de ARMEL y ARMHF. Kali Linux tiene repositorios ARM integrado con la línea principal de distribución de modo que las herramientas para ARM serán actualizada en relación con el resto de la distribución. Kali está disponible para los dispositivos ARM siguientes:
  - rk3306 mk/ss808
  - Raspberry Pi
  - ODROID U2/X2
  - MK802/MK802 II
  - Samsung Chromebook

Kali está diseñado específicamente para las pruebas de penetración y, por tanto, toda la documentación de este sitio asume el conocimiento previo del sistema operativo Linux.

2.1.1 Diferencias entre Kali Linux y Debian[2]

Kali Linux está orientado a pruebas de penetración profesional y auditorías de seguridad. Como tal, varios cambios han sido implementados en Kali Linux para que reflejen estas necesidades:

1. **Un solo usuario, acceso root por diseño:** Debido a la naturaleza de las auditorías de seguridad, Kali Linux está diseñado para ser usado en un escenario "de un solo usuario, root".
2. **Servicio de redes deshabilitado en forma predeterminada:** Kali Linux contiene ganchos sysvinit los cuales deshabilitan los servicios de redes por defecto. Estos ganchos nos permiten instalar varios servicios en Kali Linux, mientras aseguran que nuestra distribución permanezca segura en forma predeterminada, no importando que paquetes estén instalados. Adicionalmente los servicios tales como Bluetooth son también puestos en lista negra por defecto.
3. **Kernel de linux modificado:** Kali Linux usa un kernel, parchado para la inyección wireless.

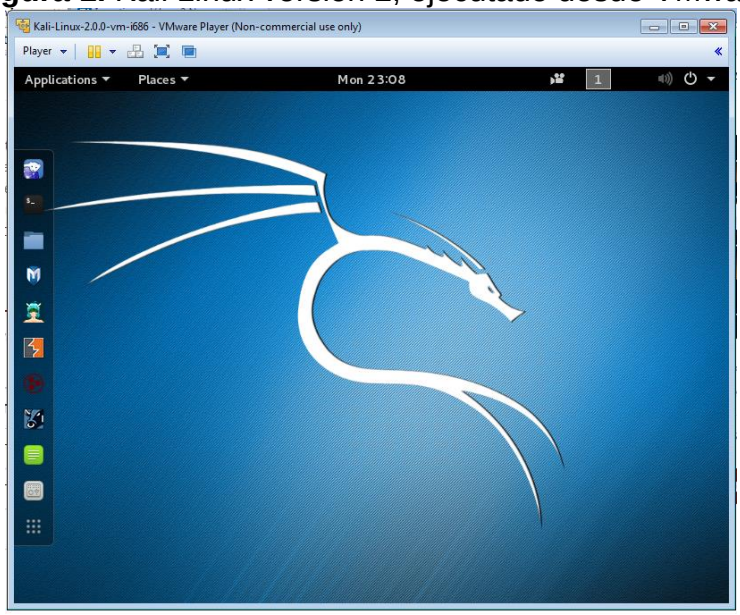
2.1.2 Es Kali Linux correcto para Tí?

Como desarrolladores de la distribución, uno esperaría que recomendáramos a todos el uso de Kali Linux. De hecho sin embargo, por ser Kali una distribución específicamente generada para profesionales en penetration testing y auditorías de seguridad, nosotros **NO** recomendamos esta distro para personas que no estén familiarizadas con Linux.

Adicionalmente, el mal uso de las herramientas de seguridad dentro de la red, sobre todo sin permiso, puede causar daños irreparables y tener consecuencias significativas.

[2] KALI LINUX Official Documentation, ¿Debería usar Kali linux?, 2015, http://es.docs.kali.org/introduction-es/deberia-usar-kali-linux [Consulta: Jueves, 10 de diciembre 2015]

Figura 1. Kali Linux versión 2, ejecutado desde VMware



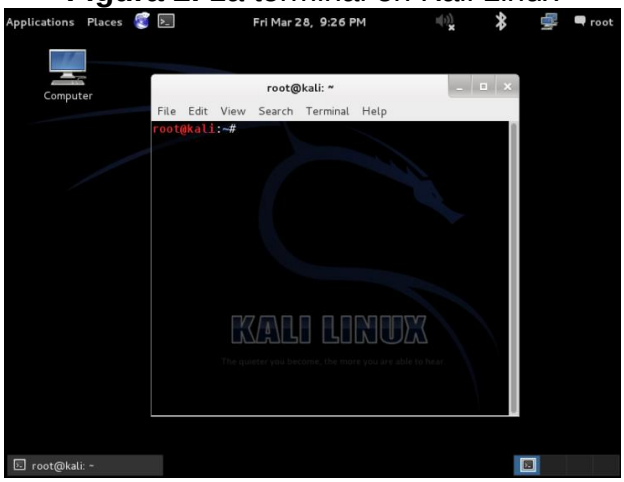
2.2 Que es la terminal?

Linux dispone de un intérprete de órdenes o terminal.
Un terminal es una forma de acceder al sistema sin utilizar la interfaz gráfica, es decir, realizar todo tipo de tareas en formato texto. La forma de utilizar el sistema de este modo es mediante órdenes.
El terminal muestra en pantalla un indicador de línea de órdenes (en inglés se conoce como *prompt*) esperando que el usuario introduzca una orden.
La terminal es una herramienta tan poderosa que puede realizar actividades que un programa mediante GUI (Interfaz Gráfica) no haría.

Funcionalidades de la terminal:

- Instalar, ejecutar o desintalar Software
- Leer documentos
- Descomprimir, comprimir Archivos
- Conectarse a Servidores
- Programar, Jugar, etc.

Figura 2. La terminal en Kali Linux

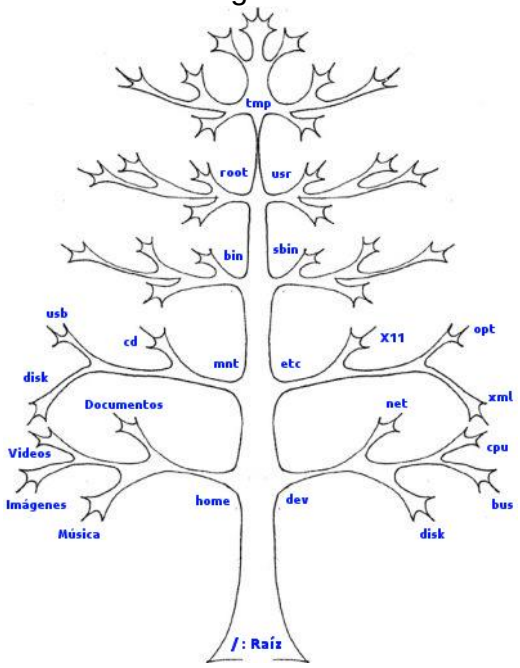


2.3 Estructura general de los directorios

En el sistema de ficheros de Linux, existen varias sub-jerarquías de directorios que poseen múltiples y diferentes funciones de almacenamiento y organización en todo el sistema. Estos directorios pueden clasificarse en:

Estáticos: Contiene archivos que no cambian sin la intervención del administrador (root), sin embargo, pueden ser leídos por cualquier otro usuario. (**/bin**, **/sbin**, **/opt**, **/boot**, **/usr/bin**…)
Dinámicos: Contiene archivos que son cambiantes, y pueden leerse y escribirse (algunos sólo por su respectivo usuario y el root). Contienen configuraciones, documentos, etc. (**/var/mail**, **/var/spool**, **/var/run**, **/var/lock**, **/home**…)
Compartidos: Contiene archivos que se pueden encontrar en un ordenador y utilizarse en otro, o incluso compartirse entre usuarios.
Restringidos: Contiene ficheros que no se pueden compartir, solo son modificables por el administrador. (**/etc**, **/boot**, **/var/run**, **/var/lock**…)
root: es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos (mono o multi usuario). root es también llamado superusuario. Normalmente esta es la cuenta de administrador. El usuario root puede hacer muchas cosas que un usuario común no puede, tales como cambiar el dueño o permisos de archivos y enlazar a puertos de numeración pequeña.
Dicha estructura se representa en forma de árbol, como se muestra en la siguiente imagen:

Figura 3. Estructura general de los directorios



Donde la raíz del árbol (***/***) es la base de toda la estructura de directorios y las ramas (**directorios y archivos**) surgen o cuelgan de dicha base.

2.4 Comando básicos [3]

Hay que tener en cuenta que en Linux el intérprete de comandos diferencia entre mayúsculas y minúsculas esto quiere decir que no es lo mismo escribir ls que Ls.

- **cd** (change directory)**:** Con este comando se puede navegar a través de los directorios.
- **cd .. :** Volver al directorio superior o anterior.
- **pwd** (print working directory)**:** Este comando permite conocer cuál es el directorio actual.
- **ls** (list)**:** Con este comando se ven todos los archivos y carpetas que se encuentran en el directorio actual, las carpetas y archivos se diferencian por colores.
- **cp** (copy)**:** Permite copiar archivos de un directorio a otro.
- **mv** (move)**:** Se utiliza para mover un archivo o directorio a otro, también permite cambiar el nombre de un archivo o directorio.

[3] WEIDMAN, Georgia. Penetration Testing. A hands-On introduction to hacking. San Francisco: No Starch Press, 2014, pág 57, [Consulta: 4 de Agosto de 2015]

- **mkdir** (make directory)**:** Para crear una nueva carpeta o directorio.
- **rmdir** (remove directory)**:** Para borrar un directorio o carpeta.
- **rm** (remove)**:** Este comando permite borrar archivos.
- **rm -r** nombre_directorio (remove recursive)**:** Con este comando se borra un directorio con todo lo que contiene dentro.
- **rm -rf** (remove recursive force)**:** Elimina todos los archivos del directorio.
- **rm arch*:** Elimina todo lo que empiece por arch. El carácter asterisco (*) se emplea como un comodín.
- **man** (manual page or man page): Permite saber más acerca del comando, como su uso, descripción y opciones de uso. Ejemplo: man ls
- **vi nombre.txt:** Crea un archivo con el editor de textos.
- **clear:** Borrar lo que está escrito en el terminal.
- **exit:** Se utiliza para cerrar la terminal.

2.5 Comando básicos utilizado en redes

- **Comando ifconfig**

Con este comando se puede configurar la dirección IP de red asociada a la máscara de subred; la dirección del hardware de la tarjeta, es decir, la dirección MAC; se podrá especificar la dirección *broadcast* de la red; permitirá habilitar o deshabilitar la tarjeta de red especificada.
Modo de uso: ifconfig *interfaz* [*dirección* [parámetros]]

- **Comando hostname**

Muestra o establece el nombre del sistema o equipo.
Modo de uso: hostname [-d] [-F nombre_archivo] [-f] [-h] [-s] [-v] [i] [I] [y]

- **Comando ping**

El comando ping es usado para probar la conexión y la latencia entre dos conexiones de red. Estas conexiones pueden ser conexiones de área local, área amplia o el Internet como un todo. El comando ping envía paquetes de información a una dirección IP específica y luego mide el tiempo que se tarda en obtener una respuesta de la computadora o dispositivo especificado.
Modo de uso: ping [-r] [-v] host [tamaño_paquete] [count]
Las teclas ctrl+z y ctrl+c se utilizan para detener el proceso y la diferencia entre estas dos es que cuando se utiliza ctrl+c nos da como resultado las estadísticas de la conexión, como los paquetes transmitidos, recibidos, paquetes perdidos y el tiempo.

- **Comando netstat**

Muestra conexiones de red, tablas de ruteo, estadísticas de interfaces, etc.
Este comando es importante, ya que es una herramienta para seguir el rastro de las conexiones a la red en su sistema, también es útil para la corrección de errores, detección de fallas de seguridad y los problemas cotidianos de la red
Modo de uso: netstat [-a] [-t] [l] [-p] [-natu] [-u]

- **Comando arp**

Este comando permite obtener la dirección MAC de una interfaz de red.
ARP, Protocolo de resolución de direcciones, es un mecanismo que permite a IP convertir las direcciones Ethernet en direcciones IP; esto es importante porque cuando envía un paquete por una red Ethernet, es necesario poner la dirección Ethernet del anfitrión destino.
Modo de uso: *arp [-v] [-t type] -d [hostname]*

- **Comando traceroute**

Muestra la ruta que siguen los paquetes desde el origen hasta el destino; además nos da una idea de la rapidez de la ruta. Al mostrar la ruta se puede tener una idea de la estructura interna (routers, gateway, etc.) de la red a la que estamos conectados.
Modo de uso: *traceroute [-m max_ttl] [-p port] [-q nqueries] [-r] [-s scr_addr] [-t tos] [-w waittime] host [packetsize]*

- **Comando route**

Este comando se utiliza para configurar las tablas de enrutamiento del kernel del sistema. Generalmente en todo equipo en una red local encontraremos 3 rutas:

- Loopback, que utiliza el dispositivo de bucle interno (lo, lo0).
- Red local, que utiliza la tarjeta de red para comunicarse con equipo dentro del mismo segmento de red.
- Default que también utiliza la tarjeta de red para enviar a un router o Gateway paquetes que son para equipos de nuestros segmentos.

Modo de uso: *route [-vn] [v] add [-net | -host] xxxx [gw GGGG] [metric MMMM] [netmask NNNN] [mss NNNN] [Windows NNNN] [dev DDDD] route [-v] del xxxx*

2.6 Programación básica en bash Shell

Bash es una de tantas Shell de Linux, la más popular en las distribuciones recientes como Ubuntu, Fedora o Mandriva. En la actualidad la gran mayoría de los scripts de configuración de las distribuciones de Gnu/Linux están programados en Bash, para quien desee personalizar su sistema a fondo el conocimiento de bash debe ser crítico.

¿Qué es un Shell?

- El Shell es un intérprete de comandos.
- Pero también es un lenguaje.
- El conjunto de comandos es un script.
- Un script sirve como 'la unión' de diversos comandos sencillos, que en conjunto son considerablemente poderosos.

¿Por qué aprender a programarlo?

- Te evita hacer tareas repetitivas.
- Es bueno conocerlo.
- Es fácil de aprender: piensa que quieres hacer - escríbelo - revísalo (ahora ponlo todo en un archivo o script).
- Usualmente no tiene que debugear mucho, es como si vaciara lo que haría en el prompt (terminal) de comandos, pero escrito en un archivo.

¿Cómo crear un script?

- Crear un archivo script.sh con tu editor de textos favorito.
- Darle permisos de ejecución: chmod +x script.sh.
- Ejecutarlo: ./script.sh

Para programar en bash se pueden utilizar todos los comandos del sistema, llamadas a otros script bash, funciones internas, y rutinas en otros lenguajes, estas características hacen que bash sea una herramienta potente que no pasa de moda.

Se pueden realizar programas utilizando operaciones aritméticas, operadores adicionales, operadores lógicos, según las necesidades del programa realizar.

A continuación una tabla con algunos operadores que pueden usar.

Tabla 1. Operaciones en bash Shell

OPERADOR	COMENTARIO
Operadores aritméticos	
+	Suma
-	Resta
* o *	Multiplicación
/	División
%	Módulo - Resto de la división
Operadores adicionales	
=	Igualdad
!=	Diferentes
>	Mayor que
>=	Mayor o igual
<	Menor que
<=	Menor o igual
!=	Distinto de
Operadores lógicos	
|	Or lógico
&	And lógico
!	NOT lógico

2.7 Permisos de archivos[4]

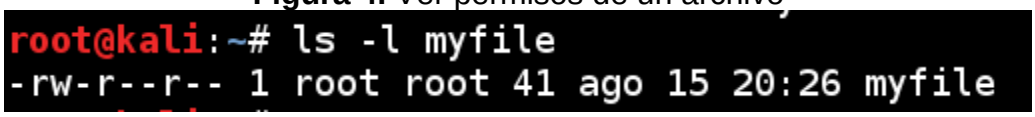
Todos los archivos que existen en kali Linux tienen ciertos permisos los cuales pueden ser de lectura, escritura o ejecución.

Si se lista un archivo con los comando **ls –l**, se puede observar los permisos del archivo.

[4] WEIDMAN, Georgia. Penetration Testing. A hands-On introduction to hacking. San Francisco: No Starch Press, 2014, pág 61, [Consulta: 4 de Agosto de 2015]

Por ejemplo:

Figura 4. Ver permisos de un archivo



-rw-r--r-- → De izquierda a derecho se puede ver el tipo y los permisos del archivo. (r,w,x)
1 → Números de link del archivo
root → usuario y grupo
41 → tamaño del archivo 41 bytes
ago 15 20:26 → ultima fecha que se editó el archivo.
myfile → Nombre del archivo.

Linux tiene permisos de lectura (read **r**), escritura (write **w**) y ejecución (execute **x**). También tiene permisos para el dueño, el grupo y los usuarios.
Las tres primeras letras son los permisos del dueño, las tres siguientes del grupo y las tres finales de los usuarios.
Esto quiere decir que el archivo myfile el dueño que es root tiene permisos de escritura y lectura (rw), el grupo root tiene permiso de lectura (r) y los usuarios solo tienen permiso de lectura (r).

2.8 WIRESHARK[5]

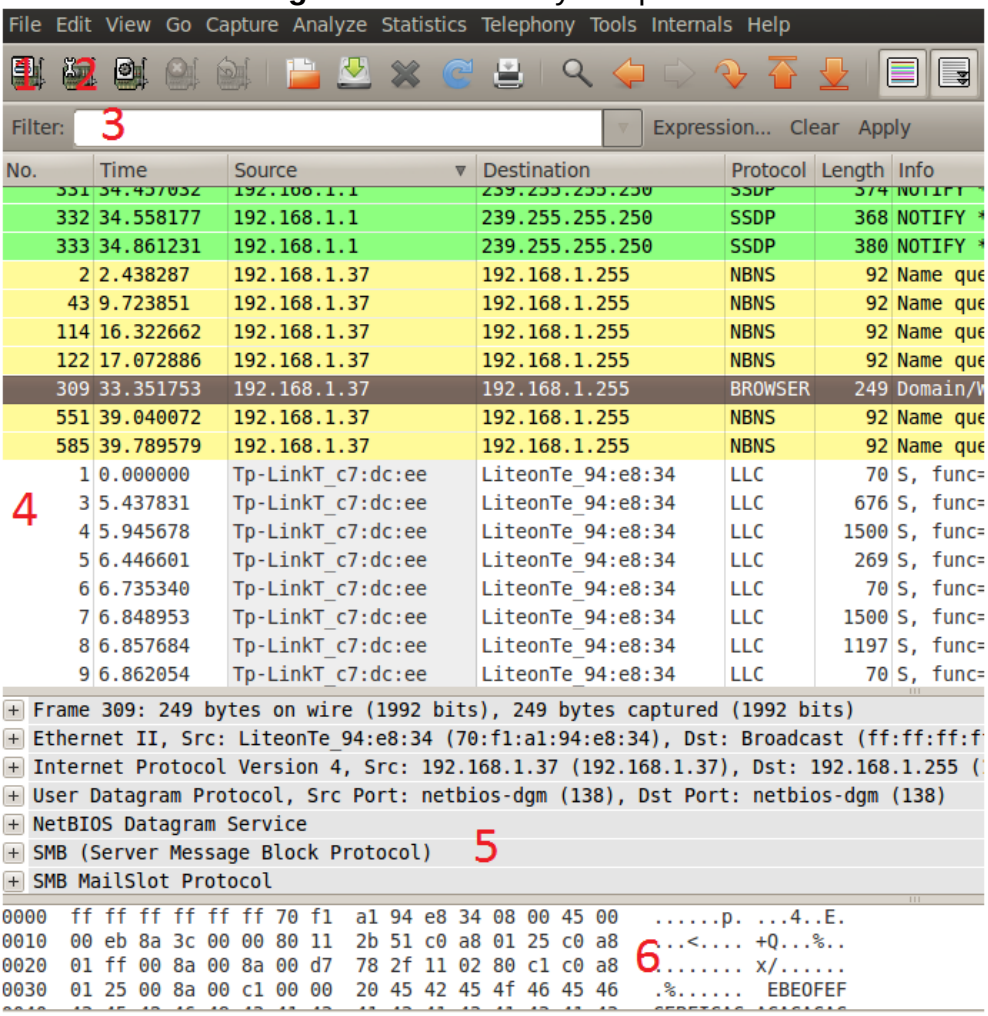
Wireshark es un analizador de paquetes de red, comúnmente llamado sniffer. Es utilizado por administradores de redes para ver todo el tráfico que está pasando en un momento específico.

Una de las ventajas que tiene, es que es open source y multiplataforma. Wireshark ofrece distintos tipos de filtros para leer los paquetes. Captura a demás cookies y passwords que veremos a continuación en este paper. Para instalar wireshark simplemente hay que ir a su página oficial y descargarlo. http://www.wireshark.org/download.html

[5] ANTRAX-LABS, Sniffing con Wireshark, 2015. http://www.antrax-labs.org/2012/01/sniffing-con-wireshark.html

2.8.1 Partes de Wireshark

Figura 5. Wireshark y sus partes



1. Muestra un listado de las interfaces disponibles que podemos poner a la escucha de paquetes.
2. Permite configurar algunos parámetros de nuestra interface.
3. El filtro permite filtras paquetes separándolos por IP, protocolos, etc.
4. Listado de paquetes. Muestra un resumen de los paquetes capturados, presionando con el otro botón del mouse se listaran opciones disponibles para manejarlos a gusto.
5. Panel de vista en Árbol. Muestra el paquete seleccionado con mayor detalle..
6. Panel de detalle de los datos. Muestra los datos del panel superior en formato hexadecimal y ascii

También podemos ver en el menú superior las siguientes opciones:

File: Contiene las funciones para manipular archivos y para cerrar la aplicación Wireshark.
Edit: Este se puede aplicar funciones a los paquetes, por ejemplo, buscar un paquete especifico, aplicar una marca al paquete y configurar la interfaz de usuario.
View: Permite configurar el despliegue del paquete capturado.
Go: Desde acá podemos ir a un paquete especifico, volver atrás, adelante, etc.
Capture: Para iniciar y detener la captura de paquetes.
Analyze: Desde analyze podemos manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.
Statistics: Podemos definir u obtener las estadísticas del trafico capturado.
Telephony: Trae herramientas para telefonía.
Tools: Opciones para el firewall
Internal: Parámetros internos de Wireshark
Help: Menú de ayuda.

2.9 Máquinas virtuales

2.9.1 ¿Que es una máquina virtual?[6]

Una máquina virtual es un programa dentro de un sistema operativo que simula ser su propio sistema operativo.

Beneficios:

- La posibilidad de tener distintos sistemas operativos sin necesidad de crear particiones o tener más discos duros.
- La posibilidad de probar software que aún no es estable (versiones beta, alfa, etc.) o instalar software teniendo la certeza que no afectara a nuestro sistema operativo base.
- Configurar los dispositivos según los recursos que se desee, siempre y cuando no supere las características del real. Es decir no puedo configurar una máquina virtual con 8 Gb de RAM si mi equipo real tiene apenas 4Gb.
- Correr algunos programas que no corren nativa mente en el sistema que tienen instalado.
- Posibilidad de simular otro dispositivo de red.

[6] CETEM, Fundación de servicios educativos EMSSANAR, ¿Qué es una maquina virtual? 2014. http://cetemso.blogspot.com/2014/01/que-es-una-maquina-virtual-y-para-que.html

Desventajas:

- La velocidad de desempeño del computador real es inversamente proporcional al número de máquinas virtuales ejecutándose en el computador.

2.9.2 Principales programas de máquinas virtuales

- **VMware**[7]

Es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un computador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (**simulador**), proporciona un *ambiente de ejecución* similar a todos los efectos a un computador físico (excepto en el *puro acceso físico* al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.
Un virtualizador por software permite ejecutar (simular) varios computadores (sistemas operativos) dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. Sin embargo al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción.
Entre este software se incluyen **VMware Workstation**, y los gratuitos **VMware Server** y **VMware Player**. El software de VMware puede funcionar en Windows, Linux.

- **VitualBox**[8]

Es un potente producto de virtualización x86 y AMD64 / Intel64 para la empresa, así como el uso doméstico. No sólo es VirtualBox un extremadamente rico en características, producto de alto rendimiento para clientes empresariales, es también la única solución profesional que está libremente disponible como software de código abierto bajo los términos de la Licencia Pública General de GNU (GPL) versión 2.

---

[7] WIKIPEDIA, VMware, https://es.wikipedia.org/wiki/VMware [Consulta: martes, 3 de noviembre de 2015]
[8] ORACLE, Welcome to virtualbox, https://www.virtualbox.org/ [Consulta: martes, 3 de noviembre de 2015]

2.10 Introducción a un Hacking ético[9]

Cuando hablamos de hacking ético nos referimos a la acción de efectuar pruebas de intrusión *controladas* sobre sistemas informáticos; es decir que el consultor o pentester, actuará desde el punto de vista de un cracker, para tratar de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, brindándole - en algunos casos - acceso al sistema afectado inclusive; pero siempre en un ambiente supervisado, en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización cliente.

Es importante enfatizar que aunque es indudable que el pentester debe poseer conocimientos sólidos sobre tecnología para poder efectuar un hacking ético, saber de informática no es suficiente para ejecutar con éxito una auditoría de este tipo. Se requiere además seguir una metodología que permita llevar un orden en nuestro trabajo para optimizar el tiempo en la fase de explotación, además de aplicar el sentido común y experiencia.

2.10.1 Fases del hacking

Tanto el auditor como el cracker siguen un orden lógico de pasos al momento de ejecutar un hacking, a estos pasos agrupados se los denomina fases.

Existe un consenso generalizado entre las entidades y profesionales de seguridad informática de que dichas fases son 5 en el siguiente orden:

1. Reconocimiento
2. Escaneo
3. Obtener acceso
4. Mantener acceso
5. Borrar huellas

Usualmente dichas fases se representan como un ciclo al que se denomina comúnmente *círculo del hacking* (ver Figura 1) con el ánimo de enfatizar que el cracker luego de borrar sus huellas puede afectar el sistema, el auditor de seguridad informática que ejecuta un servicio de hacking ético presenta una leve variación en la ejecución de las fases de esta forma:

[9] ASTUDILLO, Karina. Hacking ético 101, Cómo hackear profesionalmente en 21 días o menos!, Editorial Reviews, 2013, pág 10.

1. Reconocimiento
2. Escaneo
3. Obtener acceso
4. Escribir Informe
5. Presentar Informe

De esta manera el hacker ético se detiene en la fase 3 del círculo del hacking para reportar sus hallazgos y realizar recomendaciones de remediación al cliente.

Figura 6. Fases de hacking (Cracker)

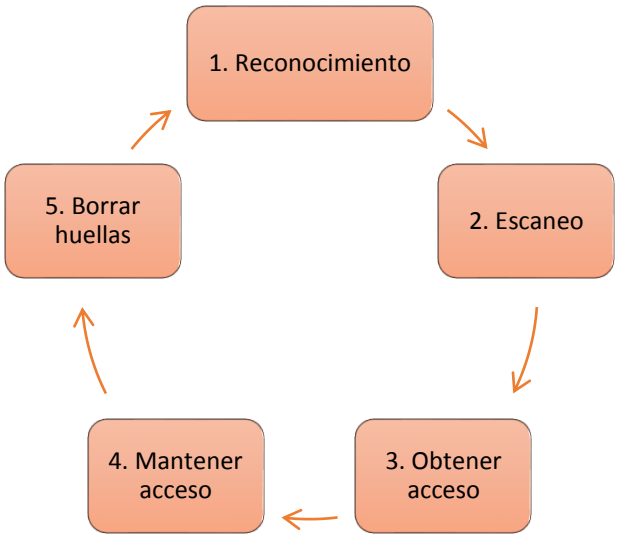
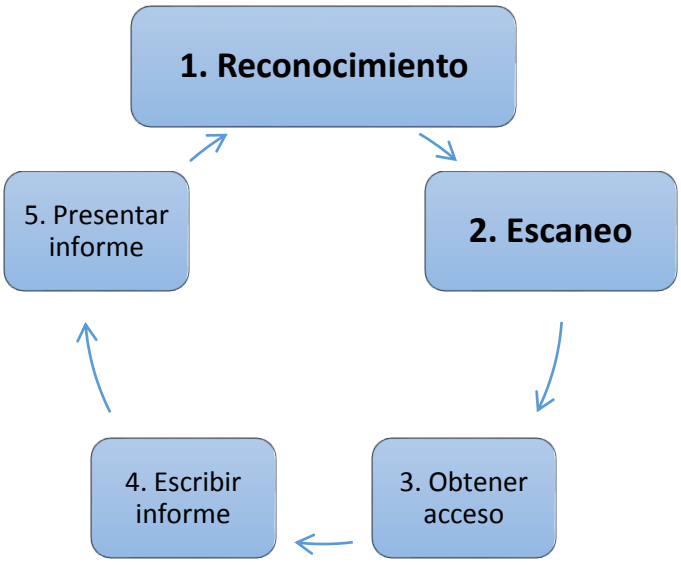


Figura 7. Fases de un hacking ético



3. METODOLOGÍA

En el transcurso del proyecto se utilizaron varios materiales, métodos y equipos necesarios para realizar el proyecto, los cuales se nombran a continuación.

3.1 MATERIALES Y EQUIPOS DE LABORATORIO

Los materiales utilizados en el proyecto son: Computadores con conexión a internet, mouse, teclado y un portátil personal.
Durante el desarrollo del proyecto se trabajó en prácticamente con 2 computadores, y un portátil, ya que un computador tenia instalado el sistema operativo de Kali Linux y el otro tenía el sistema operativo Windows 7 con el cual se trabaja para hacer las pruebas de las máquinas virtuales o para investigar información como un usuario de la red. El otro equipo utilizado es el portátil personal, con los 2 sistemas operativos en cual se utiliza para hacer pruebas por fuera de las instalaciones de la universidad y para realizar pruebas con la red de internet inalámbrica (Wifi).

Figura 8. Portátil con Kali Linux versión 2.0

3.2 MÉTODOS UTILIZADOS

Primero que todo como se va a trabajar con un sistema operativo nuevo, se tuvo la necesidad de formatear un computador e instalarle este sistema operativo llamado Kali Linux para trabajar con todas las aplicaciones necesarias que trae por defecto y aprovechar al máximo su potencial.

Luego verificar que estuviera trabajando correctamente con las últimas actualizaciones y empezar a desarrollar las principales guías de laboratorio empezando desde lo más básico hasta algo un poco más complejo.

El contenido de estas guías se crean para que el estudiante conozca otra forma de analizar las redes desde el punto de vista de Linux, ya que este sistema operativo de kali Linux se desarrolló para la auditoria en redes y tiene muchos programas potentes que le puedan interesar al estudiante y seguir por este campo de las redes.

Estas guías de laboratorio están diseñadas para que cualquier persona con un conocimiento básico en computadores y redes las pueda desarrollar y aprender de estos temas, pero principalmente están diseñadas para que sean desarrolladas por los estudiantes de ingeniería electrónica e informática de la Universidad Pontificia Bolivariana.

4. RESULTADOS

4.1 GUÍAS DE LABORATORIO

Se crearon 7 guías de laboratorio, empezando desde lo básico que es la introducción al Linux y comandos básicos, luego un poco de programación pasando por el manejo del programa Wireshark, instalación de máquinas virtuales y programas, y por último introducción al hacking ético.

Los temas que se van a desarrollar son:

- Introducción al Linux y comando básicos de Linux.
- Comandos básicos de la red para Linux.
- Programación básica en Bash Shell.
- Wireshark.
- Instalación de máquinas virtuales e instalación de programas.
- Introducción a un hacking ético fase 1.
- Introducción a un hacking ético fase 2.

La primera guía se llama **"Introducción al Linux y comandos básicos de Linux".**
En esta guía se va a conocer un poco del sistema operativo Linux, como es su estructura y los comandos básicos, los cuales son importantes para el manejo de los archivos y carpetas. Por ejemplo para copiar, cortar, mover, eliminar, ver las características de las carpetas o archivos, y es importante conocer de ellos para la realización de las siguiente guías.

La segunda guía se llama **"Comandos básicos de la red para Linux".**
En esta guía se conocerán los comandos básicos para el manejo de redes, estos comandos son importantes ya que estos facilitan estadísticas de uso de las interfaces de red y se puede conocer el comportamiento del sistema y de los registros de los eventos que suceden en el equipo.
Los comandos que se conocerán son: ifconfig, hostname, ping, netstat, traceroute y route.

La tercera guía que se llama **“Programación básica en Bash Shell”.**
En esta guía se conocerá que es el Shell, bash-shell, y como crear los scripts; los cuales son muy importantes ya que estos ayudan a evitar hacer tareas repetitivas (automatizar procesos), ahorran tiempo y su programación es muy sencilla.
Dentro del contenido de los scripts se tratarán temas como entrada y salida de datos, el manejo de las variables, operaciones aritméticas, estructuras de control (condicionales, lógicos, bucles) y funciones.
Esta guía es muy importante ya que acá el alumno podrá crear su propio programa y así ahorrar tiempo a la hora de trabajar en sus necesidades y tiene un amplio rango de posibilidades de programación.

Todas estas guías, están compuestas por unos objetivos bien definidos, marco teórico, procedimientos, ejemplos y por último un taller para que el alumno aprenda más del tema y practique lo desarrollado en la guía, lo cual podrá luego ser evaluado con el docente y despejar posibles dudas.

La cuarta guía que se llama **“Wireshark”.**
En esta guía se va a trabajar con el software gratuito llamado WIRESHARK, este software es muy importante para el análisis, prevención y solución de los diferentes problemas que ocurren a diario en las redes de comunicaciones.
Wireshark trabaja mediante la captura de tráfico de datos, esta puede ser a través de una red viva o de un archivo de captura salvado en un disco.
Este programa es muy conocido ya que es muy importante y es muy usado para el análisis de las redes, es un programa muy completo porque estos análisis tienen varios filtros y algunos gráficos en los cuales se puede entender mejor el análisis de los paquetes leídos.

La quinta guía que se llama **“Instalación de máquinas virtuales con kali Linux y programas”.**
En esta guía se va a conocer la instalación de una máquina virtual lo cual consiste en un programa que simula otro ordenador dentro del ordenador que se tiene para poder hacer pruebas sin afectar el sistema operativo principal.
También se trabajará con nuevos comandos para instalar programas, ya que estos se instalan de diferente manera a la que se está acostumbrado con Windows.

La sexta y séptima guía se llaman **“Introducción a un hacking ético fase 1”** e **“Introducción a un hacking ético fase 2”**
En la primera fase (reconocimiento) se explican las diferencias entre en hacking ético y no ético, conocer los principales programas de reconocimiento y escaneo de red y por último se investigan datos de la red.
Se trabajan con programas de reconocimiento como el Maltego, metagoofil, también por comando como el nslookup que se ejecuta desde la terminal, también se hace reconocimiento directamente en google o por medio de una base de datos en internet por medio del comando whois.
Todas estas herramientas se utilizan para saber toda la información posible acerca de un cliente, empresa o red.

En esta séptima guía se conocerá la segunda fase (Escaneo) que realiza un hacking ético, el cual consiste en escanear la red la cual se puede hacer mediante el comando ***nmap***, el cual se ejecuta en la terminal, se puede explorar la de red e investigar los puertos abiertos, direcciones Ips, sistemas operativos de los computadores en la red, entre otros.

Nmap ("Network Mapper") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Fue diseñado para escanear rápidamente pequeñas y grandes redes. Este comando también es comúnmente utilizado para las auditorías de seguridad, muchos sistemas y administradores de red resulta útil para tareas de rutina, tales como inventario de red, gestión de horarios de servicios de actualización y supervisión de host o tiempo de servicio.

Ya después de que el alumno haya desarrollados todas estas guías está en la capacidad de realizar un muy buen análisis a determinada red y sacar buenas conclusiones del tráfico de la red de que está fallando y como mejorarla. Y también analizar otras herramientas o programas que brinda Kali Linux que está hecho para la seguridad de las redes.

4.1.1 GUÍA N°1 INTRODUCCIÓN AL LINUX Y COMANDOS BÁSICOS

GUÍA N°1
INTRODUCCIÓN AL LINUX Y COMANDOS BÁSICOS

OBJETIVOS

- Conocer que es Linux y como es su estructura.
- Conocer los comandos básicos del manejo de archivos y carpetas en el terminal de KALI-LINUX.

REQUISITOS

- Computador con la versión KALI del sistema operativo LINUX.
- Manejo de computadores y programación básica.

INTRODUCCIÓN

En esta guía se va a conocer un poco del sistema operativo Linux, como es su estructura y los comandos básicos, los cuales son importantes para el manejo de los archivos y carpetas. Por ejemplo para copiar, cortar, mover, eliminar, ver las características de las carpetas o archivos, y es importante conocer de ellos para la realización de las siguientes guías.

MARCO TEÓRICO

Qué es el LINUX[10]

LINUX es un Sistema Operativo como MacOS, DOS o Windows. Es decir, Linux es el software necesario para que el computador le permita utilizar programas como: editores de texto, juegos, navegadores de Internet, etc. Linux puede usarse mediante un interfaz gráfico al igual que Windows o MacOS, pero también puede usarse mediante línea de comandos como DOS.

Linux tiene su origen en Unix. Éste apareció en los años sesenta, desarrollado por los investigadores Dennis Ritchie y Ken Thompson, de los Laboratorios Telefónicos Bell.

[10] CIBERAULA, Qué es Linux, 2014, http://linux.ciberaula.com/articulo/que_es_linux/

Qué es la terminal

Linux dispone de un intérprete de órdenes o terminal (en inglés se utiliza la palabra *shell*) que hace de interfaz entre el usuario y el propio sistema operativo y cuyo nombre es bash (acrónimo de ***B**ourne **A**gain **S**hell*).

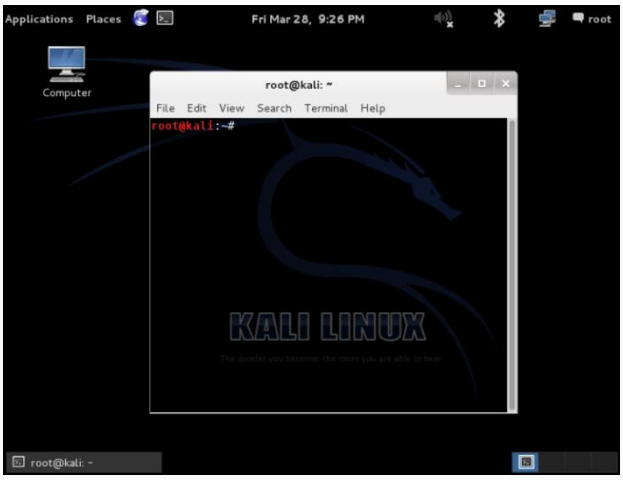
Un terminal es una forma de acceder al sistema sin utilizar la interfaz gráfica, es decir, realizar todo tipo de tareas en formato texto. La forma de utilizar el sistema de este modo es mediante órdenes.

El terminal muestra en pantalla un indicador de línea de órdenes (en inglés se conoce como *prompt*) esperando que el usuario introduzca una orden. Este indicador finaliza generalmente por un caracter, **$** cuando se usa como un usuario normal, o # cuando se usa como un súper usuario (administrador-root).

La terminal es una herramienta tan poderosa que puede realizar actividades que un programa mediante GUI (Interfaz Gráfica) no haría.

Funcionalidades de la terminal:
Instalar, ejecutar o desintalar Software
Leer documentos
Descomprimir, comprimir Archivos
Conectarse a Servidores
Programar, Jugar, etc

Figura 9. Escritorio de Kali - Linux



Estructura general de los directorios[11]

En el sistema de ficheros de Linux, existen varias sub-jerarquías de directorios que poseen múltiples y diferentes funciones de almacenamiento y organización en todo el sistema. Estos directorios pueden clasificarse en:

Estáticos: Contiene archivos que no cambian sin la intervención del administrador (root), sin embargo, pueden ser leídos por cualquier otro usuario. (**/bin**, **/sbin**, **/opt**, **/boot**, **/usr/bin**…)

Dinámicos: Contiene archivos que son cambiantes, y pueden leerse y escribirse (algunos sólo por su respectivo usuario y el root). Contienen configuraciones, documentos, etc. (**/var/mail**, **/var/spool**, **/var/run**, **/var/lock**, **/home**…)

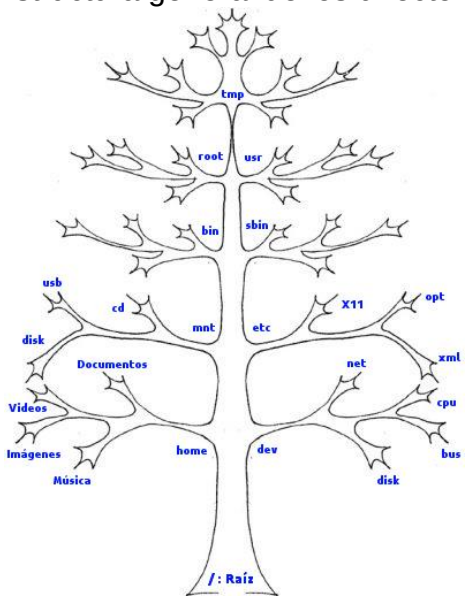
Compartidos: Contiene archivos que se pueden encontrar en un ordenador y utilizarse en otro, o incluso compartirse entre usuarios.

Restringidos: Contiene ficheros que no se pueden compartir, solo son modificables por el administrador. (**/etc**, **/boot**, **/var/run**, **/var/lock**…)

root: es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos (mono o multi usuario). root es también llamado superusuario. Normalmente esta es la cuenta de administrador. El usuario root puede hacer muchas cosas que un usuario común no puede, tales como cambiar el dueño o permisos de archivos y enlazar a puertos de numeración pequeña.

Dicha estructura se representa en forma de árbol, como se muestra en la siguiente imagen:

Figura 10. Estructura general de los directorios de Linux



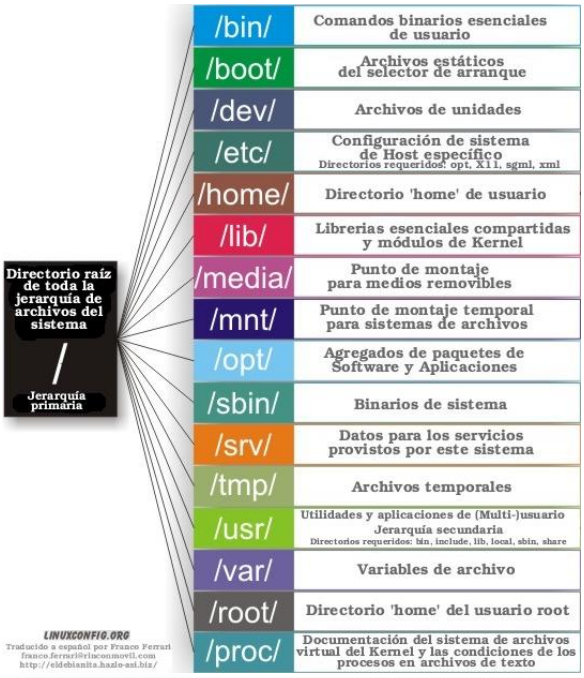
[11] PERSEO, Cómo se encuentran estructurados los directorios en GNU/Linux?, 2012. http://blog.desdelinux.net/estructura-de-directorios-en-linux/

Donde la raíz del árbol (**/**) es la base de toda la estructura de directorios y las ramas (**directorios y archivos**) surgen o cuelgan de dicha base.

Estructura del árbol de directorios en GNU/Linux

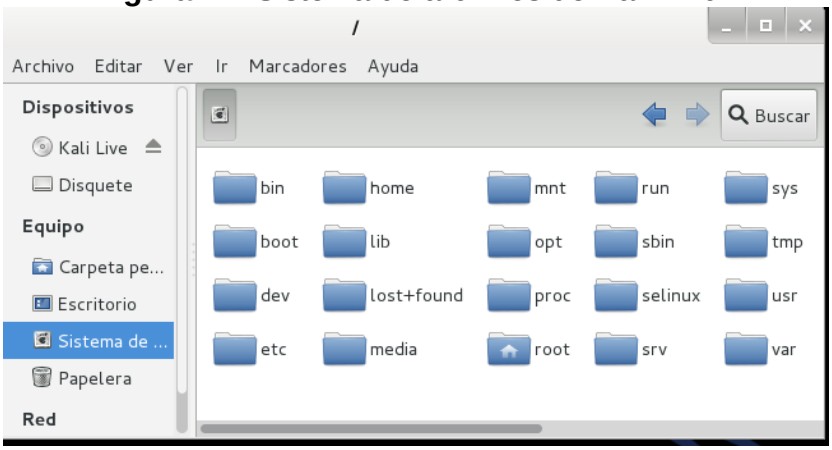
Algunas distribuciones de Linux hacen modificaciones a la estructura del árbol de directorios, para adaptarlo a sus propias necesidades. De todas formas el estándar es el siguiente:

Figura 11. Estructura del árbol de directorio en Linux



Así es como se ve en el equipo:

Figura 12. Sistema de archivos de Kali-Linux



Descripción de la estructura del árbol de directorios

***/* (raíz):** Parecido a el directorio raíz "**C:**" de los sistemas operativos DOS y Windows. Es el nivel más alto dentro de la jerarquía de directorios, es el contenedor de todo el sistema (accesos al sistema de archivos, incluyendo los discos extraíbles [CD's, DVD's, pendrives, etc.]).

/bin (binarios): Los binarios son los ejecutables de Linux (similar a los archivos **.exe** de Windows). Aquí tendremos los ejecutables de los programas propios del sistema operativo.

/boot (arranque): Aquí se encuentran los archivos necesarios para el inicio de Linux, desde los archivos de configuración del cargador de arranque (Grub – Lilo), hasta el propio kernel del sistema.

> ***Cargador de arranque (boot loader en inglés):*** *es un programa sencillo diseñado exclusivamente para preparar todo lo que necesita el sistema operativo para funcionar.*
>
> ***Núcleo o kernel:*** *es un software que constituye la parte más importante del sistema operativo. Es el principal responsable de facilitar a los distintos programas acceso seguro al hardware de la computadora o en forma básica, es el encargado de gestionar recursos, a través de servicios de llamada al sistema.*

/dev (dispositivos): Esta carpeta contiene los dispositivos del sistema, incluso los que no se les ha asignado un directorio, por ejemplo micrófonos, impresoras, pendrives (memorias USB) y dispositivos especiales (por ejemplo, **/dev/null**). Linux trata los dispositivos como si fueran un fichero más para facilitar el flujo de la información.

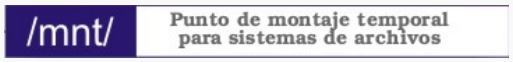
/etc (etcétera): Aquí se guardan los ficheros de configuración de los programas instalados, así como ciertos scripts que se ejecutan en el inicio del sistema. Los valores de estos ficheros de configuración pueden ser complementados o

sustituidos por los ficheros de configuración de usuario que cada uno tiene en su respectivo “home” (carpeta personal).

/home (hogar): Aquí se encuentran los ficheros de configuración de usuario así como los archivos personales del mismo (documentos, música, videos, etc.), a excepción del superusuario (administrador, root) el cual cuenta con un directorio aparte. Similar a “Mis Documentos” en Windows.

/lib (bibliotecas): Contiene las bibliotecas (mal conocidas como librerías) esenciales compartidas de los programas alojados, es decir, para los binarios en **/bin/** y **/sbin/**, las bibliotecas para el núcleo, así como módulos y controladores (drivers).

/media (media/medios): Contiene los puntos de montaje de los medios extraíbles de almacenamiento, tales como lectores de CD-ROM , Pendrives (memoria USB), e incluso sirve para montar otras particiones del mismo disco duro, como por ejemplo, alguna partición que sea utilizada por otro sistema operativo.



/mnt (montajes): Este directorio se utiliza normalmente para montajes temporales de unidades. Es un directorio semejante a /media, pero es usado mayoritariamente por los usuarios. Sirve para montar discos duros y particiones de forma temporal en el sistema; no necesita contraseña, a diferencia del directorio /media.

/opt (opcionales): Contiene Paquetes de programas opcionales de aplicaciones estáticas, es decir, que pueden ser compartidas entre los usuarios. Dichas aplicaciones no guardan sus configuraciones en este directorio; de esta manera, cada usuario puede tener una configuración diferente de una misma aplicación, de manera que se comparte la aplicación pero no las configuraciones de los usuarios, las cuales se guardan en su respectivo directorio en **/home**.

/proc (procesos): Contiene principalmente archivos de texto, sistema de archivos virtuales que documentan al núcleo y el estado de los procesos en archivos de texto (por ejemplo, uptime, network).

/root (administrador): Es el /home del administrador (solo para él). Es el único **/home** que no está incluido -por defecto- en el directorio anteriormente mencionado.

/sbin (binarios de sistema): Sistema de binarios especial, comandos y programas exclusivos del superusuario (root), por ejemplo, init, route, ifup, como mount, umount, shutdown). Un usuario puede ejecutar alguno de estas aplicaciones de comandos, si tiene los permisos suficientes, o bien, si tiene la contraseña del super usuario.

/srv (servicios): Información del sistema sobre ciertos servicios que ofrece (FTP, HTTP…).

/tmp (temporales): Es un directorio donde se almacenan ficheros temporales (por ejemplo: por el navegador de internet). Cada vez que se inicia el sistema este directorio se limpia.

/usr (usuarios): Jerarquía secundaria de los datos de usuario; contiene la mayoría de las utilidades y aplicaciones multiusuario, es decir, accesibles para todos los usuarios. En otras palabras, contiene los archivos compartidos, pero que no obstante son de sólo lectura. Este directorio puede incluso ser compartido con otras computadoras de red local.

/var (variables): Archivos variables, tales como logs, archivos spool, bases de datos, archivos de e-mail temporales, y algunos archivos temporales en general.

Generalmente actúa como un registro del sistema. Ayuda a encontrar los orígenes de un problema.

Comando básicos para el terminal

Hay que tener en cuenta que en Linux el intérprete de comandos es case-sesitive. Esto quiere decir que no es lo mismo escribir ls que Ls. El sistema diferencia entre mayúsculas y minúsculas

- **cd** (change directory)**:** Con este comando se puede navegar a través de los directorios.
- **cd .. :** Volver al directorio superior o anterior.
- **pwd** (print working directory)**:** Este comando permite conocer cuál es el directorio actual.
- **ls** (list)**:** Con este comando se ven todos los archivos y carpetas que se encuentran en el directorio actual, las carpetas y archivos se diferencian por colores.
- **cp** (copy)**:** Permite copiar archivos de un directorio a otro.
- **mv** (move)**:** Se utiliza para mover un archivo o directorio a otro, también permite cambiar el nombre de un archivo o directorio.
- **mkdir** (make directory)**:** Para crear una nueva carpeta o directorio.
- **rmdir** (remove directory)**:** Para borrar un directorio o carpeta.
- **rm** (remove)**:** Este comando permite borrar archivos.
- **rm -r** nombre_directorio (remove recursive)**:** Con este comando se borra un directorio con todo lo que contiene dentro.
- **rm -rf** (remove recursive force)**:** Elimina todos los archivos del directorio. **Ojo: No utilizarlo en el directorio root, ya que eliminaría los archivos del sistema.**
- **rm arch*:** Elimina todo lo que empiece por arch. El carácter asterisco (*) se emplea como un comodín.
- **man** (manual page or man page)[12]: Permite saber más acerca del comando, como su uso, descripción y opciones de uso. Ejemplo: man ls
- **vi nombre.txt:** Crea un archivo con el editor de textos.
- **clear:** Borrar lo que está escrito en el terminal.
- **exit:** Se utiliza para cerrar la terminal.

[12] WEIDMAN, Georgia. Penetration Testing. A hands-On introduction to hacking. San Francisco: No Starch Press, 2014, pág 57, [Consulta: 4 de Agosto de 2015]

PROCEDIMIENTO

Siga las instrucciones paso a paso.

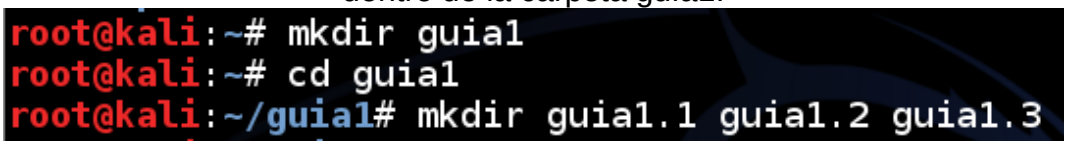
1. Para practicar con los principales comandos de Kali hay que abrir la terminal. Abra la terminal, dando click en el icono  que se encuentra en la barra de tareas en la parte superior.
   Se abrirá la ventana del terminal en la cual estará indicada que se está trabajando como usuario **root** (# superusuario) y con la versión **Kali**.
   

2. Ahora se creará la carpeta llamada **guia1**, esto se hace con el comando ***mkdir*** mas el nombre de la carpeta. Escriba ***mkdir guia1*** y enter.

3. Para entrar a una carpeta o directorio se hace con el comando ***cd*** más el nombre de la carpeta. Escriba ***cd guia1*** y enter para entrar a la carpeta **guia1**

4. A continuación se crearán 3 carpetas dentro de la carpeta **guia1**, escriba ***mkdir guia1.1 guia1.2 guia1.3*** y enter.

Figura 13. Creación de carpeta guia1 y carpetas guia1.1 guia1.2 guia1.3 dentro de la carpeta guía1.

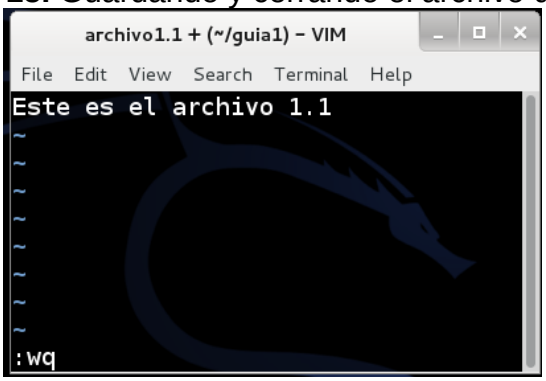


5. Para crear archivos de texto con el editor, escriba ***vi archivo1.1*** y enter.
   Se abrirá el editor, para poder escribir presione la tecla ***i*** (aparecerá en la parte inferior la palabra INSERT) y escriba ***Este es el archivo 1.1***, como se muestra en la figura siguiente.

Figura 14. Creación de archivo 1.1

Después para grabar lo que escribimos en el archivo y salir del editor presione la tecla **esc** la cual hace que se pueda volver al modo de comandos y escriba ***:wq*** y enter.

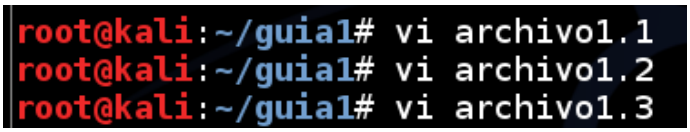
Figura 15. Guardando y cerrando el archivo de texto



En la figura se observa en la parte inferior izquierda los comandos **:wq** y cuando se le da enter, el archivo se guarda automáticamente y se cierra; y luego estamos nuevamente en la terminal.

A continuación realizar los mismos pasos explicados anteriormente para crear el **archivo1.2** y **archivo1.3** dentro de la carpeta **guia1**.

Figura 16. Creación de archivo1.1 archivo1.2 y archivo1.3

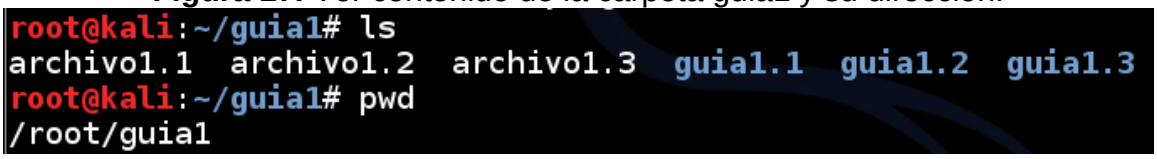


En esta figura se muestra el resultado en la terminal cuando se terminan de crear los 3 archivos.

6. Para ver el contenido del directorio **guia1**, escriba ***ls*** y enter.
   En la figura se observa que la carpeta **guia1** tiene 3 archivos y 3 carpetas, estos se diferencian por colores, los archivos en este caso son de color blanco y las carpetas tienen color azul.

7. Para mostrar la dirección del directorio actual, escriba ***pwd***.

Figura 17. Ver contenido de la carpeta guia1 y su dirección.



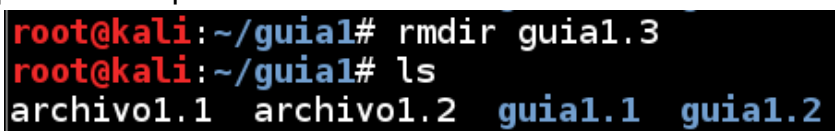
En esta figura se observa (/root/guia1), esto quiere decir que el directorio actual es la carpeta **guia1** y a su vez dentro de la carpeta **root.**

8. A continuación se va a copiar el **archivo1.1** de la carpeta **guia1** a la carpeta **guia1.1** que se encuentra dentro de esa misma carpeta. Se utiliza el comando cp más la dirección completa de donde se encuentra el archivo, luego espacio y la nueva dirección.
Escriba ***cp /root/guia1/archivo1.1 /root/guia1/guia1.1/archivo1.1***

9. Ahora se va a borrar el **archivo1.3** y a comprobar que fue borrado. Escriba ***rm archivo1.3*** para borrar este archivo y luego escribir **ls** para su comprobación.

En la figura se observa que el **archivo1.3** ya no se encuentra en la carpeta **guia1.**
Si se requiere borrar un archivo que esté en otro directorio al actual, entonces se utilizaría el comando rm con la dirección completa de donde se encuentre el archivo a eliminar ejemplo: **rm /root/guia1/archivo1.3**

10. A continuación se va a borrar la carpeta **guia1.3** y a comprobar que fue borrada. Escriba ***rmdir guia1.3*** para borrar este directorio y luego escribir **ls** para su comprobación.



En la figura se observa que la carpeta o directorio **guia1.3** ya no se encuentra en la carpeta **guia1.**

11. A continuación se va a mover el **archivo1.2** que se encuentra en la carpeta **guia1** a la carpeta **guia1.2**, esto se hace con el comando **mv**.
Escriba ***mv /root/guia1/archivo1.2 /root/guia1/guia1.2/archivo1.2***

Ahora escriba **ls** para comprobar que el **archivo1.2** no se encuentra porque fue movido a la carpeta **guia1.2**.

12. Ir a la carpeta **guia1.2** para comprobar que el **archivo1.2** fue movido a esta carpeta.
Para entrar a la carpeta **guia1.2** escriba ***cd guia1.2*** y para comprobar que el archivo se encuentra, escriba ***ls***.

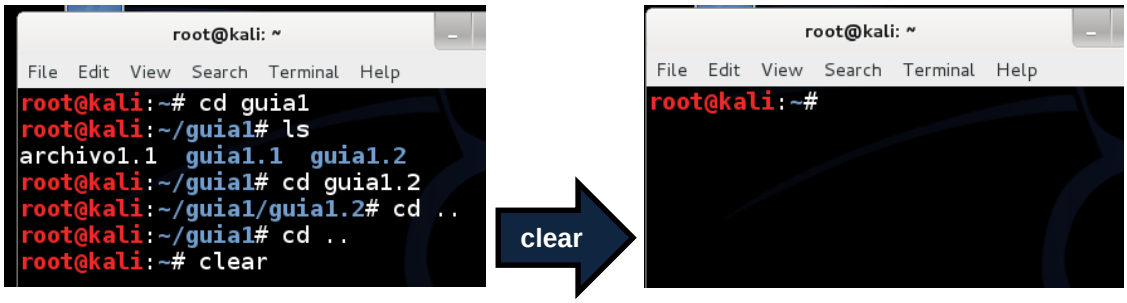
```
root@kali:~/guia1# mv /root/guia1/archivo1.2 /root/guia1/guia1.2/archivo1.2
root@kali:~/guia1# ls
archivo1.1  guia1.1  guia1.2
root@kali:~/guia1# cd guia1.2
root@kali:~/guia1/guia1.2# ls
archivo1.2
```

Como se observa en la figura, este archivo si fue movido; también con este comando **mv** podemos mover las carpetas y los archivos y al mismo tiempo cambiarles el nombre si es necesario.

13. Ahora se regresará al directorio principal, para esto se usa el comando **cd ..** escriba ***cd ..*** para ir a una carpeta superior o anterior, por lo tanto regresamos al directorio **guia1**. Luego nuevamente escribir ***cd ..*** para ir al directorio **root.**

```
root@kali:~/guia1/guia1.2# cd ..
root@kali:~/guia1# cd ..
root@kali:~#
```

En algunas ocasiones tenemos mucha información en la terminal y queremos borrar la pantalla y empezar en la primera línea, esto se puede hacer con el comando **clear**. Escriba **clear** y enter. La terminal quedará borrada mas no eliminará los procesos que se realizaron.



A continuación un tema para simplificar enormemente la introducción de instrucciones.

EDICIÓN DE ÓRDENES[13]

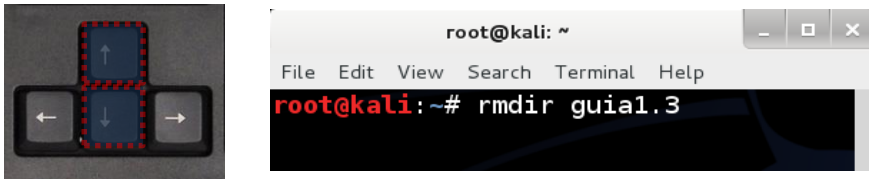
Utilizando la combinación de teclas apropiadas se puede, entre otras, borrar parte o toda la línea que se haya escrito, añadir nuevos caracteres, recuperar un orden que se haya ejecutado anteriormente o completar el nombre de un archivo.

Completar nombres de órdenes y archivos: Si teclea parte del nombre del archivo que se va a utilizar y luego pulsa la tecla TAB, el shell lo completará buscando el archivo cuyo nombre comience por el prefijo indicado.
Por ejemplo estamos en la carpeta guia1 y escribimos ***cd gu*** y presionamos la tecla **TAB**, entonces nos completará a **cd guia1.** luego escribiremos guia1.1 o guia1.2 depende la que se requiera.

Figura 18. Tab para completar nombres

Historial de órdenes: Cuando se trabaja con Linux algunas veces necesitamos un comando utilizado anteriormente, Linux permite revisar el historial y esto se hace con las flechas, con la flecha arriba (↑) recuperará la última orden del historial, si la pulsa de nuevo pasará a la orden anterior, y así sucesivamente. De igual forma puede pulsar la tecla hacia abajo (↓) para pasar a la siguiente orden de la lista.

Figura 19. Flechas para recuperar órdenes anteriores.



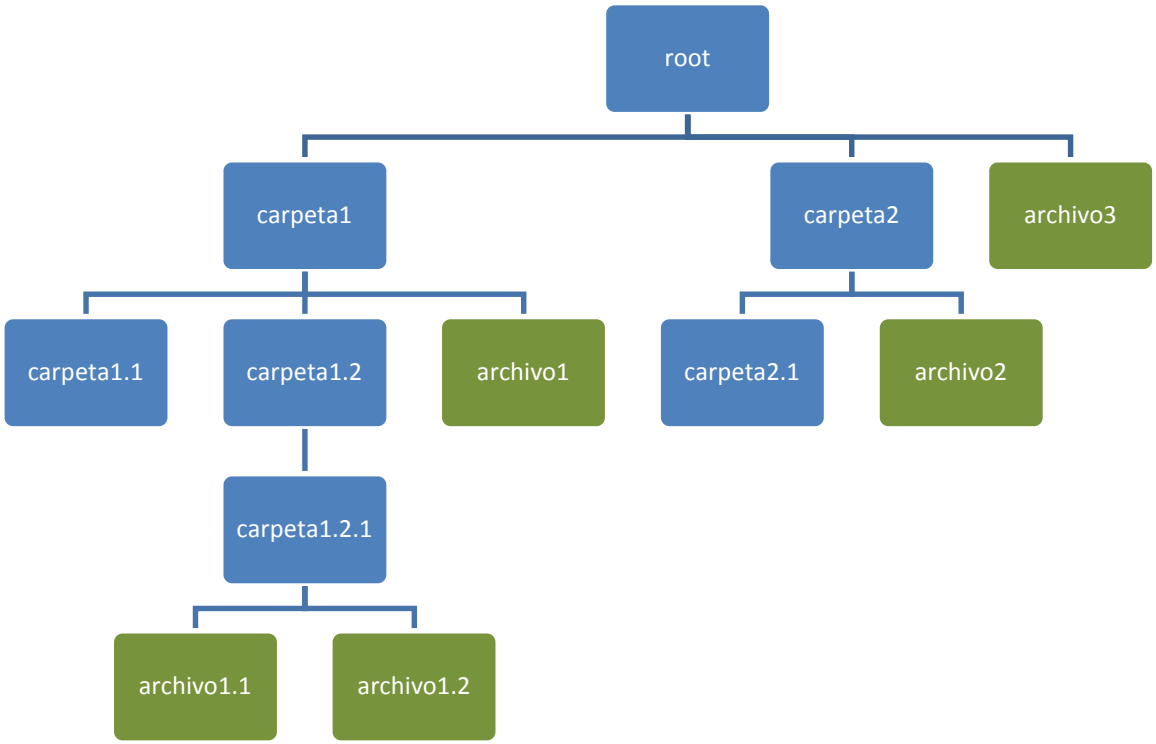
Para salir de la terminal escribimos exit y enter o click en la X que está ubicada en una de las esquinas de la terminal.

Por último, algunas combinaciones del teclado que usamos comúnmente en Windows, como copiar (Ctrl+c), pegar (Ctrl+v), no sirven en la terminal de Kali-Linux.
En la terminal se selecciona y con el click derecho seleccionar copy (copiar) y luego paste (pegar).

[13] CATALINA GALLEGO, Alfredo y Miguel, Unix/Linux: Iniciación y Referencia, 2a. ed, Madrid: McGraw-Hill, pág. 82, [Consulta: 11 de agosto de 2014]

INFORME - TALLER

Crear el siguiente árbol de directorios.



Para borrar el archivo archivo1.2 escribo: _____

Si estoy en el directorio carpeta2.1 y escribo pwd, me sale:
_____

Escribir el método corto y largo (paso a paso) para entrar en el directorio carpeta1.2.1

_____
_____
_____

Para copiar el archivo 1.1 a la carpeta 2.1 escribo:

_____
_____

Se puede borrar un directorio con el comando rm? _____

Escoger un comando e investigarlo con el comando man. Nombre, sinopsis y descripción.

_____
_____

CONCLUSIONES

_____
_____
_____
_____
_____

4.1.2 GUÍA N°2 COMANDOS BÁSICOS DE RED PARA LINUX

GUÍA N°2
COMANDOS BÁSICOS DE RED PARA LINUX

OBJETIVOS

- Conocer los comandos básicos para el manejo de redes para el sistema Linux.

SOFTWARE Y HARDWARE REQUERIDOS

- Computador con sistema operativo LINUX.
- Cable UTP de conexión a red Ethernet.
- Conexión de Red LAN Ethernet a la cual interconectar el computador.

CONOCIMIENTO PREVIO

- Manejo de comandos básicos de Linux.

INTRODUCCIÓN

En esta guía se conocerán los comandos básicos para el manejo de redes, estos comandos son importantes ya que estos facilitan estadísticas de uso de las interfaces de red y se puede conocer el comportamiento del sistema y de los registros de los eventos que suceden en el equipo.
Los comandos que se conocerán son: ifconfig, hostname, ping, netstat, traceroute y route.

MARCO TEÓRICO

- **Comando ifconfig**[14]

Con este comando se puede configurar la dirección IP de red asociada a la máscara de subred; la dirección del hardware de la tarjeta, es decir, la dirección

[14] KIRCH, Olaf, Editado por O'Reilly, Guía de Administración de Redes con Linux, O'Reilly & Associates, 2000. http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-iface.ifconfig.html

MAC; se podrá especificar la dirección *broadcast* de la red; permitirá habilitar o deshabilitar la tarjeta de red especificada.

El comando ifconfig[15] acepta muchos parámetros.
Modo de uso: ifconfig *interfaz* [*dirección* [parámetros]]
Opciones
-a: Muestra la información de todas las tarjetas.
-v: Muestra más información sobre las tarjetas de red.
-s: Muestra los parámetros de las tarjetas de red en forma de tabla.
[IP]: Configura la dirección IP de la tarjeta de red (se debe especificar el *interface* de la tarjeta de red).
netmask <dirección>: Se especifica la máscara de subred (se debe especificar el *interface* de la tarjeta de red).
up: Activa una tarjeta de red, si se va a añadir una dirección IP a la tarjeta, **ifconfig** sobreentiende que la tarjeta debe estar activada, por ello se puede omitir este parámetro (se debe especificar el *interface* de la tarjeta de red).
down: desactiva un tarjeta de red (se debe especificar el *interface* de la tarjeta de red).
[-] arp: permite el uso de paquetes arp, si se especifica un menos delante, se desactiva (se debe especificar el *interface* de la tarjeta de red).
[-] <dirección>: aquí se añade o se quita (con el uso del guion antes del parámetro), la dirección de broadcast de la red (se debe especificar el *interface* de la tarjeta de red).
[-] allmulti: activa o desactiva (con el uso del guión antes del parámetro) el modo promiscuo de la tarjeta de red (se debe especificar el *interface* de la tarjeta de red).
Hw <m.a.c>: configura la dirección MAC de la tarjeta de red si el driver lo permite.

- **Comando hostname**

Muestra o establece el nombre del sistema o equipo.

Modo de uso: hostname [-d] [-F nombre_archivo] [-f] [-h] [-s] [-v] [i] [I] [y]

Algunas opciones:
hostname -f Muestra el nombre de "mi" máquina completo, con dominio DNS.
hostname -i Muestra la dirección IP de la maquina

[15] WIKIPEDIA, ifconfig, 2015, https://es.wikipedia.org/wiki/Ifconfig

hostname -aMuestra los alias.

hostname --fqdn muestra el FQDN (Nombre de Dominio Completamente Especificado).

hostname nuevo_nombre Cambia el nombre de mi sistema a nuevo_nombre, esto lo realiza solo para la sesión actual, para hacer los cambios permanentes editar los archivos /etc/hostnam y /etc/hosts.

- **Comando ping**[16]

El comando ping es usado para probar la conexión y la latencia entre dos conexiones de red. Estas conexiones pueden ser conexiones de área local, área amplia o el Internet como un todo. El comando ping envía paquetes de información a una dirección IP específica y luego mide el tiempo que se tarda en obtener una respuesta de la computadora o dispositivo especificado.

Modo de uso: ping [-r] [-v] host [tamaño_paquete] [count]

Las teclas ctrl+z y ctrl+c se utilizan para detener el proceso y la diferencia entre estas dos es que cuando se utiliza ctrl+c nos da como resultado las estadísticas de la conexión, como los paquetes transmitidos, recibidos, paquetes perdidos y el tiempo.

- **Comando netstat**

Muestra conexiones de red, tablas de ruteo, estadísticas de interfaces, etc.
Este comando es importante, ya que es una herramienta para seguir el rastro de las conexiones a la red en su sistema, también es útil para la corrección de errores, detección de fallas de seguridad y los problemas cotidianos de la red

Modo de uso: netstat [-a] [-t] [l] [-p] [-natu] [-u]

Algunas opciones

netstat -t	muestra solo las conexiones activas TCP/IP
netstat -u	muestra solo las conexiones activas UDP
netstat -p	trata de identificar el proceso que esta manejando esta conexión
netstat -l	lista los puertos que están abiertos (conexiones establecidas)
netstat -r	muestra las rutas (similar a ejecutar route -r)
netstat -lnp64	forma abreviada de netstat -n -l -p –inet

[16] WIKIHOW, Cómo hacer ping en Linux, 2014, http://es.wikihow.com/hacer-ping-en-Linux

- **Comando arp**

Este comando permite obtener la dirección MAC de una interfaz de red.
ARP, Protocolo de resolución de direcciones, es un mecanismo que permite a IP convertir las direcciones Ethernet en direcciones IP; esto es importante porque cuando envía un paquete por una red Ethernet, es necesario poner la dirección Ethernet del anfitrión destino.

Modo de uso: *arp [-v] [-t type] -d [hostname]*

Algunas opciones

-v Indica al comando el modo verbose
-a obtiene todas las entradas ARP de la tabla
-t type Al leer la tabla ARP, este parámetro le diche que tipo de entradas deberán ser chequeadas.
-d [hostname] suprime la entrada de nombr_nodo de la tabla ARP
-s hostname hw_addr Crea una entrada en la table ARP de forma manual asociando hostname con hw_addr

- **Comando traceroute**[17]

Muestra la ruta que siguen los paquetes desde el origen hasta el destino; además nos da una idea de la rapidez de la ruta. Al mostrar la ruta se puede tener una idea de la estructura interna (routers, gateway, etc.) de la red a la que estamos conectados.

Modo de uso: *traceroute [-m max_ttl] [-p port] [-q nqueries] [-r] [-s scr_addr] [-t tos] [-w waittime] host [packetsize]*

-m max_ttl Setea el maximo ttl usado por los paquetes de prueba salientes. El valor por defecto es de 30
-p port Setea el número del puerto usado en las pruebas, por defecto es el puerto 333434.
-q nqueries Setea el número de pruebas por ttl a nqueries, el valor por defecto es 3.
-r Salta las tablas de ruteo normales y envía el paquete directamente a un host en la red local.

[17] FRANCISCONI, Hugo Adrián, Guía de Referencia Rápida de Linux, Venezuela, 2010, http://francisconi.org/sites/default/files/guia_de_referencia_rapida_de_linux.pdf

-s scr_addr Usa la siguiente IP como dirección de fuente en los paquetes de prueba de salida.
-t tos Setea el tipo de servicio en los paquetes de prueba a el siguiente valor el cual puede ser un entero entre 0 y 255, el valor por defecto es 0.
-v Setea el comando a verbose. Esta opción muestra los resultados intermedios (modo verbose)
-w Setea el valor por defecto es de 3 segundos.

- **Comando route**

Este comando se utiliza para configurar las tablas de enrutamiento del kernel del sistema. Generalmente en todo equipo en una red local encontraremos 3 rutas:

- Loopback, que utiliza el dispositivo de bucle interno (lo, lo0).
- Red local, que utiliza la tarjeta de red para comunicarse con equipo dentro del mismo segmento de red.
- Default que también utiliza la tarjeta de red para enviar a un router o Gateway paquetes que son para equipos de nuestros segmentos.

Si el comando es llamado sin parámetros este listara el estado de las tablas de ruteo.

Modo de uso: *route [-vn] [v] add [-net | -host] xxxx [gw GGGG] [metric MMMM] [netmask NNNN] [mss NNNN] [Windows NNNN] [dev DDDD] route [-v] del xxxx*

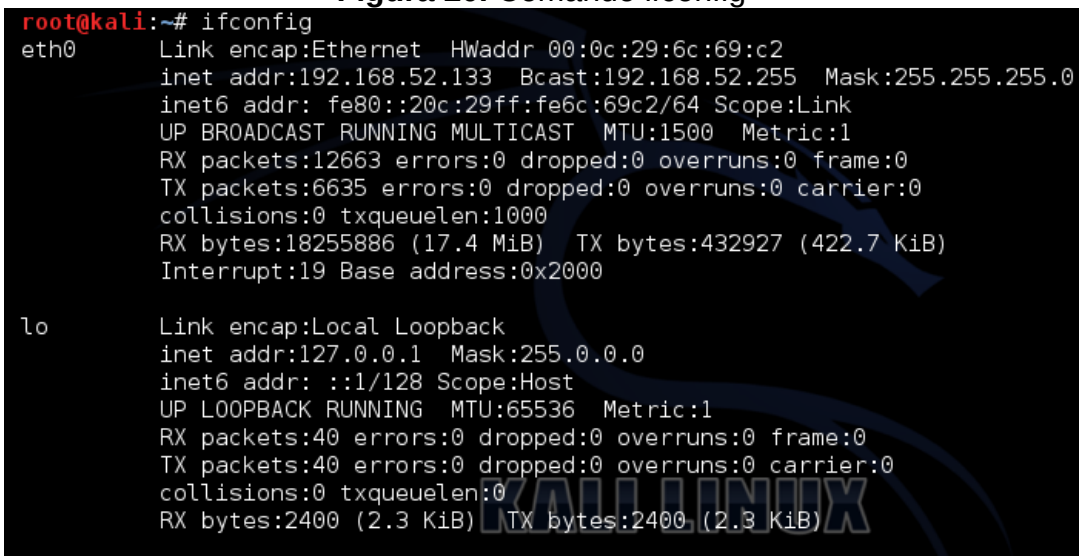
Algunas opciones
-n Igual a no pasarle parámetros, pero muestra en cambio las direcciones numéricas.
-v Setea el modo verbose (no es usado actualmente)
-del xxxx Borra las rutas asociadas con la dirección de destino xxxx
add [-net | -host] Adhiere una ruta a la dirección IP xxxx. La ruta es la ruta de red si el parámetro –net es usado o xxxx se encuentra en xxxx.
xxxx [gw GGGG] El argumento gw GGGG significa que algún paquete IP enviado a esta dirección debe ser ruteado al Gateway específico.
metric MMMM No está implementado actualmnete
netmask NNNN Especifica la máscara de red de la ruta a ser adherida.
dev DDDD Fuerza la asociación entre la ruta y un dispositivo específico

PROCEDIMIENTO

- **Comando *ifconfig*** (información sobre la red del sistema)

A continuación un ejemplo del comando ifconfig.

Figura 20. Comando ifconfig



En la figura se encuentran 2 interfaces de red **eth0** que es la interfaz de Ethernet y **lo** que es la interfaz de local loopback, también podemos encontrar otra interfaz la **wlan0** que es la interfaz Ethernet pero inalámbrica.

En la interfaz **eth0** se ven las siguientes características
Link encap: Ethernet → Tipo de interfaz Ethernet
Hwaddr 00:0c:29:6c:69:c2 → Dirección hardware o MAC
inet addr: 192.168.52.133 → Dirección IP asignada a la interfaz de red
Bcast: 192.168.52.255 → Dirección de difusión, broadcast
Mask: 255.255.255.0 → Mascara de subred, netmask
inet6 addr: fe80::20c::29ff::fe6c::69c2/64 → Dirección de red IPV6
MTU: 1500 → Valores de la Unidad Máxima de Transferencia
Metric: 1 → Métrica de la interfaz, algunos sistemas operativos lo usan para calcular el coste de la ruta, Linux no usa este valor por el momento, pero lo define por razones de compatibilidad.
RX paquets: 12663 → Paquetes recibidos sin errores, numero de errores ocurridos, de cuántos paquetes han sido descartados (seguramente por memoria insuficiente), y cuántos han sido perdidos por desbordamiento, condición que ocurre cuando la recepción de paquetes es demasiado rápida y el núcleo es incapaz de dar servicio al paquete anterior antes de la llegada del nuevo paquete

TX paquets: 6635 → Paquetes transmitidos sin errores, número de errores ocurridos, paquetes descartados y los que se han perdido por desbordamientos.

Ahora abra el terminal y escriba:
ifconfig
Identifique y escriba en el informe las principales características y detalles como por ejemplo las interfaces de red, dirección IP, broadcast, mascara de red, dirección mac, dirección IPV6, RX y TX.

- **Comando hostname (**Muestra o establece el nombre del sistema o equipo)

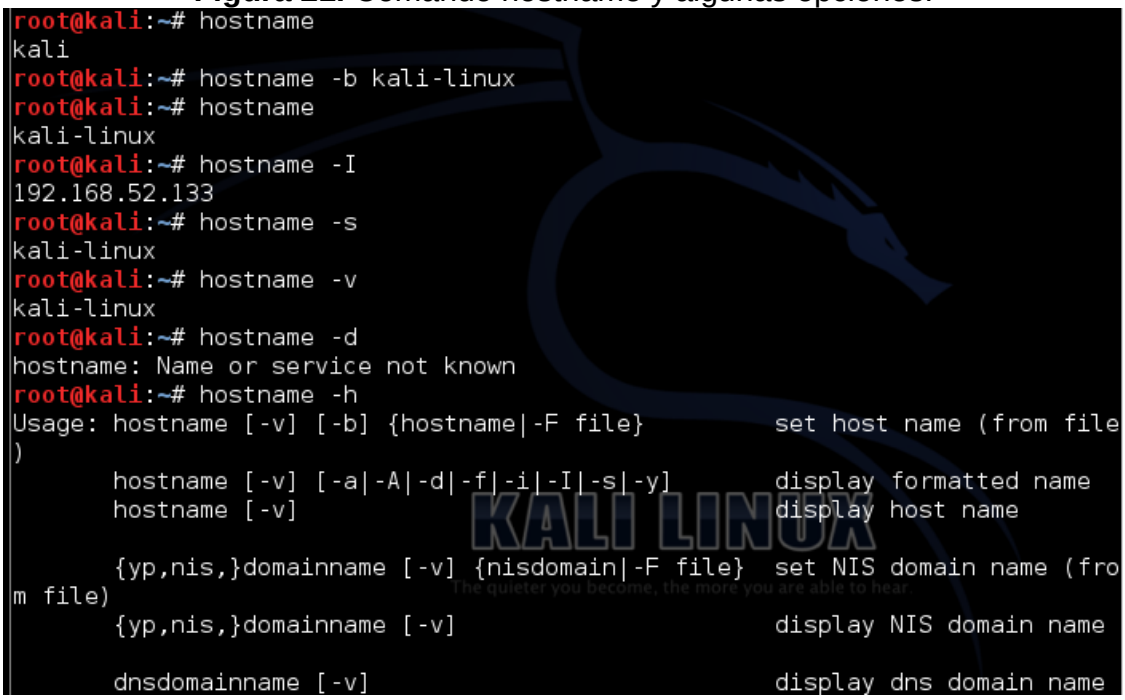
Escriba en el terminal el comando:
hostname
Anote la respuesta: _____
Este es el nombre de su sistema.

Para cambiar el nombre del sistema.
Escriba:
hostname kali-nuevo o ***hostname -b kali-nuevo***
Nuevamente escriba hostname para comprobar que se hizo el cambio

Para ver otras opciones del comando hostname.
Escriba:
hostname -h
Escriba 2 opciones de este comando y sus respuestas.
_____
_____
_____

A continuación unos ejemplos del comando *hostname*

Figura 21. Comando hostname y algunas opciones.



En esta figura se observa que el nombre del sistema es kali, luego lo cambiamos a kali-linux, con la opción i muestra la IP.

- **Comando ping** (para probar la conexión y la latencia entre dos conexiones de red)

A continuación se va a probar la conexión entre el computador y la página de internet de google.
En el terminal escriba:
ping www.google.com, luego de unos segundos teclee **ctrl+z**

Luego nuevamente escriba:
ping www.google.com, pero esta vez luego de unos segundos teclee **ctrl+c**

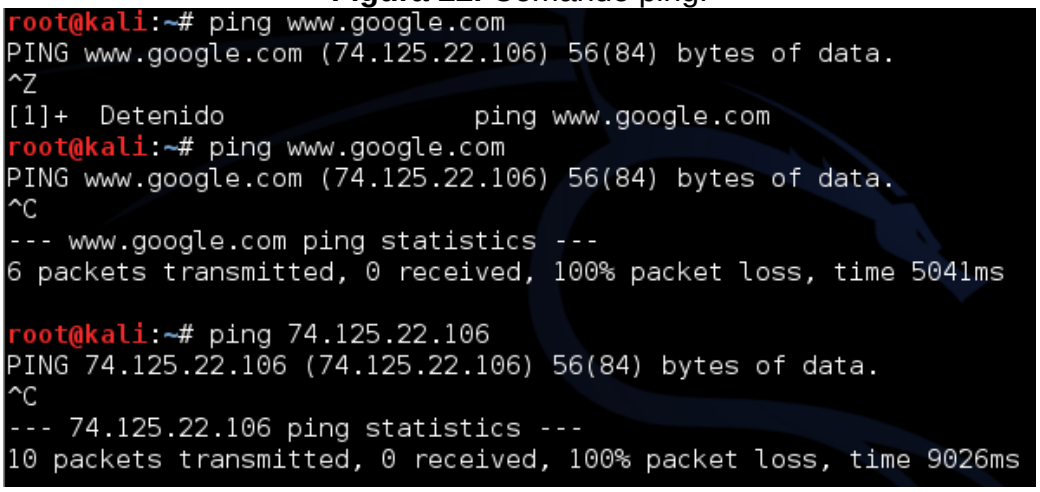
Escriba los resultados de las pruebas anteriores, por ejemplo la dirección IP de la página y las estadísticas de los paquetes y el tiempo.

_____
_____
_____

Cada página de internet tiene su propia dirección IP, por lo tanto también se puede hacer ping con su dirección IP respectiva.

A continuación un ejemplo del comando *ping*.

Figura 22. Comando ping.

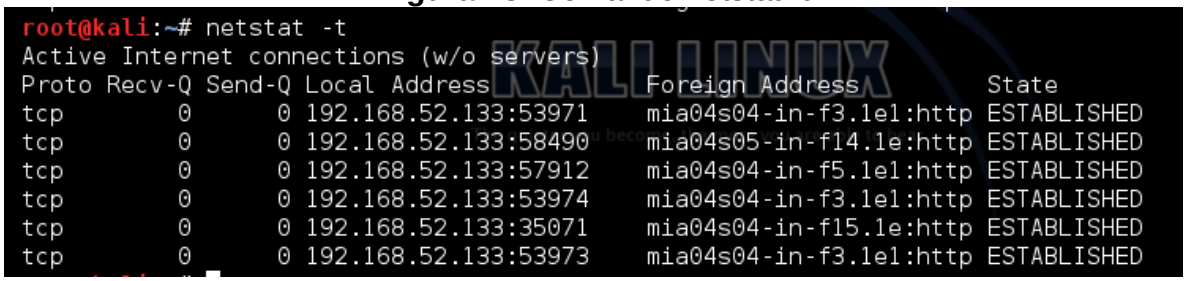


- **Comando netstat** (Muestra conexiones de red, tablas de ruteo, estadísticas de interfaces, etc)

Primero hay que abrir alguna página en el explorador de internet, por ejemplo www.youtube.com.

Ejemplo: comando ***netstat -t***

Figura 23. Comando netstat -t



Explicación de los resultados de este comando:

Proto → Indica el puerto, en este caso el puerto es TCP.
Recv-Q → (receive queue, lista de recepción), numero de bytes recibidos por el núcleo, pero no leídos por el proceso.
Sen-Q → Número de bytes enviados hacia el otro lado de la conexión, pero que no han sido reconocidos.

Local Address → Dirección local, dirección IP y el número de puerto de su propio servidor; el número del puerto está separado de la dirección IP por medio de dos puntos.
Foreign Address → Dirección extranjera, identifica el otro lado de la conexión.
State → Estado de la conexión, en este caso está en ESTABLISHED (establecida).

Ahora abra una o varias páginas de internet y escriba:
netstat -r
Esta opción nos muestra la tabla de enrutamiento del kernel, explique los resultados.

_____
_____
_____
_____

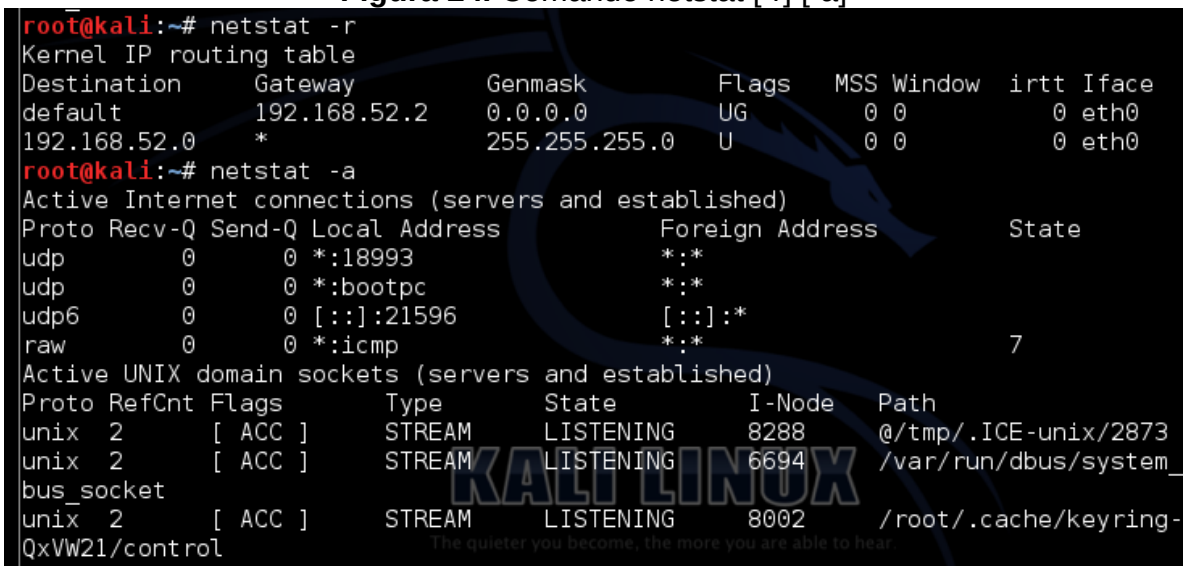
Escriba
netstat -a
Esta opción nos muestra toda la información de las conexiones y los sokets.
Explique los resultados.

_____
_____
_____
_____

Escriba
netstat –u
Para que sirve y explique los resultados.

_____
_____
_____
_____

Figura 24. Comando netstat [-r] [-a]



- **Comando arp** (permite obtener la dirección MAC de una interfaz de red)

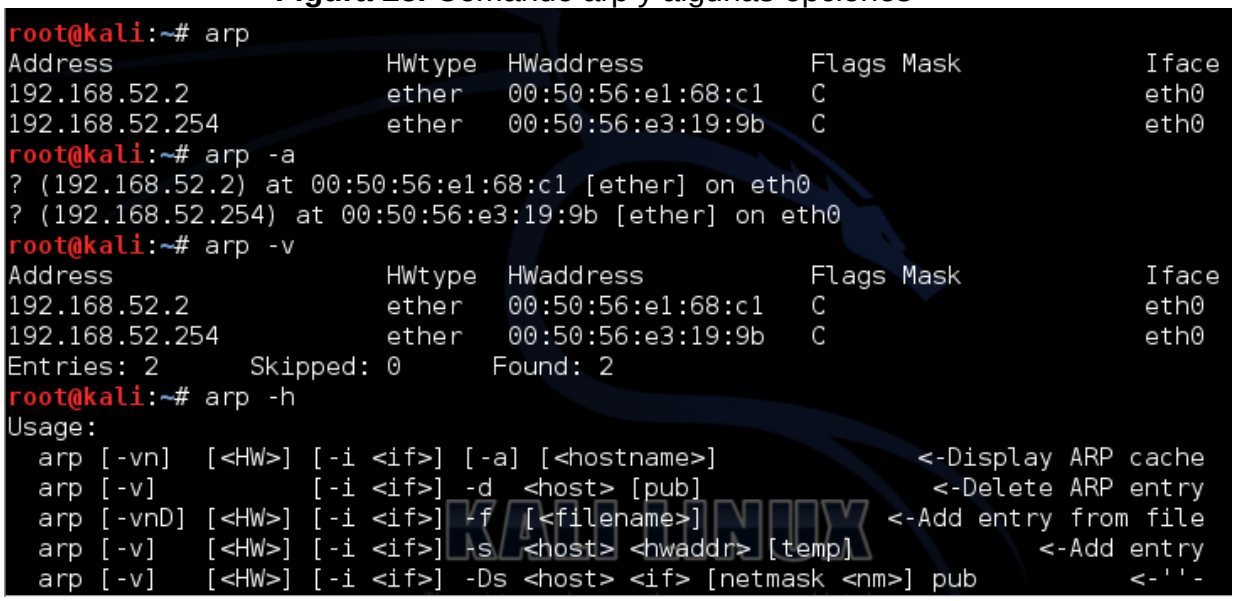
En la terminal escriba:
arp
Explique la tabla.

_____
_____
_____
_____
_____

Escriba
arp -a
Explique el resultado.

_____
_____
_____
_____
_____

Figura 25. Comando arp y algunas opciones



En la figura se observa varias opciones del uso del comando arp, por ejemplo una opción muestra que tiene 2 entradas arp y con interface eth0.

- **Comando traceroute** (Muestra la ruta que siguen los paquetes desde el origen hasta el destino).

Ejemplo:
traceroute www.google.com

Figura 26. Comando traceroute

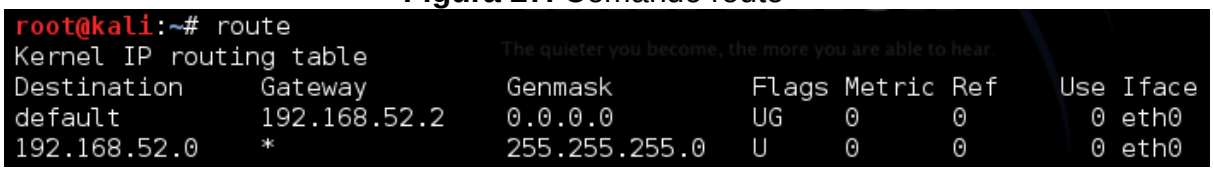
En la figura se observa el número de salto (1), el nombre y la dirección IP del nodo por el que pasa y posteriormente viene los tres tiempos siguientes son el tiempo de respuesta para los paquetes enviados (un asterisco indica que no se obtuvo respuesta).

Utilice el comando **traceroute** para otra página de internet y explique sus resultados.

- **Comando route** (Este comando se utiliza para configurar las tablas de enrutamiento del kernel del sistema)

Ejemplo:

Figura 27. Comando route



Explicación de la tabla:
Destination → Dirección Ip del destino
Gateway → Dirección IP de la puerta de acceso
Genmask → mascara de subred
Flags → Resumen del estado de la conexión, existen 3 estados. U (la conexión es up), H (el destino es un anfitrión) y G (El destino es una puerta de acceso).
Metric → El costo de una ruta, por lo general medido en saltos. En el núcleo linux no se usa esta información.
Ref → el número de referencias para esta ruta. Esto no se usa en el núcleo Linux.
Use → El número de bucles cerrados caché con éxito en la ruta. Para ver este valor, use la opción –F al llamar route.
Iface → Interfaz de red.

Escriba route y explique la tabla a continuación.

INFORME TALLER

- Investigar y dar un ejemplo con el comando **netstat -antp.**
- Utilizar una de las opciones del comando **route** y explicarlo.
- Utilizar una de las opciones del comando **traceroute** y explicarlo.

4.1.3 GUÍA N°3 PROGRAMACIÓN BÁSICA EN BASH SHELL

GUÍA N° 3
PROGRAMACIÓN BÁSICA EN BASH SHELL

OBJETIVOS

- Conocer y crear scripts.
- Conocer los comandos principales de Linux para crear scripts y manejo del bashshell.

REQUISITOS

- Manejo básico de programación.
- Conocimiento de comandos básicos para el terminal de Linux.

INTRODUCCIÓN

En esta guía se conocerá que es el Shell, bash-shell, y como crear los scripts; los cuales son muy importantes ya que estos ayudan a evitar hacer tareas repetitivas (automatizar procesos), ahorran tiempo y su programación es muy sencilla.
Dentro del contenido de los scripts se tratarán temas como entrada y salida de datos, el manejo de las variables, operaciones aritméticas, estructuras de control (condicionales, lógicos, bucles) y funciones.

MARCO TEÓRICO

Bash es una de tantas shell de Linux, la más popular en las distribuciones recientes como Ubuntu, Fedora o Mandriva. En la actualidad la gran mayoría de los scripts de configuración de las distribuciones de Gnu/Linux están programados en Bash, para quien desee personalizar su sistema a fondo el conocimiento de bash debe ser crítico.

¿Qué es un shell?

- El shell es un intérprete de comandos.
- Pero también es un lenguaje.
- El conjunto de comandos es un script.
- Un script sirve como 'la unión' de diversos comandos sencillos, que en conjunto son considerablemente poderosos.

¿Por qué aprender a programarlo?

- Te evita hacer tareas repetitivas.
- Es bueno conocerlo.
- Es fácil de aprender: piensa que quieres hacer - escríbelo - revísalo (ahora ponlo todo en un archivo o script).
- Usualmente no tiene que debugear mucho, es como si vaciara lo que haría en el prompt (terminal) de comandos, pero escrito en un archivo.

¿Cómo crear un script?

- Crear un archivo script.sh con tu editor de textos favorito.
- Darle permisos de ejecución: chmod +x script.sh.
- Ejecutarlo: ./script.sh

Para programar en bash se pueden utilizar todos los comandos del sistema, llamadas a otros script bash, funciones internas, y rutinas en otros lenguajes, estas características hacen que bash sea una herramienta potente que no pasa de moda.

Entrada y salida de datos

La salida de datos se realiza por pantalla con el comando *echo* y la entrada de datos, además de poder realizarla con el paso de parámetros se realiza con el comando *read*.

Manejo de variables

El nombre de una variable puede estar formado por cualquier conjunto de caracteres alfabéticos y pueden incluir números.

Para asignar un valor a una variable deberá escribir el nombre de la variable, el operador de asignación (=) y el valor asignado (Entre la variable, el **=** y el valor no deben existir espacios)

Al invocar una variable se le antepone el signo **$** al nombre de esta.

OPERACIONES ARITMÉTICAS[18]

Para realizar operaciones se utiliza el comando *expr* y para realizar comparaciones se utiliza el comando *test*

Comando expr

Se utiliza para realizar operaciones aritméticas simples y su sintaxis es:

$ expr arg1 op arg2 [op arg3 …]

[18] GÓMEZ LÓPEZ, Julio. Administración de sistemas operativos: Un enfoque práctico, 2a.ed México: Alfaomega Grupo editor, 2011, pág. 383. [Consulta: 19 de agosto de 2014]

A continuación una tabla de las operaciones que se puedes realizar con el comando expr

Tabla 2. Operaciones de expr

OPERADOR	COMENTARIO
Operadores aritméticos	
+	Suma
-	Resta
* o *	Multiplicación
/	División
%	Módulo - Resto de la división
Operadores adicionales	
=	Igualdad
!=	Diferentes
>	Mayor que
>=	Mayor o igual
<	Menor que
<=	Menor o igual
!=	Distinto de
Operadores lógicos	
|	Or lógico
&	And lógico
!	NOT lógico

let

Permite utilizar asignaciones y operaciones de asignación equivalentes a las de ***C***, otras operaciones son:

- incremento **+=**
- decremento **-=**
- multiplicar por ***=**
- dividir por **/=**

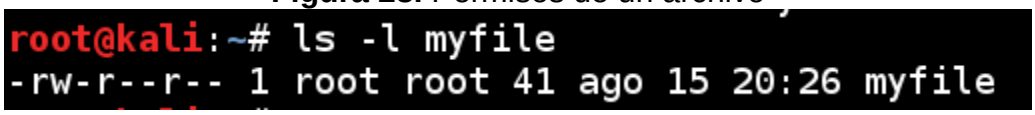
- modulo por **%=**
- incremento en 1 **++**
- decremento en 1 **--**

Permisos de archivos[19]

Si se lista un archivo con los comando **ls –l**, se puede observar los permisos del archivo.

Por ejemplo:

Figura 28. Permisos de un archivo



-rw-r--r-- → De izquierda a derecho se puede ver el tipo y los permisos del archivo.
1 → Números de link del archivo
root → usuario y grupo
41 → tamaño del archivo 41 bytes
ago 15 20:26 → ultima fecha que se editó el archivo.
myfile → Nombre del archivo.

Linux tiene permisos de lectura (read **r**), escritura (write **w**) y ejecución (execute **x**). También tiene permisos para el dueño, el grupo y los usuarios.

Las tres primeras letras son los permisos del dueño, las tres siguientes del grupo y las tres finales de los usuarios.

Esto quiere decir que el archivo myfile el dueño que es root tiene permisos de escritura y lectura (rw), el grupo root tiene permiso de lectura (r) y los usuarios solo tienen permiso de lectura (r).

PROCEDIMIENTO

Creación de un script

Ir a Aplicaciones → Accesorios →Leafpad (editor de texto)

Se abrirá el editor de texto y escribir:

#!/bin/bash →Un programa en bash siempre comienza con esta línea

echo "Este es un script" →Imprime o muestra en pantalla

[19] WEIDMAN, Georgia. Penetration Testing. A hands-On introduction to hacking. San Francisco: No Starch Press, 2014, pág 61, [Consulta: 4 de Agosto de 2015]

Luego guardar con el nombre ***script.sh***, en la carpeta root y cerrar el archivo.

Abrir la terminal y para ejecutar el script escriba:
chmod +x script.sh →(chmod) Cambia permiso, le da permiso (+) de ejecución (x)
./script.sh → Para ejecutar el script del directorio actual (./)
Le aparecerá el mensaje: Este es un script

```
root@kali:~# chmod +x script.sh
root@kali:~# ./script.sh
Este es un script
```

Como podemos ver la primera línea (***#!/bin/bash***) le indica al sistema qué programa ejecutará el resto de instrucciones que están en el script. En este caso el programa es bash y la ruta donde está ubicado el binario es /bin/bash.
La segunda línea (***echo "Este es un script"***) es una instrucción de bash, que permite imprimir en pantalla la frase "Este es un script".
Si se requiere escribir un comentario en el script se puede hacer con el signo "**#**" y luego el comentario.

Entrada y salida de datos
A continuación un ejemplo utilizando los comandos ***echo*** *(salida)* y ***read*** *(entrada)* de la variable.

Figura 29. script entrada y salida de datos

```
#!/bin/bash
echo -n "ingrese su nombre: "
read nombre
echo "Hola $nombre"
```

```
root@kali:~# chmod +x read.sh
root@kali:~# ./read.sh
ingrese su nombre: Ricardo
Hola Ricardo
```

Como se puede ver, se da la opción de preguntar por el valor de una variable, para luego leerla y utilizarla. El parámetro -n se utiliza para evitar el salto de línea.

Manejo de variables: (Asignar valor a una variable y luego invocarla)
Abrir y escribir en el editor y guardar el archivo como **variable.sh**:

```
#!/bin/bash
universidad="UPB"
echo $universidad       #imprime en pantalla UPB
```

Luego ejecute el script desde el terminal, escriba:

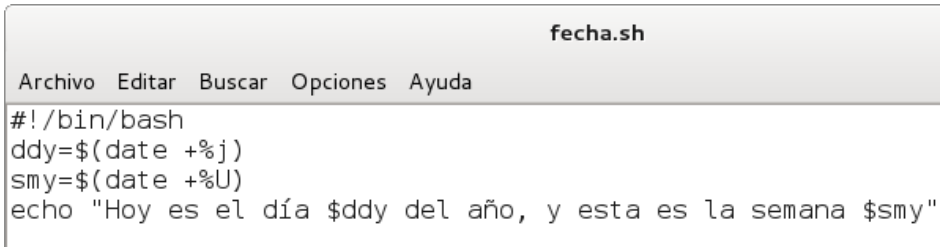
```
root@kali:~# chmod +x variable.sh
root@kali:~# ./variable.sh
UPB
```

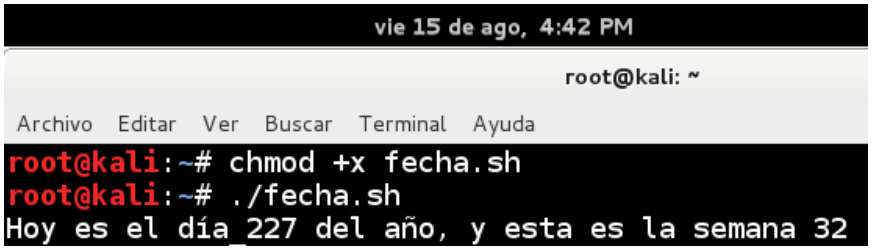
Como se puede ver, se crea una variable y luego se muestra en pantalla.

Otra utilización puede ser la siguiente:
Escriba y guarde el archivo como **variable2.sh**:
#!/bin/bash
universidad="UPB"
echo "$universidad Bucaramanga"
Ejecute el script y registre su resultado a continuación.

Nótese que con las comilla sigue siendo el resultado el mismo (UPB y no **$universidad UPB**)

En la utilización de variables su potencialidad es mayor cuando se puede almacenar en una variable el resultado de alguna operación, por ejemplo, se podría crear un bash que indique algunos datos del día y semana del año en curso, como el script que sigue:





Crear el script con el nombre de fecha.sh y escribir su resultado:

Nótese que para asignar un valor de un comando, este necesita ser evaluado, para ello es que se utiliza el **$( )**

OPERACIONES ARITMÉTICAS

Para realizar operaciones se utiliza el comando *expr* y para realizar comparaciones se utiliza el comando *test*

Comando expr

Ejemplo: Multiplicación de 2 variables

```
#!/bin/bash
echo -n “Introduce un valor: ”
read var1
echo -n “Introduce un valor: ”
read var2
resultado=$(expr $var1 \* $var2)
echo “El resultado de la multiplicación es ”$resultado
```

Figura 30. Script comando expr

```
root@kali:~# chmod +x expr.sh
root@kali:~# ./expr.sh
“Introduce un valor: ”7
“Introduce un valor: ”9
“El resultado de la multiplicación es ”63
```

En este ejemplo se preguntó por el valor de 2 variables, y el resultado es la multiplicación entre estas 2 variables.

Ahora realice un script con una operación adicional u operadores lógicos, escriba el script y sus resultados a continuación.

Ejemplo de evaluaciones numéricas:

Se crea un script llamado *operaciones.sh* en el cual se realiza la operación de la multiplicación y la suma.

```
#!/bin/bash
total=$((5+10*2))
echo $total
```

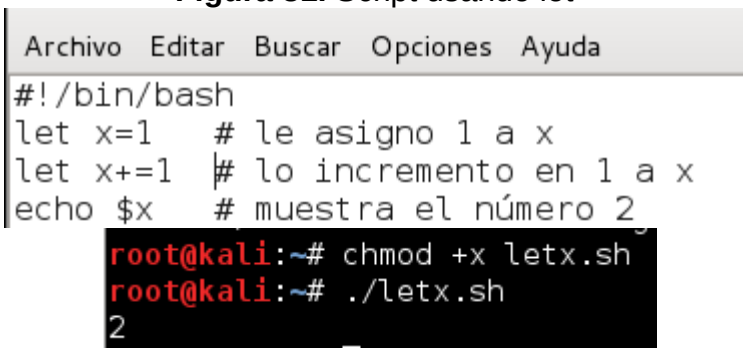
```
root@kali:~# chmod +x operaciones.sh
root@kali:~# ./operaciones.sh
25
```

También se pueden utilizar las otras operaciones matemáticas, como resta, suma, multiplicación, división, entre otras.

Crear y ejecutar un script que realice otras operaciones matemáticas diferentes a las del ejemplo anterior. Adjunte sus resultados a continuación.

Ejemplo utilizando let

Figura 31. Script usando let



Como ver en la figura ***let*** permite utilizar asignaciones y operaciones de asignación equivalentes a las de ***C***.
Realice un script utilizando let y que involucre otra de las opciones, como decremento, multiplicado por, dividido por, etc. Adjunte resultados a continuación.

Concatenación de cadenas

Ejemplo.

```
#!/bin/bash
cadena1="Universidad"
espacio="  "
cadena2="Pontificia"
cadena3="Bolivariana"
echo $cadena1$espacio$cadena2$espacio$cadena3
```

```
root@kali:~# chmod +x concatenacion.sh
root@kali:~# ./concatenacion.sh
Universidad Pontificia Bolivariana
```

Caracteres especiales

- **#** indica un comentario
- **;** separador, permite tener dos o más instrucciones en la misma línea
- **;;** terminador de bloques en la instrucción **case**
- **:** instrucción que no hace nada, el típico **NOP** (do-nothingoperation)
- **!** indica negación
- ***** indica todo, si se usa como operación aritmética, indica multiplicación
- ****** multiplicación exponencial.

Sentencias de Control

Antes de comenzar con las sentencias propiamente tal, nos detendremos en un par de operadores para crear las sentencias condicionales y así poder armar algunas expresiones a evaluar.

Algunos operadores

Operadores para operaciones numéricas y lógicas

- No **!**
- y **&&**
- o ||
- menor o igual **-le**
- mayor o igual**-ge**
- mayor que **-gt**
- menor que**-lt**
- igual que **-eq**
- distinto que **-ne**
- operador lógico AND **-a**
- operador lógico OR **-o**

if else

Ejemplos:

```
#!/bin/bash
if((4 < 6)); then
 echo "cuatro es menor que seis"
fi
root@kali:~# chmod +x ifelse.sh
root@kali:~# ./ifelse.sh
cuatro es menor que seis
```

*ifelsefi.sh

Archivo Editar Buscar Opciones Ayuda

```
#!/bin/bash
if((4 > 6)); then echo "cuatro es mayor que seis"
else echo "cuatro no es mayor que seis"
fi
root@kali:~# chmod +x ifelsefi.sh
root@kali:~# ./ifelsefi.sh
cuatro no es mayor que seis
```

case

El siguiente script recibe un parámetro e indicará el valor en palabras, en caso que sea uno de los que estén en la lista de lo contrario no hará nada.

Ejemplo:

```
Archivo  Editar  Buscar  O
#!/bin/bash
numero=$1
case $numero in
1)
 echo "uno"
;;
2)
 echo "dos"
;;
3)
 echo "tres"
;;
4)
 echo "cuatro"
;;
5)
 echo "cinco"
;;
6)
 echo "seis"
;;
7)
 echo "siete"
;;
8)
 echo "ocho"
;;
9)
 echo "nueve"
;;
esac
```

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# chmod +x case.sh
root@kali:~# ./case.sh 3
tres
root@kali:~# ./case.sh 12
root@kali:~# ./case.sh 8
ocho
root@kali:~#
```

for

Ejemplo de un **for** aplicando la lógica tradicional de los lenguajes de programación.

Escriba:

#!/bin/bash
cadena=""
for((a=0;a<8;a++))
do
cadena=$cadena$a
echo $cadena
done

```
#!/bin/bash
cadena=""
 for((a=0;a<8;a++))
  do
    cadena=$cadena$a
    echo $cadena
  done
```

donde se obtiene como resultado lo siguiente:

```
root@kali:~# chmod +x for.sh
root@kali:~# ./for.sh
0
01
012
0123
01234
012345
0123456
01234567
```

while

ejemplo:

```
#!/bin/bash
CONTADOR=0
while [  $CONTADOR -lt 10 ]; do
   echo El contador es $CONTADOR
   let CONTADOR=CONTADOR+1
done
```

```
root@kali:~# chmod +x while.sh
root@kali:~# ./while.sh
El contador es 0
El contador es 1
El contador es 2
El contador es 3
El contador es 4
El contador es 5
El contador es 6
El contador es 7
El contador es 8
El contador es 9
```

until

Ejemplo:

```
#!/bin/bash
CONTADOR=20
until [  $CONTADOR -lt 10 ]; do
    echo El contador $CONTADOR
    let CONTADOR-=2
done
```

```
root@kali:~# chmod +x until.sh
root@kali:~# ./until.sh
El contador 20
El contador 18
El contador 16
El contador 14
El contador 12
El contador 10
```

Manipulación de Cadenas

En Bash podemos realizar múltiples manipulaciones de Cadenas, sin embargo algunas funcionalidades es mucho más rápida realizarlas apoyándose en herramientas externas y que por lo general son parte de la mayoría de las instalaciones básicas de los sistemas Unix.

expr, sed y awk

expr, sed y awk son 3 herramientas que nos son muy útiles para el manejo de cadenas en Bash.

expr : es una utilidad para evaluar expresiones

sed : es considerado un editor de textos no interactivo

awk : es un lenguaje de patrones interpretados enfocados en el procesamiento, muy poderoso.

Manipulando caracteres especiales

Es común que necesitemos ocasionalmente manipular caracteres "raros" en nuestras rutinas. Para esto podemos optar al manejo de tales caracteres en sus códigos ascii. Así:

echo -e "\x41\x20\x42\x20\x43"

```
root@kali:~# echo -e "\x78\x20\x82\x20\x03"
x
```

Como podemos ver en la imagen el código \x78 es la letra x, el código \x20 es el espacio, el código \x82 es un carácter de signo de interrogación y por último el código \x03 es un carácter del número 0003.

Funciones

La utilización de funciones dentro de cualquier script pueden simplificar mucho el código, además de mejorar estéticamente la presentación y comprensión del mismo.

Veamos un ejemplo simple:

*funcion.sh

Archivo Editar Buscar Opciones Ayuda

```
#!/bin/bash
 function funcion1 {
   echo "estamos en la 1 y le pasamos el parametro:"$1
 }
 function funcion2 {
   echo "estamos en la 2 y le pasamos el parametro:"$1
 }

 # ahora a ejecutarlas!
 funcion1 hola
 funcion2 chao
```

la salida en este caso es la siguiente:

estamos en la 1 y le pasamos el parametro:hola

estamos en la 2 y le pasamos el parametro:chao

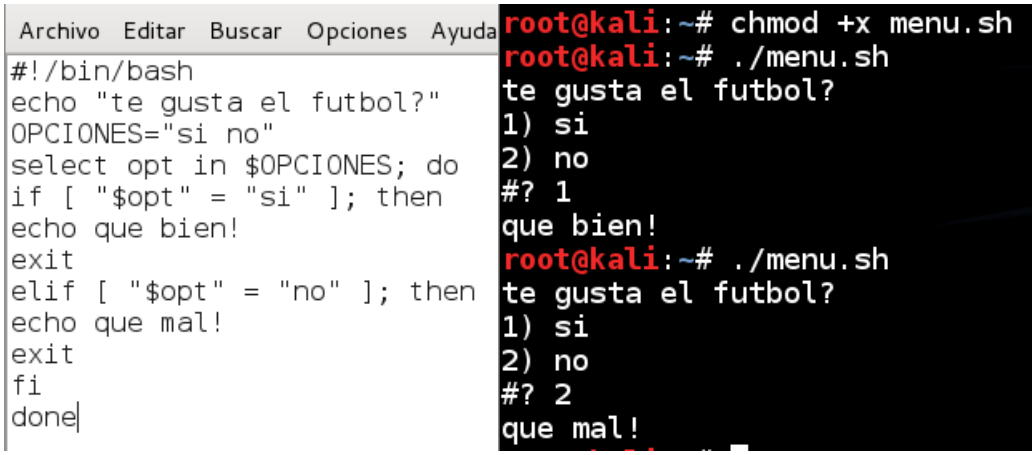
root@kali: ~

Archivo Editar Ver Buscar Terminal Ayuda

```
root@kali:~# chmod +x funcion.sh
root@kali:~# ./funcion.sh
estamos en la 1 y le pasamos el parametro:hola
estamos en la 2 y le pasamos el parametro:chao
```

Menús de selección sencillos

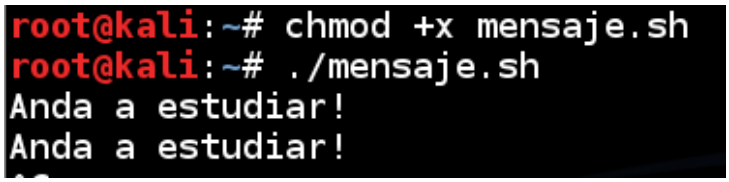
un ejemplo simple:



Ejemplo de script: Cada 10 minuto mostrar el mensaje "Anda a estudiar!"

```
#!/bin/bash
total=$((10*60)) # 10 minutos son 10*(60 segundos)
while ((0==0)); do
sleep $total
echo "Anda a estudiar!"
done
```

pantallazo para cada minuto mostrar “Anda a estudiar”



Ejemplo script: Listando el tamaño de un archivo o directorio

Listará el tamaño de un archivo o directorio que se le entrega como parámetro, indicará un mensaje de error en caso que la ejecución no sea la correcta.

Figura 32. Script listando el tamaño de un archivo

```
#!/bin/bash

Error(){
        echo "Error. Sintaxis de uso: $0/ archivo | directorio"
}

if [ $# -lt 1 ]; then
        Error
elif [ -d $1 ]; then
        echo "$1 es un directorio y su tamaño es el siguiente:"
        du -hs $1
   elif [ -f $1 ]; then
        echo "$1 es un archivo regular y su tamaño es el siguiente:"
        du -hs $1
   else echo "$1 no existe."
fi
```

```
root@kali:~# chmod +x lista.sh
root@kali:~# ./lista.sh script.sh
script.sh es un archivo regular y su tamaño es el siguiente:
4,0K    script.sh
root@kali:~# ./lista.sh guia1
guia1 es un directorio y su tamaño es el siguiente:
8,0K    guia1
root@kali:~#
```

Otra opción sencilla es la utilización del comando du:
#Ejemplo 1 para saber tamaño total del home de usuario knx (incluye tamaño de todos los subdirectorios)
du -h -s /home/knx/

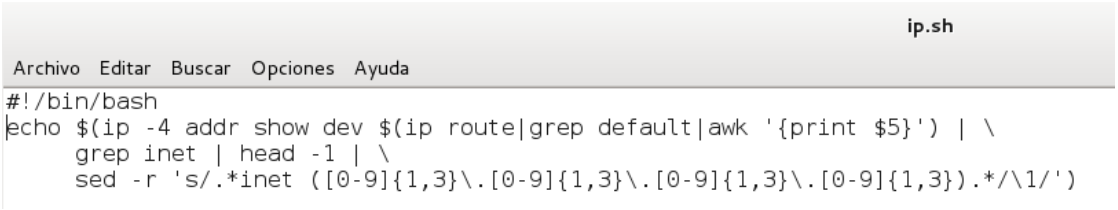
Ejemplo 2 , lo mismo pero con detalle
du -h /home/knx/

Ejemplo script: Obteniendo la IP de la interfaz que mantiene la conexión activa hacia Internet

A continuación vemos 2 formas de obtener cual es la IP de conexión activa que actualmente esta utilizando el sistema para salir a Internet. Para obtenerla se han utilizado los comandos grep, ip, awk,sed. Esta IP no necesariamente corresponde a la ip pública del usuario, pero si a la IP por la cual está conectado a la red. Esto puede ser utilizado por ejemplo en firewall iptables en los cuales se necesita conocer la IP activa asignada a la interfaz con la cual se está saliendo a Internet.

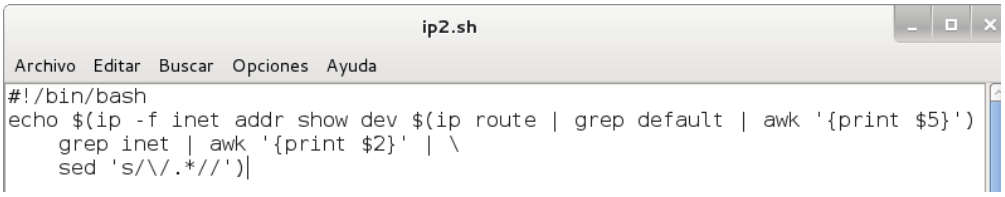
Forma 1

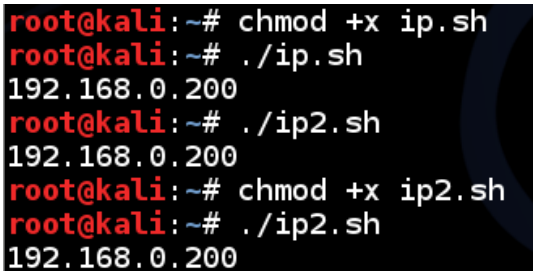
```
echo $(ip -4 addr show dev $(iproute|grepdefault|awk '{print $5}') | \
grepinet | head -1 | \
sed -r 's/.*inet ([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}).*/\1/')
```



Forma 2

```
echo $(ip -f inetaddr show dev $(ip route | grep default | awk '{print $5}') | \
grepinet | awk '{print $2}' | \
sed 's/\/.*//')
```





Como se puede observar en la imagen, por cualquiera de las 2 formas da la misma respuesta, y también hay otras maneras de hacer esta programación, esta se hace según las necesidades y exigencias del usuario.

Escoger una de estas 2 formas y registrar los resultados.

TRABAJO

1. Crear una calculadora que haga operaciones de suma, resta, multiplicación y división entre 2 números.

2. Crear un conversor de moneda en pesos a valor en dólar, euro, bolívar o libras esterlinas.

4.1.4 GUÍA N°4 WIRESHARK

GUÍA N°4
WIRESHARK

OBJETIVOS

- Conocer el programa WIRESHARK.

SOFTWARE Y HARDWARE REQUERIDOS

- Computador con sistema operativo LINUX.
- Cable UTP de conexión a red Ethernet.
- Conexión de Red LAN Ethernet a la cual interconectar el computador.

INTRODUCCIÓN

En esta guía se va a trabajar con el software gratuito llamado WIRESHARK, este software es muy importante para el análisis, prevención y solución de los diferentes problemas que ocurren a diario en las redes de comunicaciones.
Wireshark trabaja mediante la captura de tráfico de datos, esta puede ser a través de una red viva o de un archivo de captura salvado en un disco.

PROCEDIMIENTO

Para abrir el programa, hay 3 opciones.

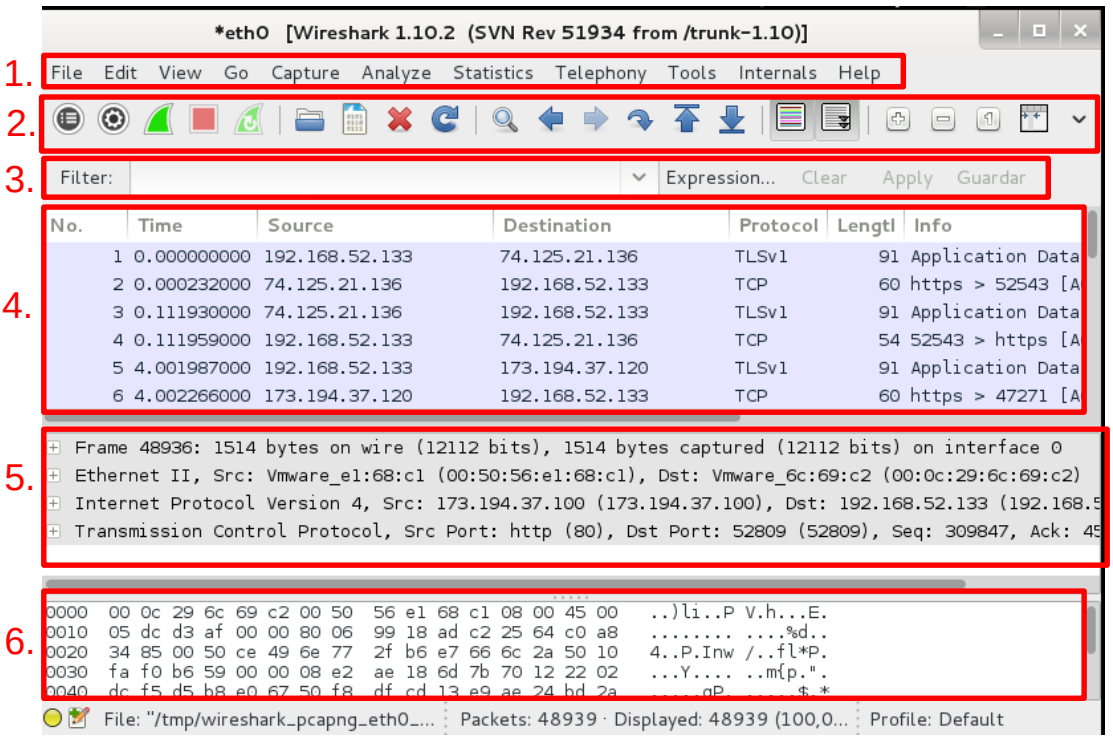
- Aplicaciones → internet → Wireshark
- Aplicaciones → Kali Linux →Top 10 Security Tools → Wireshark
- Aplicaciones → Kali Linux → Recopilación de información → Análisis de trafico → Wireshark

Luego en la opción **Start** escoger la interfaz con la que se va a trabajar, en este caso se escoge la interfaz **eth0** y dar click en el icono de Start  .
Luego abrir el explorador de internet y por unos minutos navegar por varias páginas de internet.

Para detener la captura de datos dar click en el icono Stop  .

Luego de terminar la captura de paquetes se podrá observar una ventana como la figura siguiente.

Figura 33. Wireshark analizando tráfico de red.



1. Barra de menús:[20]

File: Este menú contiene opciones para abrir y combinar archivos de captura, guardar / imprimir / exportar archivos de captura en su totalidad o en parte, y para salir de Wireshark.

Edit: Este puede aplicar funciones a los paquetes, por ejemplo, buscar un paquetes especifico, aplicar una marca al paquete y configurar la interfaz de usuario.

View: Permite configurar el despliegue del paquete capturado, mostrar barra de herramientas y paneles de los paquetes.

Go: Desde acá se puede ir a un paquete especifico, volver atrás, adelante, etc.

Capture: Para iniciar, detener y configurar la captura de paquetes.

Analyze: Se usa para manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.

[20] VÁSQUEZ, Junior, Manual Wireshark En Español, Medellín, 2013, http://manualwireshark.blogspot.com.co/

Statistics: Podemos definir u obtener las estadísticas del trafico capturado.
Telephony: Trae herramientas para telefonía.
Tools: Opciones para el firewall.
Internal: Parámetros internos de Wireshark
Help: Menú de ayuda (ayuda básica, manual, preguntas frecuentes, descargas, página principal de Wireshark)

2. Barra de herramientas principal.

Se encuentra la lista de interfaces de captura, opciones de captura, inicio, detener y reanudar la captura, abrir, guardar, cerrar, reanudar el archivo de captura, filtros y colores de los paquetes de captura.

3. Barra de filtros:

Filter: Abre el diálogo de construcción del filtro. Una comprobación de sintaxis de la cadena de filtro se hace mientras usted está escribiendo. El fondo se convertirá en verde cuando se introduce una cadena válida. Puede hacer clic en la flecha desplegable para seleccionar una cadena de filtro introducido anteriormente en una lista.
Expression: Permite editar un filtro de pantalla agregando una expresión.
Clear: Cambie el filtro de pantalla actual y borra el área de edición.
Guardar: Aplicar el valor actual en el área de edición como el nuevo filtro de visualización.

4. Panel de la lista de paquetes:[21]

Cada línea corresponde a un paquete capturado, al seleccionar una de estas, ciertos detalles son desplegados en el resto de paneles (detalles y bytes).

Las columnas muestran datos del paquete capturado.
No.: Posición del paquete en la captura.
Time: Muestra el Timestamp del paquete. Su formato puede ser modificado desde el menú *View → Time Display Format*.
Source: Dirección origen del paquete.
Destination: Dirección destino del paquete
Protocol: Nombre del protocolo del paquete.
Length: Longitud de los paquetes.
Info: Información adicional del contenido del paquete.

[21] ANTRAX-LABS, Sniffing con Wireshark, 2015. http://www.antrax-labs.org/2012/01/sniffing-con-wireshark.html

5. Panel de detalles de paquetes:

Muestra el paquete seleccionado con mayor detalle.

Se efectúa el análisis de acuerdo a la información arrojada con la información detallada de cada paquete.

Protocolo, interfaz, bytes, puerto, tiempo de captura

6. Panel de la lista de bytes de paquetes:

Muestra los datos del panel superior en formato hexadecimal y ascii.

ESTADÍSTICAS DE PAQUETES[22]

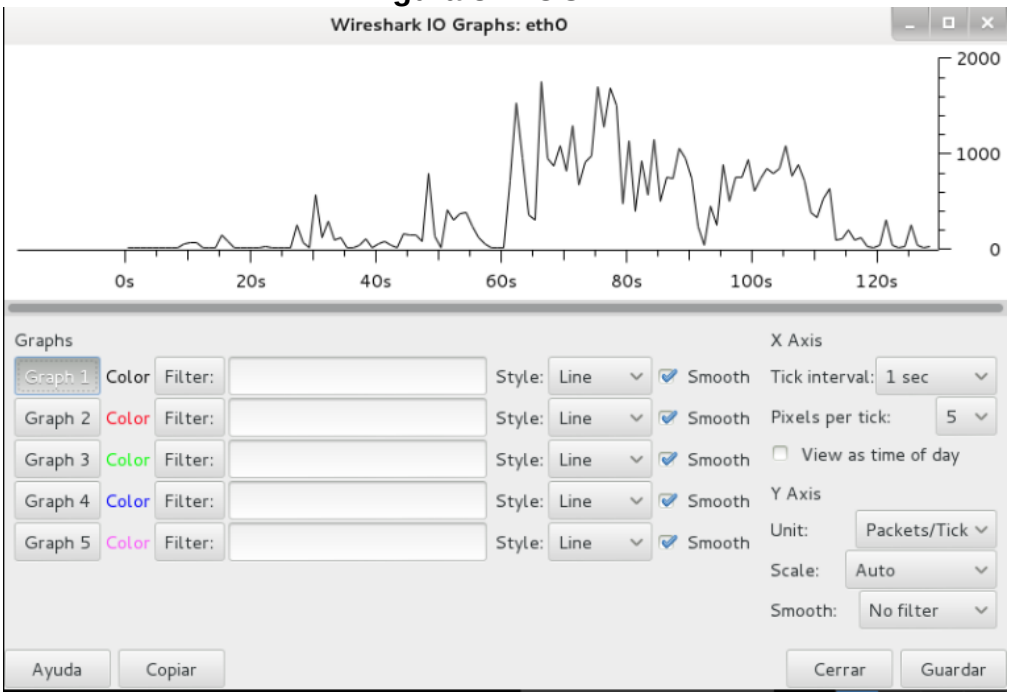
A continuación se utilizarán algunas herramientas para el análisis de paquetes

IO GRAPHS

Statistics → IO Graphs

Gráfica específica del usuario (número de paquetes a lo largo del tiempo)

Figura 34. IOGRAF



El usuario puede configurar las siguientes cosas:

[22] SAMBONI, Diana Marcela, Manual básico de Wireshark, Medellín, 2012, http://www.slideshare.net/DIANYSS2012/manual-bsico-de-wireshark

Graphs (Gráficos)

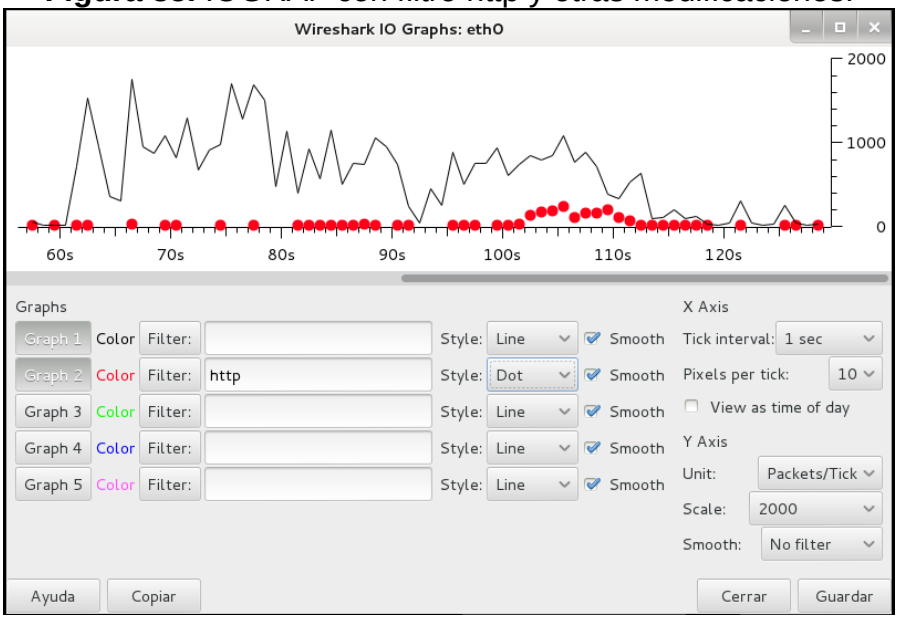
Gráfico 1-5: permitir la gráfica específica 1.5 (el gráfico 1 se activa por defecto)
Color: Color del gráfico (no se puede cambiar)
Filtro: Filtro de pantalla para este gráfico (sólo los paquetes que pasan este filtro se tendrán en cuenta para este gráfico)
Estilo: Estilo de la gráfica (Línea / Impulse / fbar / Dot)
Eje X

Marque interval: intervalo de tiempo en la dirección x (0.001sec, 0.01sec, 0,1 sec, 1 sec, 10 sec, 1min, 10 min)
Píxeles por señal: utilizan 10, 5, 2, 1 píxeles por intervalo de señal.
Ver la hora del día: opción para ver las etiquetas de dirección x como la hora del día en lugar de segundos o minutos.

Eje Y

Unidad: La unidad de la dirección (paquetes /Tick, Bytes/Tick, Bits/ Tick, avanzadas...).
Escala: La escala de la unidad (logarítmica, Auto, 10, 20, 50, 100, 200,...)
Guardar: guardará la parte visualizada actualmente del gráfico como uno de varios formatos de archivo.

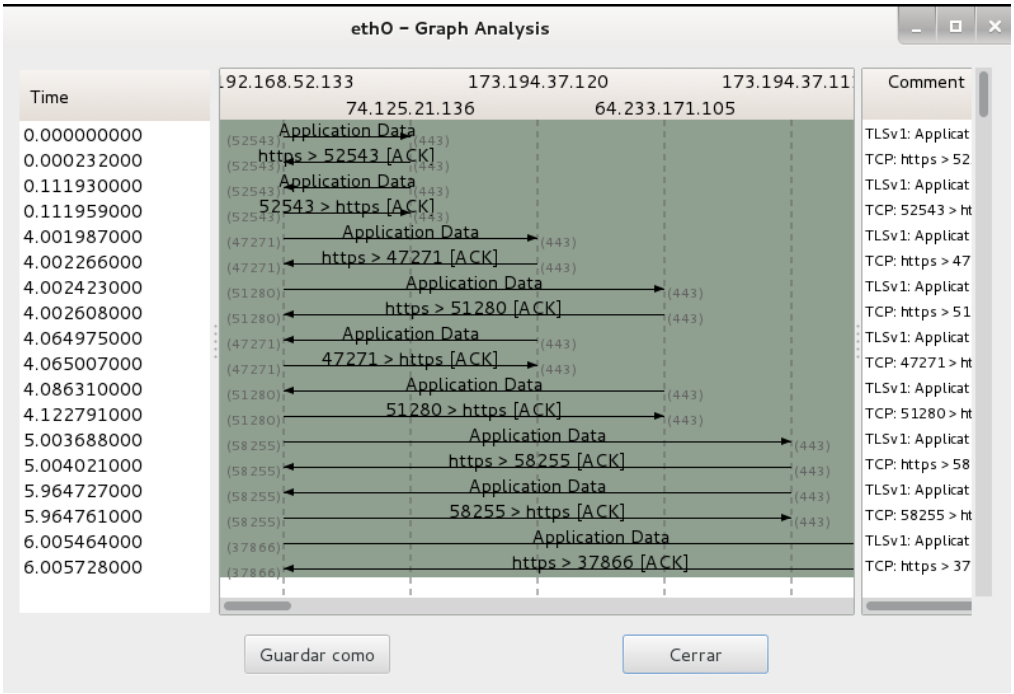
Figura 35. IOGRAF con filtro http y otras modificaciones.



Flow Graph

Statistics → Flow Graph
Esto muestra el flujo de mensajes entre uno o más sistemas finales, en su orden cronológico.

Figura 36. Flow Graph

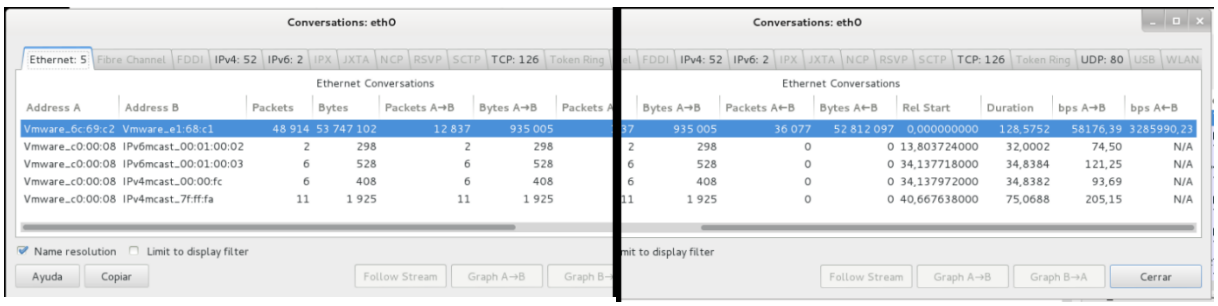


Conversations

Statistics → Conversations

Muestra una lista de conversaciones (tráfico entre dos puntos finales)

Figura 37. Conversations



Esta figura proporciona información sobre las conversaciones presentes en la red, con quien se está comunicando cada host, en el caso específico ilustrado se puede observar que se detectaron 5 conversaciones ethernet, 52 conversaciones ipv4, 2 conversaciones IPV6, 126 conversaciones tcp y 80 conversaciones UDP.

Para cada conversación es posible ver la cantidad de paquetes y byte transmitidos en cada dirección, esto puede ayudar a identificar que hosts son los que están acaparando más el ancho de banda.
Con un clic en cualquiera de los campos se ordena en base a ese parámetro, ya sea en orden ascendente o descendente.

En la parte inferior aparece un botón de *copiar*, con este se copia el contenido de estadísticas y se puede pegar en un documento de texto o en un documento de excel con todos los valores separados por comas, por lo que posteriormente es posible abrir el archivo en Excel o en cualquier hoja de cálculo, para generar gráficas, o hacer un análisis más a fondo.

TALLER

1. Abrir Wireshark y capturar paquetes durante 5 minutos.
2. Utilizar una de las herramientas de estadística anteriormente vista.
3. Analizar los paquetes con Protocol Hierarchy Statistic y explicar sus resultados.
4. Guardar la captura de datos, abrir el archivo con Microsoft Excel y generar una gráfica con su respectiva explicación.

4.1.5 GUÍA N°5 INSTALACIÓN DE MAQUINAS VIRTUALES Y PROGRAMAS CON KALI

GUÍA N°5
INSTALACIÓN DE MAQUINAS VIRTUALES Y PROGRAMAS CON KALI

OBJETIVOS

- Conocer e instalar máquinas virtuales.
- Conocer los comandos principales para la instalación de diferentes programas en Kali Linux.

REQUISITOS

- Computador con internet para descargar los programas.
- Manejo de computadores y programación básica.

INTRODUCCIÓN

En esta guía se va a conocer la instalación de una máquina virtual lo cual consiste en un programa que simula otro ordenador dentro del ordenador que se tiene para poder hacer pruebas sin afectar el sistema operativo principal.

También se trabajará con nuevos comandos para instalar programas, ya que estos se instalan de diferente manera a la que se está acostumbrado con Windows.

MARCO TEÓRICO

¿QUE ES UNA MAQUINA VIRTUAL?[23]

Una máquina virtual es un programa dentro de un sistema operativo que simula ser su propio sistema operativo.

Beneficios:

- La posibilidad de tener distintos sistemas operativos sin necesidad de crear particiones o tener más discos duros.

[23] CETEM, Fundación de servicios educativos EMSSANAR, ¿Qué es una máquina virtual? 2014. http://cetemso.blogspot.com/2014/01/que-es-una-maquina-virtual-y-para-que.html

- La posibilidad de probar software que aún no es estable (versiones beta, alfa, etc.) o instalar software teniendo la certeza que no afectara a nuestro sistema operativo base.
- Configurar los dispositivos según los recursos que se desee, siempre y cuando no supere las características del real. Es decir no puedo configurar una máquina virtual con 8 Gb de RAM si mi equipo real tiene apenas 4Gb.
- Correr algunos programas que no corren nativa mente en el sistema que tienen instalado.
- Posibilidad de simular otro dispositivo de red.

Desventajas:

- La velocidad de desempeño del computador real es inversamente proporcional al número de máquinas virtuales ejecutándose en el computador.

PRINCIPALES PROGRAMAS DE MAQUINAS VIRTUALES

VMware[24]

Es un sistema de virtualización por software. Un sistema virtual por software es un programa que simula un sistema físico (un computador, un hardware) con unas características de hardware determinadas. Cuando se ejecuta el programa (**simulador**), proporciona un *ambiente de ejecución* similar a todos los efectos a un computador físico (excepto en el *puro acceso físico* al hardware simulado), con CPU (puede ser más de una), BIOS, tarjeta gráfica, memoria RAM, tarjeta de red, sistema de sonido, conexión USB, disco duro (pueden ser más de uno), etc.

Un virtualizador por software permite ejecutar (simular) varios computadores (sistemas operativos) dentro de un mismo hardware de manera simultánea, permitiendo así el mayor aprovechamiento de recursos. Sin embargo al ser una capa intermedia entre el sistema físico y el sistema operativo que funciona en el hardware emulado, la velocidad de ejecución de este último es menor, pero en la mayoría de los casos suficiente para usarse en entornos de producción.

Entre este software se incluyen **VMware Workstation**, y los gratuitos **VMware Server** y **VMware Player**. El software de VMware puede funcionar en Windows, Linux. El nombre corporativo de la compañía es un juego de palabras usando la interpretación tradicional de las siglas «**VM**» en los ambientes de computación, como máquinas virtuales (**V**irtual **M**achines).

[24] WIKIPEDIA, VMware, https://es.wikipedia.org/wiki/VMware [Consulta: martes, 3 de noviembre de 2015]

VMware Player Es un producto gratuito para uso personal que permite ejecutar máquinas virtuales creadas con productos de VMware. Las máquinas virtuales se pueden crear con productos más avanzados como VMware Workstation, o con el propio VMware Player desde su versión 3.0 (las versiones anteriores no incluyen dicha funcionalidad).

VitualBox[25]

Es un potente producto de virtualización x86 y AMD64 / Intel64 para la empresa, así como el uso doméstico. No sólo es VirtualBox un extremadamente rico en características, producto de alto rendimiento para clientes empresariales, es también la única solución profesional que está libremente disponible como software de código abierto bajo los términos de la Licencia Pública General de GNU (GPL) versión 2.

Actualmente, VirtualBox se ejecuta en Windows, Linux, Macintosh y anfitriones Solaris y soporta un gran número de sistemas operativos invitados incluyendo pero no limitado a Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8), DOS / 3.x Windows, Linux (2.4, 2.6 y 3.x), Solaris y OpenSolaris, OS / 2, y OpenBSD.

VirtualBox está siendo desarrollado activamente con lanzamientos frecuentes y tiene una creciente lista de características, los sistemas operativos invitados compatibles y plataformas que se ejecuta. VirtualBox es un esfuerzo de la comunidad, el respaldo de una empresa dedicada: todo el mundo se anima a contribuir mientras que Oracle garantiza que el producto siempre cumple con los criterios de calidad profesional.

[25] ORACLE, Welcome to virtualbox, https://www.virtualbox.org/ [Consulta: martes, 3 de noviembre de 2015]

PROCEDIMIENTO

Se realizara instalación de kali Linux con 2 programas, VMWARE PLAYER y VIRTUALBOX, también se puede utilizar directamente kali Linux sin necesidad de instalación y por último la instalación de programas. Entonces escoger el procedimiento según las necesidades.

1. INSTALAR KALI LINUX EN UNA MAQUINA VIRTUAL CON VMWARE PLAYER

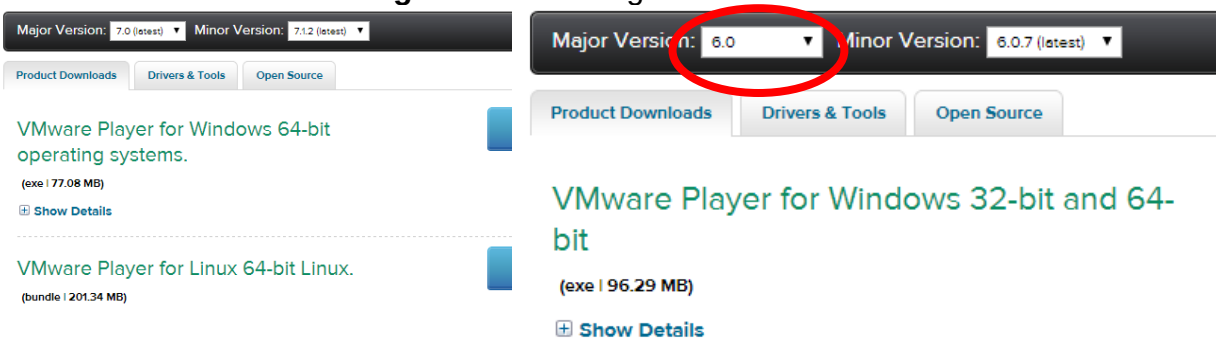
Lo primero que se debe hacer es descargar e instalar el programa Vmware player que es gratuito para uso personal para sistemas operativos como Microsoft Windows y Linux.

Ir a la página principal: http://www.vmware.com/co

Luego ir a la pestaña de Downloads → free product download → player; o al siguiente link.
https://my.vmware.com/web/vmware/free#desktop_end_user_computing/vmware_player/7_0

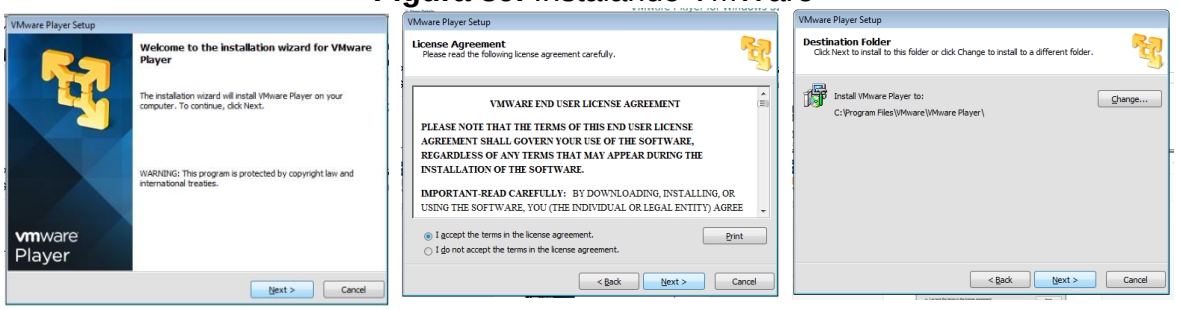
Y descargar la versión para Windows.

Figura 38. Descargar VMware



Por defecto aparece la última versión que es la versión 7.1.2 para sistemas de 64-bit. Si su sistema operativo no es de 64 bits, entonces escoger la versión 6 que es para 32 y 64 bits.

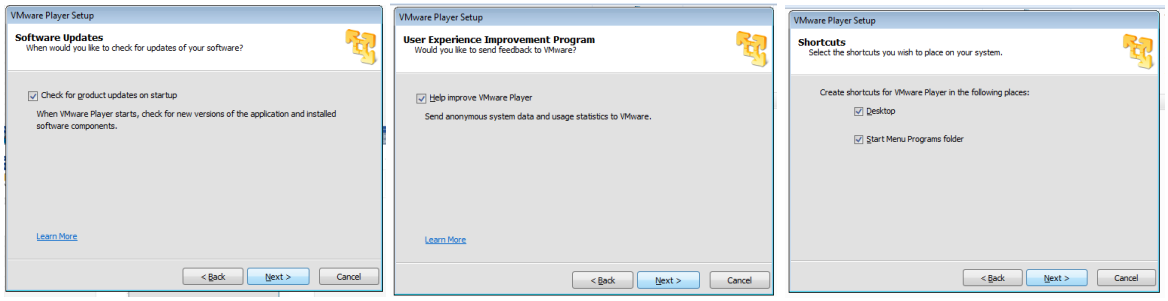
Figura 39. Instalando VMWare



Luego de que se descargue se ejecuta para instalarlo.

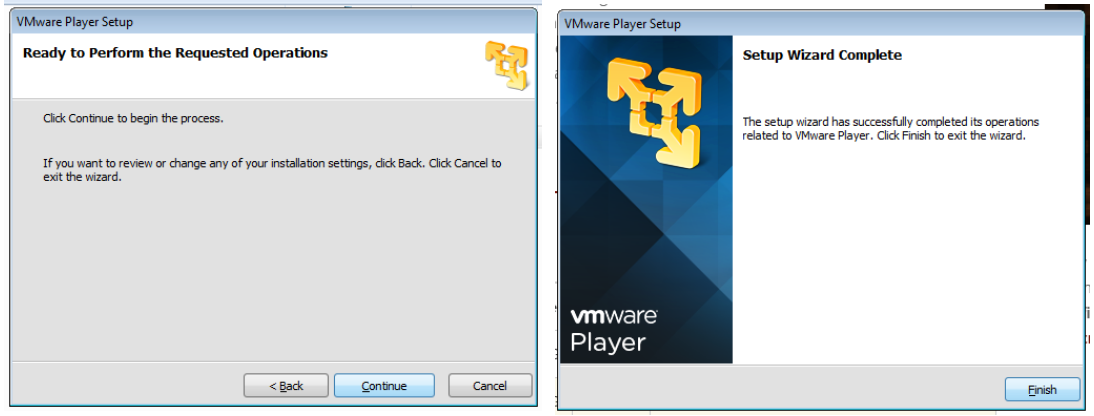
- Aparece el instalador diciendo que se va a instalar el programa. Para continuar dar click en **Next >**
- Aceptar los términos, dar click en **Next >**
- Escoger la carpeta de instalación, dar click en **Next >**

Figura 40. Instalando VMWare (Actualizaciones, acceso directo)



- Revisar actualizaciones, dar click en **Next >**
- Ayudar a mejorar el programa VMware Player, dar click en **Next >**
- Crear accesos directos en el escritorio y en el menú, dar click en **Next >**

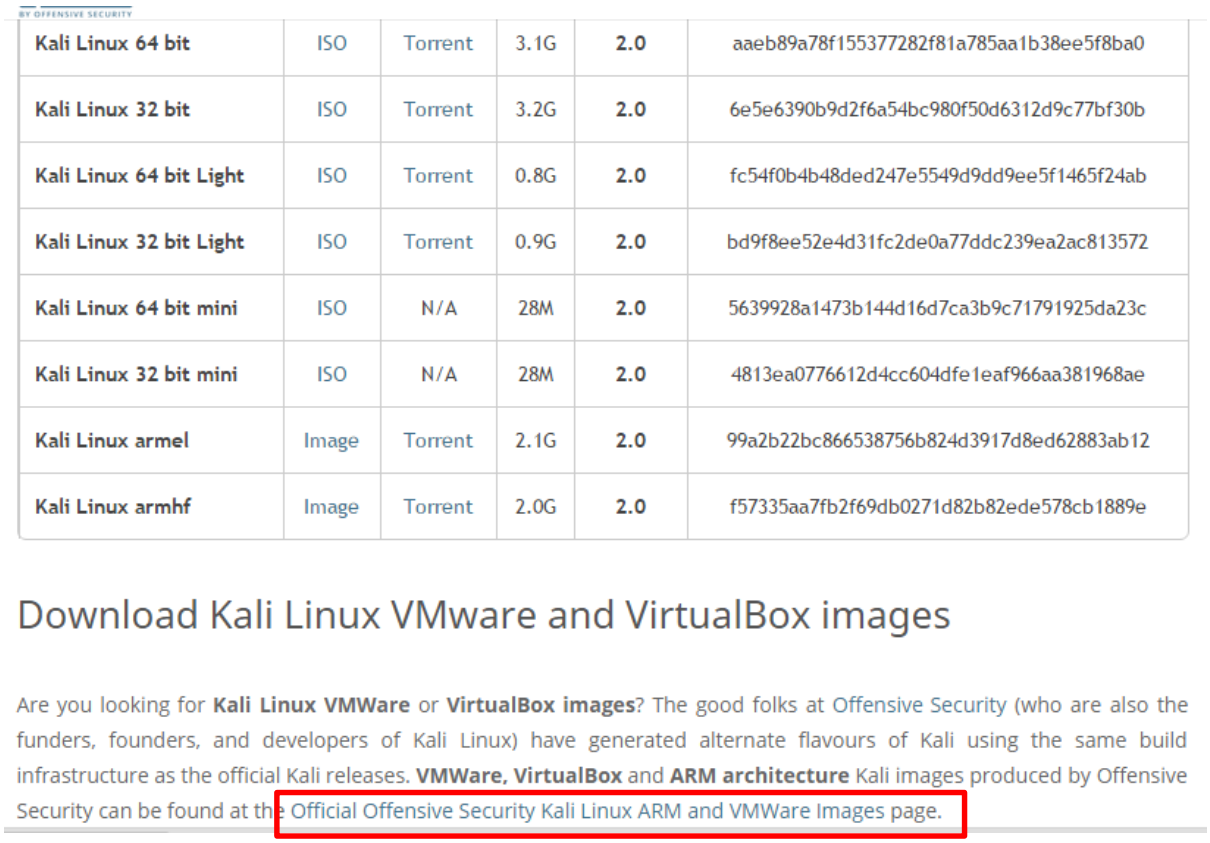
Figura 41. Terminando instalación de VMWare



- Si quiere realizar algún cambio de la instalación con la opción <back, pero para seguir con la instalación dar click en el botón **Continue**.
- Se terminó la instalación, para finalizar dar click en **Finish**.

Ahora se va a descargar e instalar la versión de kali linux
Ir a la página principal de KALI (http://www.backtrack-linux.org/) e ir a la pestaña de **DOWNLOADS.**

Figura 42. Página de Kali Linux para descargarlo



Kali Linux 64 bit	ISO	Torrent	3.1G	**2.0**	aaeb89a78f155377282f81a785aa1b38ee5f8ba0
Kali Linux 32 bit	ISO	Torrent	3.2G	**2.0**	6e5e6390b9d2f6a54bc980f50d6312d9c77bf30b
Kali Linux 64 bit Light	ISO	Torrent	0.8G	**2.0**	fc54f0b4b48ded247e5549d9dd9ee5f1465f24ab
Kali Linux 32 bit Light	ISO	Torrent	0.9G	**2.0**	bd9f8ee52e4d31fc2de0a77ddc239ea2ac813572
Kali Linux 64 bit mini	ISO	N/A	28M	**2.0**	5639928a1473b144d16d7ca3b9c71791925da23c
Kali Linux 32 bit mini	ISO	N/A	28M	**2.0**	4813ea0776612d4cc604dfe1eaf966aa381968ae
Kali Linux armel	Image	Torrent	2.1G	**2.0**	99a2b22bc866538756b824d3917d8ed62883ab12
Kali Linux armhf	Image	Torrent	2.0G	**2.0**	f57335aa7fb2f69db0271d82b82ede578cb1889e

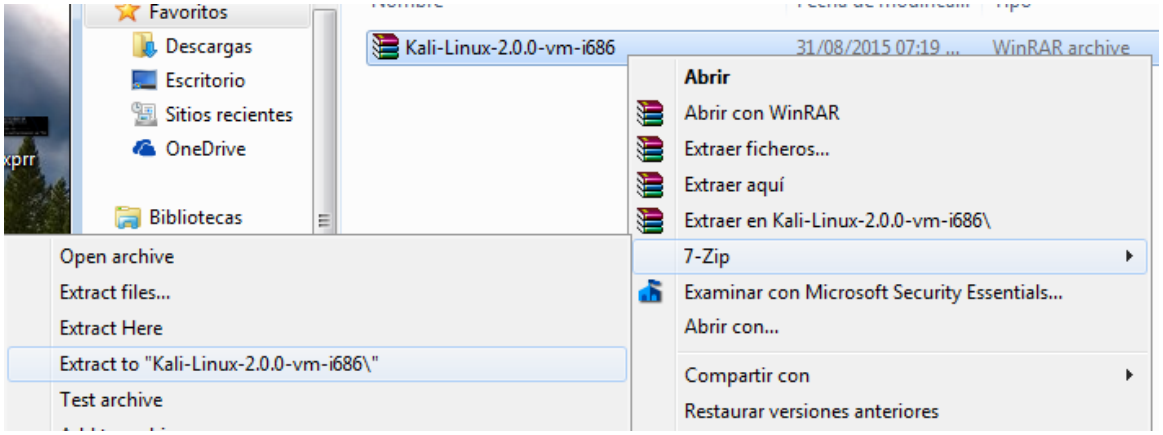
Aparece la última versión de Kali Linux para descargar en diferentes opciones según la necesidad del usuario y las características del equipo, en este caso se va a descargar la imagen que ya tiene establecida para el programa Vmware player.
Descargar la imagen de kali linux para vmware en el siguiente link.
https://www.offensive-security.com/kali-linux-vmware-arm-image-download/

Figura 43. Versiones de kali linux para descargar.

Image Name	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit VM	Torrent	2.6G	2.0	f48bab05669c7a1db93ef0e4f72df736ff2c2c91
Kali Linux 32 bit VM PAE	Torrent	2.6G	2.0	60dd1cbbc25019aec43d8807a6070931651887be
Kali Linux 32 bit	N/A	3.0G	1.1.0c	245477d1cfd5ff82254432ffe62af6e923adcfdc

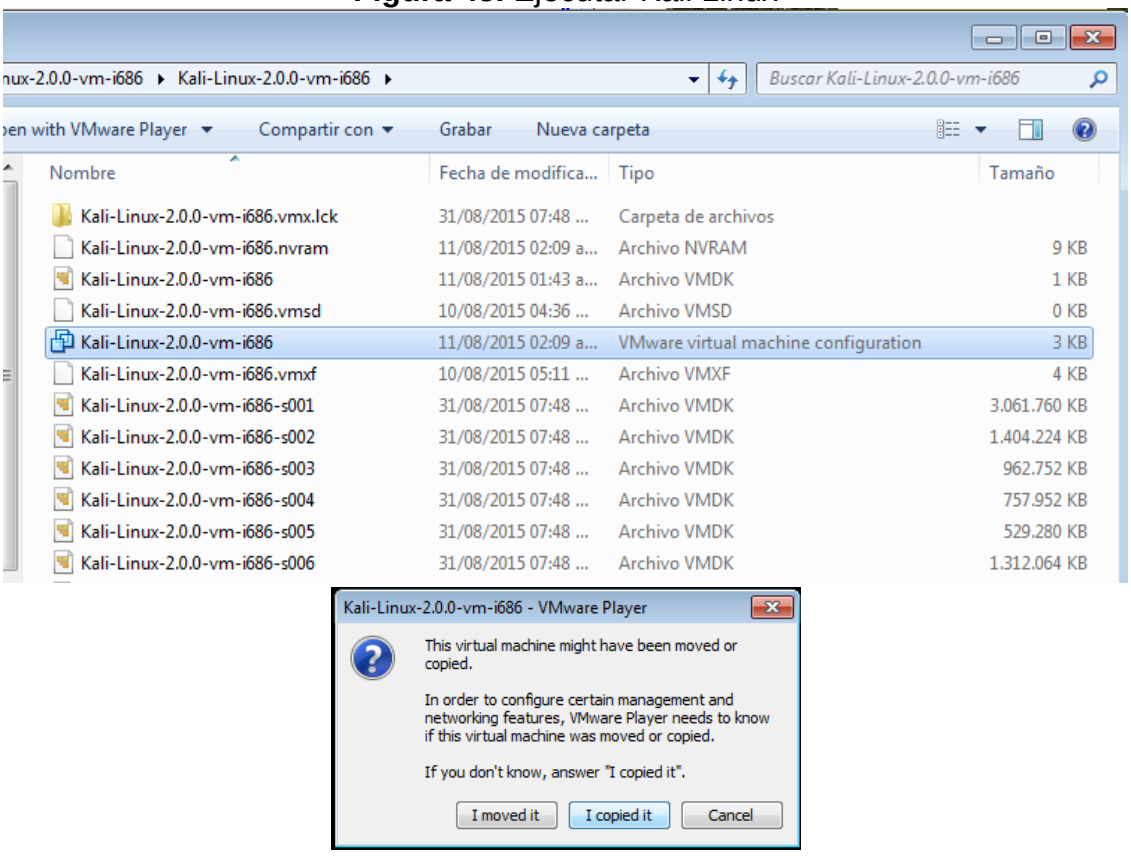
En esta ocasión actualizaron la versión de Kali Linux, por lo tanto aparece la versión 2.0, entonces escoger la segunda opción **Kali Linux 32 bit VM PAE.** Y así se descarga la imagen para VMware player.
Esta imagen viene comprimida entonces hay que extraerla a una carpeta con el programa 7zip. (http://www.7-zip.org/).
Al archivo de la imagen de Kali Linux se extrae dándole click derecho, 7-Zip, Extract to “Kali-linux-2.0….” como muestra la imagen a continuación.

Figura 44. Extraer imagen de Kali Linux



Luego ir a la carpeta y buscar el archivo **kali-linux-2.0.0-vm-i686** (tipo de archivo VMware virtual machine configuration) y ejecutarlo.

Figura 45. Ejecutar Kali Linux



Dar click en “**I copied it**”

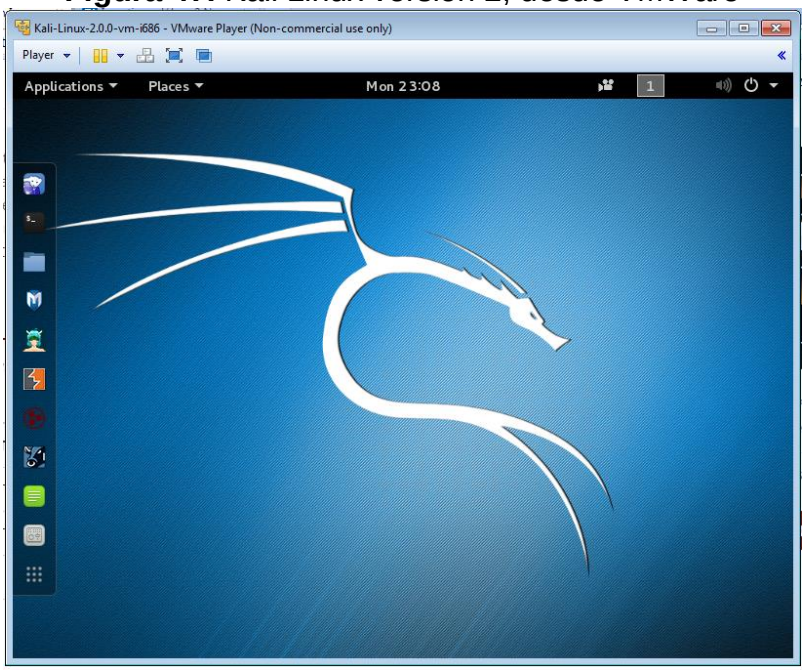
Arranca el Sistema operativo Kali linux versión 2, el usuario escribimos **root** y la contraseña **toor**

Figura 46. Usuario y clave de Kali Linux

Nombre de usuario, escribir **root**

Contraseña: **toor**

Figura 47. Kali Linux versión 2, desde VMWare



Esta figura corresponde al sistema operativo Kali Linux versión 2.0 ejecutado desde el programa VMware.

Para volver a los controles del pc, con las teclas Ctrl+alt.

2. INSTALAR KALI LINUX EN UNA MAQUINA VIRTUAL CON VIRTUALBOX

Ir a la página de virtualbox (https://www.virtualbox.org/wiki/Downloads) y descargar el programa según el sistema operativo a donde la vamos a instalar, en este caso escogemos virtualbox para Windows.

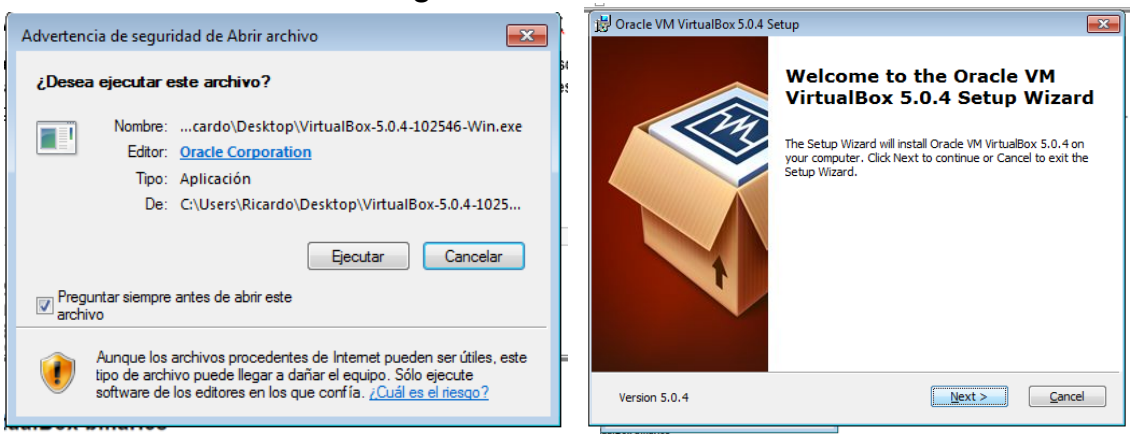
VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

- **VirtualBox platform packages**. The binaries are released under the terms of the GPL version 2.
  - **VirtualBox 5.0.4 for Windows hosts** ⇨x86/amd64
  - **VirtualBox 5.0.4 for OS X hosts** ⇨amd64
  - **VirtualBox 5.0.4 for Linux hosts**
  - **VirtualBox 5.0.4 for Solaris hosts** ⇨amd64

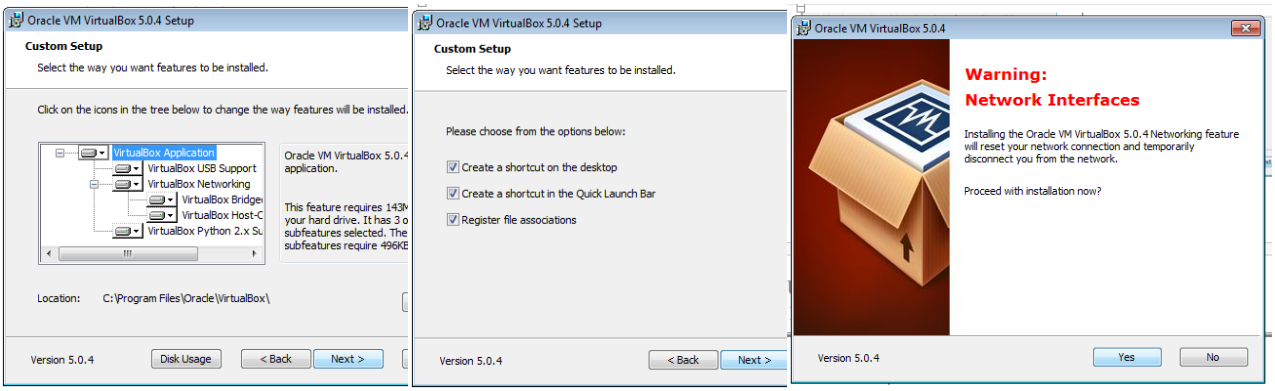
Ejecutar el programa.

Figura 48. Instalar VirtualBox



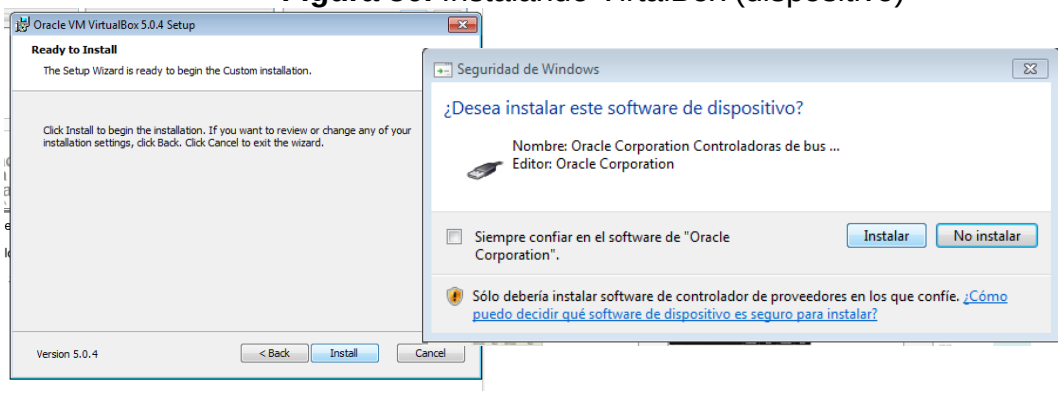
- Desea ejecutar este archivo? **Ejecutar**
- Bienvenido, se va a instalar Virtualbox **Next>**

Figura 49. Instalando VirtalBox (seleccionar carpeta)



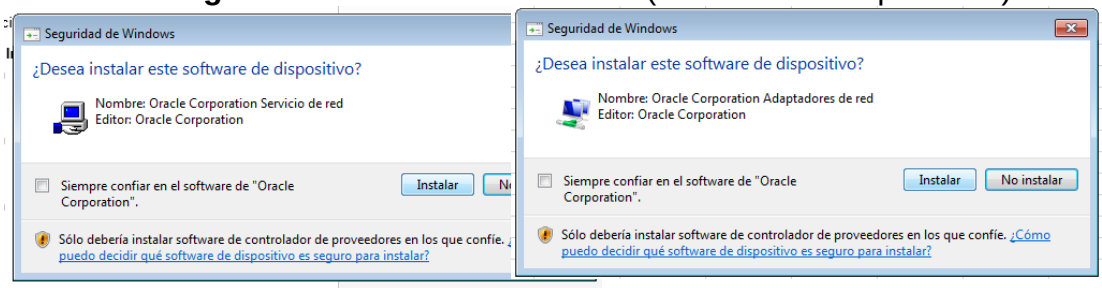
- Seleccionar en donde se va a instalar. **Next>**
- Seleccionar lo que se va a instalar. **Next>**
- Advertencia: Su red se va a reiniciar mientras se instala el programa. **Yes>**

Figura 50. Instalando VirtalBox (dispositivo)



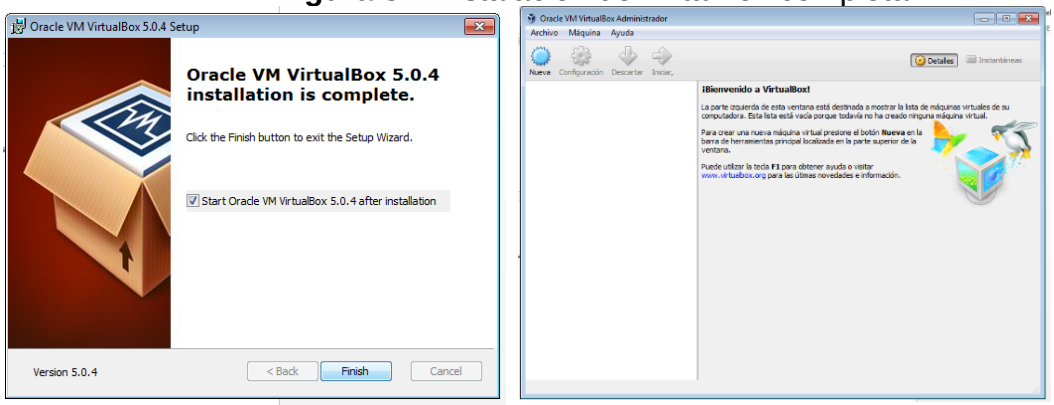
- Listo para instalar, se va a empezar la instalación. **Install >**
- Desea instalar este software de dispositivo?. **Instalar**

Figura 51. Instalando VirtualBox (Software de dispositivos)



- Desea instalar este software de dispositivo?. **Instalar**
- Desea instalar este software de dispositivo?. **Instalar**

Figura 52. Instalación de VirtalBox completa



- La instalación está completa **Finish**
- Y por último se abre el programa VirualBox.

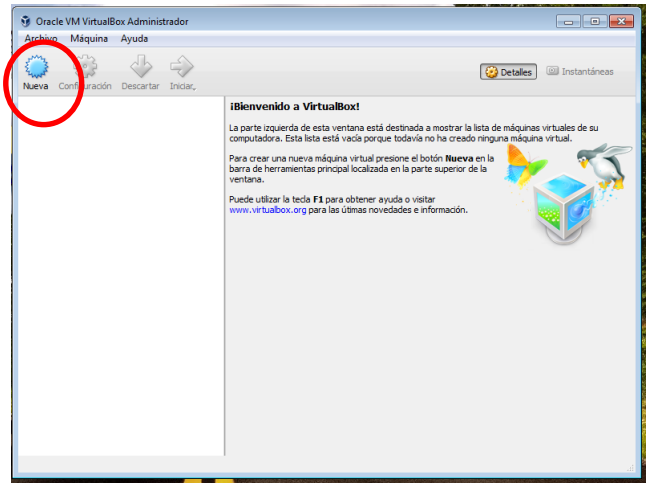
Ahora se va a descargar e instalar la versión de kali linux

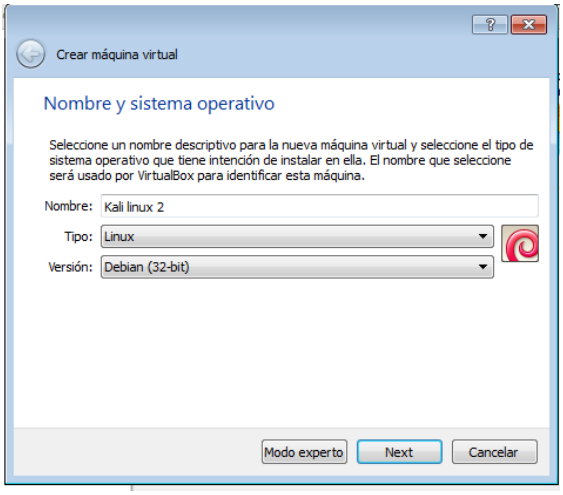
Ir a la página principal de KALI (http://www.backtrack-linux.org/) e ir a la pestaña de **DOWNLOADS.**

Kali Linux 64 bit	ISO	Torrent	3.1G	2.0	aaeb89a78f155377282f81a785aa1b38ee5f8ba0
Kali Linux 32 bit	ISO	Torrent	3.2G	2.0	6e5e6390b9d2f6a54bc980f50d6312d9c77bf30b
Kali Linux 64 bit Light	ISO	Torrent	0.8G	2.0	fc54f0b4b48ded247e5549d9dd9ee5f1465f24ab
Kali Linux 32 bit Light	ISO	Torrent	0.9G	2.0	bd9f8ee52e4d31fc2de0a77ddc239ea2ac813572
Kali Linux 64 bit mini	ISO	N/A	28M	2.0	5639928a1473b144d16d7ca3b9c71791925da23c

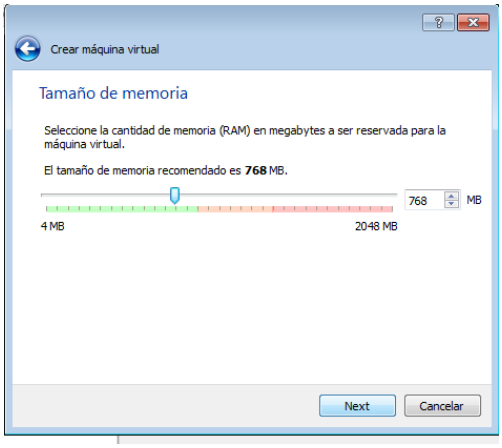
Aparece la última versión de Kali Linux para descargar en diferentes opciones según la necesidad del usuario y las características del equipo, en este caso se va a descargar kali Linux 32 bit con formato .ISO

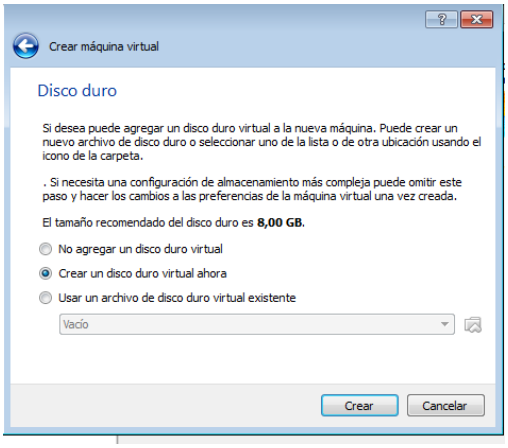
Cuando ya esté descargado, abrir el programa Virtualbox



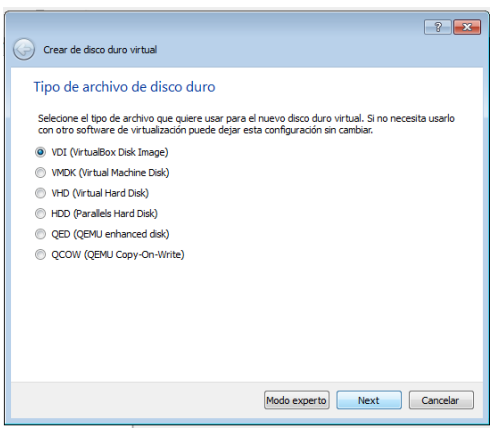


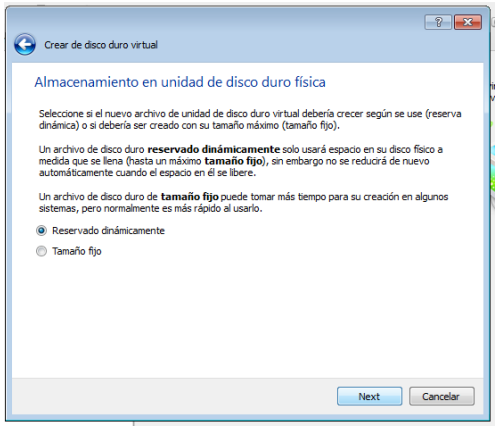
- Click en el icono que dice **Nueva.**
- Luego escoger el Nombre: Kali Linux 2, Tipo: Linux, Versión: Debian (32 bit), y click en **Next**.



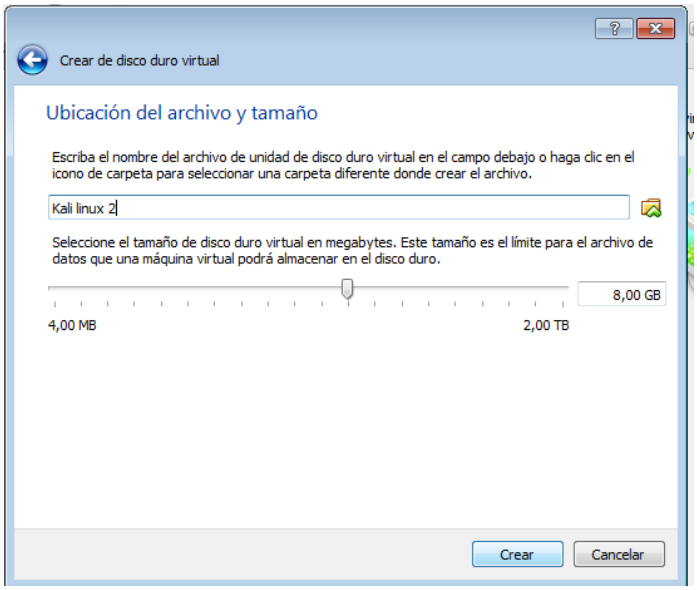


- Escoger el tamaño de la memoria, dejar el valor recomendado, y click en Next
- Crear un disco duro virtual con tamaño recomendado de 8GB, **Crear**.

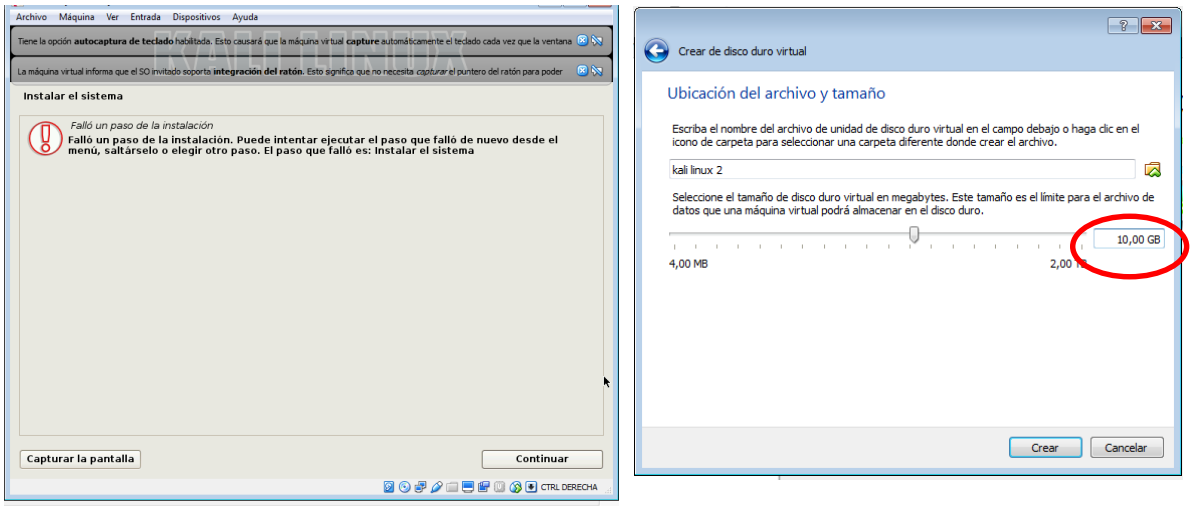




- Seleccionar el tipo de archivo de disco duro, por defecto se deja en VDI (Virtualbox Disk Image), **Next**.
- Almacenamiento en unidad de disco duro física, se deja la opción reservado dinámicamente, y **Next**.

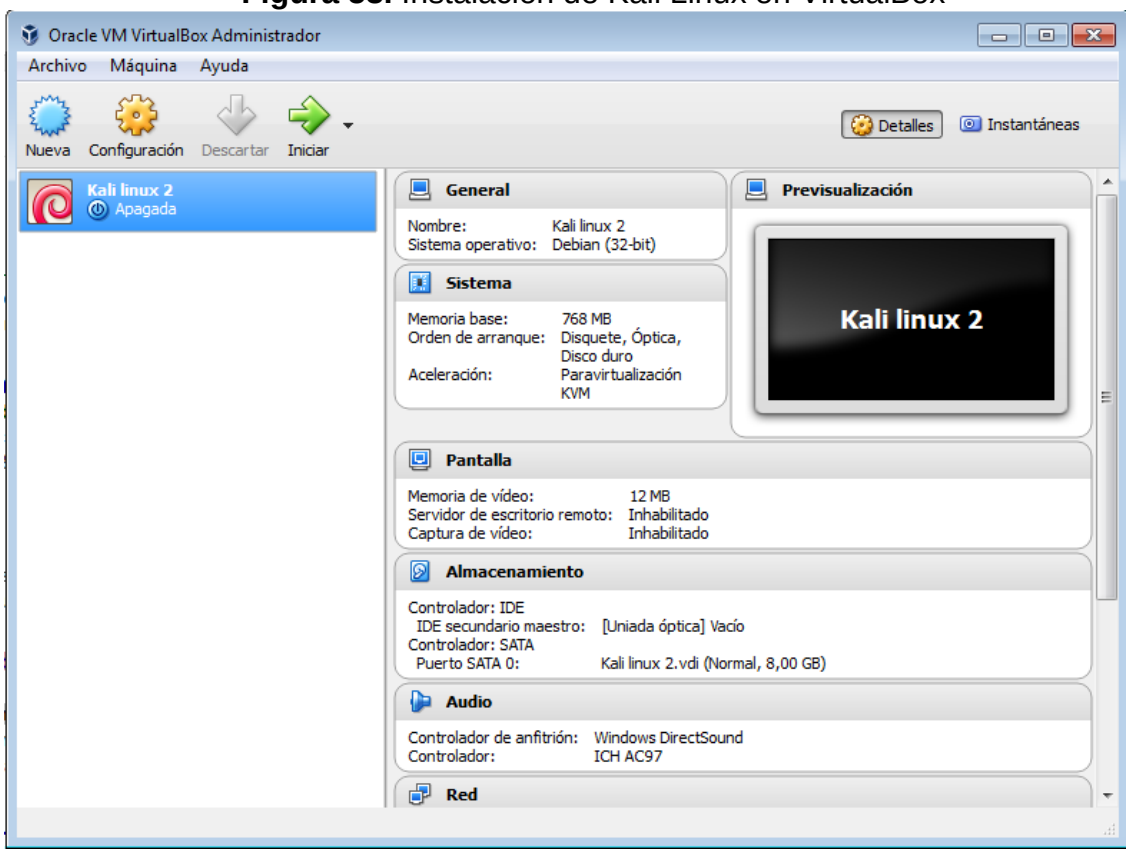


Seleccionar el nombre, ubicación del archivo y el tamaño del disco duro, por defecto se deja 8 GB, **Crear**. Pero a veces suele ocurrir el siguiente error. (Fallo un paso de la instalación)

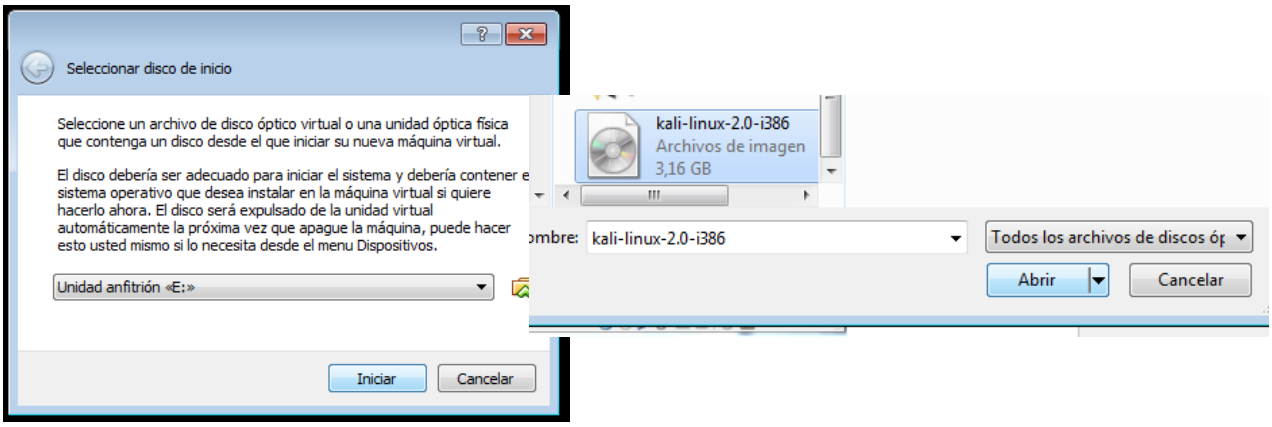


Entonces lo mejor es aumentarle un poco al tamaño del disco, como mínimo a 10 GB. **Crear**.

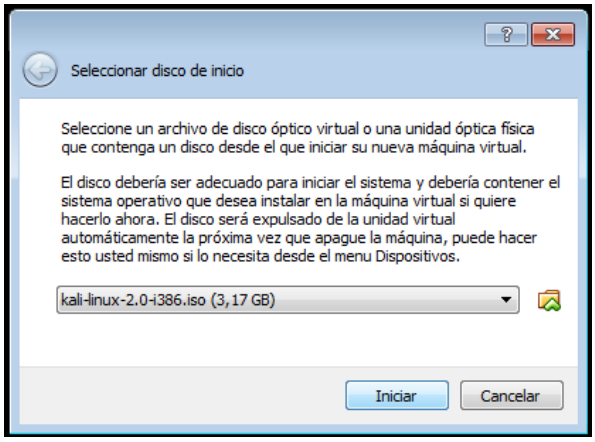
Figura 53. Instalación de Kali Linux en VirtualBox

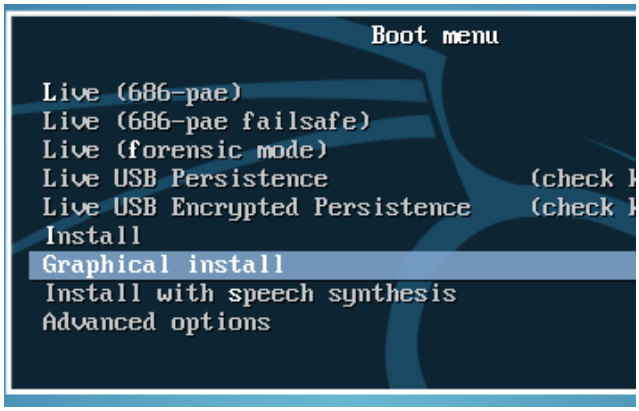


- Ahora dar click en el icono que dice **Iniciar**.



Aca se debe escoger el disco con el que se va a iniciar la máquina virtual, entonces dar Click a la carpeta de la derecha y buscar en donde esté guardado la imagen de kalilinux.iso y dar click en **abrir**.

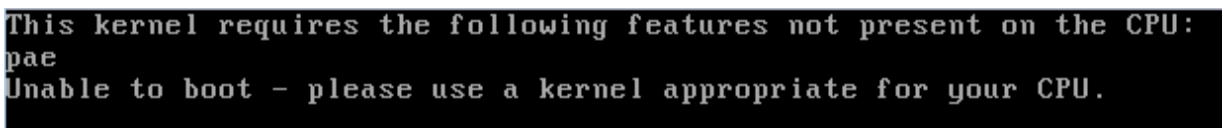


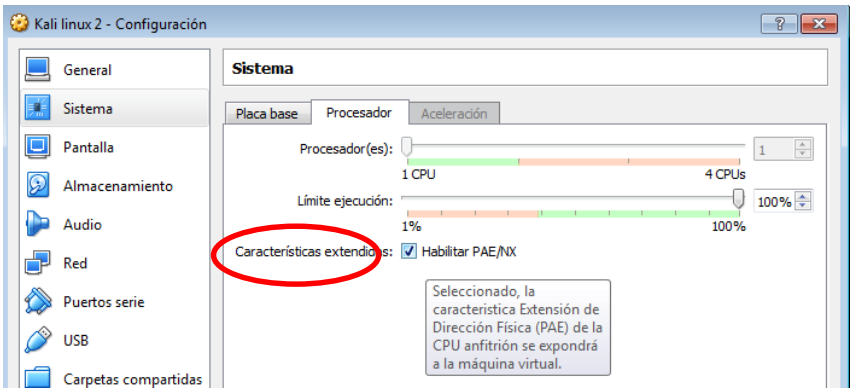


- Acá ya está seleccionado el disco kali Linux y dar click en **Iniciar.**
- Arranca la instalación de kali Linux, escoger la opción **Graphical Install.**

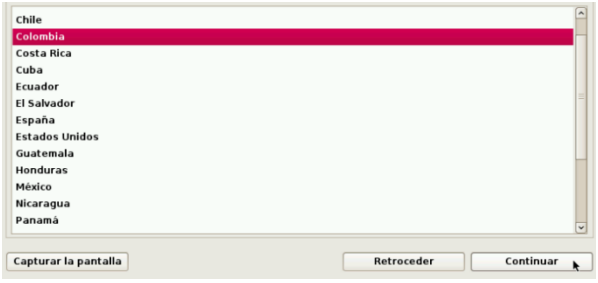
Si no lo desea instalar, puede usar la primera opción **Live (686-pae)** para trabajarlo directamente sin necesidad de instalarlo.

Si tiene inconvenientes a la hora de instalar por ejemplo que dice que el kernel no está presente en la CPU, entonces ir a la pestaña de Sistema, Procesador y marcar la casilla de **habilitar PAE/NX.**

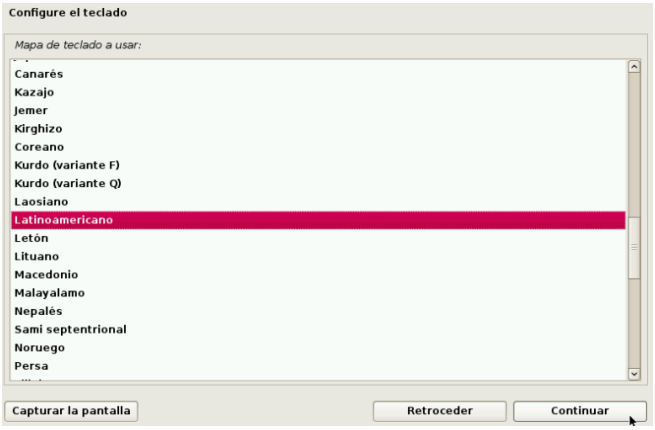


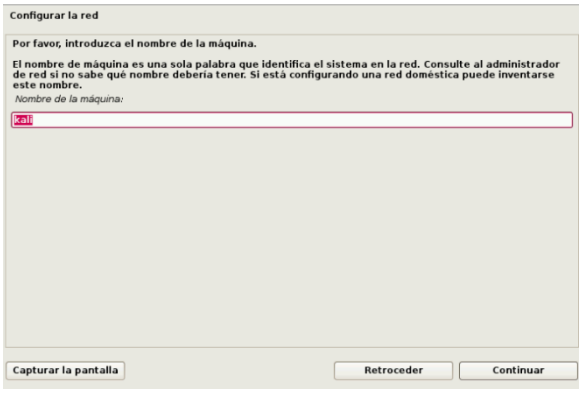


Entonces

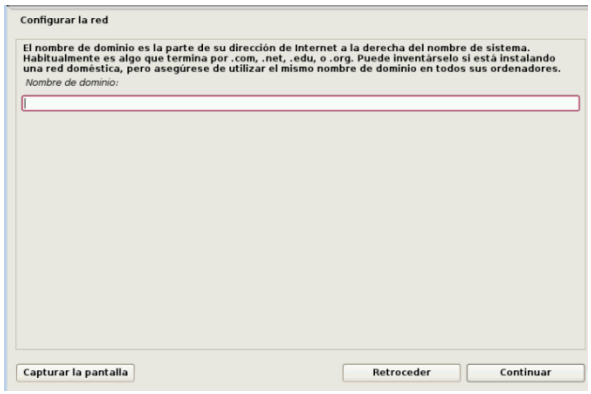


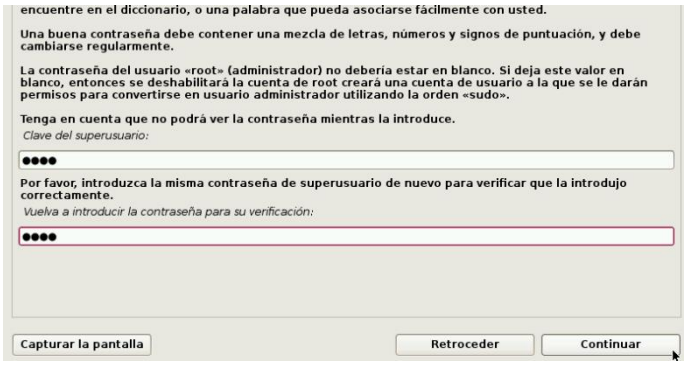
- Escoger el idioma: **Español** o según el que necesite el usuario y **Continue**.
- Escoger el país, territorio o Área: **Colombia** y **Continuar.**



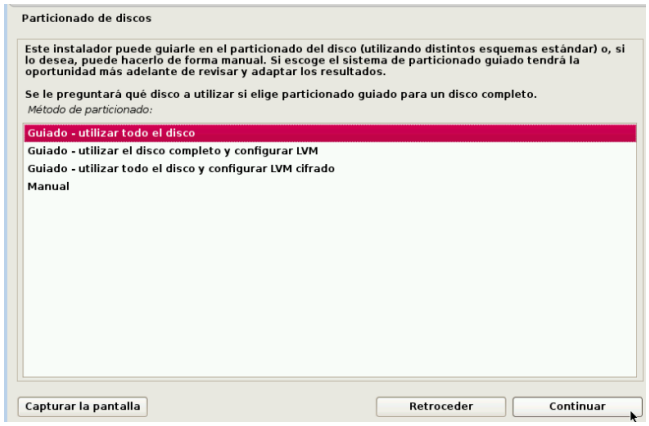


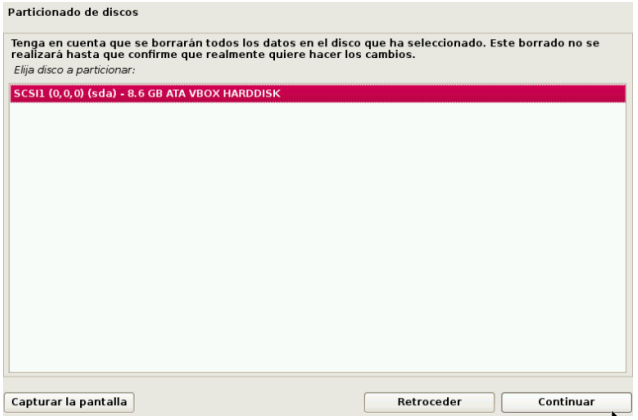
- Configurar el teclado: **Latinoamericano** y **Continuar**.
- Nombre de la maquina: **kali** y **Continuar**.



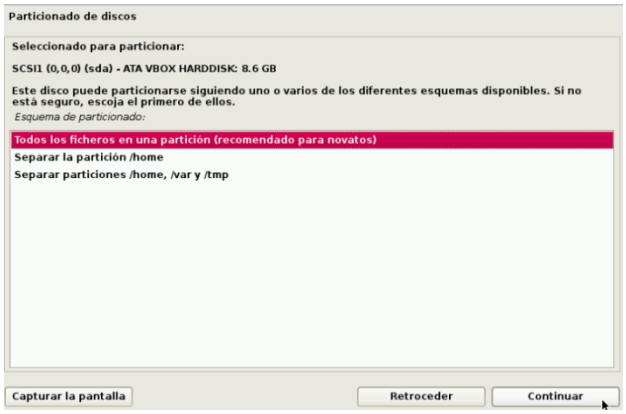


- Introducir el nombre de dominio: **kali,** si no conoce el nombre de dominio se puede dejar en blanco. **Continuar.**
- Clave de superusuario: en este caso es **toor**
- Volver a introducir la contraseña: **toor,** y **Continuar.**



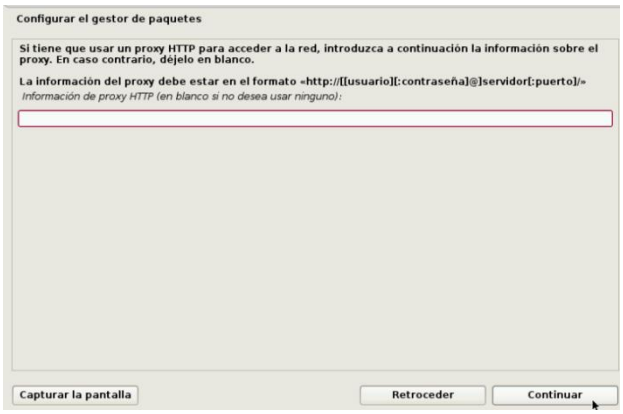


- Método de partición de discos: **Guiado – Utilizar todo el disco, Continuar.**
- Elegir el disco a particionar, **Continuar.**

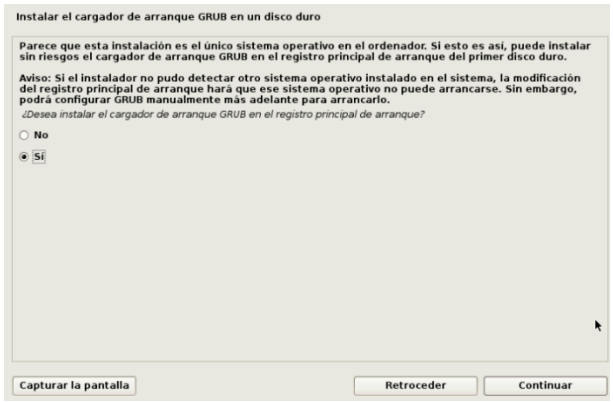


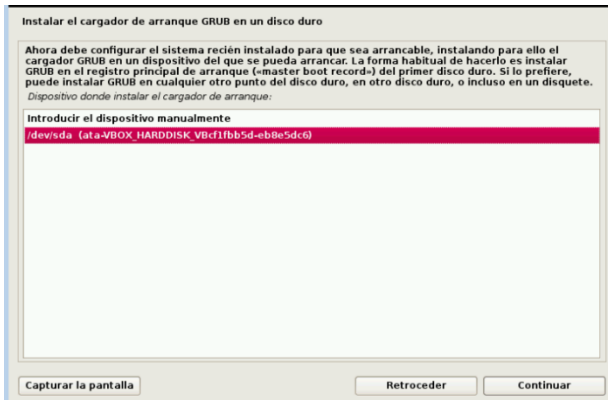
- Esquema de particionado: **Todos los ficheros en una partición (recomendada), Continuar.**

- Resumen de las particiones: **Finalizar el particionado y escribir los cambios en el disco, Continuar.**

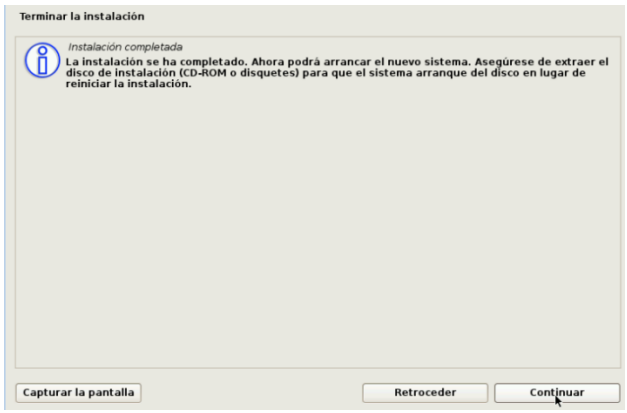


- Desea escribir los cambios en el disco: **Si, Continuar.**
- Si tiene que usar una proxy HTTP para acceder a la red: Se deja en blanco, **Continuar**.

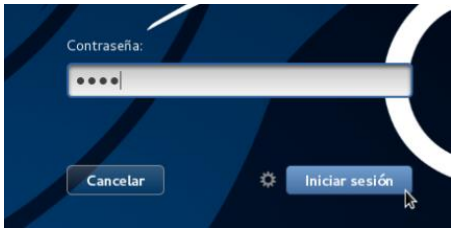




- Instalar el cargador de arranque GRUB en el registro principal de arranque?: **Si, Continuar.**
- Dispositivo donde instalar el cargador de arranque: **/dev/sda …., Continuar.**



- Instalación completada: **Continuar.**
- Nombre de usuario: **root** y **Siguiente.**



- Contraseña: **toor** e **Iniciar sesión**.
- Sesión iniciada de Kali Linux versión 2.

3. Instalación de programas en kali Linux.

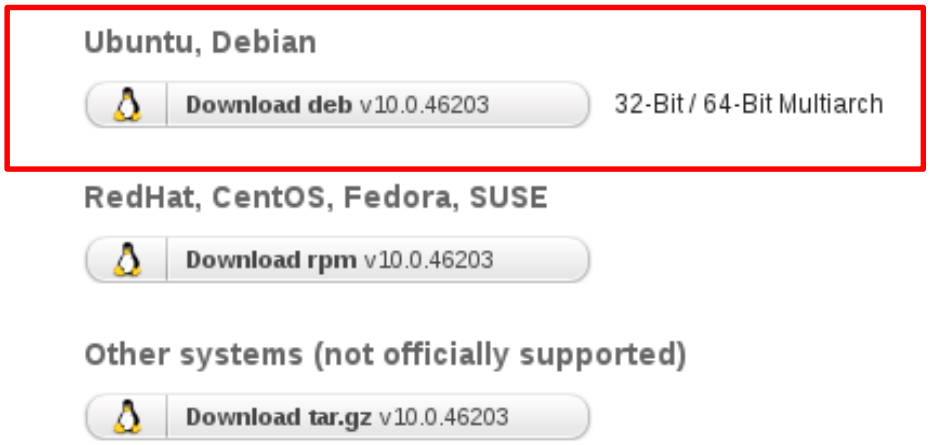
Instalar archivos con extensión .deb

Por ejemplo se va a instalar el programa Teamviewer.

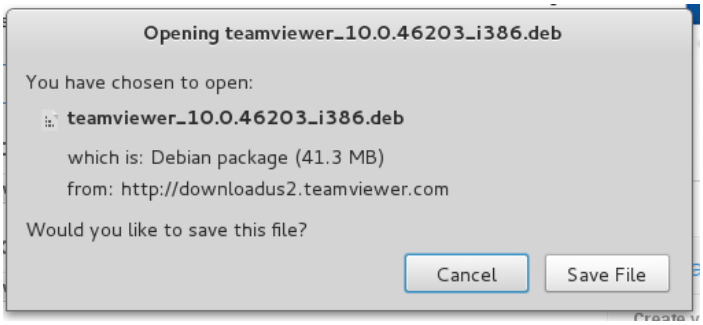
Abrir el explorador de internet y buscar la dirección del programa Teamviewer.

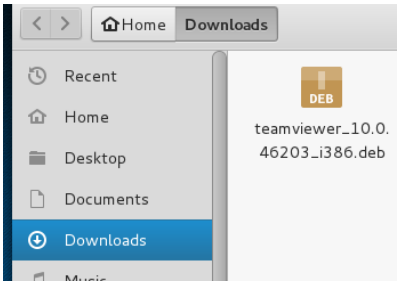
www.teamviewer.com

Dar click en descargas y aparecerán 3 opciones de descarga según el sistema operativo, en este caso escoger la descarga del sistema operativo **Ubuntu, Debian**.



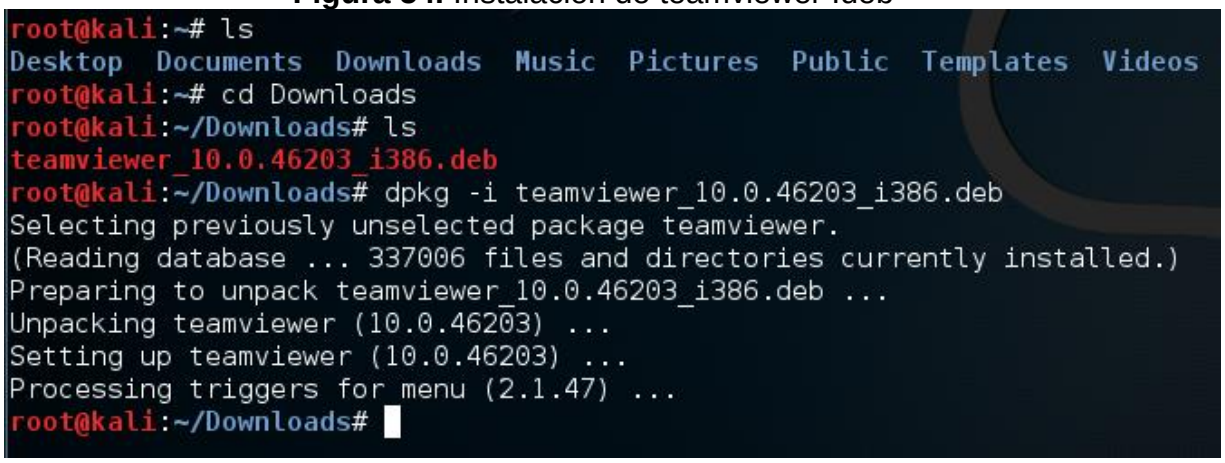
- Luego guardar el archivo (**Save File**)





Por defecto queda guardado en la carpeta de descargas (**Downloads**)
Para instalar este programa primero se debe abrir la terminal e ir al directorio en donde se descargó el programa y ejecutarlo con el comando:
dpkg -i nombredelprograma.deb

Figura 54. Instalación de teamviewer .deb

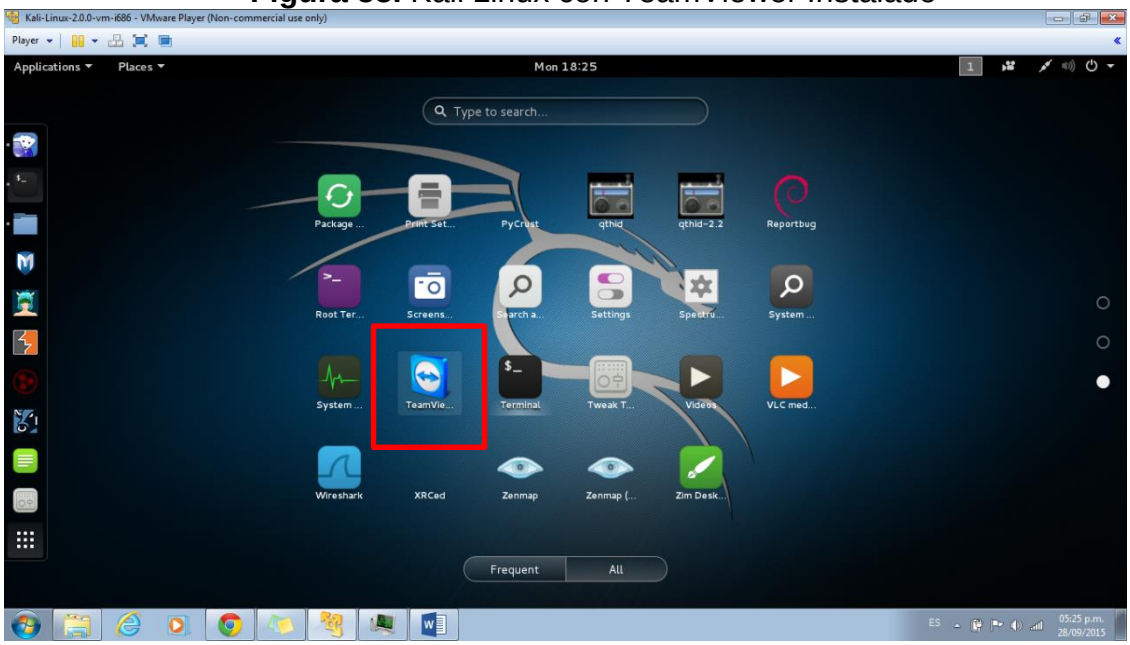


En la figura anterior están los pasos que se requieren para instalar el programa **.deb**

- Primero ir a la carpeta en donde se descargó el programa: **cd Downloads**
- Luego si quiere saber qué archivos están en esa carpeta escribir el comando **ls**.
- Ahora para instalar escribir **dpkg –i teamviewer_10.0.46203_i386.deb**

Para agilizar un poco, como el nombre del archivo es un poco largo podemos escribir **dpkg –i te** y le damos la tecla **Tab** y nos completará el nombre del archivo.

Figura 55. Kali Linux con TeamViewer Instalado

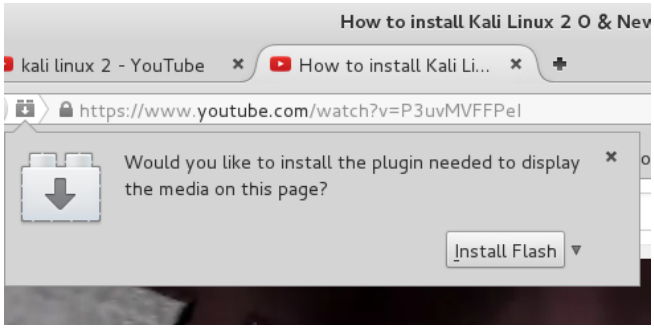


Luego en el menú se puede observar que el programa fue instalado.

Instalar Archivo con extensión .tar.gz (Adobe Flash Player)

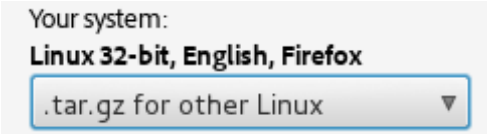
Para reproducir algunos archivos por ejemplo en www.youtube.com se necesita instalar el Adobe flash Player,

Al reproducir un video nos recomiendan instalar el plugin el cual es el Adobe Flash Player.



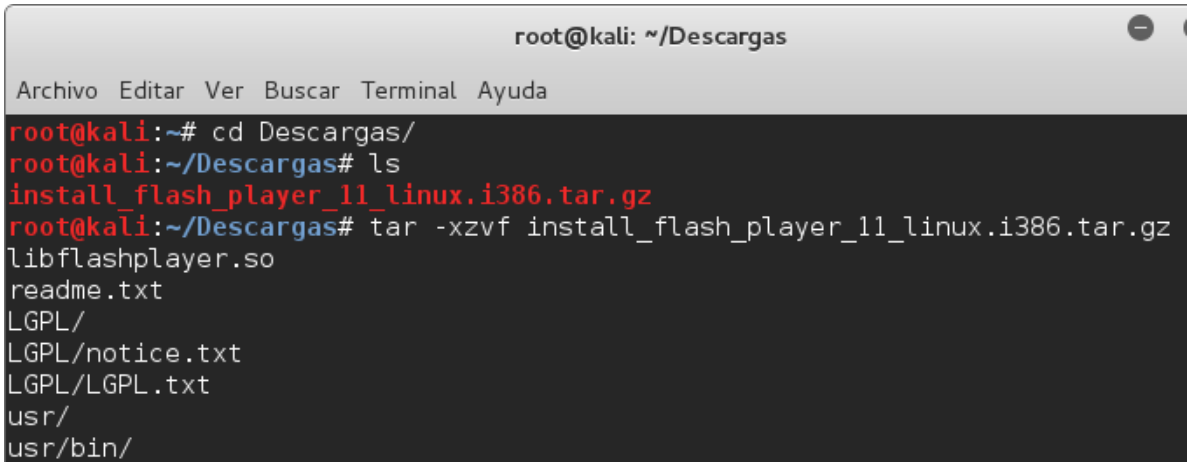
Los pasos a seguir son:
Ir a la página principal de Adobe Flash Player, descargar y guardar la versión para Linux con el formato *.tar.gz*, luego abrir la terminal e ir a la carpeta de descargas y ejecutar los comandos para ejecutar e instalar el archivo.

1. Página para descargar Adobe Flash Player: https://get.adobe.com/flashplayer/
2. Escoger la versión y descargarla: **.tar.gz for other Linux**



3. Abrir la terminal e ir a la carpeta en donde se guardó el archivo, en este caso la carpeta de **Descargas**.
   - Escribir: **cd Descargas**
   - Luego escribir **ls** para comprobar que el archivo se encuentra en esta carpeta.
   - Para descomprimir el archivo escribir el comando:

   tar -xzvf install_flash_player_11_linux.i386.tar.gz (Se empieza a descomprimir el archivo).



Luego se copia el archivo **libflashplayer.so** a la carpeta donde se encuentran los plugings, escribir:

- cp libflashplayer.so /usr/lib/mozilla/plugins/

Si se tiene abierto el explorador de internet, hay que cerrarlo y abrirlo nuevamente para comprobar que el programa fue instalado correctamente, también se puede encontrar en el menú de los programas.

TRABAJO

1. Instalar algún programa en Linux y documentarlo.
Por ejemplo SKYPE tiene extensión .deb

2. ¿Qué diferencia hay al instalar un programa .tar.gz y tar.bz2 ?

4.1.6 GUÍA N°6 INTRODUCCIÓN A UN HACKING ÉTICO FASE 1

GUÍA N°6
INTRODUCCIÓN A UN HACKING ÉTICO

FASE 1

OBJETIVOS

- Conocer las diferencias entre en hacking ético y no ético.
- Conocer los principales programas de reconocimiento de red.
- Investigar datos de la red.

REQUISITOS

- Manejo básico de programación de red.
- Conocimiento de comandos básicos para el terminal de Linux.

INTRODUCCIÓN

En esta guía se conocerá la primera fase (Reconocimiento) que realiza un hacking ético, el cual consiste en investigar información del cliente, esto se realizará con un programa llamado ***Maltego*** el cual se encuentra en los programas de Kali Linux, este programa nos puede dar información como dominios de la paginas e Ips utilizados.
Por medio del comando ***whois*** se podrá consultar información acerca del cliente a investigar.

MARCO TEÓRICO

Introducción al Hacking ético
Cuando hablamos de hacking ético nos referimos a la acción de efectuar pruebas de intrusión *controladas* sobre sistemas informáticos; es decir que el consultor o pentester, actuará desde el punto de vista de un cracker*,* para tratar de encontrar vulnerabilidades en los equipos auditados que puedan ser explotadas, brindándole - en algunos casos - acceso al sistema afectado inclusive; pero siempre en un ambiente supervisado, en el que no se ponga en riesgo la operatividad de los servicios informáticos de la organización cliente.

Es importante enfatizar que aunque es indudable que el pentester debe poseer conocimientos sólidos sobre tecnología para poder efectuar un hacking ético, saber de informática no es suficiente para ejecutar con éxito una auditoría de este tipo. Se requiere además seguir una metodología que permita llevar un orden en nuestro trabajo para optimizar el tiempo en la fase de explotación, además de aplicar el sentido común y experiencia.

Fases del hacking

Tanto el auditor como el cracker siguen un orden lógico de pasos al momento de ejecutar un hacking, a estos pasos agrupados se los denomina fases.

Existe un consenso generalizado entre las entidades y profesionales de seguridad informática de que dichas fases son 5 en el siguiente orden:

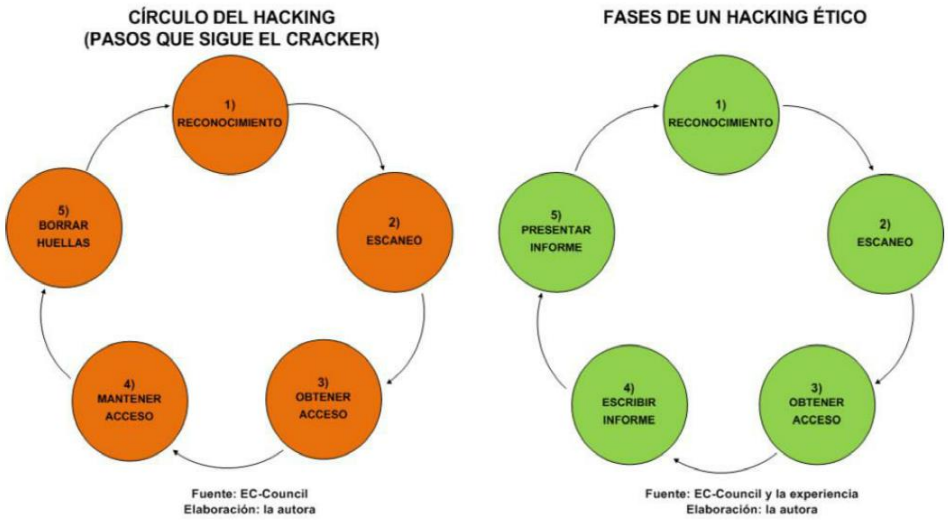
1. Reconocimiento
2. Escaneo
3. Obtener acceso
4. Mantener acceso
5. Borrar huellas

Usualmente dichas fases se representan como un ciclo al que se denomina comúnmente *círculo del hacking* (ver Figura 1) con el ánimo de enfatizar que el cracker luego de borrar sus huellas puede afectar el sistema, el auditor de seguridad informática que ejecuta un servicio de hacking ético presenta una leve variación en la ejecución de las fases de esta forma:

1. Reconocimiento
2. Escaneo
3. Obtener acceso
4. Escribir Informe
5. Presentar Informe

De esta manera el hacker ético se detiene en la fase 3 del círculo del hacking para reportar sus hallazgos y realizar recomendaciones de remediación al cliente.

Figura 56. Fases del Hacking



En este laboratorio se hará la fase 1 la cual consisten en hacer reconocimiento a determinado cliente o red.

FASE 1

El *reconocimiento o footprinting*, es la primera fase en la ejecución de un hacking ético o no-ético y consiste en descubrir la mayor cantidad de información relevante de la organización cliente o víctima.

Reconocimiento pasivo

Cuando no se tiene una interacción directa con el cliente o víctima.

Por ejemplo, entramos a un buscador como Google e indagamos por el nombre de la empresa auditada, entre los resultados conseguimos el nombre de la página web del cliente y descubrimos que el nombre del servidor web, luego hacemos una búsqueda DNS y se obtiene la dirección IP de ese servidor.

También se puede buscar información del cliente o en empresa por medio de las redes sociales como Facebook, twitter, linkedin, entre otros.

Reconocimiento activo

En este tipo de reconocimiento hay una interacción directa con el objetivo o víctima.

Ejemplos de reconocimiento activo:

- ***Barridos de ping*** para determinar los equipos públicos activos dentro de un rango de IP's.

- ***Conexión a un puerto de un aplicativo*** para obtener un *banner* y tratar de determinar la versión.
- ***Uso de ingeniería social*** para obtener información confidencial.
- ***Hacer un mapeo de red*** para determinar la existencia de un firewall o router de borde.

Nota: Un hacker ético jamás realiza pruebas de intrusión sobre sistemas, a menos que haya obtenido autorización de la organización propietaria de los mismos.

Who-Is

El *Who-Is* es un protocolo que permite hacer consultas a un repositorio en Internet para recuperar información acerca de la propiedad de un nombre de dominio o una dirección IP.

Cuando una organización solicita un nombre para su dominio a su proveedor de Internet (ISP), éste lo registra en la base *Who-Is* correspondiente.

En el caso de los dominios de alto nivel (.com, .org, .net, .biz, .mil, etc.) es usualmente el *ARIN* (*American Registry for Internet Numbers*) quien guarda esta información en su base *Who-Is*; pero en el caso de los dominios de países (.ve, .ec, .co, .us, .uk, etc.) quien guarda la información normalmente es el NIC (Network Information Center) del país respectivo.

Se puede consultar tanto de la página de internet o por medio del comando.

Nota: Es importante recalcar que podemos efectuar consultas Who-Is sin solicitar autorización, debido a que se trata de información que se encuentra en una base de datos pública.

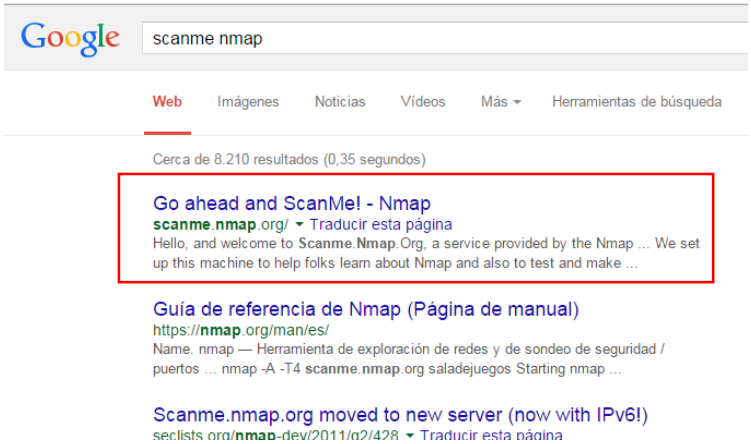
PROCEDIMIENTO

FASE 1 ESCANEO
google, nslookup whois. Aplicativo como maltego

Google

Buscar por el nombre de la empresa víctima, la cual será por ahora el proyecto *Scanme* de *Nmap.* (Se escoge esta victima ya que está autorizado a realizar pruebas de reconocimiento y escaneo solamente).

Abrir google y buscar “scanme nmap”

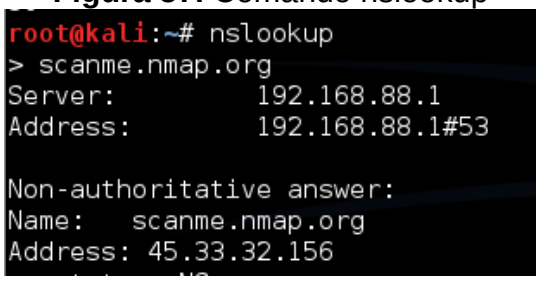


Arroja cerca de 8.210 resultados relacionadas con la organización *NMAP*, pero, la que interesa es ***scanme.nmap.org.***
Luego se realizará la resolución de nombres DNS.

nslookup
Este comando se utiliza para hacer consulta de nombres.

Abrir la terminal de Kali-Linux y escribir:
nslookup
scanme.nmap.org

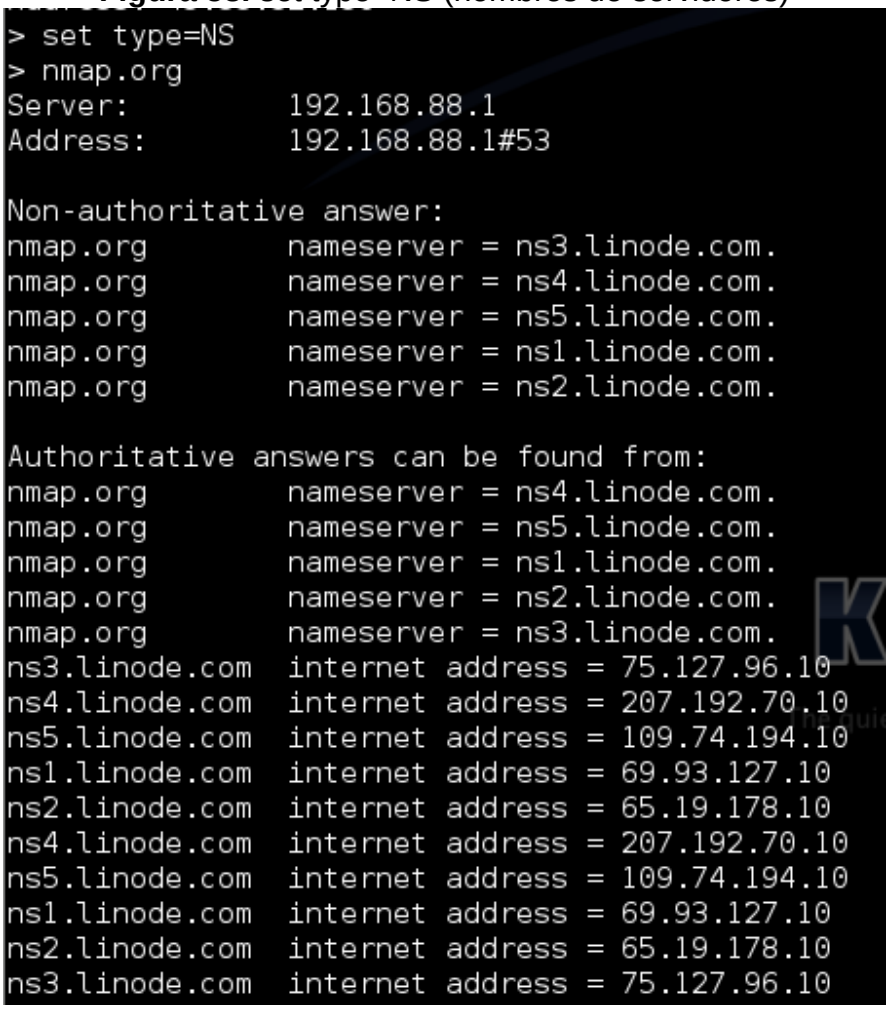
Figura 57. Comando nslookup



El resultado es una dirección Ipv4 (45.33.32.156)

Ahora se realizará 2 tipos de consultas, el servicio de nombres NS y el servicio de correo MX para el dominio de nuestro objetivo, en este caso ***nmap.org***.
set type = [NS | MX]
Escriba:
set type=NS
nmap.org

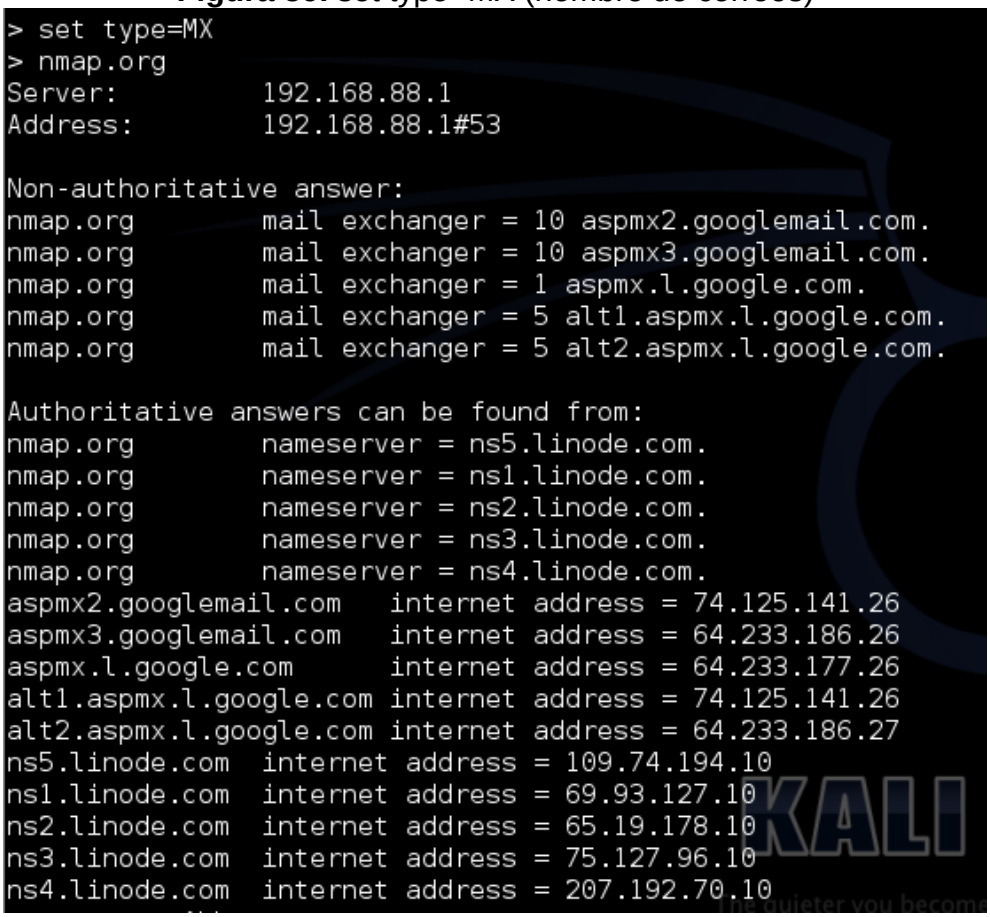
Figura 58. set type=NS (nombres de servidores)



En la Figura se observa que al establecer el tipo de consulta como NS, nos devuelve información respecto a los servidores de nombres para el dominio en que se encuentra nuestro objetivo.

Escriba:
set type=MX
nmap.org

Figura 59. set type=MX (nombre de correos)



La figura muestra la consulta tipo MX (mail exchanger), brinda además información acerca de quiénes son los servidores de correo para dicho dominio. Estas simples consultas adicionales nos reportan valiosa información de la red pública de nuestro objetivo, como por ejemplo:

1. Que en realidad el dominio *nmap.org* está alojado en un servidor de *hosting* externo provisto por la empresa *Linode.*
2. Que el servicio de correo es provisto por el servidor es *googlemail.com* con IP diferente a la del servidor *scanme.nmap.org*.

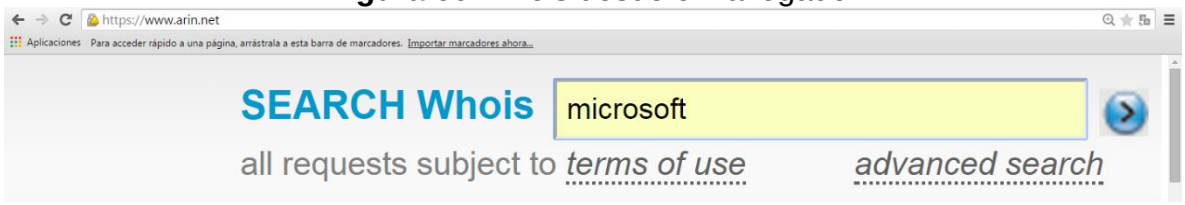
Whois

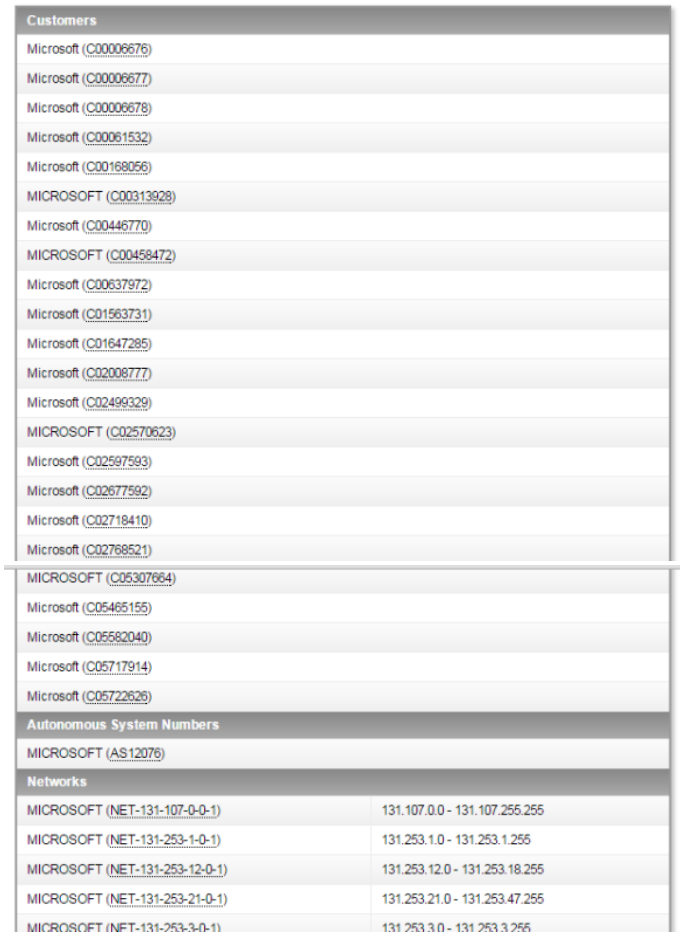
Por ejemplo se va a consultar sobre la empresa Microsoft, como su dominio es microsoft.com entonces se puede acudir al ARIN para nuestra consulta.

En internet podemos consultar páginas como http://whois.arin.net y https://www.whois.net/ entre otras.

Para ello apuntamos nuestro navegador a **http://whois.arin.net** y en la caja de texto denominada “SEARCH WHOISRWS” ingresamos el nombre de la organización, para este ejemplo: *Microsoft*

Figura 60. whois desde el navegador





Customers	
Microsoft (C00006676)	
Microsoft (C00006677)	
Microsoft (C00006678)	
Microsoft (C00061532)	
Microsoft (C00168056)	
MICROSOFT (C00313928)	
Microsoft (C00446770)	
MICROSOFT (C00458472)	
Microsoft (C00637972)	
Microsoft (C01563731)	
Microsoft (C01647285)	
Microsoft (C02008777)	
Microsoft (C02499329)	
MICROSOFT (C02570623)	
Microsoft (C02597593)	
Microsoft (C02677592)	
Microsoft (C02718410)	
Microsoft (C02768521)	
MICROSOFT (C05307664)	
Microsoft (C05465155)	
Microsoft (C05582040)	
Microsoft (C05717914)	
Microsoft (C05722626)	
Autonomous System Numbers	
MICROSOFT (AS12076)	
Networks	
MICROSOFT (NET-131-107-0-0-1)	131.107.0.0 - 131.107.255.255
MICROSOFT (NET-131-253-1-0-1)	131.253.1.0 - 131.253.1.255
MICROSOFT (NET-131-253-12-0-1)	131.253.12.0 - 131.253.18.255
MICROSOFT (NET-131-253-21-0-1)	131.253.21.0 - 131.253.47.255
MICROSOFT (NET-131-253-3-0-1)	131.253.3.0 - 131.253.3.255

Nos arroja resultados acerca de las redes, números de sistemas autónomos y clientes.

Si abrimos la primera red nos dará más información.

Figura 61. Información de Microsoft con whois

Network	
Net Range	131.107.0.0 - 131.107.255.255
CIDR	131.107.0.0/16
Name	MICROSOFT
Handle	NET-131-107-0-0-1
Parent	NET131 (NET-131-0-0-0-0)
Net Type	Direct Assignment
Origin AS	
Organization	Microsoft Corporation (MSFT)
Registration Date	1988-11-11
Last Updated	2013-08-20
Comments	
RESTful Link	http://whois.arin.net/rest/net/NET-131-107-0-0-1
See Also	Related POC records.
See Also	Related organization's POC records.
See Also	Related delegations.

Como por ejemplo el rango de direcciones Ips, el día de registros, país, entre otros.

Ahora utilizando la otra página de internet: https://www.whois.net/

Figura 62. Utilizando whois para información de Microsoft

También nos arroja información del dominio, ciudad, código postal, nombre del administrador, teléfono, etc.

Utilizando el comando whois
Para saber la dirección Ip de una página se tiene que hacer una conexión mediante el comando ping.

Escriba:
ping www.microsoft.com

```
root@kali:~# ping www.microsoft.com
PING e10088.dspb.akamaiedge.net (23.218.210.155) 56(84) bytes of data.
^Z
[1]+  Detenido                ping www.microsoft.com
```

Después de obtener la dirección Ip detenga el escaneo de ping.

Escriba:
whois 23.218.210.155

Figura 63. Comando whois a dirección IP

```
root@kali:~# whois 23.218.210.155

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# http://www.arin.net/public/whoisinaccuracy/index.xhtml
#


#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=23.218.210.155?showDetails=true&showARIN=false&sho
#

NetRange:       23.192.0.0 - 23.223.255.255
CIDR:           23.192.0.0/11
NetName:        AKAMAI
NetHandle:      NET-23-192-0-0-1
Parent:         NET23 (NET-23-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Akamai Technologies, Inc. (AKAMAI)
RegDate:        2013-07-12
Updated:        2013-08-09
Ref:            http://whois.arin.net/rest/net/NET-23-192-0-0-1


OrgName:        Akamai Technologies, Inc.
OrgId:          AKAMAI
Address:        8 Cambridge Center
City:           Cambridge
StateProv:      MA
PostalCode:     02142
Country:        US
RegDate:        1999-01-21
Updated:        2014-03-19
Ref:            http://whois.arin.net/rest/org/AKAMAI
```

Da como resultado nombre de la red, días de registros, direcciones, código postal, ciudad, país, entre otros.

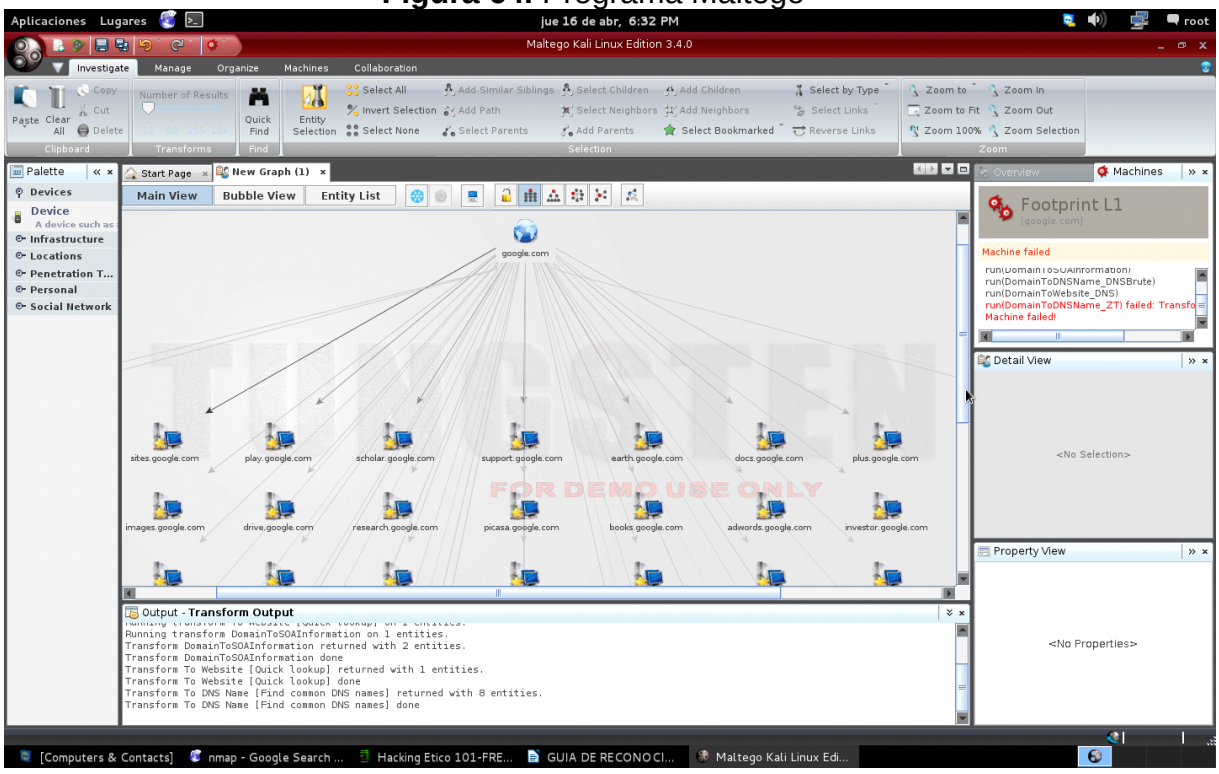
Programa maltego

Aplicaciones --> Kali Linux --> Recopilación de información --> Analisis DNS --> Maltego
Aplicaciones --> Kali Linux --> Top 10 security tools --> Maltego
Cuando se inicia, toca registrarse para poder usar este programa.

Luego agregamos un dominio, en este caso es google.com

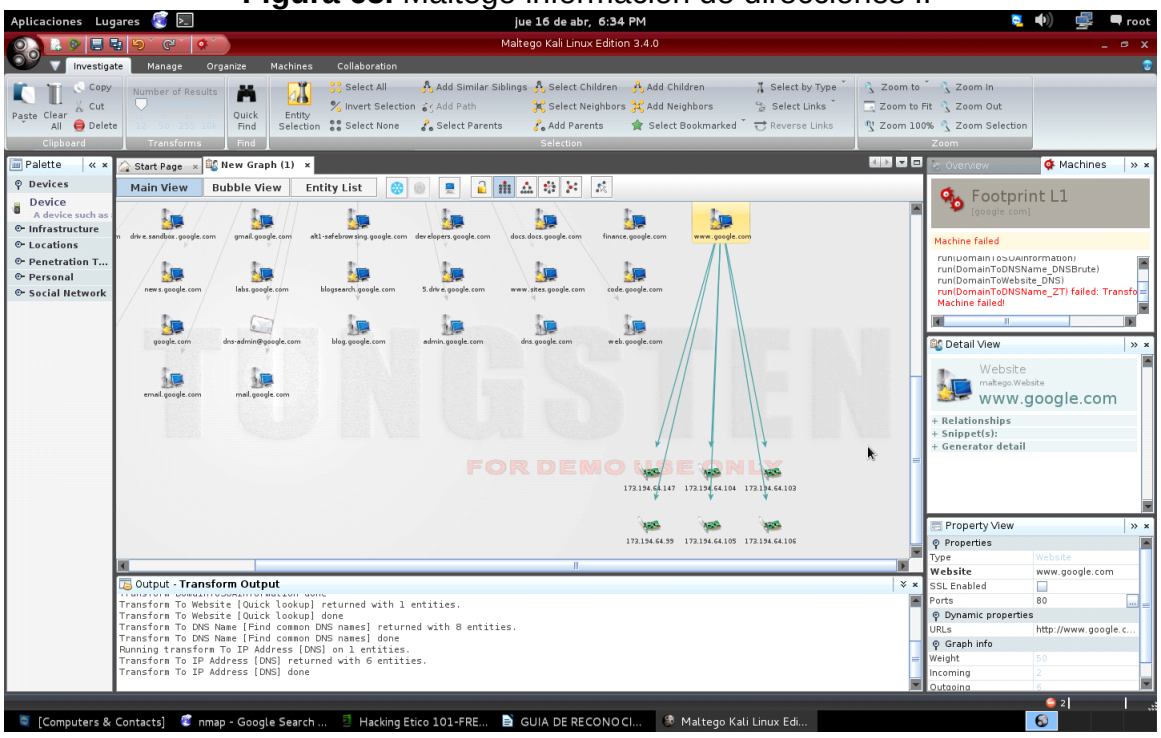
Nos arroja varios resultados, como por ejemplo picasa.google.com, earth.google.com, docs.google.com, play.google.com, etc.
Y así sucesivamente podemos trabajar con uno de estos subdominios.

Figura 64. Programa Maltego



Trabajaremos con www.google.com y nos da como resultado varias direcciones de dominios por ejemplo la 173.194.64.147, 173.194.64.103, 173.194.64.104.

Figura 65. Maltego información de direcciones IP



Estos resultados también los podemos ver en forma gráfica de burbujas (Bubble View) o en una lista (Entity list).

Figura 66. Maltego en forma gráfica de burbujas

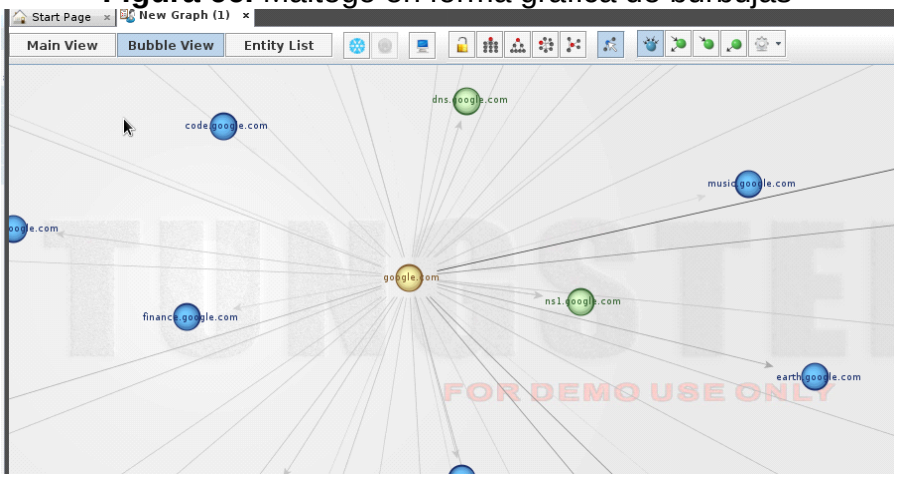
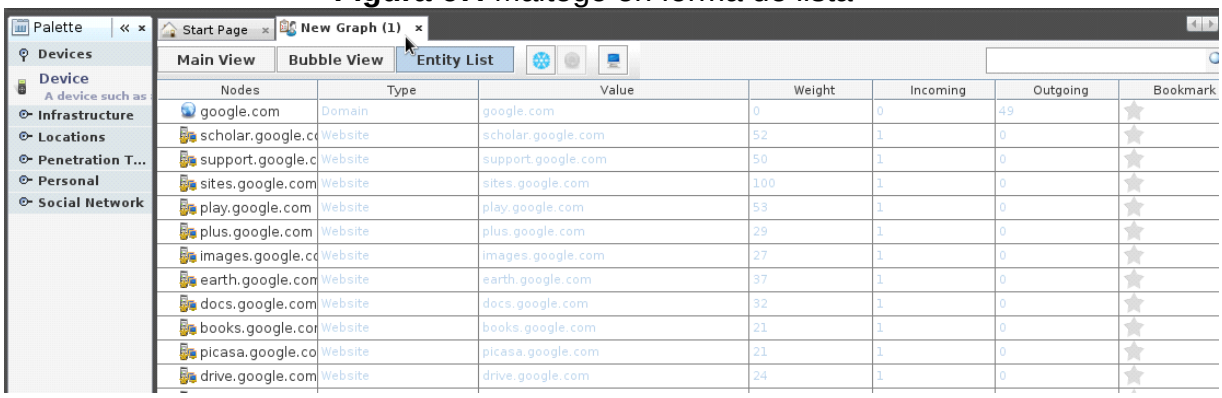


Figura 67. Maltego en forma de lista



Metagoofil [26]

Metagoofil es una herramienta diseñada para capturar información mediante la extracción de metadatos desde documentos públicos (pdf, doc, xls, ppt, odp, ods, docx, pptx, xlsx) correspondientes a la empresa objetivo.

Abrir la terminal y escribir: metagoofil

Figura 68. metagoofil

```
root@kali:~# metagoofil

*********************************************************
*      /\/\   ___| |_ __ _  __ _  ___   ___  / _(_) | *
*     /    \ / _ \ __/ _` |/ _` |/ _ \ / _ \| |_| | | *
*    / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | | *
*    \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_| *
*                             |___/                     *
* Metagoofil Ver 2.2                                    *
* Christian Martorella                                  *
* Edge-Security.com                                     *
* cmartorella_at_edge-security.com                      *
*********************************************************

 Usage: metagoofil options

        -d: domain to search
        -t: filetype to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
        -l: limit of results to search (default 200)
        -h: work with documents in directory (use "yes" for local analysis)
        -n: limit of files to download
        -o: working directory (location to save downloaded files)
        -f: output file

 Examples:
  metagoofil.py -d apple.com -t doc,pdf -l 200 -n 50 -o applefiles -f results.ht
ml
  metagoofil.py -h yes -o applefiles -f results.html (local dir analysis)
```

[26] CABALLERO, Alonso, Hacking con Kali Linux, 2015, http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

La opción “-d” define el dominio a buscar. La opción “-t” define el tipo de archivo a descargar (pdf, doc, xls, ppt, odp, ods, docx, pptx, xlsx) La opción “-l” limita los resultados de búsqueda (por defecto a 200). La opción “-n” limita los archivos a descargar. La opción “-o” define un directorio de trabajo (La ubicación para guardar los archivos descargados). La opción “-f” define un archivo de salida

Escribir:

metagoofil -d nmap.org -t pdf -l 200 -n 10 -o /tmp/ -f /tmp/resultados_mgf.html

Figura 69. metagoofil (extraer información de formato pdf)

Figura 70. metagoofil (usuarios, software y correos encontrados)

El resultado son 41 archivos en formato pdf encontrados y 10 archivos en formato pdf descargados.
También da una lista de 5 usuarios, lista de software encontrado en la cual aparecen diferentes versiones de lectores de pdf y por último da una lista de correos encontrados.

Taller

Realizar un reconocimiento de determinada empresa o página, para investigar todo la información posible de este cliente. Usando los programas o comandos explicados anteriormente.

4.1.7 GUÍA N°7 INTRODUCCIÓN A UN HACKING ÉTICO FASE 2

GUÍA N°7
INTRODUCCIÓN A UN HACKING ÉTICO
FASE 2

OBJETIVOS

- Conocer los principales programas de escaneo de red.
- Investigar datos de la red, como por ejemplo puertos abiertos, IP, sistema operativo.

REQUISITOS

- Manejo básico de programación de red.
- Conocimiento de comandos básicos para el terminal de Linux.

INTRODUCCIÓN

En esta guía se conocerá segunda fase (Escaneo) que realiza un hacking ético, el cual consiste en escanear la red la cual se puede hacer mediante el comando ***nmap***, el cual se ejecuta en la terminal, se puede explorar la de red e investigar los puertos abiertos, direcciones Ips, sistemas operativos de los computadores en la red, entre otros.

MARCO TEÓRICO

Escáner de puertos: NMAP

Algunas de las opciones más utilizadas de NMAP:
Sintaxis: nmap [tipo(s)_de_escaneo] [opciones] {red|host_objetivo}

Modos de escaneos permitidos por *nmap*
-sn : ping scan
-sS : syn/half scan
-sT : tcp/connect scan
-sA : ack scan
-sN : null scan
-sU : udp scan

-sF : fin scan
-sX : xmas scan
-sV : detección de versión de servicios
-O : detección de sistema operativo
-T<0-5>: temporizador, el valor más alto es más rápido
-v : salida detallada

Nmap[27] ("Network Mapper") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Fue diseñado para escanear rápidamente pequeñas y grandes redes. Nmap utiliza paquetes IP en bruto en formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y versión) estos equipos ofrecen, qué sistemas operativos (y versiones del sistema operativo) que se están ejecutando, qué tipo de filtros de paquetes / cortafuegos están en uso, y docenas de otras características. Mientras Nmap es comúnmente utilizado para las auditorías de seguridad, muchos sistemas y administradores de red resulta útil para tareas de rutina, tales como inventario de red, gestión de horarios de servicios de actualización y supervisión de host o tiempo de servicio.

Características

1. ¿Qué equipos se ejecutan en la red local?
2. ¿Qué direcciones IP se ejecutan en la red local?
3. ¿Cuál es el sistema operativo de su equipo de destino?
4. Para saber qué puertos están abiertos en la máquina que usted acaba de escanear?
5. Averigüe si el sistema está infectado con malware o virus.
6. Búsqueda de servidores no autorizados o servicios de red en la red.
7. Buscar y quitar los equipos que no cumplen con el nivel mínimo de la organización de la seguridad.

Con nmap -h podremos ver sus posibles opciones las cuales se dividen por ejemplo en descubrir host, escanear puertos, detectar servicios o versiones, detectar sistemas operativos, entre otros.

[27] ADMIN, Tutorial nmap para Kali Linux, 2013, http://kalilinux.foroactivo.com/t12-tutorial-nmap-para-kali-linux

PROCEDIMIENTO

FASE 2 ESCANEO

Abrir la terminal y escribir ***nmap -h*** para ver todas las opciones que se pueden utilizar con este comando.

Figura 71. comando nmap -h

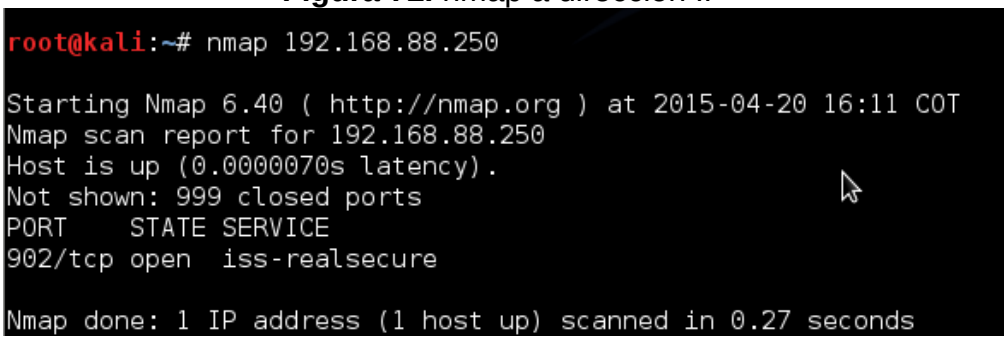
A continuación algunos ejemplos del uso del escaneo con nmap[28].

Ejemplo 1: Escanear un host o una direción IP (IPv4), se escaneará los 1000 puertos tcp por defecto.

- *nmap 192.168.88.250* Se realiza el escaneo de la dirección IP

[28] IPAUDITA, Top 30 de Nmap ejemplos de comandos para SYS / Red Admins, 2013, https://ipaudita.wordpress.com/2013/02/13/top-30-de-nmap-ejemplos-de-comandos-para-sys-red-admins/

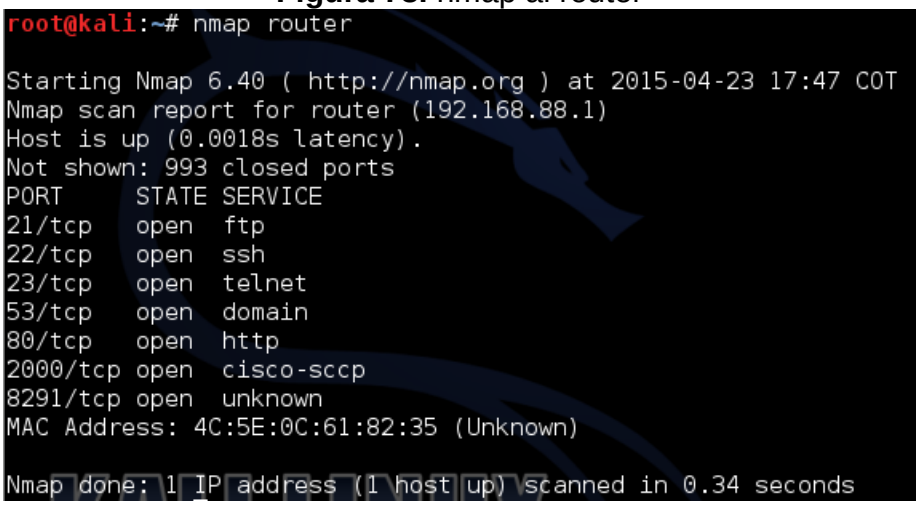
Figura 72. nmap a dirección IP



El resultado es que el host está activo, 999 puertos cerrados. El puerto tcp 902 está abierto y es seguro, 1 dirección IP y el tiempo escaneado de 0.27 segundos.

- *nmap router* Se realiza el escaneo del host, si se quieren más detalles se debe escribir *nmap -v router.*

Figura 73. nmap al router



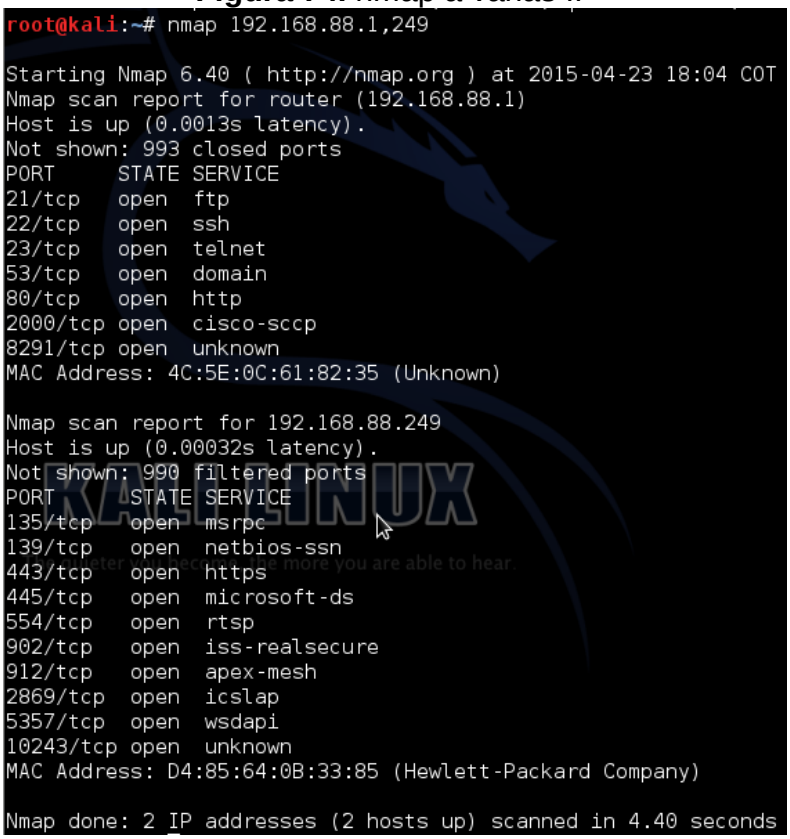
El resultado esque el host está activo, tiene 7 puertos abiertos, 993 puertos cerrados y su dirección MAC.

El escaneado con la opción -v (nmap -v router), da los mismos resultados pero con un poco más de información, por ejemplo la dirección IP del host router, y número de paquetes enviados y recibidos, entre otros.

Ejemplo 2: Escanear varias direcciones IP o subred (Ipv4)

- *nmap 192.168.88.1,249* Se escanearán 2 direcciones IP (192.168.88.1 y 192.168.88.249)

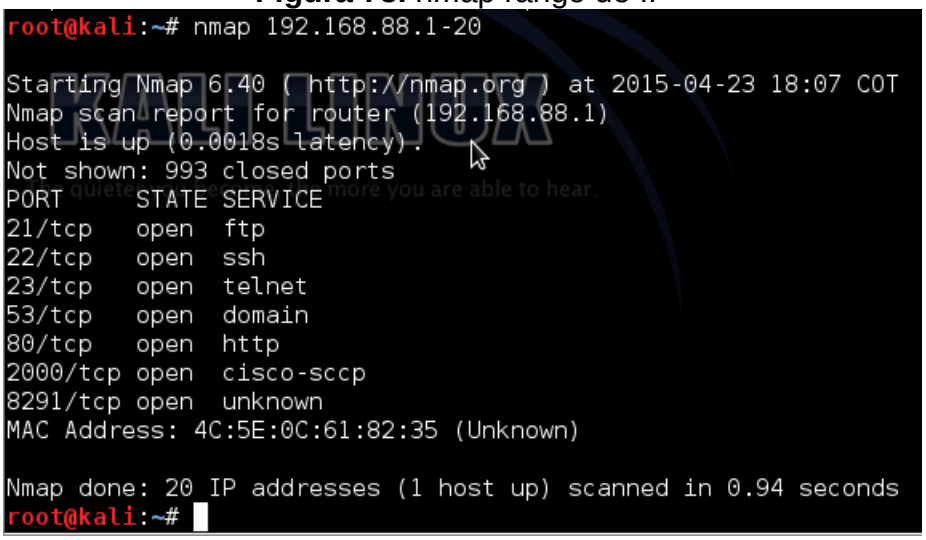
Figura 74. nmap a varias IP



Da como resultado su respectivo análisis para cada dirección IP, con sus puertos abiertos, cerrados, su respectiva dirección MAC.

- *nmap 192.168.88.1-20* Escanear un rango de direcciones IP

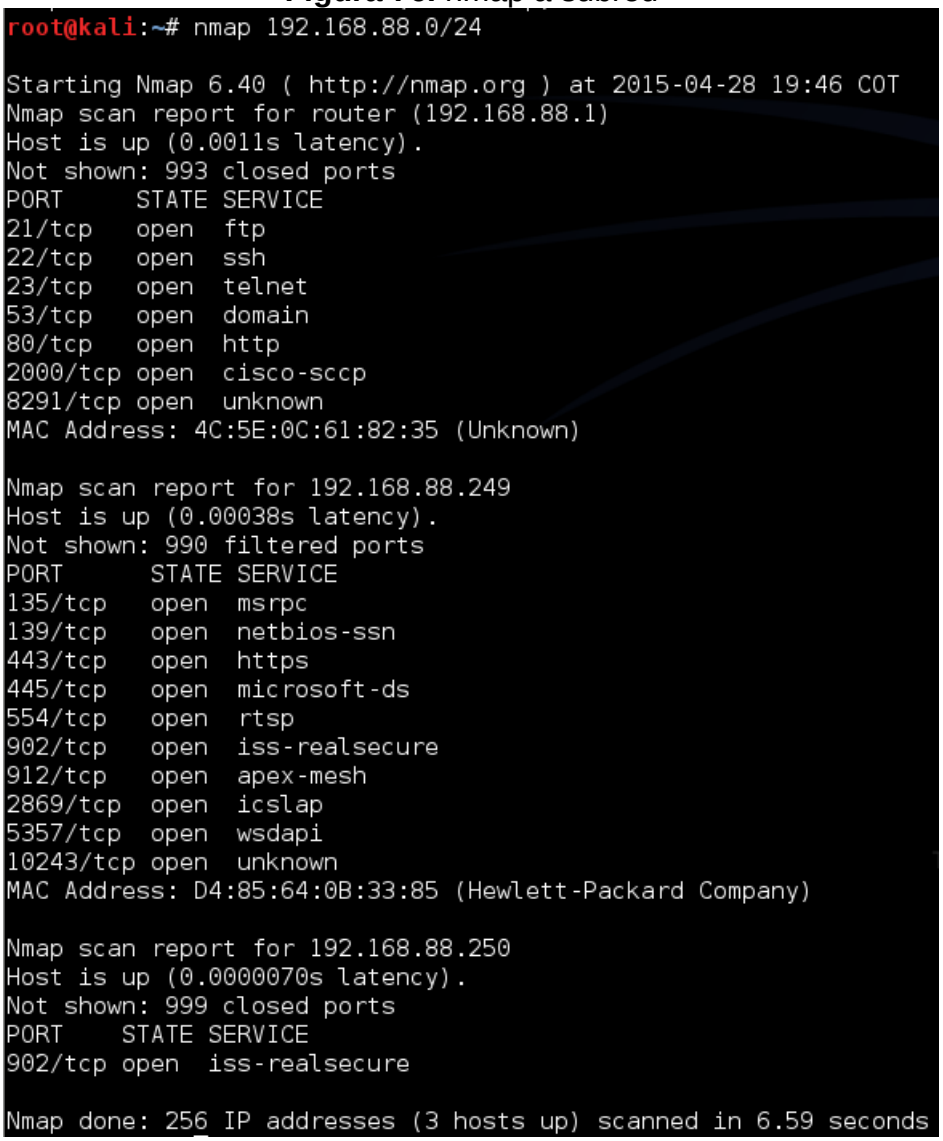
Figura 75. nmap rango de IP



Se escanearon 20 direcciones IP, pero solo 1 host activo que es el del router.

- *nmap 192.168.88.0/24* Escanear una subred completa

Figura 76. nmap a subred



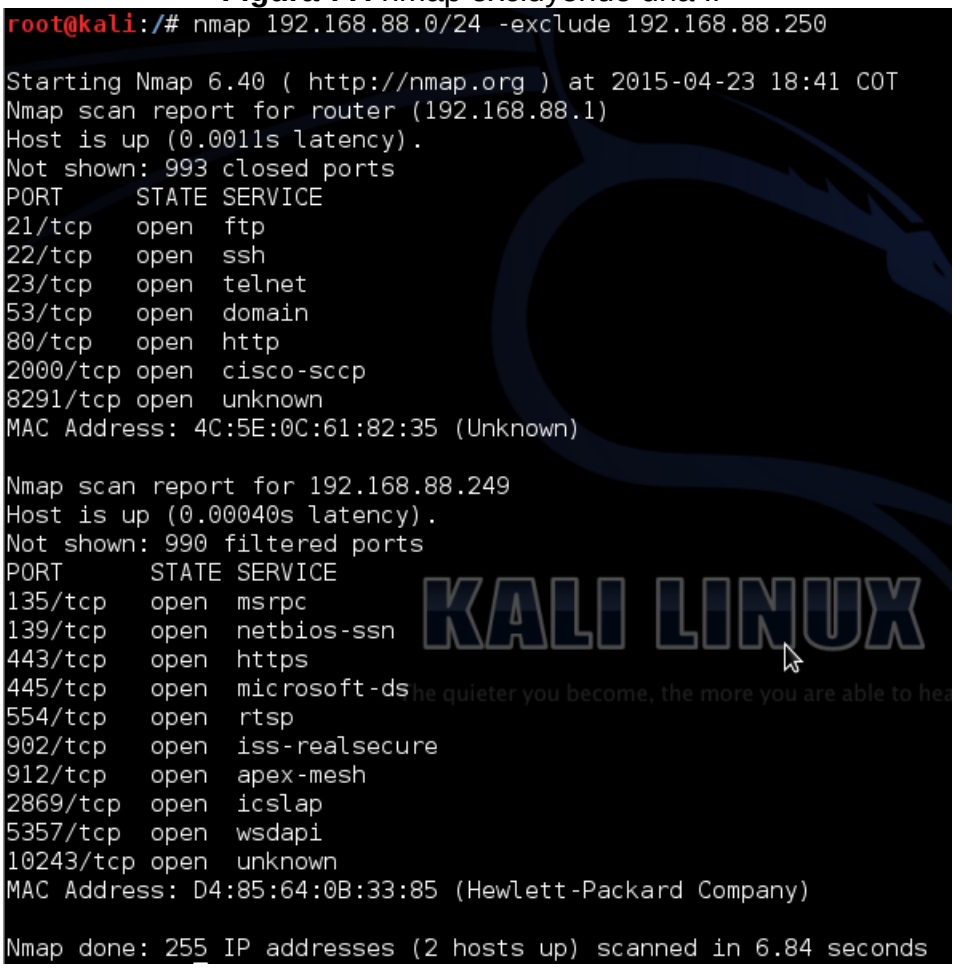
El resultado son 3 host activos uno es el del router con 7 puertos abiertos, también muestra su dirección MAC y 256 IP escaneadas. El segundo host es de un computador de la red con 10 puertos abiertos, con su dirección MAC e indica que es de la compañía Hewlett Packard. El otro host es del computador que se está utilizando con 1 puerto abierto.

Ejemplo 3: Exclusión de host / redes Ipv4

Al escanear un gran número de hosts / redes se pueden excluir los hosts de una exploración.

- *nmap 192.168.88.0/24 -exclude 192.168.88.250* Se escanearán todos las redes menos la dirección 192.168.88.250

Figura 77. nmap excluyendo una IP

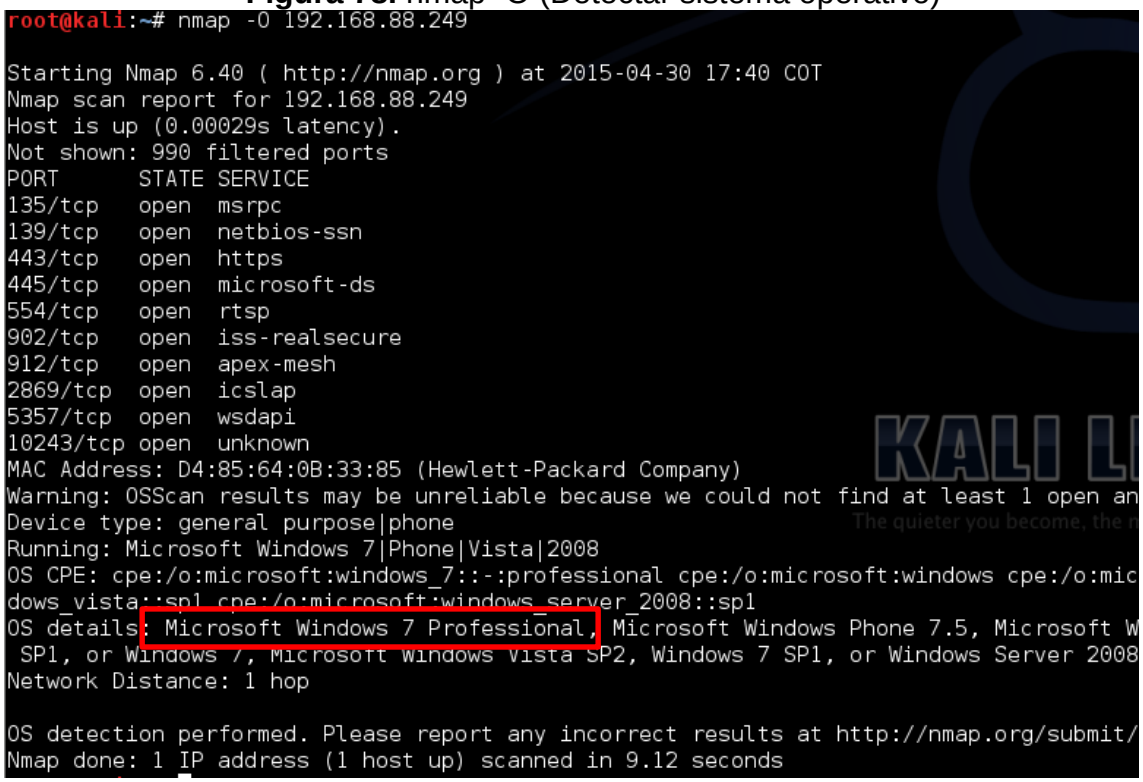


El resultado es el escaneo de toda la subred, pero se excluye una dirección IP.

Ejemplo 4. Detectar el sistema operativo. Esto lo hace mediante varios tipos de pruebas, como pruebas de sentencia de TCP, paquetes SYN, NULL, FIN, URG, PSH, ACK, UDP con diversas opciones a puertos abiertos y cerrados.

- nmap -O 192.168.88.249

Figura 78. nmap -O (Detectar sistema operativo)



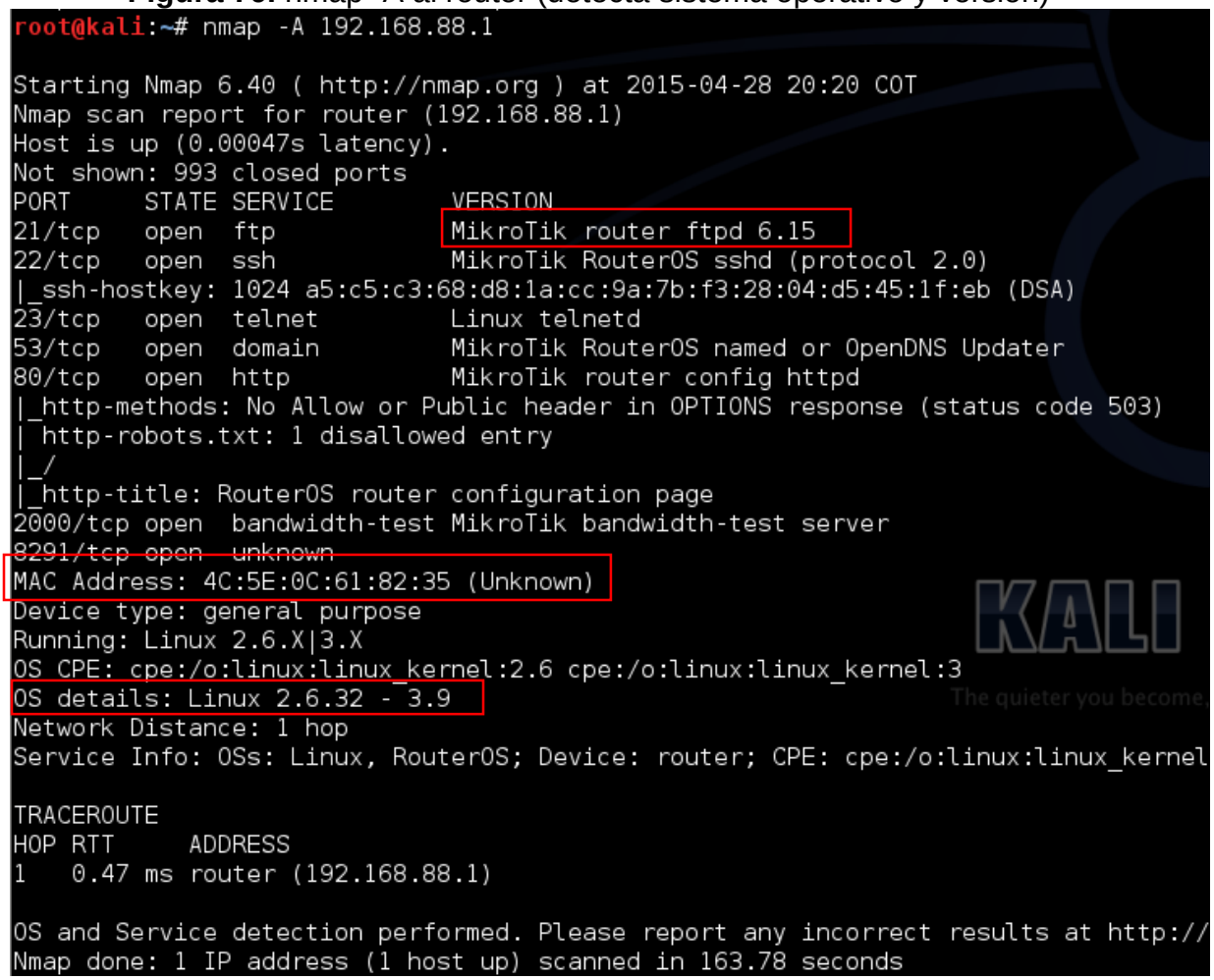
Como resultado dice que el sistema operativo es Microsoft Windows 7 y detalladamente que es la versión Professional.

A veces este resultado no es del todo acertado ya que Windows no ha presentado mayores mejoras entre versiones de Windows anteriores entonces como resultado nos puede arrojar un sistema operativo similar por ejemplo en este caso, también detectó el sistema operativo microsoft windows phone 7.5, vista, y server 2008..

Para ver mayores detalles de este escaneo puede escribir: *nmap –vv –sS 192.168.88.259*

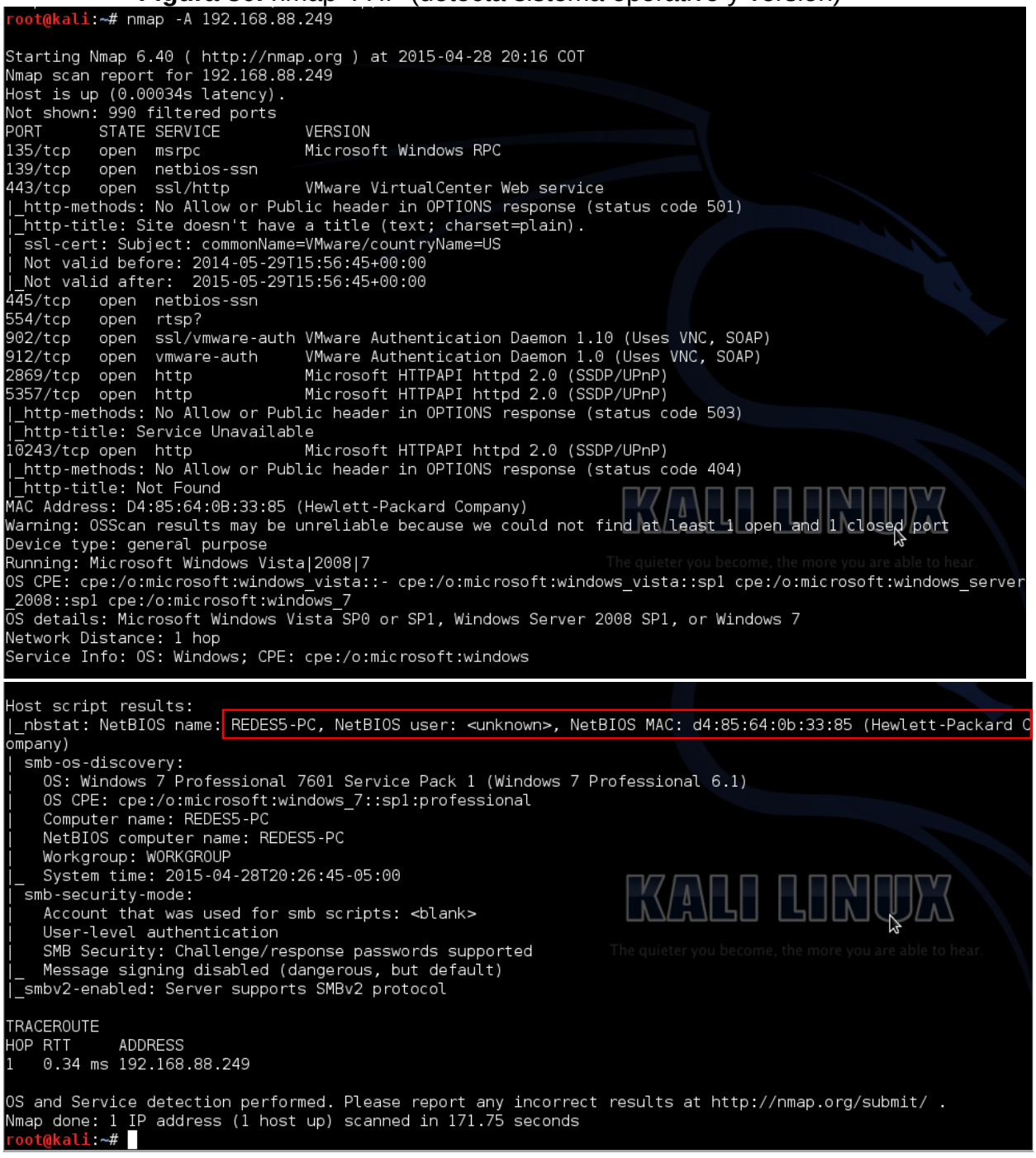
Ejemplo 5.

Figura 79. nmap -A al router (detecta sistema operativo y versión)



Esta opción de nmap detecta la versión del router utilizado el cual es MikroTick, con su respectiva dirección MAC y sistema operativo Linux.

Figura 80. nmap -A IP (detecta sistema operativo y versión)



En este análisis con nmap -A a una dirección IP, da como resultado su sistema operativo (Windows 7 profesional), el nombre del computador en la red (REDES5-PC), dirección MAC y de la compañía Hewlett-packard.

TRABAJO

Realizar todos los ejemplos anteriores usando su dirección IP y registrar información acerca de cuáles y que tipos de puertos están abiertos y cerrados, su dirección MAC, cuantos host están conectados en la red y algunas características de cada uno, detectar el sistema operativo del computador que está utilizando.

Investigar que más información se puede escanear con el comando nmap y un ejemplo.

5. CONCLUSIONES Y RECOMENDACIONES

En este proyecto desde un principio se empieza trabajando con el sistema operativo Backtrack 5 R3, pero durante el desarrollo de las guías hubo una actualización en la cual Backtrack ya no iba a tener soporte técnico y le dieron paso a un nuevo sistema operativo llamado Kali Linux, por lo tanto lo mejor era empezar nuevamente a realizar las pruebas con las guías para entregar un proyecto actualizado.

Al principio fue un poco complicado ya que como era un sistema operativo nuevo entonces no había mucha información en la cual se pudiera basar para el desarrollo de las guías.
Entonces se comenzó a realizar las guías nuevamente que se habían trabajado con Backtrack, pero ahora con kali Linux para probarlas y mirar los cambios que hubieron, también seguir buscando información y temas para las siguientes guías a desarrollar.

Los temas de las guías se empiezan a desarrollar de los temas más básicos que son los principales comandos de Linux hasta los más complejos que son las practicas programación y de hacking ético, en estas guías se recuerda la importancia por la cual se están desarrollando y para qué sirven.
Luego de probar todas las guías se hicieron ciertos arreglos, por ejemplo algunas guías tenía mucho contenido entonces se reduce el contenido para que la guía pueda ser desarrollada en el tiempo que dura un laboratorio, otra guía se divide en 2 guías ya que tenía mucho contenido y no se podían omitir esos temas ya que son muy importantes.

Al finalizar las guías el estudiante tendrá muy buenos conocimientos de las redes en Kali Linux y quedará motivado a seguir investigando acerca de estos temas ya que son muy actuales y no pasarán de moda, ya que las redes se usan en todas partes en donde estemos, y este sistema operativo de kali Linux es muy potente en estos casos y lo mejor de todo es que es gratis y actualmente ya hay mucha información en la cual se puedan basar para futuros proyectos.

BIBLIOGRAFÍA

ADMIN, Tutorial nmap para Kali Linux, 2013, http://kalilinux.foroactivo.com/t12-tutorial-nmap-para-kali-linux

ANTRAX-LABS, Sniffing con Wireshark, 2015. http://www.antrax-labs.org/2012/01/sniffing-con-wireshark.html

ASTUDILLO, Karina. Hacking ético 101, Cómo hackear profesionalmente en 21 días o menos!, Editorial Reviews, 2013, pág 10.

CABALLERO, Alonso, Hacking con Kali Linux, 2015, http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

CATALINA GALLEGO, Alfredo y Miguel, Unix/Linux: Iniciación y Referencia, 2a. ed, Madrid: McGraw-Hill, pág. 82, [Consulta: 11 de agosto de 2014]

CETEM, Fundación de servicios educativos EMSSANAR, ¿Qué es una máquina virtual? 2014. http://cetemso.blogspot.com/2014/01/que-es-una-maquina-virtual-y-para-que.html

CIBERAULA, Qué es Linux, 2014, http://linux.ciberaula.com/articulo/que_es_linux/

FRANCISCONI, Hugo Adrián, Guía de Referencia Rápida de Linux, Venezuela, 2010,
http://francisconi.org/sites/default/files/guia_de_referencia_rapida_de_linux.pdf

GÓMEZ LÓPEZ, Julio. Administración de sistemas operativos: Un enfoque práctico, 2a.ed México: Alfaomega Grupo editor, 2011, pág. 383. [Consulta: 19 de agosto de 2014]

IPAUDITA, Top 30 de Nmap ejemplos de comandos para SYS / Red Admins, 2013, https://ipaudita.wordpress.com/2013/02/13/top-30-de-nmap-ejemplos-de-comandos-para-sys-red-admins/

KALI LINUX Official Documentation, Introducción, ¿Qué es kali linux?, 2015, http://es.docs.kali.org/introduction-es/que-es-kali-linux [Consulta: Jueves, 10 de diciembre 2015]

KIRCH, Olaf, Editado por O'Reilly, Guía de Administración de Redes con Linux,

ORACLE, Welcome to virtualbox, https://www.virtualbox.org/ [Consulta: martes, 3 de noviembre de 2015]

O'Reilly & Associates, 2000. http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-iface.ifconfig.html

PERSEO, Cómo se encuentran estructurados los directorios en GNU/Linux?, 2012. http://blog.desdelinux.net/estructura-de-directorios-en-linux/

SAMBONI, Diana Marcela, Manual básico de Wireshark, Medellín, 2012, http://www.slideshare.net/DIANYSS2012/manual-bsico-de-wireshark

VÁSQUEZ, Junior, Manual Wireshark En Español, Medellín, 2013, http://manualwireshark.blogspot.com.co/

WEIDMAN, Georgia. Penetration Testing. A hands-On introduction to hacking. San Francisco: No Starch Press, 2014, pág 57, [Consulta: 4 de Agosto de 2015]

WEIDMAN, Georgia. Penetration Testing. A hands-On introduction to hacking. San Francisco: No Starch Press, 2014, pág 61, [Consulta: 4 de Agosto de 2015]

WIKIHOW, Cómo hacer ping en Linux, 2014, http://es.wikihow.com/hacer-ping-en-Linux

WIKIPEDIA, ifconfig, 2015, https://es.wikipedia.org/wiki/Ifconfig

WIKIPEDIA, VMware, https://es.wikipedia.org/wiki/VMware [Consulta: martes, 3 de noviembre de 2015]

WIKIPEDIA, VMware, https://es.wikipedia.org/wiki/VMware [Consulta: martes, 3 de noviembre de 2015]