Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

"ELABORACIÓN DE UN TUTORIAL DE PRACTICAS PARA EL LABORATORIO DE SISTEMAS OPERATIVOS"

Trabajo de graduación previo a la obtención del título de

Ingeniero en Sistemas

Autor: Rómulo Arturo Izquierdo Pérez

Director: Ing. Pablo Esquivel

Cuenca, Ecuador

2008

DEDICATORIA

La culminación de este trabajo va dedicada con mucho cariño a mi madre y a mi padre quienes con su apoyo y sacrificio me enseñaron a no desmayar en los momentos difíciles, además supieron encaminarme a la realización de mis ideales y la culminación de mis estudios superiores de un modo desinteresado e incondicional.

A mi familia quienes, me apoyaron y creyeron en mí brindándome la seguridad y capacidad de llegar al éxito.

Rómulo Arturo

AGRADECIMIENTOS

Un muy sincero agradecimiento a Dios por haberme brindado la fuerza necesaria para cumplir esta meta y culminar esta etapa de mi vida, sobre todo a mis padres que con gran esfuerzo y amor incondicional me apoyaron siempre, a mis amigos, compañeros, profesores y demás personas que estuvieron brindándome el apoyo indispensable para llegar a ser mejor persona y profesional.

Al Ingeniero Esquivel quien con su experiencia y sin egoísmo alguno me brindo conocimientos que me fueron útiles en la realización de esta monografía.

Rómulo Arturo

RESPONSABILIDAD DE AUTOR

Las ideas vertidas en la presente monografía son de exclusiva responsabilidad de su autor.

_____

Rómulo Arturo Izquierdo Pérez

Código: 28178

C.I: 010236224-1

ÍNDICE DE CONTENIDOS

Contenido

RESUMEN

El presente proyecto pretende realizar un Tutorial de Prácticas para la cátedra de Laboratorio de Sistemas Operativos. El Tutorial contendrá información paso a paso para realizar prácticas sobre transferencia de archivos, seguridad, conectividad remota, administración de redes. De esta forma el estudiante se familiarizará en la forma de manejar un sistema operativo para la ejecución de aplicaciones de servidor y los comandos que necesita.

Se tratará en lo posible que el desarrollo de la práctica dure las dos horas de clase razón por la cual el documento de la práctica tiene que estar completamente detallado de la forma cómo realizarla y además todo el software necesario para desarrollar la práctica previamente instalado.

ABSTRACT

This project intends to develop a Tutorial of Practices for the subject of Operative Systems Laboratory. The tutorial will contain step-by-step information to make practices about file transfers, safety, remote connectivity, and net administration. Thus the student will familiarize with the way of handling an operative system for the execution of applications of a server and the controls that he needs.

The development of the practice will be planned to last for the two hours of class in as much as possible. For that reason, the form for the practice has to be completely detailed regarding the way to do it, and the software necessary to develop the practice has to be previously installed.

INTRODUCCION

El uso de software libre se ha ido incrementando, debido a que brinda libertad a los usuarios ya que este puede ser usado, copiado, estudiado, modificado y redistribuido libremente.

Debido a esto se vió la necesidad de crear un Tutorial de Prácticas para la materia de tercer ciclo Laboratorio de Sistemas Operativos. El Tutorial contendrá información paso a paso para realizar prácticas sobre transferencia de archivos, seguridad, conectividad remota, etc. De esta forma el estudiante se familiarizará en la forma de manejar un sistema operativo para la ejecución de aplicaciones de servidor y los comandos que necesita.

El documento de la práctica tiene que estar completamente detallado de la forma cómo realizarla y además todo el software necesario para desarrollar la práctica previamente instalado.

CAPITULO 1: INSTALACIÓN DEL SOFTWARE A UTILIZAR

1.1 Introducción

Este primer capítulo trata sobre los requisitos y la instalación de todo el software que utilizaremos para la realización de prácticas en este tutorial, como son la Máquina Virtual VMWARE y la versión de Linux CentOS5.

1.2 Requisitos de instalación

- Windows XP
- Procesador Pentium 4 o superior
- 512 MB de RAM o superior
- 20 GB de disco duro como mínimo
- Tarjeta de red
- Unidad de CD o DVD

1.3 Instalación de la Máquina Virtual VMWARE

La instalación de la Máquina Virtual VMWARE es un procedimiento sencillo que describiremos a continuación:

- Ejecutamos el instalador, damos click en siguiente o next.

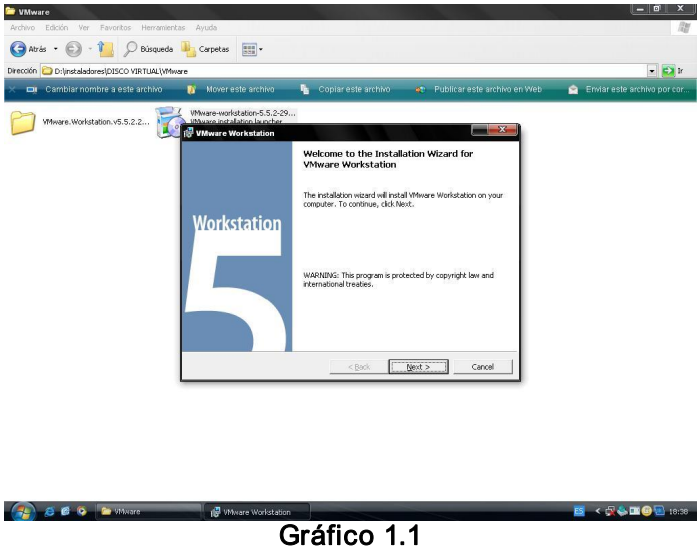

Gráfico 1.1

- Escogemos el directorio de instalación o dejamos el que tiene.

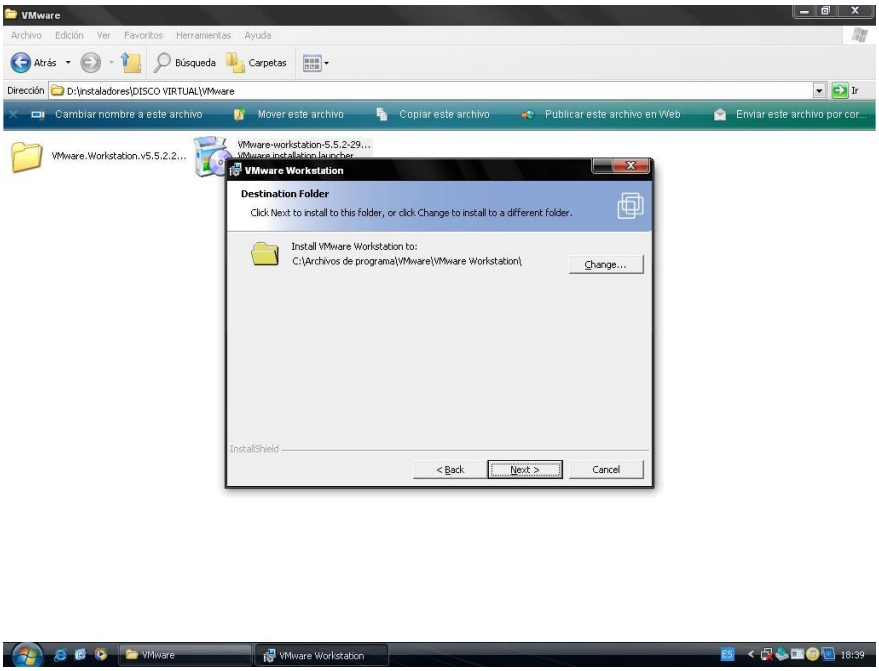

Gráfico 1.2

- Escogemos donde queremos que se instale los accesos directos al programa.

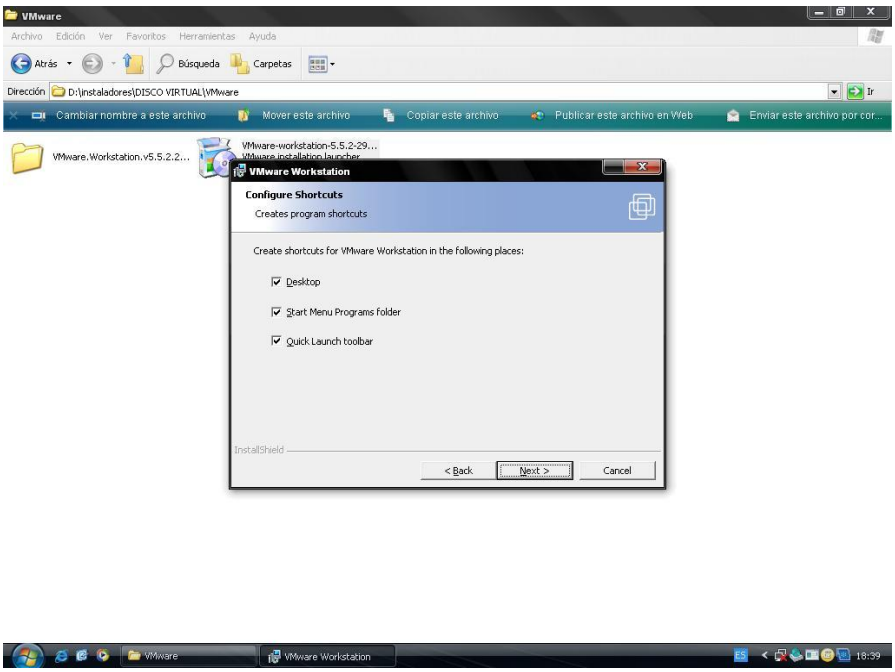

Gráfico 1.3

- Configuramos el producto deshabilitamos el autorun para el CD-ROM

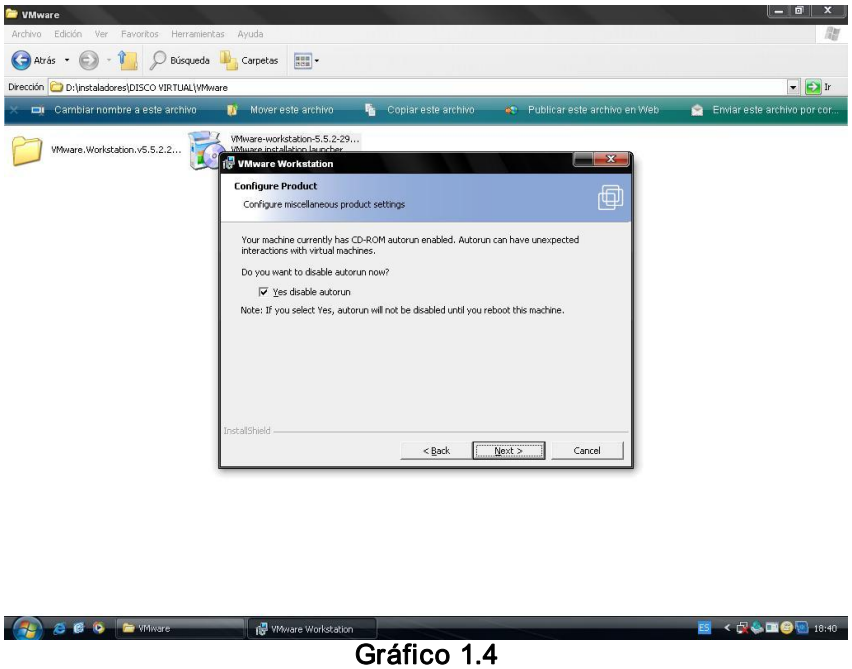

Gráfico 1.4

- Ahora si instalamos el producto dando un clic en install.

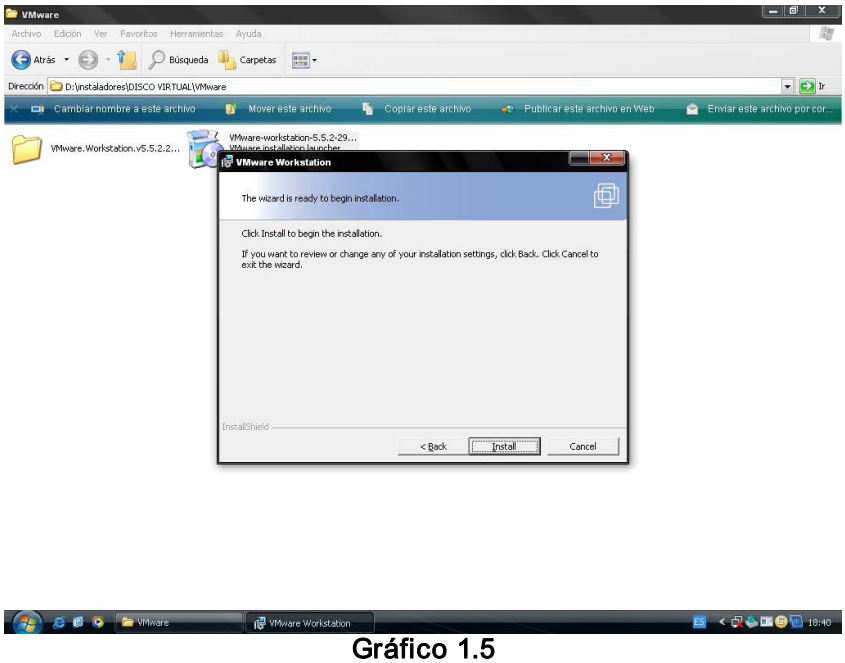

Gráfico 1.5

- Si nos pide una clave ejecutamos el archivo keygen que se encuentra dentro de la carpeta del VMWARE y así obetenemos la clave .

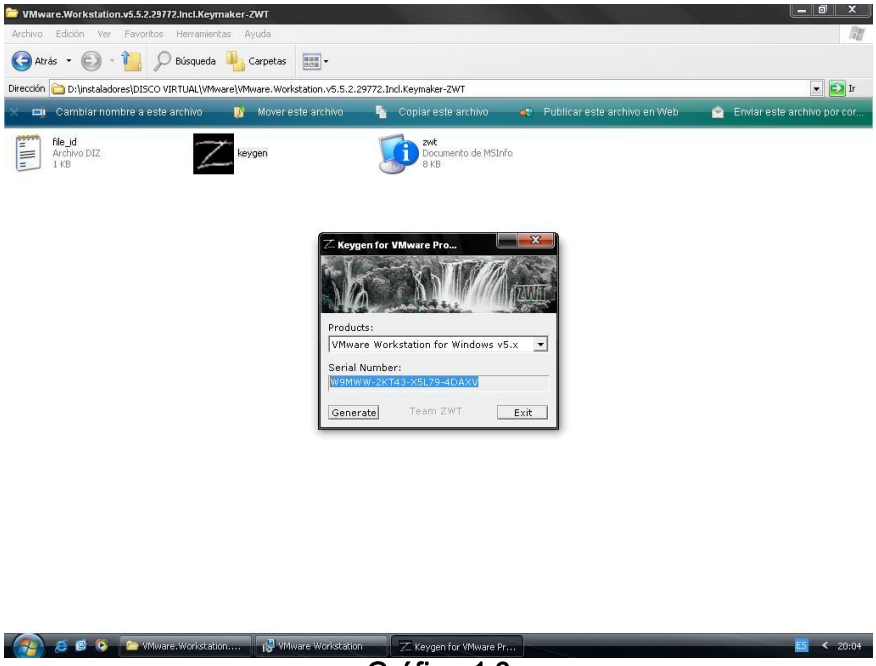

Gráfico 1.6

- Luego finalizamos la instalación y así ha quedado instalado el producto.

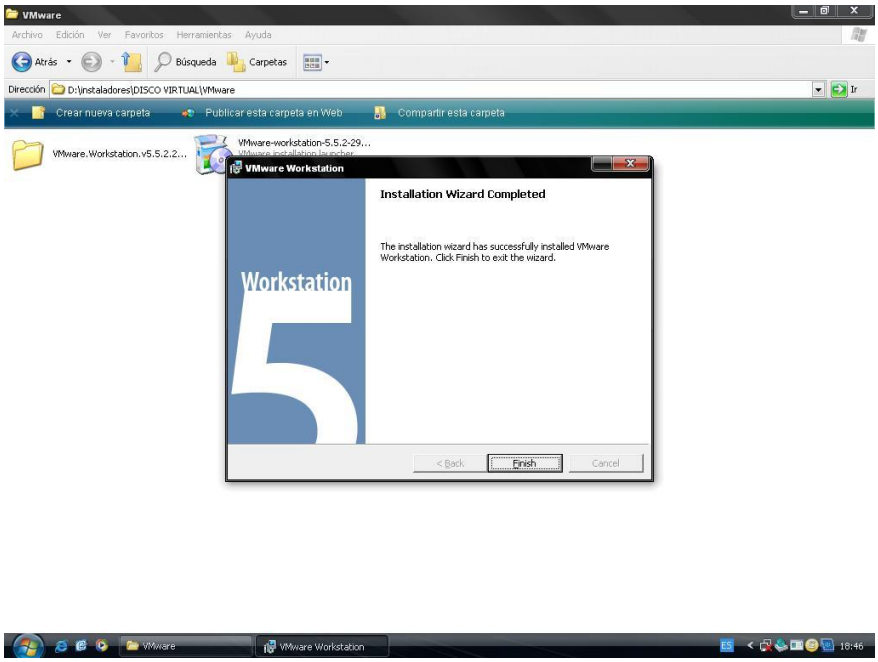

Gráfico 1.7

1.4 Creación y configuración de la máquina virtual para la instalación de Linux

- Para la instalación de Linux dentro de VMWARE escogemos la opción **New virtual machine.**

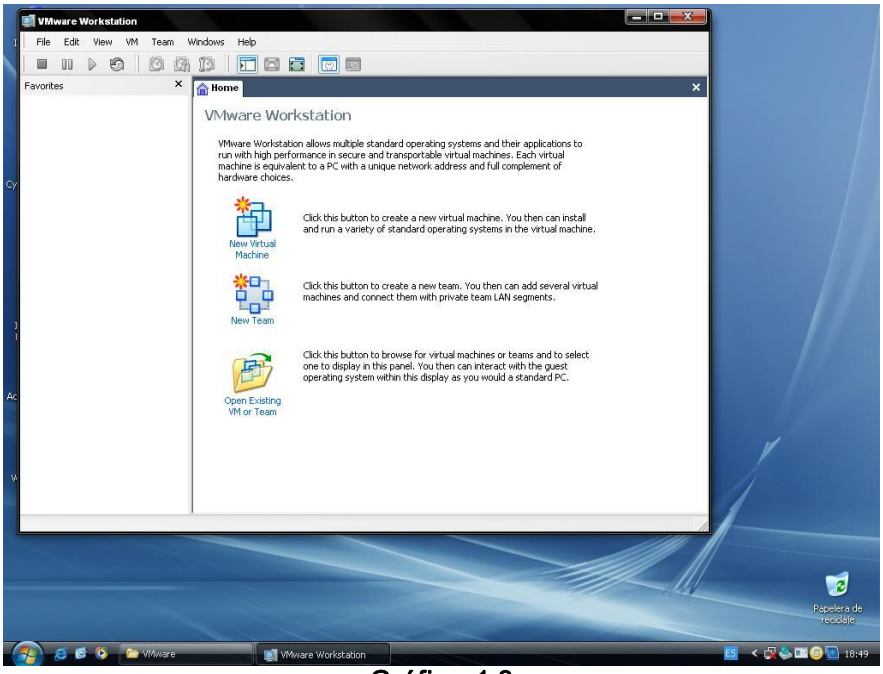

Gráfico 1.8

- Damos clic en siguiente

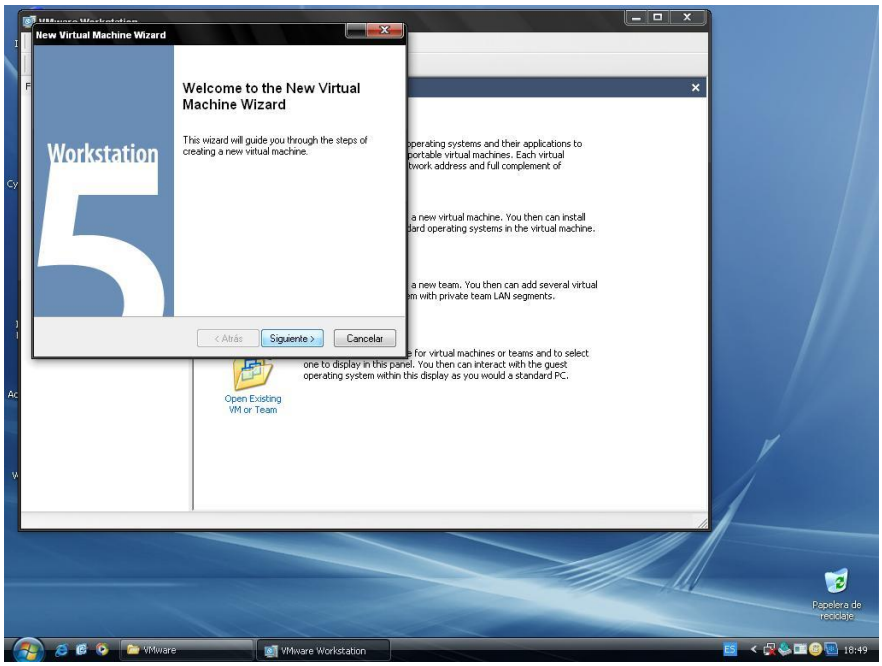

Gráfico 1.9

- Es cogemos la opción personalizado o **Custom**

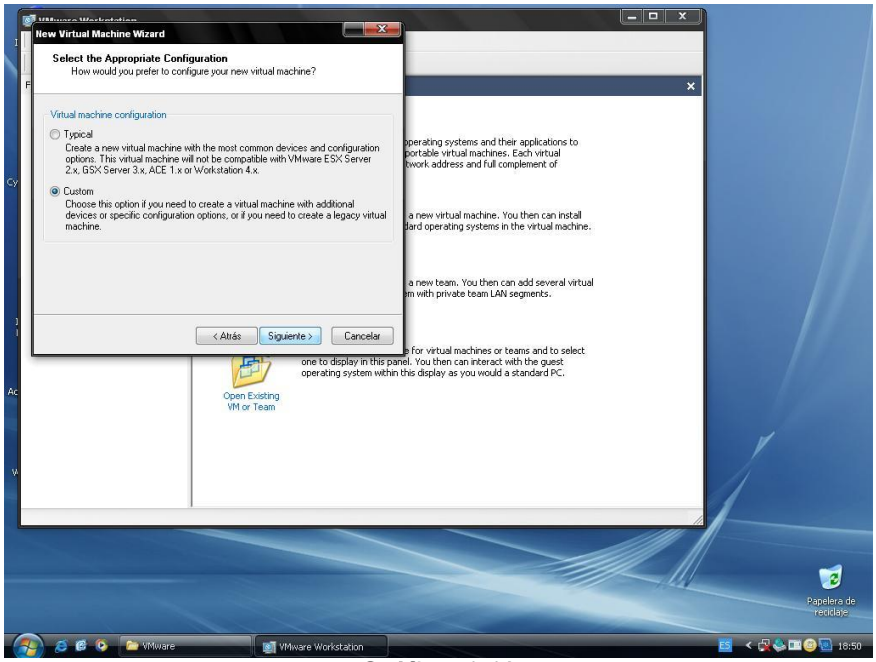

Gráfico 1.10

- Escogemos la opción nueva estación de trabajo ó **New Workstation 5**

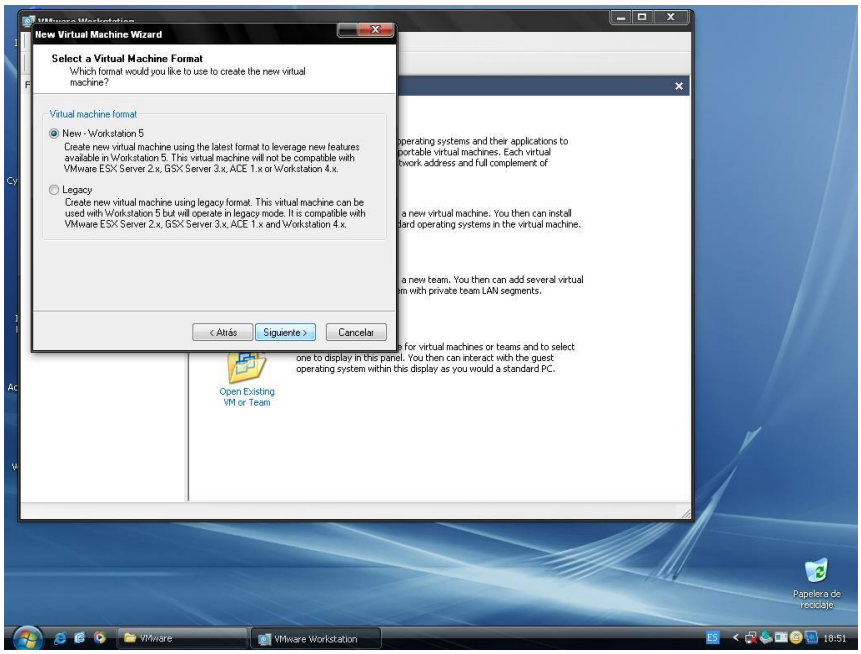

Gráfico 1.11

- En este ejemplo se instaló la versión CENTOS 5.0 de Linux, para ello escogemos en Sistema Operativo **Linux** y en versión escogemos **Red Hat Enterprise linux 4** debido a que no se encuentra en este listado la versión de CENTOS y al escoger la anterior nos permite instalar sin ningún problema.

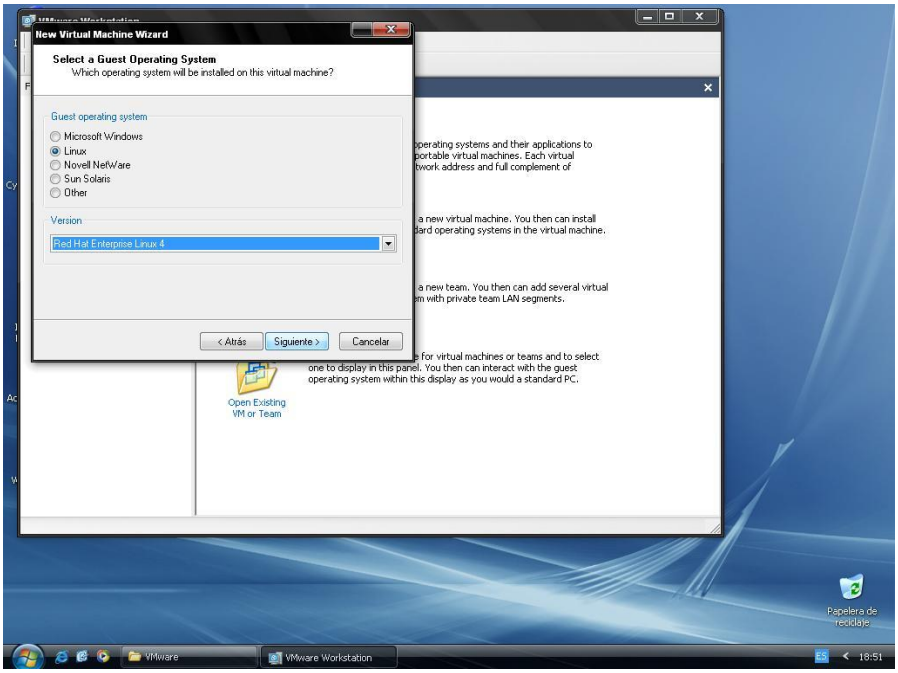

Gráfico 1.12

- Escribimos el nombre de la máquina virtual y la ubicación en disco.

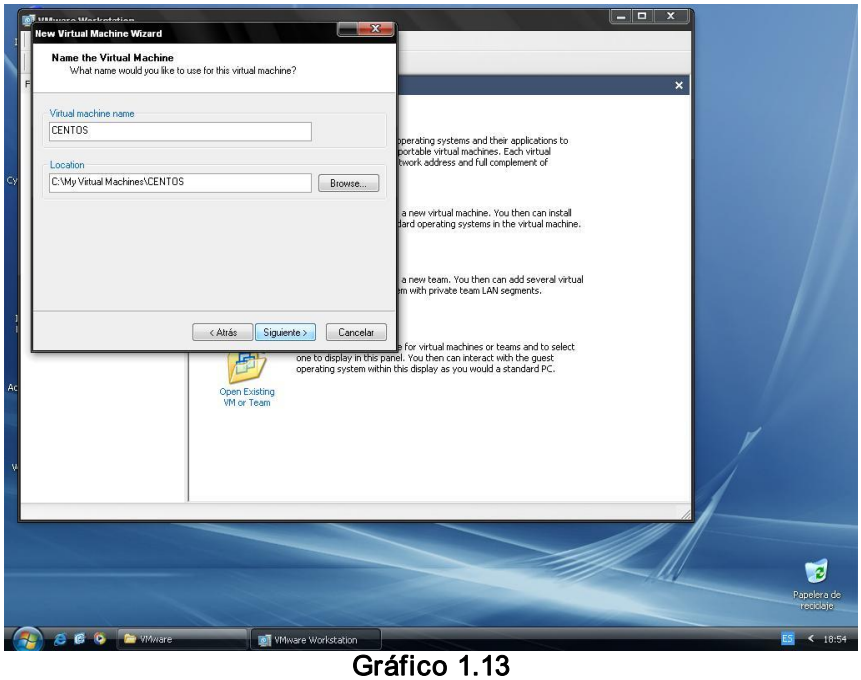

Gráfico 1.13

- Escogemos el número de procesadores en este caso escogemos uno ó **One.**

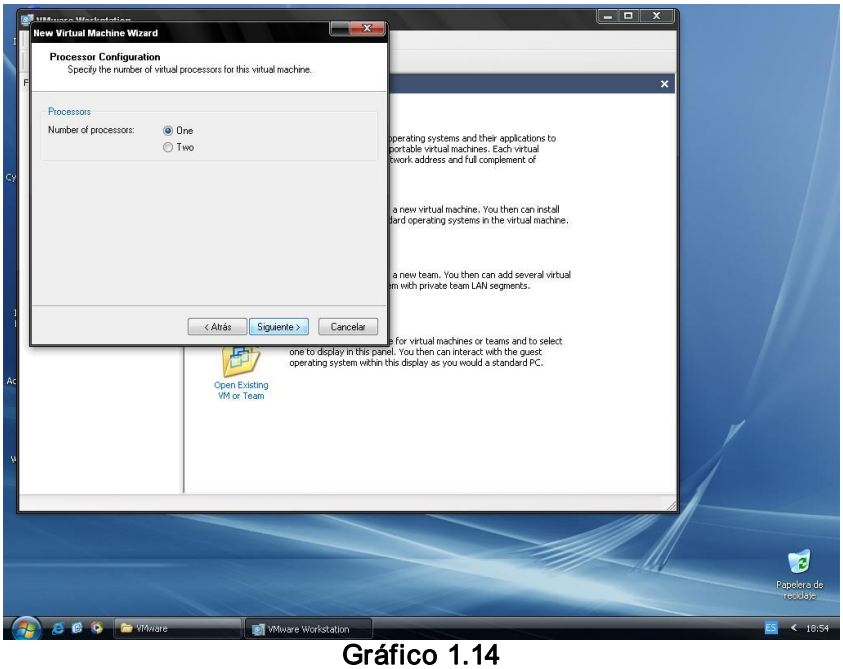

Gráfico 1.14

- Especificamos la cantidad de memoria a compartir con la máquina virtual. Esto depende de cuanto sea la memoria del computador donde se realiza la instalación. Podría ponerse la mitad de la memoria total del computador.

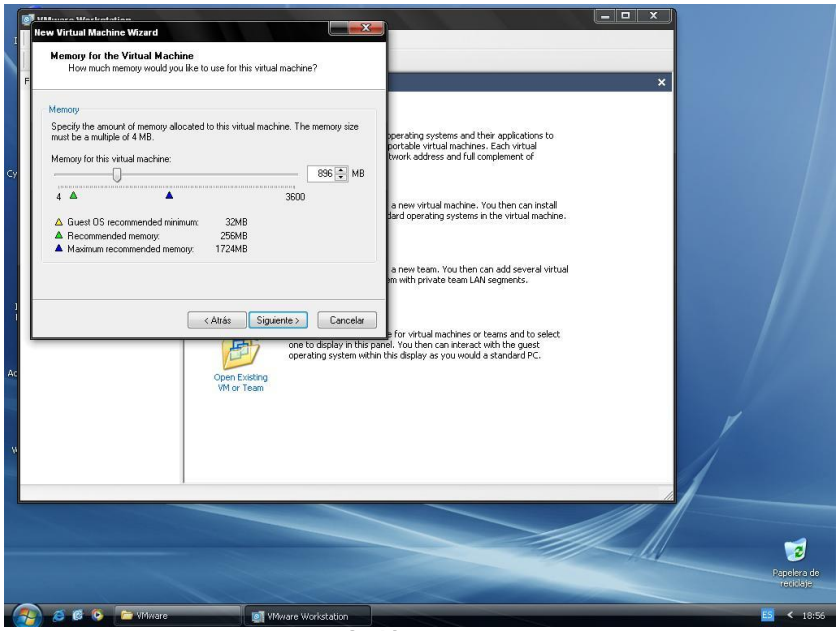

Gráfico 1.15

- Escogemos la conexión de red en este caso la opción **Use bridged networking**

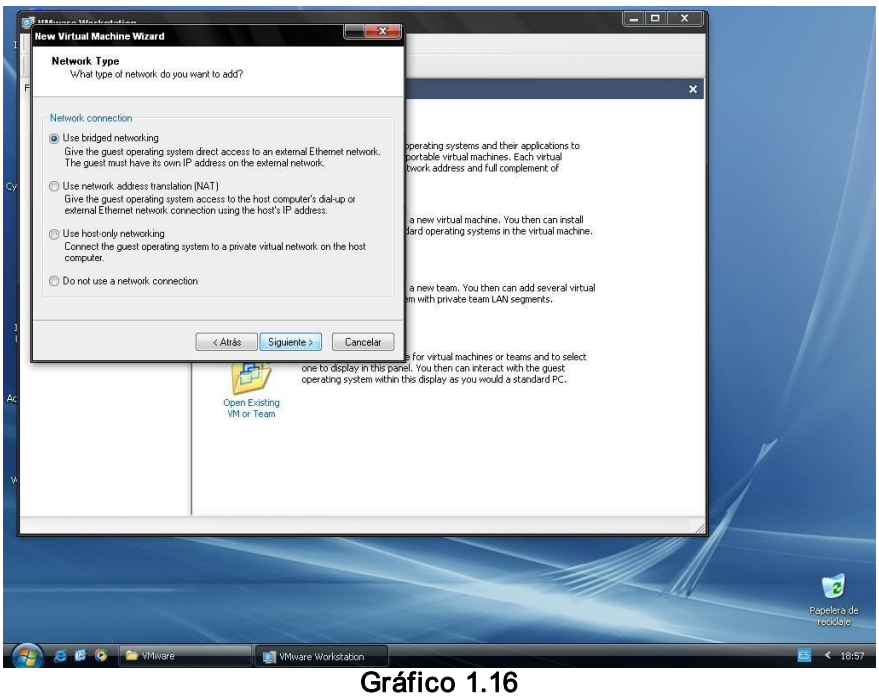

Gráfico 1.16

- Dejamos la selección actual del tipo de adaptador de I/O en este caso **LSI logic.**

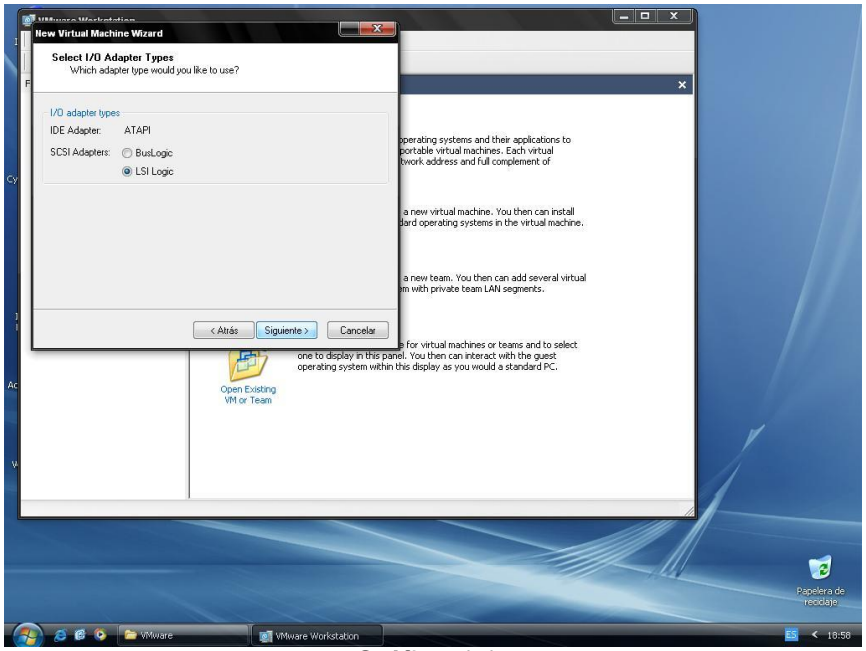

Gráfico 1.17

- Seleccionamos la opción crear un nuevo disco virtual ó **Create a new virtual disk**

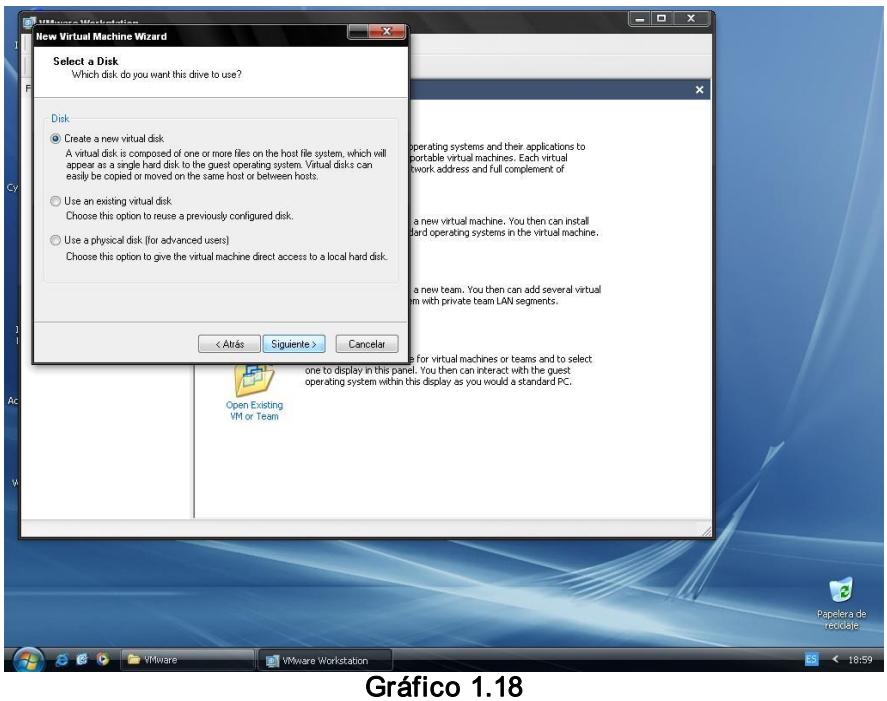

Gráfico 1.18

- Seleccionamos el tipo de disco en este caso dejamos SCSI (Recomended)

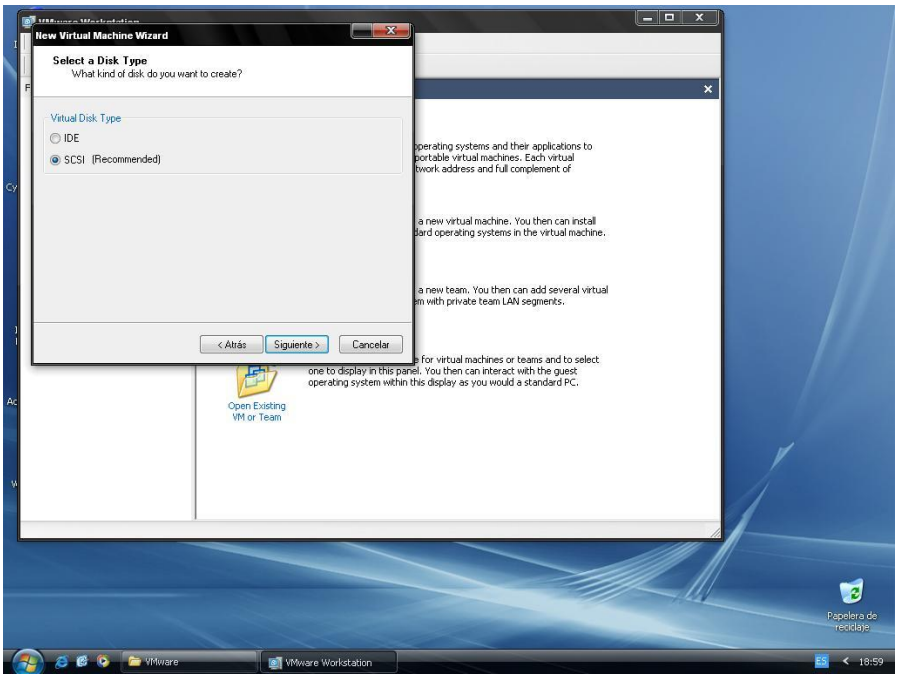

Gráfico 1.19

- Especificamos el espacio virtual en disco. Para Linux es recomendable dar 20 GB como mínimo.

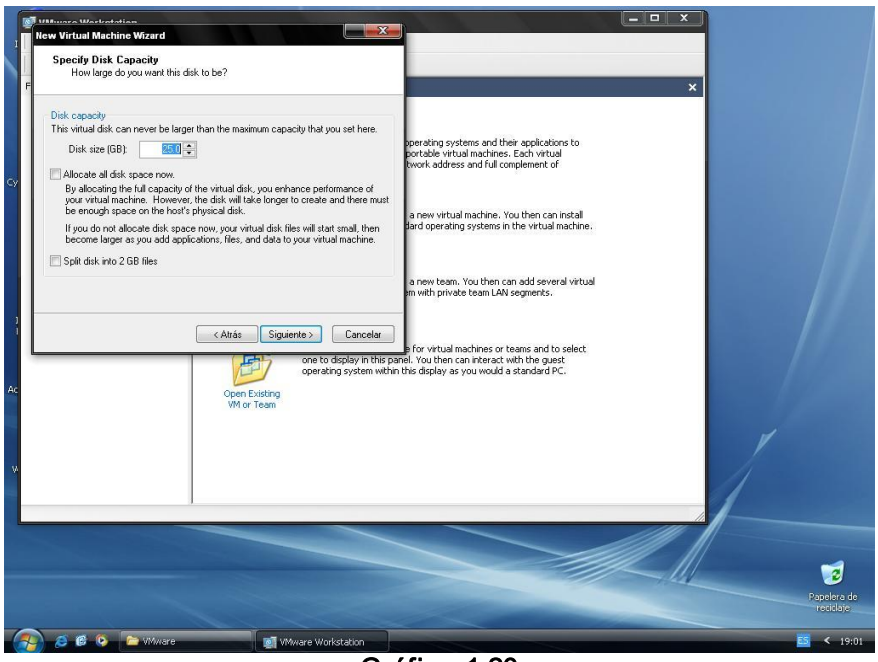

Gráfico 1.20

- Especificamos el nombre del archivo en disco y finalizamos la instalación.

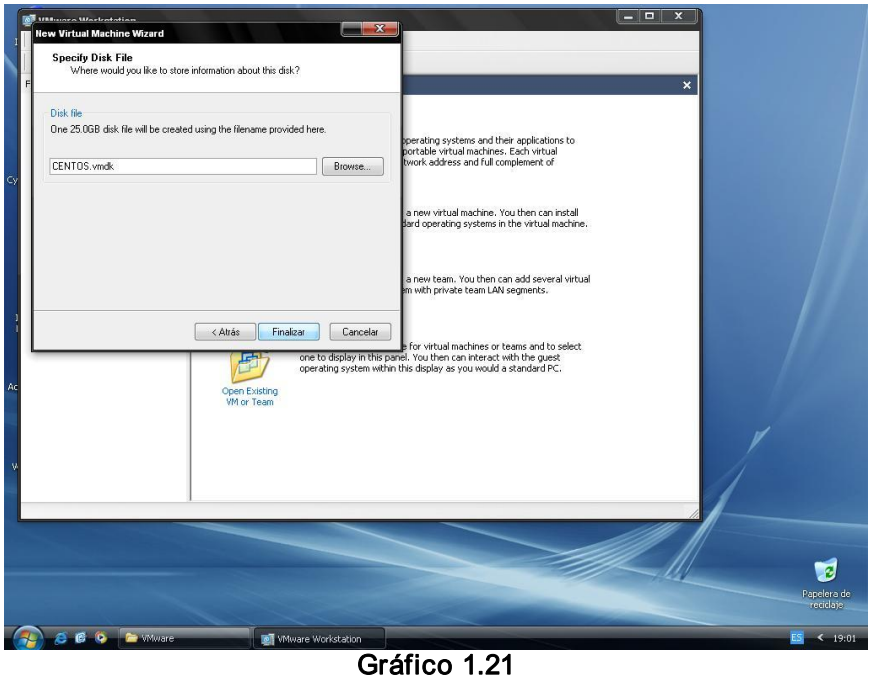

Gráfico 1.21

1.5 Instalación de Linux usando VMWARE.

- Dentro de VMWARE podremos cambiar las opciones de los dispositivos en el comando **Edit virtual machine** y también podremos ejecutar Linux al dar clic sobre **Start virtual machine.**

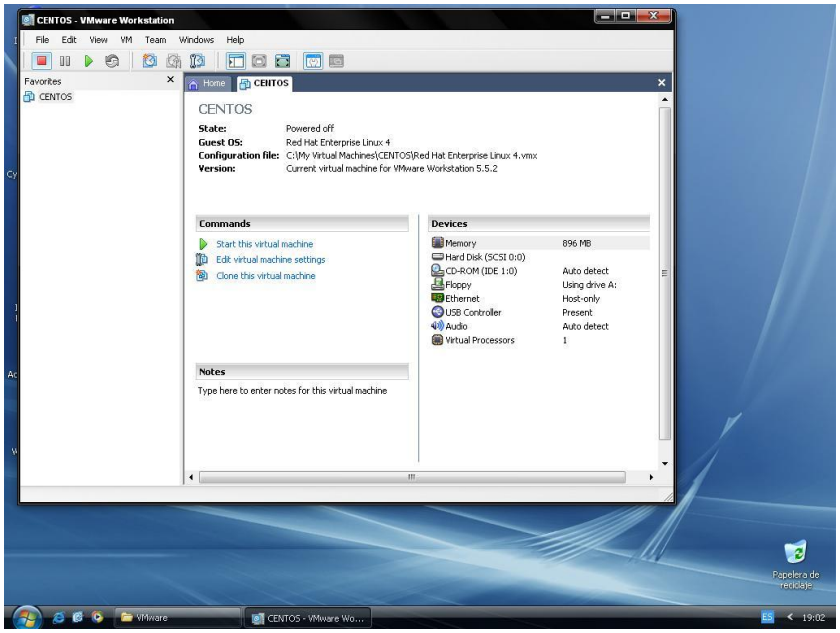

Gráfico 1.22

- Para cargar el Sistema Operativo introducimos el cd y damos clic en **Start the virtual machine** se mostrará lo siguiente.
- Escogemos la primera opción damos un Enter

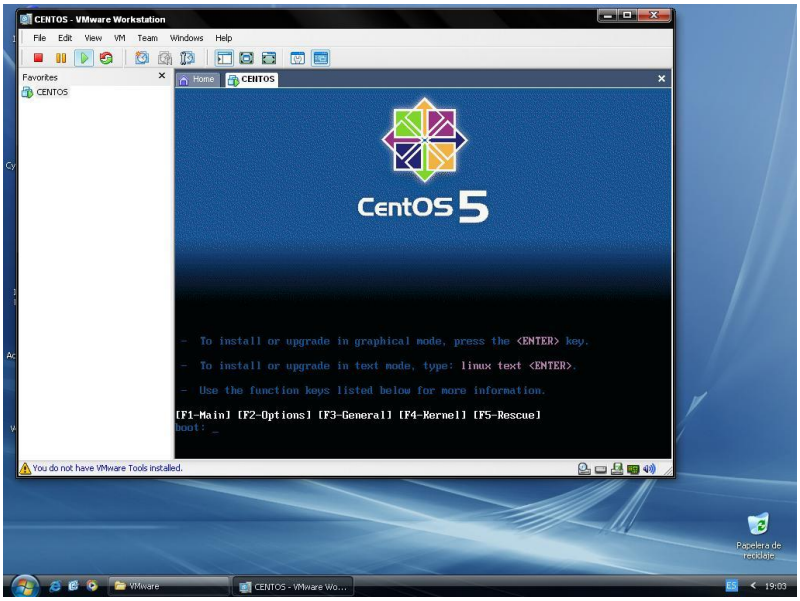

Gráfico 1.23

- Aparecerá una opción para comprobar el disco de instalación, escogemos la opción **Skip** para saltar esta comprobación.

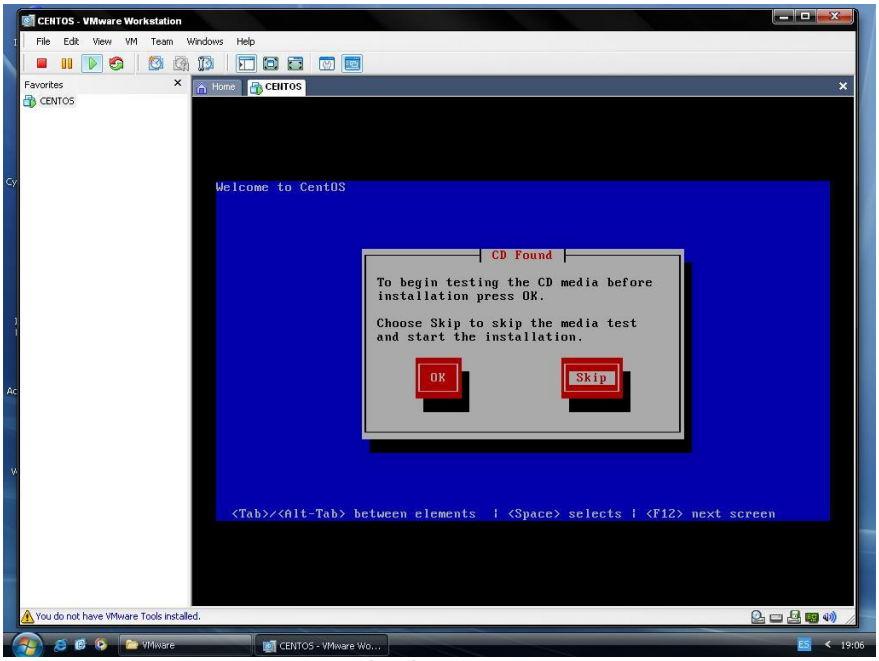

Gráfico 1.24

- Empieza la instalación escogemos la opción NEXT.

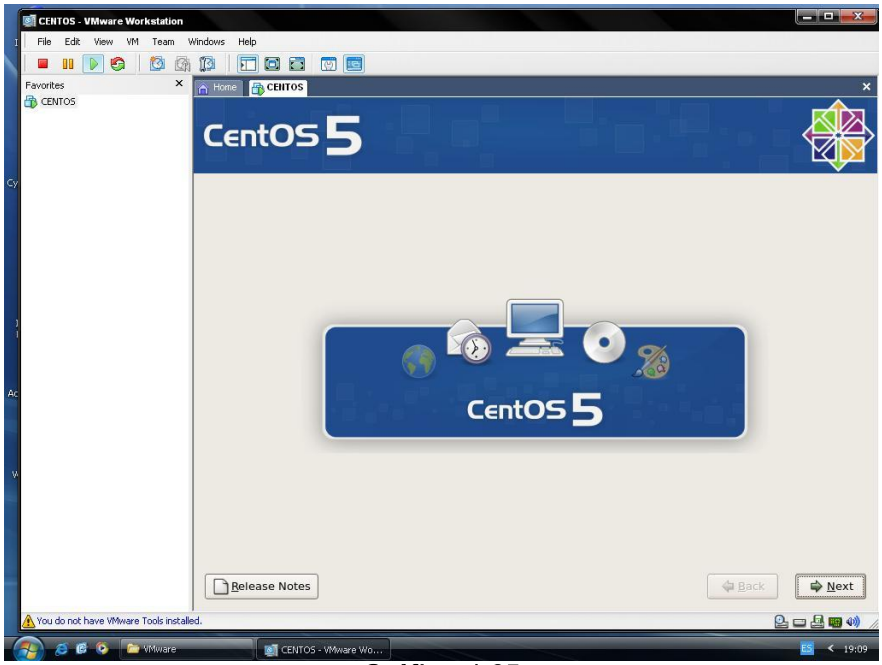

Gráfico 1.25

- Escogemos el idioma en nuestro caso Español.

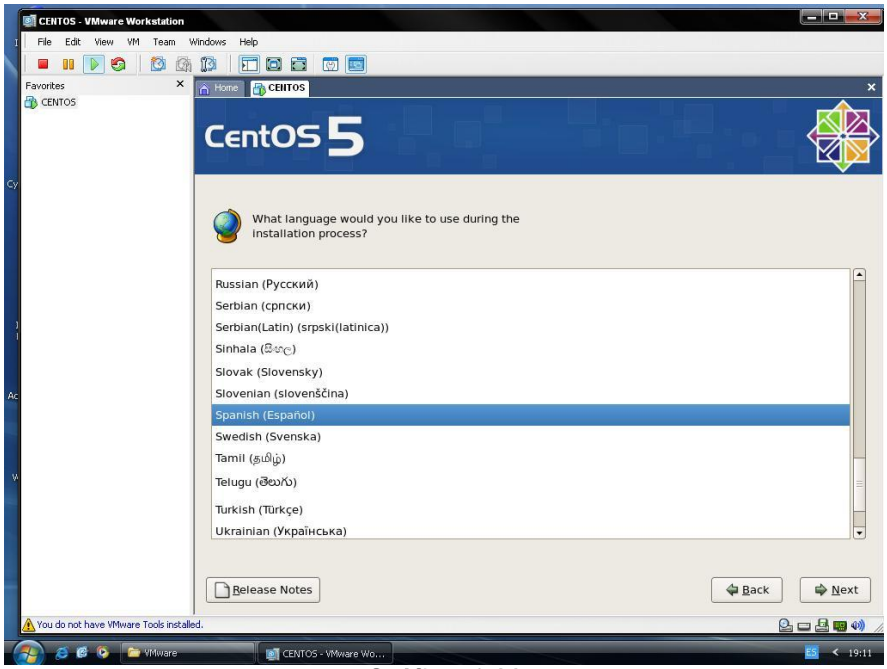

Gráfico 1.26

- Seleccionamos el idioma de teclado

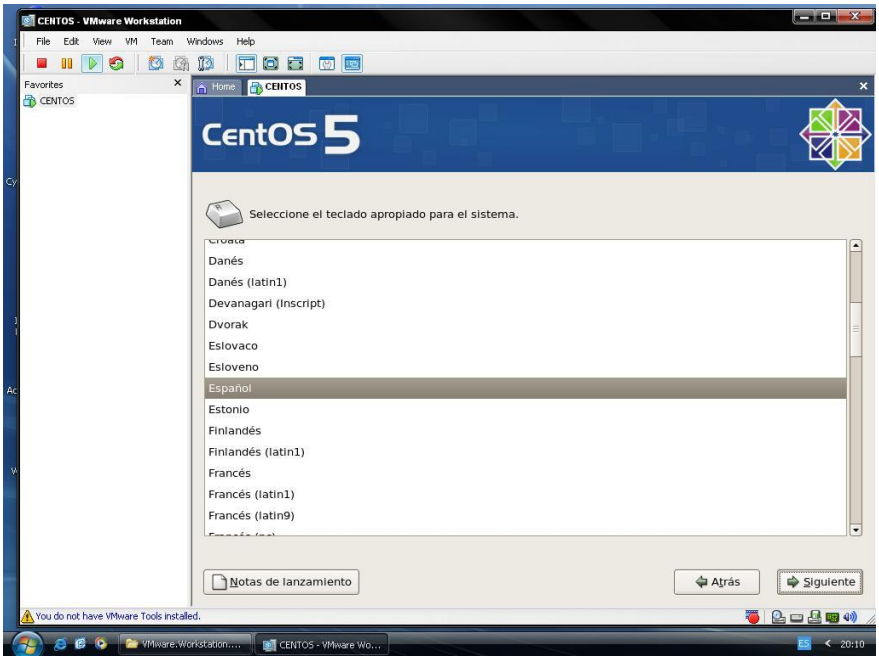

Gráfico 1.27

- Aparecerá un mensaje de error en el cual escogeremos la opción Sí

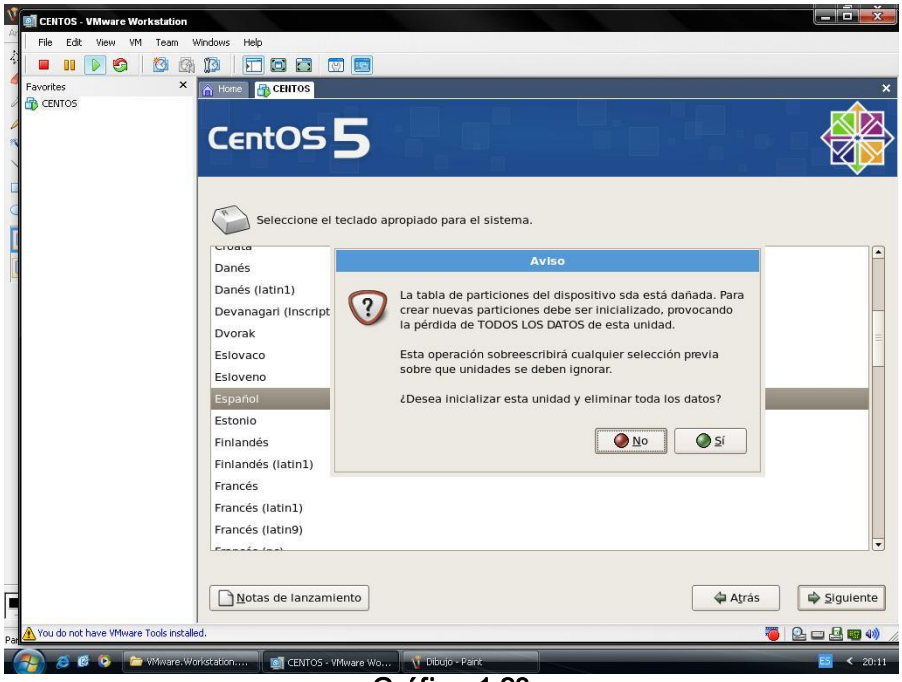

Gráfico 1.28

- En esta pantalla dejaremos las opciones tal como se muestra en el Gráfico luego escogeremos siguiente.

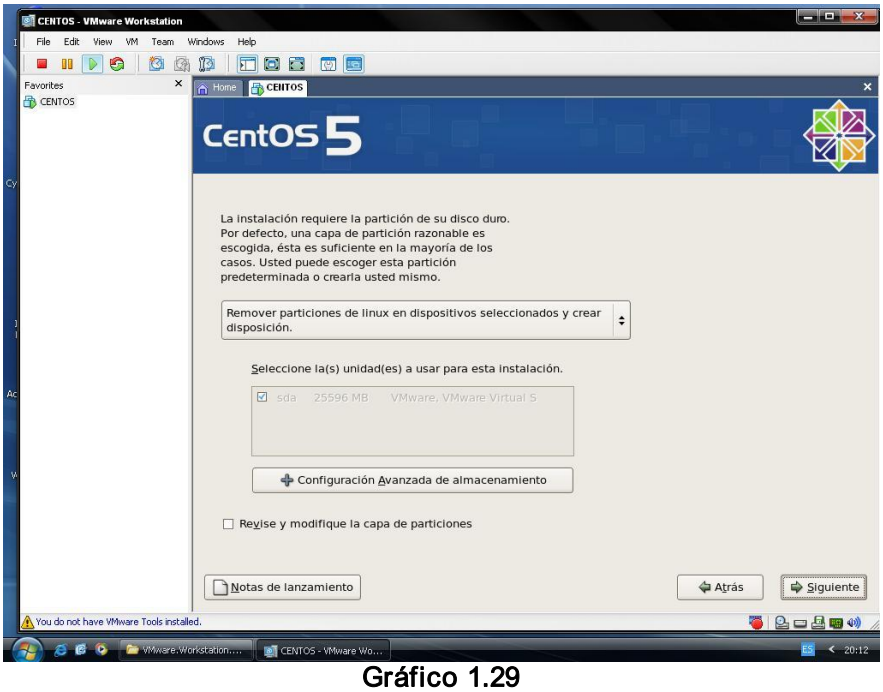

Gráfico 1.29

- Aparecerá una pantalla de aviso en la que escogeremos la opción Sí.

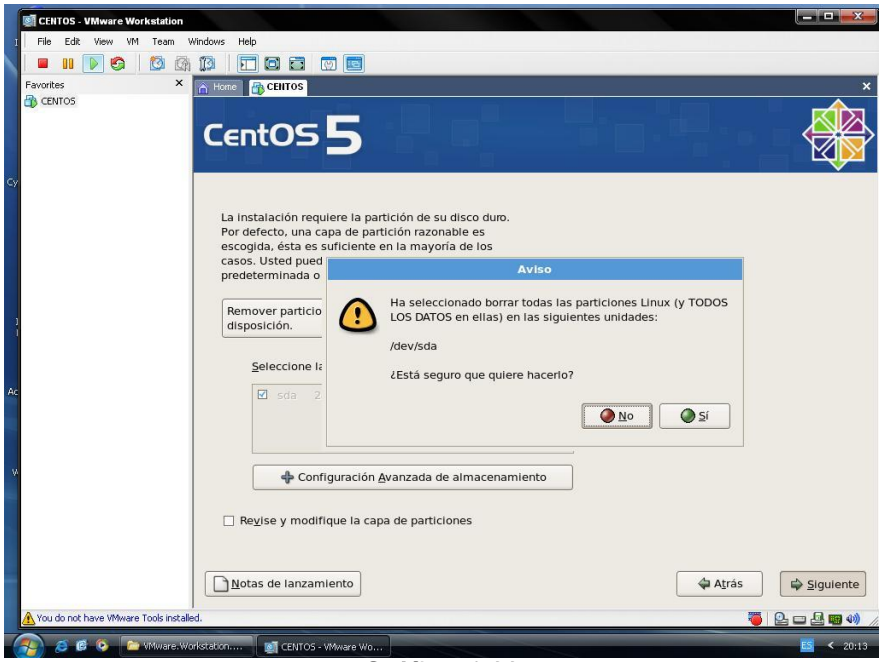

Gráfico 1.30

- En esta pantalla dejaremos las opciones tal como se encuentran y escogemos **siguiente.**

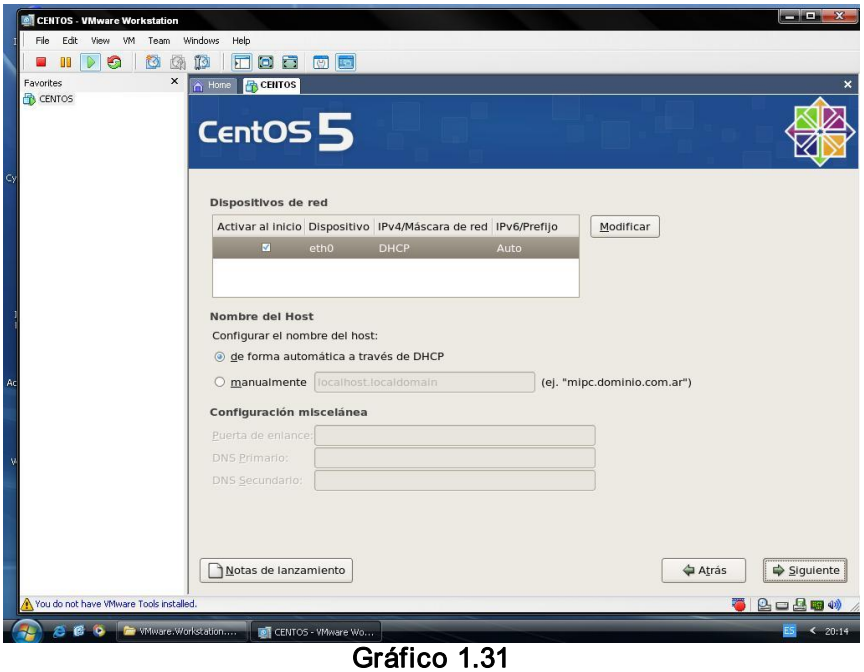

Gráfico 1.31

- Seleccionamos la región en nuestro caso América/Guayaquil

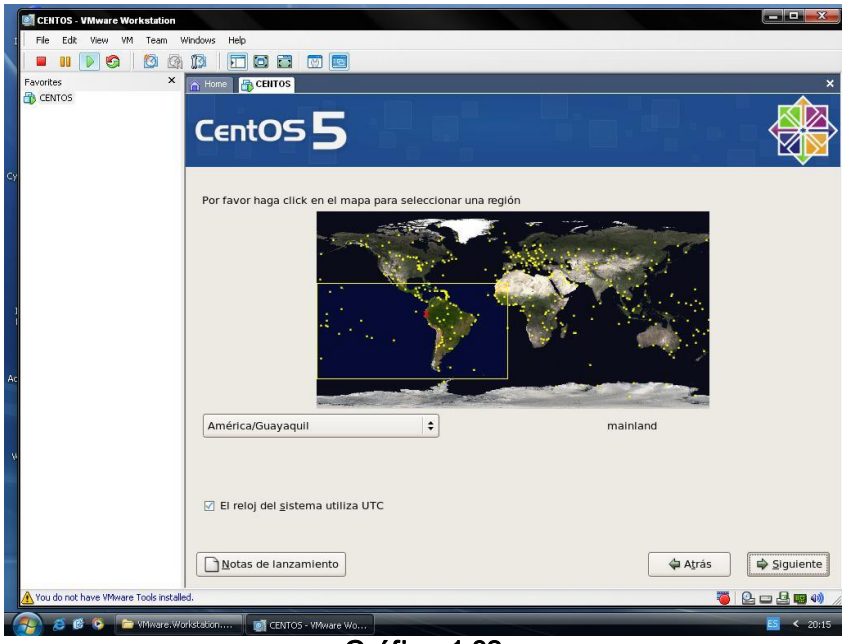

Gráfico 1.32

- Introducimos una contraseña para el usuario root. Ejemplo: root

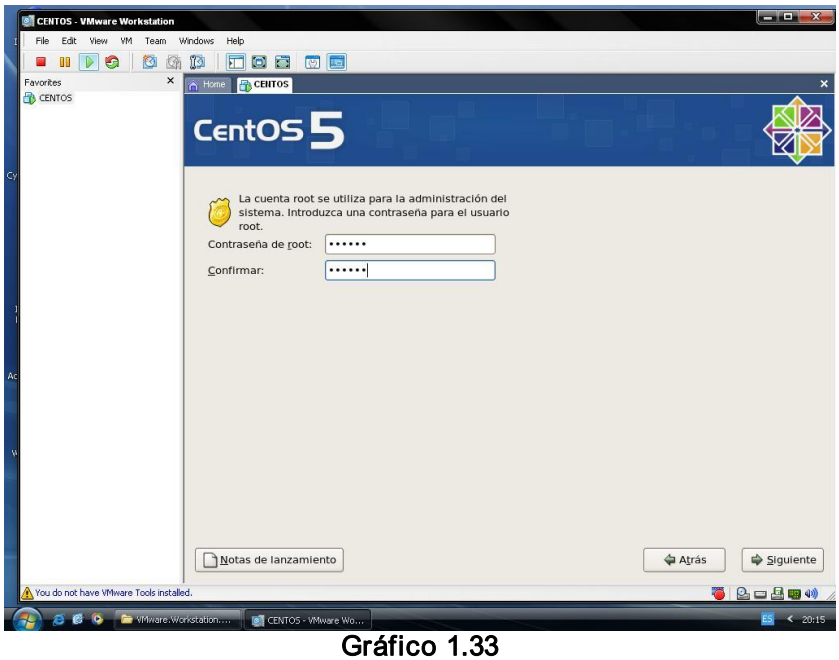

Gráfico 1.33

- En esta pantalla escogemos todas las aplicaciones para el uso de internet y escogemos la opción personalizar ahora y luego damos clic en **siguiente**.

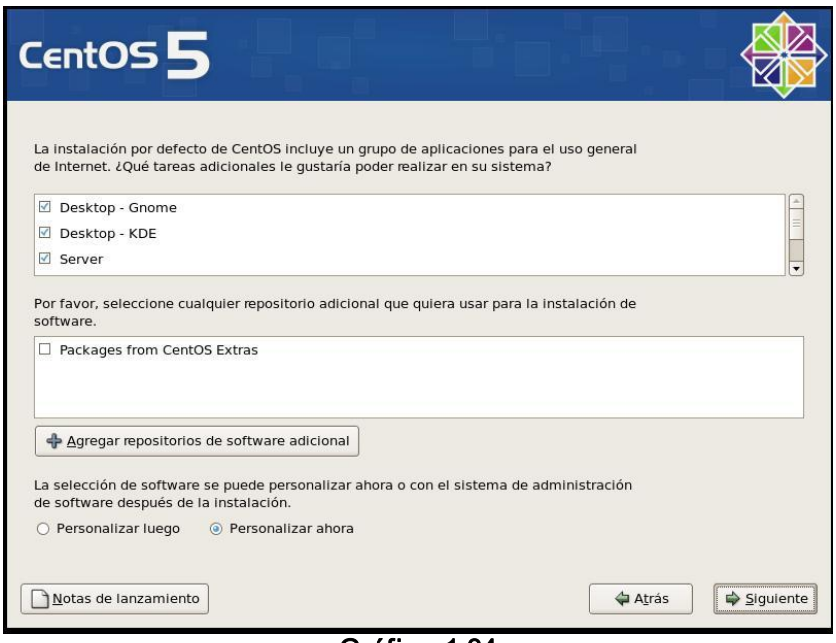

Gráfico 1.34

- En esta pantalla seleccionamos todas las opciones para cada aplicación y damos clic en siguiente.

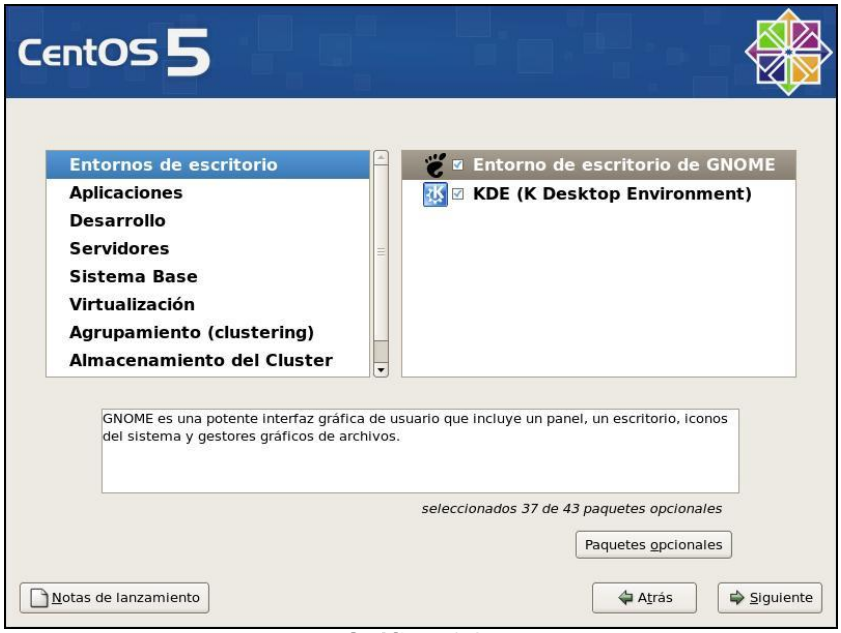

Gráfico 1.35

- En esta ventana damos clic en siguiente para iniciar la instalación.

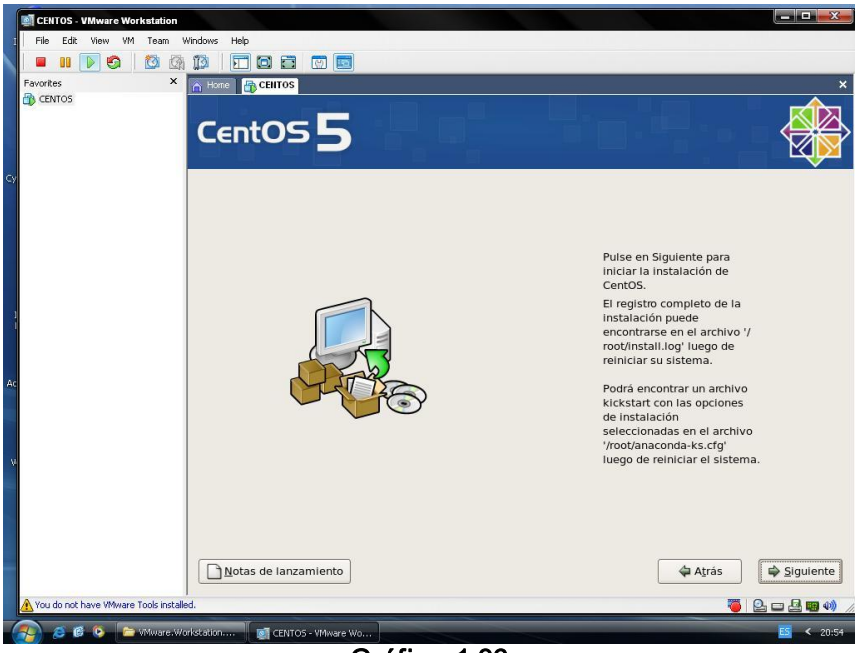

Gráfico 1.36

- Inicia la instalación

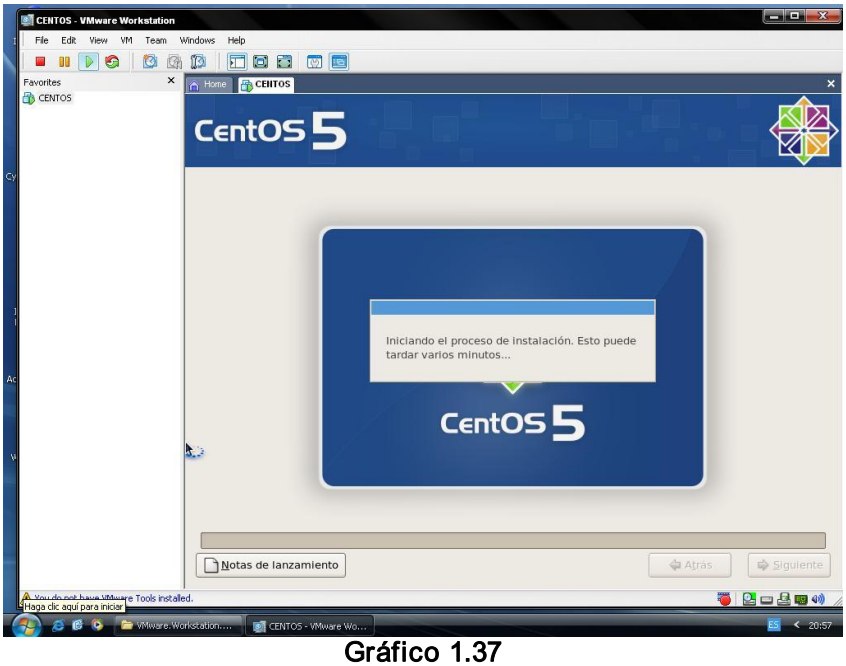

Gráfico 1.37

- Cuando finaliza la instalación escogemos la opción reiniciar

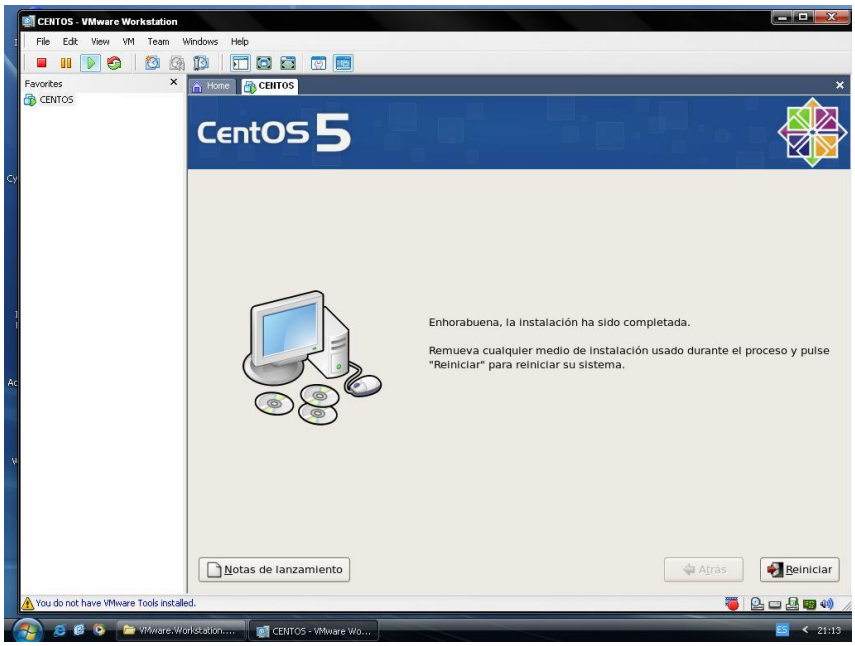

Gráfico 1.38

- Luego empieza la instalación de los últimos pasos damos clic en adelante.

Gráfico 1.39

- Luego configuramos el cortafuego y escogemos la opción deshabilitado y damos clic en adelante.

Gráfico 1.40

- Nos saldrá un mensaje en el que escogeremos la opción SI

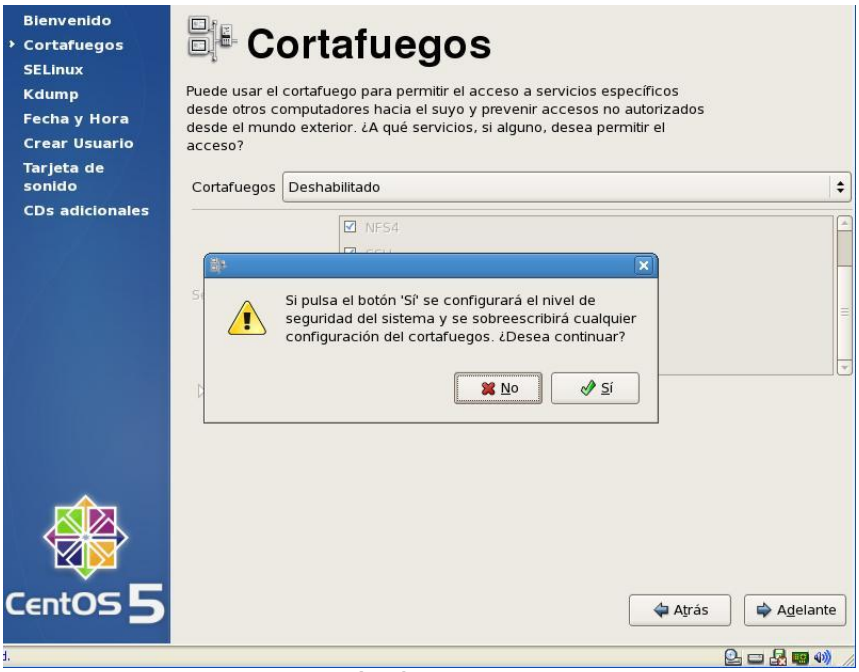

Gráfico 1.41

- Configuramos el **SELinux** como **Deshabilitado**

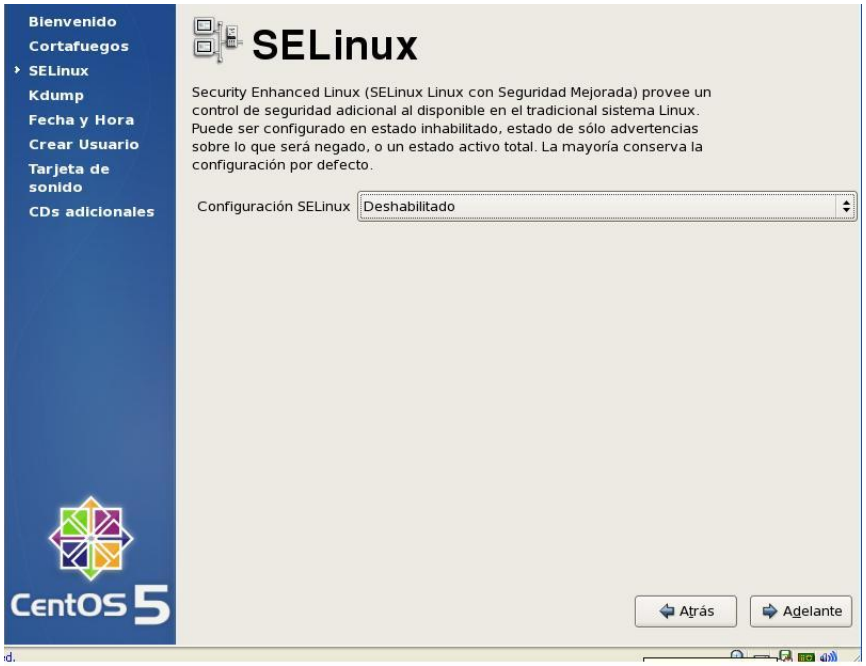

Gráfico 1.42

- En la configuración de Kdump dejamos deshabilitado el kdump.

Gráfico 1.43

- Configuramos la fecha y hora y damos clic en adelante.

Gráfico 1.44

- Configuramos el usuario y la contraseña

Gráfico 1.45

- En la configuración de la tarjeta de sonido escogemos adelante.

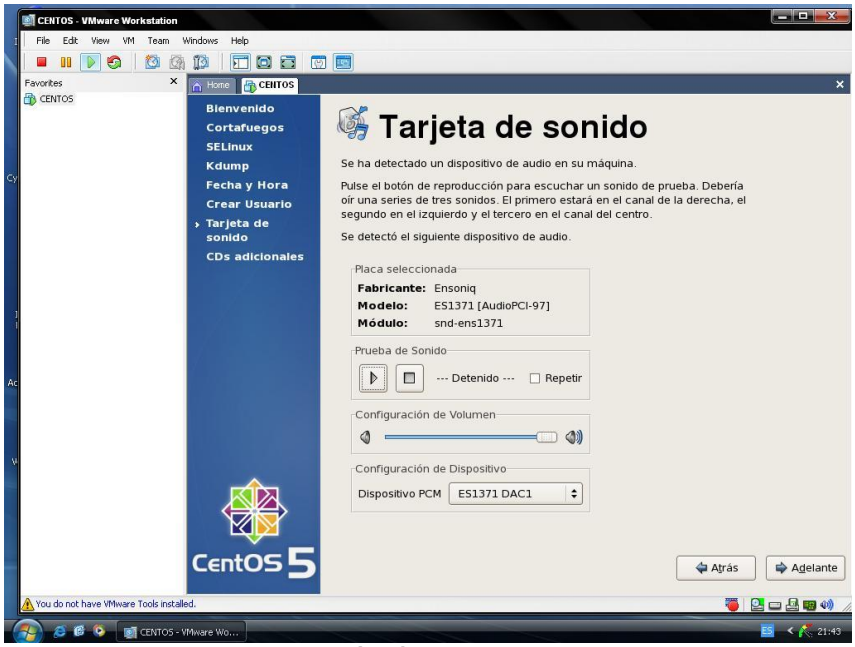

Gráfico 1.46

- Luego finalizamos la instalación.

Gráfico 1.47

- Luego aparece la ventana de inicio de sesión para poder utilizar todos los comandos iniciamos como root.

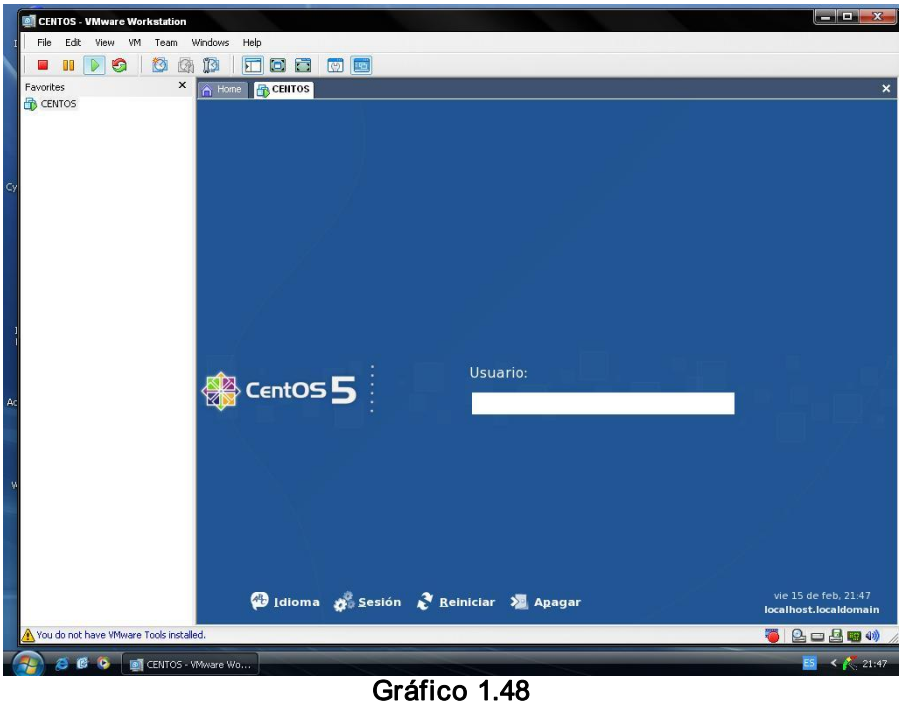

Gráfico 1.48

1.6 Conclusión:

En este capítulo se indicó paso a paso como se instalan las herramientas (software) que utilizaremos para desarrollar las prácticas, en nuestro caso usamos la Máquina Virtual VMWARE v5.5 que servirá como base para instalar el sistema operativo en nuestro caso CentOS5.

CAPITULO 2: COMANDOS BÁSICOS

2.1 Introducción

Este capítulo sirve de guía para la utilización de comandos básicos y nos servirá de mucha utilidad para la realización de todas las prácticas siguientes de configuraciones.
Con esto se pretende dar información de los comandos más utilizados en el manejo del sistema.

2.2 Primeros pasos

Antes de comenzar deberemos haber iniciado sesión como usuario root y con la contraseña que se dio en la instalación con el fin de utilizar todos los comandos.

Gráfico 2.1

Para el manejo de los comandos utilizaremos la ventana de terminal, para abrirla procederemos a dar botón derecho del ratón en el Escritorio de Linux, se desplegara un menú y escogeremos la opción **Abrir Terminal** como se muestra en el Gráfico.

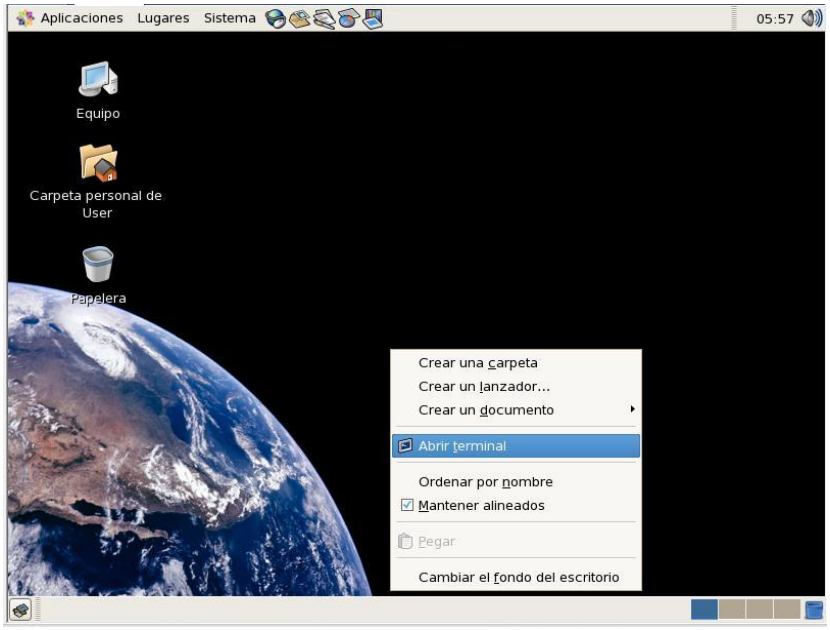

Gráfico 2.2

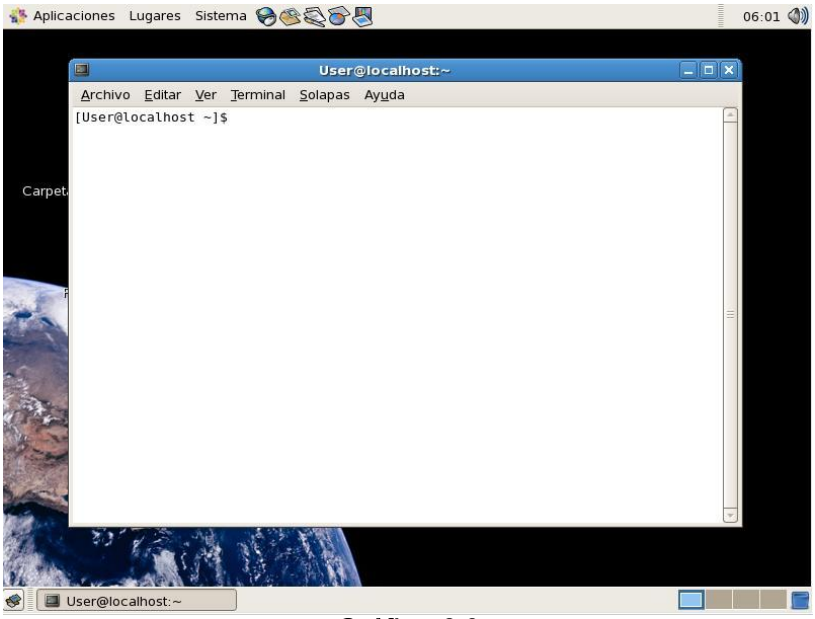

Gráfico 2.3

Nota: En la explicación de los comandos "[]" indica que son opcionales. "…" que puede ir más de una. Las opciones suelen comenzar con "-" o "—". Si en la explicación del comando se acaba con "…" es porque hay muchas más opciones o información.

2.3 Comando para ayuda

man [opciones...] página

Muestra la documentación de un determinado comando (en realidad también de cualquier documentación, no sólo comandos).

Por ejemplo “man ls” nos dará todas las opciones del comando ls.

Cada documento se denomina “página”, las páginas están divididas por “secciones”.

A veces existen páginas en secciones distintas con el mismo nombre, para especificar la sección se usa el número de ella como opción.

Por ejemplo “man 3 printf”.

“man -a printf” mostrará todas las páginas, en sucesión, de printf en todas las secciones. Si se quiere buscar.

“man -k printf” mostrará un listado resumido de todas las páginas donde aparezca printf en la descripción corta. El número mostrado entre paréntesis es la sección.

Se puede indicar que muestra la documentación en otros idiomas (si están instalados en el sistema).

Por ejemplo:
“man -L es ...” en castellano
“man -L en ...” en inglés

2.4 Comandos para manejo de archivos o directorios

ls [opciones...] [directorio/fichero ...]

Lista el contenido del directorio, sin argumentos lista el contenido del directorio actual de trabajo. La opción más habitual es “-l” que muestra información más

completa de cada directorio y fichero. La opción “-R” hace un listado recursivo en la jerarquía de directorios.

ls –l	Listado largo
ls –a	Listado de ficheros ocultos
ls –la	Listado largo con ficheros ocultos

ls –l ejemplo	Listado largo de los archivos del directorio ejemplo

pwd

Imprime el directorio actual de trabajo.

Ejemplo: pwd
Retorna: /home

cd [directorio]

Cambia de directorio. Sin argumentos lleva al directorio del usuario (HOME). Si el directorio es “..” sube un nivel.

Ejemplo: cd /home/User

mkdir [opciones...] directorio

Crea el directorio con el nombre indicado.

Ejemplo: mkdir ejemplo

vi [opciones] archivo

Es un editor de texto.

Ejemplo: vi ejemplo

Para editar el archivo presionamos “i”, para salir del modo INSERTAR presione ESC

Dentro del editor los siguientes comandos sirven para:

:w	Esto graba el contenido del archivo.

:q	Sale del editor sin grabar.
:wq	Graba el contenido y sale del editor.
:w!	Graba así no tenga permisos de escritura
:234	Va a la línea 234
u	Deshace el último cambio
x	Borra carácter bajo el cursor.
dd	Borra la línea queda guardado.
a	Inserta después del cursor
n	Repite la búsqueda
i	Inserta antes del cursor
Ctrl-f	Una pantalla adelante
Ctrl-b	Una pantalla atrás
1G	Comienzo del archivo
G	Fin del archivo
I	Insertar al principio de la línea
A	Insertar al final de la línea
:/cadena	Busca la cadena
yy	Copia una línea
P	Pega antes del cursor
p	Pega después del cursor

rm [opcions...] ficheros

Borra ficheros. Las opciones más habituales son "-f" para forzar el borrado sin preguntar al usuario (la opción contraria es "-i").

"-r" borra recursivamente todos los subdirectorios

Ejemplo: rm ejemplo

rmdir [opciones...] directorio...

Borra un o varios directorios si están vacíos.

Ejemplo: rmdir carpeta

mv [opciones...] fuente... destino

Cambia el nombre de un fichero por otro o mueve una serie de ficheros y directorios a un directorio destino.

Ejemplo: mv /home/User/ejemplo2/otro /home/User/ejemplo

El ejemplo anterior mueve el archivo **otro** que está dentro del directorio **ejemplo2** al directorio **ejemplo.**

cp [opciones...] fuente... destino

Permite copiar un fichero, o varios ficheros a un directorio. Quizás la opción más usada es "-r" que permite copiar recursivamente directorios hacia otros directorios.

Ejemplo: cp –r /home/User/ejemplo/directorio /home/User/ejemplo2

El ejemplo anterior copia el directorio llamado **"directorio"** que está dentro del directorio **ejemplo** al directorio **ejemplo2**

mcopy [opciones…] archivo a:

Copia archivos desde y hacia diskettes

Ejemplo: mcopy imagen1.jpg a:

cat [opciones...] [ficheros...]

Muestra el contenido de los ficheros por la "salida estándar". Si no se especifican ficheros, lee de la "entrada estándar".

Ejemplo: cat prueba

sort [opciones...] [ficheros...]

Imprime la concatenación ordenada lexicográficamente de los ficheros o entrada estándar. Opción "-n" ordena numéricamente.

Opción "-r" en orden inverso.

"--field-separator=SEP" hace que SEP sea el separador de campos...

Ejemplo: sort -n prueba

more [opciones...] [ficheros]

Muestra el contenido de los ficheros o la entrada estándar página a página cada 25 líneas y espera que el usuario indique las acciones a tomar. Estas acciones se suelen indicar con una tecla, por ejemplo "<ESPACIO>" es para avanzar una

página, “<ENTER>” avanza una línea. “h” da la ayuda, “/” sirve para buscar una cadena, “q” para salir...

Ejemplo: more prueba

ln [opciones] destino [nuevo_alias]

Crea un enlace a un fichero, apuntará a los mismos datos que el fichero “destino”, siempre.

La opción “-s” hace que se cree un enlace simbólico, es lo que se conoce como “Acceso Directo” en Windows, o “Enlace” en la interfaz gráfica de Macintosh.

Ejemplo: mkdir /root/enlace
ln -s /tmp /root/enlace
rm /root/enlace (Borra enlace)

wc [opciones...] [ficheros]

Indica la cantidad de caracteres, palabras y líneas que tienen los ficheros. “-l” indica sólo número de líneas, “-w” palabras y “-c” los bytes, “-m” caracteres.

Ejemplo: wc archivo.txt

1	2	6	archivo.txt
Líneas	Palabras	bytes	

du [opciones…] [ficheros]

Instrucción para ver el tamaño de archivos o carpetas

Ejemplo: du /var/spool/mail
du –sh /var muestra el tamaño total del directorio

grep

Busca cadenas dentro de archivos

Ejemplo: grep cadena *

grep –RH cadena *

-R busca en forma recursiva
-H muestra el nombre del archivo por cada coincidencia

También se puede utilizar para recuperar archivos de la siguiente forma.

grep -a -B[size before] -A[size after] 'text' /dev/[partiticion]

grep -a -B2 -A200 "hola" /dev/hda1

stat

Despliega información detallada sobre el archivo especificado como: fechas de modificación y cambio, dueño del archivo, etc.

Ejemplo: stat archivo.txt

find

Busca un archivo

Ejemplo: find / -name “nombre.txt” -print

Para localizar los ficheros secundados (S para el usuario) podemos utilizar la orden

find / -perm -4000 -type f –print

Mientras que para localizar los segundados (S para el grupo) podemos utilizar

find / -perm -2000 -type f –print

tail

Permite ver el final de un archivo, este comando es útil ya que los archivos de registros "logs" crecen constantemente tail --f /var/log/messages

tail --f --line 15 /var/log/messages

Este comando anterior despliega las ultimas 15 líneas del archivo messages (el default es de 10). La --f mantiene el archivo abierto para poder observarlo conforme se agregan eventos.

which

Ve el path de cualquier programa o comando

Ejemplo: which awk
/bin/awk

2.5 Comandos para el manejo de usuarios y grupos

useradd [opciones…] [LOGIN]

Instrucción para crear un usuario

Ejemplo: useradd -c "Antonio Alonso Martinez" -d /home/aalonso -g mail -m aalonso

usermod [opciones…] [LOGIN]

Modifica a un usuario.

Ejemplo: usermod –g apache aalonso

userdel [opciones…] [LOGIN]

Instrucción para borrar usuarios.

Ejemplo: userdel –r aalonso

passwd

Instrucción para cambiar de password a un usuario

finger

Muestra información sobre el usuario

Ejemplo: finger usuario

groupadd

Crea un nuevo grupo

groupdel

Borra un grupo

gpasswd

Asignación de usuarios existentes a grupos existentes.

Ejemplo: gpasswd -a usuario-que-sea grupo-que-sea

Chgrp

Cambia el grupo al cual pertenece un archivo o directorio

chgrp –R actúa en forma recursiva

chown

Cambia el usuario al cual pertenece un archive o directorio

chown –R actúa en forma recursiva

history

Lista los últimos comandos utilizados por el usuario

En la carpeta del usuario el archivo donde se almacena es .bash_history

echo $HISTFILE variable donde se almacena el archivo que utiliza history

su

Permite cambiarse de usuario sin salirse del usuario actual. Para salir del usuario se digita la palabra exit.

sudo

Permite ejecutar un comando como si fuera otro usuario. Ejemplo:

sudo –u root vi /etc/passwd

who

Muestra los usuarios de sistema que han iniciado una sesión

2.6 Comando para configurar permisos de acceso a los ficheros

chmod

Cambia los permisos de acceso de ficheros

0 = sin permisos.

1 = ejecución.

2 = escritura.

3 = escritura y ejecución.

4 = lectura.

5 = lectura y ejecución.

6 = lectura y escritura.

7 = lectura, escritura y ejecución.

Octal	Binario		Permisos
0	000	- - -	ninguno
1	001	- - x	ejecución
2	010	- w -	escritura
3	011	- w x	escritura y ejecución
4	100	r - -	lectura
5	101	r – x	lectura y ejecución
6	110	r w -	lectura y escritura
7	111	r w x	lectura, escritura y ejecución

Ejemplo: chmod 751 texto.txt

Permisos: Usuario => 111 => r w x
Grupo => 101 => r - x
Otros => 001 => - - x

Clases de usuarios:
u => usuario propietario
g => grupo
o => otros

Cambiar permisos

Modo absoluto
chmod 652 notas => r w - r - x - w -

Se ejecuta con los permisos del propietario del archivo

chmod -s Desactiva

chmod u+s Usuario
chmod g+s Grupo
Chmod 644 nombre_ archivo

Hace que "nombre_ archivo" sea de lectura / escritura para el propietario, de lectura para los demás.
(Octal modo).

Chmod 444 nombre_archivo
Hace "nombre_archivo" sólo lectura para todos.
Modificación del archivo (por ejemplo, con un editor de texto)
+ No permitido para un usuario que no tiene la propiedad, el archivo (con excepción de raíz)
+ E incluso el dueño del archivo tiene a la fuerza que salvar el archivo
+ Si modifica el archivo.
Igual restricciones se aplican para suprimir el archivo.

Chmod 1777 directorio-nombre

Da a todos permisos de leer, escribir y ejecutar el permiso en el directorio,
+ Sin embargo también establece el "sticky bit".
Esto significa que sólo el propietario del directorio,
+ Propietario del archivo, y, por supuesto, la raíz
+ Puede borrar cualquier archivo en ese directorio.

Chmod 111 directorio-nombre
Da permisos de ejecutar a todos en un directorio.
Esto significa que puede ejecutar archivos de la LEA y en ese directorio
+ (Ejecutar permiso incluye necesariamente permiso de lectura
+ Porque no se puede ejecutar un archivo sin que se pueda leerlo).
Pero no se puede listar los archivos o la búsqueda de ellos con la "encontrar".
Estas restricciones no se aplican a la raíz.

Chmod 000 directorio-nombre
No en todos los permisos de ese directorio.
No se puede leer, escribir o ejecutar archivos en el mismo.
No se puede siquiera en la lista de archivos o "cd" a la misma.

Sin embargo, puede cambiar el nombre (mv), el directorio
+ O eliminarla (rmdir) si está vacío.
También puede enlace a los archivos en el directorio,
+, Pero no puede leer, escribir o ejecutar los enlaces simbólicos.
Estas restricciones no se aplican a la raíz.

2.7 Comandos para el manejo del FILE SYSTEM

lsattr

Lista atributos de file system ext3

chattr

Modifica los atributos de file system ext3

chattr +a fichero	a modo solo de añadir del fichero
chattr +Ss fichero	i no permite hacer cambios al fichero o borrarlo
chattr -sa fichero	-R actua en forma recursiva s cuando se borra el archivo con atributo s el sistema rellena con ceros el contenido del archivo S hace que los cambios sobre el archivo se escriban inmediatamente en el disco en lugar de esperar el sync del sistema operativo

2.8 Comandos para el manejo de procesos en el sistema

ps

Muestra los procesos que se están ejecutando en el sistema.

Ejemplos:

ps –aux
Para encontrar la cantidad de procesos de bash:
ps -A | grep bash | wc -l (esto demostrará la cantidad de procesos)

ps	muestra los procesos del usuario actual
ps –a	muestra los procesos de todos los usuarios

ps –A muestra los procesos de todo el sistema incluido la de todos los usuarios

ps –x muestra los procesos que no estén ligados a una tty

ps –l muestra los procesos según su prioridad columna PRI el valor mas elevado de PRI es el que tiene menos prioridad

kill

Elimina un proceso dándole el número de proceso.

Ejemplo: kill -9 8909

Killall

Elimina un proceso dándole el nombre

Ejemplo: killall gateway

2.9 Comandos para el manejo de puertos servicios de correo, servicios de red e internet.

Service

Instrucción para arrancar, apagar o restart un servicio.

service httpd start

Netstat

Para ver el servicio ligado al puerto es:

Ejemplos: netstat –ltunp o sino tambien

netstat –pel

netstat –anp |grep 953

Usted puede encontrar la cantidad de conexiones a Apache con este comando:

netstat -nt | grep :80 | wc -l

l : muestra todos los puertos que están en modo listen.

t : muestra todos los tcp.

u : muestra todos los udp

n : no resuelve nombres.
p : muestra el PID y el nombre asociado
e : muestra información extendida
a : los puertos que están esperando conexión

netstat –i da la estadísticas de las interfaces
netstat –ta muestra todas las conexiones activas

Archivo donde están todos los puertos conocidos con el nombre del servicio /etc/services.

Ifconfig

Configura la tarjeta de red

Ejemplo:

ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up
ifconfig –a consulta la configuración actual

Para cambiar direccion mac en Linux ath0=Wireless eth0= Ethernet

ifconfig eth0 down
ifconfig eth0 hw ether 00:11:22:33:44:55
ifconfig eth0 up

También se puede poner los gateways editando los siguientes archivos según las tarjetas que tenga

/etc/sysconfig/network-scripts/ ifcfg-eth0
/etc/sysconfig/network-scripts/ ifcfg-eth0:1
/etc/sysconfig/network-scripts/ ifcfg-eth1
/etc/sysconfig/network-scripts/ ifcfg-eth1:1
/etc/sysconfig/network-scripts/ ifcfg-eth1:2
/etc/sysconfig/network-scripts/ ifcfg-eth1:3
Ejemplo del contenido de un archive ifcfg-eth0

GATEWAY=192.188.47.3

BOOTPROTO=none
TYPE=Ethernet
HWADDR=00:0D:60:EB:BF:AA
DEVICE=eth0
NETMASK=255.255.255.0
BROADCAST=192.188.47.255
IPADDR=192.188.47.2
NETWORK=192.188.47.0
ONBOOT=yes
USERCTL=no
IPV6INIT=no
PEERDNS=yes

Ifup

Habilita la interfase especificada

Ejemplo: ifup eth0

Ifdown

Deshabilita la interface especificada

Ejemplo: ifdown eth0

route

Configura el gateway del equipo o las rutas del equipo.

Ejemplo: route muestra las rutas actuales
route add default gw 192.168.0.1 añade una ruta
route del default gw 192.168.0.1 borra una ruta

Para guiar toda la información de la red 206.171.55.16 netmask 255.255.255.240 vía la interfase eth0
route add -net 206.171.55.16 255.255.255.240 eth0

Ping

Envía un paquete a un host y este le responde si esta activo y el tiempo que se demoro.

Ejemplo: ping -l 65000 127.0.0.1 -i 0
ping -l 65527 127.0.0.1

-i Específica cada cuántos segundos hace el ping el valor máximo es 255
-l Especifica la longitud, en bytes, del campo Datos del mensaje de solicitud de eco enviado. El valor predeterminado es 32. El tamaño máximo es 65.527.

Traceroute

Ve por que servidores pasa la señal hasta llegar a un servidor determinado. El número de saltos máximo es de 30. Los tres tiempos son el tiempo de respuesta para los paquetes enviados. En la dirección http://www.mapulator.com/ se puede encontrar un traceroute gráfico que indica el país de ubicación del equipo. Otra página en donde están algunas utilidades incluida traceroute es http://www.dnsstuff.com/

traceroute www.google.com

nslookup

Cuando un sitio Web no se puede visualizar, no tiene porque estar caído, puede ser que los servidores DNS que se este usando no estén funcionando correctamente para ese dominio. Se puede comprobar si un DNS resuelve bien la IP de un servidor mediante el comando llamado “nslookup“que existe tanto en unix como en Windows.

nslookup www.google.com 157.100.1.2 el primer parámetro es el sitio Web que se quiere ver cual es la IP, el segundo parámetro es el servidor DNS a quien se le pregunta.

Se puede entrar a modo interactivo digitando nslookup sin ninguna opción y allí se puede optar por preguntas mas especificas con el subcomandos set q=

Set q=a	Especifica la dirección IP un equipo.
Set q=ANY	Especifica todos los tipos de datos.
Set q=CNAME	Especifica un nombre canónico para un alias.
Set q=MX	Especifica el intercambiador de correo.
Set q=TXT	Especifica la información de texto.

Set q=ns Especifica registros de nombres de servidores (NS)

Con el subcomando Server se especifica el servidor al cual se quiere preguntar ejemplo Server 157.100.1.2. Para salir del modo interactivo se escribe la instrucción exit.
Ejercicio para ver cómo funcionan los DNS resolviendo el dominio uazuay.edu.ec

nslookup
server c.root-servers.net. (Pregunta al servidor raíz)
set q=ns
ec.
server dns1.nic.ec
edu.ec.
server dns2.nic.ec
uazuay.edu.ec.
server gye2.satnet.net.
set q=any
uazuay.edu.ec

Una actualización del archivo de los servidores raíz se la encuentra en ftp://ftp.internic.net/domain/named.cache este archivo se lo coloca en /var/named/named.ca

Dig

Igual que nslookup

Host

Igual que nslookup

mail

Envía un correo electrónico

mail jleon@yahoo.com
Subject: Asunto
Cuerpo del mensaje
. --> para salir se pone punto y se da un enter
Cc: copias

mail –v jleon@yahoo.com (muestra detalles de como resuelve el mail)

mail jleon@yahoo.com < archivo.txt envía un archivo por mail

mail	si se ejecuta solo el comando mail este lee el archivo de mails
	los comandos mas usados en este entorno son:
h	lista los mail
h60	comienza el listado de mails desde el mail 60
60	lee el mail 60
z	pasa a la siguiente página
d1	borra el mail 1
d1-10	borra los mail desde el 1 hasta el 10
x	sale grabando los cambios
q	sale sin grabar los cambios

mailq

Muestra los mails encolados

ftp

Cliente para la transferencia de archivos

Ejemplo: ftp 162.168.0.1

Comandos más utilizados

ascii	para transferencia en modo ASCII
binary	para transferencia en modo binario
dir	para ver el contenido de una carpeta
get	transfiere un archivo de la maquina remota a la local
mget	transfiere un varios archivos (*) de la maquina remota a la local
mput	transfiere un varios archivos (*) de la maquina local a la remota
mkdir	crea un directorio en la maquina remota
put	transfiere un archivo de la maquina local a la remota
pwd	muestra el path actual
quit	sale

telnet

Cliente para conexión remota

Ejemplo: telnet 162.168.0.0.1

Ssh

Cliente para conexión remota encriptada

Ejemplo: ssh jleon@168.0.0.1

sftp

Cliente para conexión remota de ftp encriptada

Ejemplo: sftp jleon@168.0.0.1

hostname

Muestra o cambia el nombre del equipo.

hostname	para mostrar el nombre del equipo
hostname otronombre	para cambiar el nombre del equipo

nmap

Herramienta para exploración de red y scanner de seguridad. El archivo donde se pueden encontrar los servicios conocidos y sus puertos son /etc/services

Modo detallado

nmap –v 127.0.0.1

Lanza un sondeo de tipo SYN (envia un paquete como si fuera un conexión real y espera la respuesta) sigiloso contra cada una de las 255 máquinas en la “clase C” de la red donde está el sistema "scanme.namp.org". También intenta determinar cual es el sistema operativo que se ejecuta en cada máquina que esté encendida (Opcion O).

nmap -sS -O scanme.nmap.org/24

Ve la versión del servicio (-sV) que se esta ejecutando en los puertos (-p) 22,53,110,143,4564 (22 sshd, 53 DNS, 110 pop3, 143 imap) desde la red 198.116.0 hasta la red 198.116.255 pero solo los 127 primeras direcciones ip

nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127
analiza la red 216.163.128.20/20 (4096 ips) sin enviar ping (-P0) para descubrir si esta activo el equipo y los resultados los graba en formato xml (-oX) y tambien en formato txt (-oG)

nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20

Para conocer el sistema operativo (-O) que se esta ejecutando en 127.0.0.1

nmap -O 127.0.0.1

Para ver cuales hosts estan activos en la red 192.168.0.0 mediante ping (-sP)

nmap -sP 192.168.0.1-255

iptraf

Muestra en aplicación de consola la cual analiza todo el tráfico de red IP, UDP, ICMP.
Permite utilizar filtros, y es muy útil para diagnostico y depuración de errores de red

Tcpdump

Herramienta para análisis de tráfico de red

wget

wget es una herramienta de Software Libre que permite la descarga de contenidos desde servidores web de una forma simple. Su nombre deriva de «World Wide Web» (w), y de «obtener» (get), esto quiere decir: obtener desde WWW. Actualmente soporta descargas mediante los protocolos HTTP, HTTPS y FTP.

wget http://www.mat.univie.ac.at/~flo/linux/dsniff-2.4b1-11.i386.rpm (programa que las claves de los accesos al servidor)

wget http://easynews.dl.sourceforge.net/sourceforge/webadmin/webmin-1.290-1.noarch.rpm (administrator de Linux median interface web)

chkconfig

chkconfig sendmail off

chkconfig --level 2345 MailScanner on

chkconfig --list sendmail

sendmail 0:desactivado 1:desactivado 2:desactivado 3:activado 4:desactivado 5:desactivado 6:desactivado Muestra en que nivel esta activado o desactivado sendmail

lynx

Navegador de Texto el gráfico es htmlview

lynk www.google.com

2.10 Comandos para el manejo del disco duro

df

Muestra el espacio en disco disponible.

Ejemplo: df, df –h

-h añade un letra indicativa para el tamaño

Si no se pone ninguna opción las unidades son de 1024 bytes

fdisk

Crea tabla de particiones

fdisk –l para ver las particiones

fdisk /dev/hda para particionar el primer disco IDE

mount

Monta unidades de disco duro, diskette, cdrom.

mount /dev/hda /media/cdrom

El archivo del sistema donde están las unidades que se montan cuando se inicia el servidor es /etc/fstab

Para montar un archivo iso en la carpeta /centos para ver o copiar su contenido
mount -t iso9660 -o ro,loop=/dev/loop0 /var/CentOS-5.0-i386-bin-1of6.iso /centos

Para montar un USB
mount -t vfat/dev/sda /usb

umount

Desmonta unidades.

Ejemplo: umount /dev/hda

fsck

File system check es una herramienta que revisa el disco duro y repara la estructura de ficheros dañada. Para revisar la estructura de un disco primero hay que desmontarlo

fsck –y /dev/hda1
fsck –y /dev/sda1

La opción –y indica a fsck que responda "sí" a todas sus preguntas sobre arreglos, reparaciones o copias de seguridad de la información.

hdparm

Ve el rendimiento del disco duro

Ejemplo: hdparm -tT /dev/hda
hdparm -tT /dev/sda3
hdparm -tT /dev/sda1

-T para ver los tiempos de lectura del cache
-t para ver los tiempos de lectura del disco

badblocks

Descubre los sectores malos de un disco y los graba a un archivo ejemplo:

badblocks -v /dev/hda1 > bad luego se puede formatear el disco indicándole cuales son los sectores malos de la siguiente manera:

mkfs.vfat -F 32 -l bad /dev/hda1 para fat32
mkfs.ext3 -l bad /dev/hda1 para ext3

También se pueden ver los sectores malos con fsck -f /dev/hda1

2.11 Comandos para el empaquetar o comprimir archivos

tar

El programa tar es usado para almacenar archivos y directorios en un solo archivo que por lo general tiene la extensión tar. Si utiliza ampliamente en el respaldo de archivos.

Instrucciones para empaquetar y desempaquetar

tar -cvf nombre_del_archivo.tar directorio
tar –xvf nombre_del_archivo.tar

Si se quiere hacer con gzip para empaquetarlo y comprimirlo habría que poner:
tar cfvz nombre_del_archivo.tar.gz directorio

Ahora para desempaquetarlo y descomprimirlo se haría de la siguiente forma:
tar- xfvz nombre_del_archivo.tar.gz

Ahora para hacer lo mismo pero comprimiéndolo con bzip2 habría que poner:
tar -jfvc nombre_del_archivo.tar.bz2 directorio

Ahora para desempaquetarlo y descomprimirlo se pondría:
tar -jfvx nombre_del_archivo.tar.bz2

gzip

Comprime archivos.
Ejemplo: gzip install.log producirá un archivo llamado install.log.gz

gunzip

Desempaqueta paquetes en formato gz.

Ejemplo: gunzip install.log.gz

unzip

Desempaqueta paquetes en formato zip.

Ejemplo: unzip install.zip

2.12 Comandos para el manejo de fecha y hora del sistema

uptime

Muestra la hora actual, tiempo que lleva el sistema corriendo desde el último "reboot", usuarios conectados al servidor, carga del sistema en los últimos 1,5 y 15 minutos.

date

Muestra o configura la fecha y hora del sistema.

vie sep 1 11:13:24 ECT 2006

date 010102022005 el formato es MMDDhhmmYYYY

2.13 Comandos para la configuración del sistema

set

Muestra todas las variables de entorno y sus valores

JAVA=”/etc/jdsk”

export JAVA

JAVA_HOME="/usr/java/jdk1.5.0_04"

export JAVA_HOME

init

Instrucción que vuelve a leer los parámetros que se encuentran en /etc/inittab.

init 0 apaga el equipo

Niveles en Linux

Archivo /etc/inittab

0 – apaga el equipo
1 – modo monousuario
2 – modo multiusuario sin NFS sin red
3 – modo multiusuario con red
4 – no usado
5 - X11 ambiente gráfico
6 – reboot del equipo

ntsysv

Ambiente para manejo de los programas que se quieren cargar cuando se inicia el equipo.

Para cargar algo cuando arranque el servidor lo que se quiere que arranque se pone en el archivo /etc/rc.d/rc.local

setup

Ambiente para configuración del equipo.

Free

Ve la memoria Libre.

free –m

-m para que muestre en megas

Top

Monitorea el sistema.

vmstat

Es muy similar a top ya que es un condensado de los procesos del sistema, para que esta herramienta se vuelva dinámica se deben especificar los argumentos: vmstat -n <numero de segundos por actualización> vmstat -n 1

uname

Muestra información del sistema.

uname –a muestra toda la información del sistema

Linux uazuay 2.6.9-34.ELsmp #1 SMP Wed Mar 8 00:27:03 CST 2006 i686 i386 GNU/Linux

i686 (Pentium Pro, Pentium II, Pentium III, Celeron, Xeon, Pentium 4, Pentium M, Pentium D, Pentium Extreme Edition, Core, Core 2)

reset

Reinicia el equipo.

poweroff

Apaga el equipo.

2.14 Comandos para el manejo de paquetes

rpm

Package Manage originalmente llamado Red Hat Package Manager es una herramienta de administración de paquetes pensada básicamente para Linux. Es capaz de instalar, actualizar, desinstalar, verificar y solicitar programas. RPM es el formato de paquete de partida del Linux Standard Base.

rpm –e sendmail	elimina el paquete sendmail
rpm -q sendmail	pregunta por el paquete sendmail
rpm –qa	lista los paquetes instalados
rpm -ivh bindd.rpm	instala el paquete bind
rpm –Uvh bindd.rpm	actualiza el paquete bind
rpm --test -i bind.rpm	realiza un test par aver si puede instalar el paquete
rpm –ql sendmail	lista el contenido del paquete sendmail
rpm -qf /bin/ls	muestra que paquete instalo el comando ls
rpm –V sendmail	verifica paquete

i	instala
U	actualiza
e	borra
q	query

v muestra información de progreso de instalación
h muestra información mas detallada se usa con v
V verifica un paquete

2.15 Comandos para el manejo de parches

Diff

Busca diferencias entre dos archivos. Se lo utiliza comúnmente para generar parches para los programas Ejemplo:
diff -Naur archivo_original archivo_cambiado > parche.diff

patch

Aplica parches generados con diff a un programa fuente. Ejemplo:
patch archivo_a_parchear parche.diff

2.16 Programas y lenguajes de programación

md5sum

Md5sum es un programa para comprobar y crear archivos MD5. MD5 es un algoritmo que se suele utilizar para realizar la comprobación de la integridad de ficheros binarios, siendo muy utilizado, para por ejemplo, la posterior verificación de imágenes ISO o programas descargados de Internet. Ejemplo:

Para generar un archivo con la cadena md5 de verificación.

md5sum linux.iso > archivo.md5

Para verificar el archivo bajado con un archivo que tiene la cadena md5 del archivo

md5sum –c archivo.md5

Awk

Es un lenguaje de programación diseñado para procesar datos basados en texto, ya sean ficheros o flujos de datos. El nombre AWK deriva de los apellidos de los autores: Alfred V. Aho, Peter J. Weinberger, y Brian W. Kernighan.

```
awk -F: '{print "useradd -c \""$5"\" -d /home/"$1" -g mail -m "$1}' passwd > cuentas2.sh
awk -F: '{ if ($8<12960) if (length($8)!=0)  print "userdel -r "$1;}' /etc/shadow > borrar.sh

find  -name "openwebmailrc" -print > lista.txt
awk '{print "rm -f " $0}' lista.txt > borra.sh
awk '{if (length($0) > 0) print $0}' alumnos.csv > alumnos2.csv
```

Webmin

Webmin es un programa desarrollado en perl que permite administrar sistemas Unix mediante una interfase Web. La página web de webmin es http://www.webmin.com/ soporta varios sistemas operativos basados en Unix y entre esos Centos. Para instalarlo se baja el paquete http://prdownloads.sourceforge.net/webadmin/webmin-1.290-1.noarch.rpm y se instala con la instrucción rpm –ivh webmin*.rpm. Para ingresar a la interfase de webmin se va a un navegador o browser y se pone http://127.0.0.1:10000

Para asegurar el acceso hacia Webmin se instala la librería de perl http://www.uazuay.edu.ec/linux/Net_SSLeay.pm-1.30.tar.gz (Net::SSLeay) que nos permitirá conectarnos hacia la interfase Web mediante el protocolo https. Si se utiliza webmin para instalar esta librería se debe elegir construir e instalar y no construir, verificar e instalar.

Luego de instalar la librería se va al icono de Webmin luego Configuración de Webmin y finalmente a Encriptación SSL. Se activan las siguientes opciones:

¿Habilitar SSL si está disponible? Si
¿Redireccionar peticiones no SSL al modo SSL? Si
Y se graban los cambios

Como siguiente paso se procede a configurar los controles de acceso en Webmin, Configuración de Webmin, Control de Acceso a IP, se escoge la opción Sólo permitir desde las direcciones listadas y en el recuadro de a lado se colocan las IPS desde las cuales se puede conectar hacia Webmin. En este listado se debe aumentar la IP 127.0.0.1 al listado si se necesita conectarse a webmin desde el mismo servidor donde está instalado Webmin

2.17 Ejercicios prácticos

1.- Crear la siguiente estructura de directorio a partir de vuestro directorio de trabajo (/root/userxx)

2.- Crear un archivo de texto con 4 líneas llamado ejemplo1 en la carpeta ejecutable.

3.-Mover el archivo ejemplo1 al directorio ptextos.

4.-Establecer permisos de lectura y escritura para usuarios, lectura para grupos y ejecución para otros al archivo ejemplo1.txt.

5.- Mostrar los procesos que se están ejecutando en el sistema.

6.- Cree un Usuario con su nombre.

7.-Cree un Grupo llamado Uda.

8.- Descargue un fichero de internet usando el comando adecuado

9.- Activar el servicio httpd.

10.- Cerrar el proceso Mozilla Firefox

11.- Configurar la red con la siguiente dirección 192.168.0.1 y utilice la máscara 255.255.255.0

12.- Enviar un correo electrónico a una dirección de correo con el asunto prueba.

13.- Realice una conexión remota o telnet a otro equipo de su red.

14.- Muestre el tamaño de disco disponible.

15.- Comprima el archivo ejemplo1.txt.

16.- Realice un monitoreo del sistema.

17.- Utilice el comando para apagar el sistema.

2.18 Conclusión:

Con este capítulo se pretendió dar una guía de comandos básicos en el terminal de Linux para la realización de las prácticas de los capítulos siguientes.

CAPITULO 3: PROGRAMACION EN BASH

3.1 Introducción

Este capítulo pretende ayudarle a comenzar a programar shell scripts a un nivel básico/intermedio. No pretende ser un documento avanzado y mediante la descripción de instrucciones básicas de su uso como son variables, operadores, estructuras, etc, se pretende darlos a conocer para utilizarlos en configuración y programación de archivos en el estudio de prácticas posteriores.

3.2 Que es Bash

Bash es un intérprete de lenguaje de comandos sh-compatible que ejecuta comandos leídos desde la entrada Standard o desde un archivo.

Bash también incorpora características de uso de las shells Korn y C (ksh y csh).

3.3 La orden echo

Puede usarse para visualizar mensajes, muestra sus argumentos en el terminal, que es el dispositivo de salida Standard. Sin argumento produce una línea vacía y por defecto agrega una nueva línea al final de la salida.

Ejemplo:

```
[root@localhost~]# echo Hola Mundo
Hola Mundo
[root@localhost~]#
```

Nota: La cadena de argumentos puede tener cualquier número de caracteres. Sin embargo si la cadena contiene algún meta carácter deberá escribirse entre comillas.

3.4 Variables de Shell

- Las Variables en la Shell se escriben generalmente con mayúsculas.
- No hay espacios blancos a uno y otro lado del signo igual.
- Y son visualizadas con el signo dollar $.
- Para que una variable sea numérica utilizamos let

Ejemplo: let A

Ejemplo:

```
[root@localhost~]# SISTEMA=linux
[root@localhost~]# MSG="mi sistema operativo"
[root@localhost~]# echo $SISTEMA $MSG
linux mi sistema operativo
[root@localhost~]#
```

3.5 Tipos de variables

Existen cuatro tipos de variables: variables definidas por el usuario, variables parámetros, variables especiales y variables de entorno.

3.5.1 Variables definidas por el usuario.

Son el caso del ejemplo anterior, su nombre solo debe contener caracteres alfanuméricos y el guión bajo (_), excepto el primer carácter no debe ser un dígito (0 a 9).

Ejemplos:

```
[root@localhost~]# NOMBRE=Pepe
[root@localhost~]# EDAD=20
[root@localhost~]# echo Hola $NOMBRE
Hola Pepe
[root@localhost~]# NOMBRE2=$NOMBRE
[root@localhost~]# echo $NOMBRE2
Pepe
```

Se puede asignar valor a más de una variable en una única línea:

```
[root@localhost~]# NOMBRE=Pepe EDAD=20
[root@localhost~]# echo $NOMBRE tiene $EDAD
Pepe tiene 20
```

La asignación se realiza de izquierda a derecha.

```
[root@localhost~]# X=1 Y=$X
[root@localhost~]# echo $Y
1
```

Para quitarle el valor a una variable podemos utilizar el comando unset.

```
[root@localhost~]# X=1
[root@localhost~]# echo $X
1
[root@localhost~]# unset X
[root@localhost~]# echo X
```

Variables no modificables (solo lectura).

Para asegurarse que el valor de una variable no sea modificado, se puede indicar como de solo lectura de la siguiente manera:

```
[root@localhost~]# readonly variable
```

Ejemplo:

```
[root@localhost~]# X=1
[root@localhost~]# readonly X
[root@localhost~]# X=2
bash: X: readonly variable
$ echo $X
1
```

3.5.2 Variables de parámetros.

Como vimos al principio del texto, cuando el intérprete procesa un comando, la primera palabra es el nombre del ejecutable y las siguientes son argumentos.

Cuando el ejecutable es un script para bash, los parámetros son pasados al script mediante las variables parámetros, el primer parámetro será la variable.

Los nombres de las variables son de 1 a 9, el signo "$" es para poder leer su valor.
Veamos un ejemplo de un script en bash que visualiza los dos primeros parámetros pasados.

Editamos un archivo llamado script y le agregamos lo siguiente:

```
echo
echo
```

Luego lo hacemos ejecutable:

```
[root@localhost~]# chmod +x script.
```

Y por ultimo lo probamos:

```
[root@localhost~]#  script parametro1 parametro2
```

Script iniciado el fichero es parámetro 1

El nombre del ejecutable se almacena en la variable {sp_content}.
Pero si los parámetros pasados son más de 9.

3.5.3 Variables de entorno.

Son variables que utilizan los programas para obtener información del usuario. Cualquier programa puede utilizar variables de entorno, normalmente en la documentación del programa (página del manual) se indica que variables de entorno usara.
Veamos el nombre y su uso de algunas variables de entorno comunes:

HOME

Esta variable se inicializa cuando se ejecuta el bash y contiene el directorio home del usuario (/home/usuario)
Por ejemplo cuando al comando cd no le inidicamos el directorio, ósea hacemos "cd", este comando lee la variable de entorno HOME y realiza "cd $HOME".

PATH

Cuando ejecutamos bash, lo primero que hace es ejecutar los scripts /etc/profile, $HOME/.bash_profile y $HOME/.profile, durante la ejecución de estos, una de las tareas que realiza es cargarle un valor a la variable PATH, la cual indica los directorios donde bash buscara los archivos ejecutables.
$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/bin/X11:/usr/games

PS1

Se inicializa cuando se ejecuta bash y contiene el valor del símbolo de espera (prompt) de bash, que normalmente es "$" para un usuario ordinario o "#" para el superusuario.

PS2

Contiene el símbolo de espera del shell secundario (shell hijo), normalmente es ">".

MAIL

Específica la ruta completa del archivo de la casilla de correo del usuario.

MAILCHECK

Específica cada cuanto tiempo se verificara si hay nuevo correo en el archivo de la casilla de correo (60).

TERM

Especifica el tipo de terminal que se está utilizando (xterm, vt100, ansi, etc).

3.5.4 Variables especiales de Shell

$# Contiene el numero de parámetros de la línea de orden
$$ Contiene el numero PID (ID del proceso) del proceso en ejecución
$? Contiene el estado de salida de la última orden

$0 Contiene el nombre del guión, tal como se escribe en la línea de orden
$@ o $. Contiene todos los parámetros de la línea de orden
$1 , $2 .. $9 Las Variables especiales $1, $2, ... $9. Contienen los argumentos del 1 al 9, respectivamente. Se ignoran los argumentos de la línea de orden posteriores al 9.

3.6 Caracteres especiales

Los meta caracteres tienen significados especiales para el Shell. A veces, se requiere inhibir esos significados. El Shell le proporciona un conjunto de caracteres que anula el significado de los meta caracteres. Este proceso de anular el significado especial de los meta caracteres se denomina escape.

(\ ) Slash invertido: Utilizado para indicar que el carácter que le sigue se interpreta como un carácter alfa-numérico ordinario.

Ejemplo:

```
[root@localhost~]# echo \"\'\<\>\?\&\$\\
"'<>?&$\
[root@localhost~]#
```

Las dobles comillas (“): Puedes usar las dobles comillas para anular el significado de la mayoría de los caracteres especiales. Cualquier carácter especial entre un par de dobles comillas pierde su significado especial, excepto el signo de dollar $. (Utilice el slash invertido para eliminar sus significados especiales.).

Ejemplo:

```
[root@localhost~]#echo "*"
*
[root@localhost~]#
```

Ahora inténtalo sin las comillas y podrás visualizar otro resultado.
Otro ejemplo pero con el signo de dollar $:

```
[root@localhost~]#echo "$HOME"
/root
[root@localhost~]#
```

Las comillas sencillas (‘): Las comillas sencillas funcionan de manera análoga a las dobles comillas. Cualquier carácter especial entre un par de comillas simples pierde su significado especial, excepto la comilla simple.

Ejemplo:

```
[root@localhost~]#echo '* $HOME ? & " '
* $HOME ? & "
[root@localhost~]#
```

La comilla de acento grave (`): Esta distinción es muy importante. El shell interpreta dentro de los signos de acento grave como una orden ejecutable.

Ejemplo:

```
[root@localhost~]#echo La fecha actual es `date`
La fecha actual es mar feb 25  09:22:49 ECT 2008
[root@localhost~]#
```

3.7 La orden read

Realizada principalmente para interactuar con el usuario, por medio de la entrada standart.

Ejemplo:

```
[root@localhost~]#read YOSOY
Arturo Izquierdo <--- texto tipiado por mi.
[root@localhost~]#echo $YOSOY
Arturo Izquierdo<--- mostrando el contenido de la variable capturada
[root@localhost~]#
```

3.8 Operadores

+ Suma
- Resta
* Multiplicación
/ División
% Módulo
( ) Paréntesis (Agrupa operaciones)

[root@localhost~]# C=(($A + $B)) Adición Suma de $A y $B.
[root@localhost~]# C=(($A - $B)) Resto Diferencia entre $A y $B.
[root@localhost~]# C=(($A * $B)) Multiplicación Producto de $A and $B.
[root@localhost~]# C=(($A / $B)) División Cociente de $A entre $B.
[root@localhost~]# C=(($A % $B)) Módulo Resto de $A dividido entre $B.

3.9 Operadores lógicos

Los Operadores lógicos efectúan operaciones sobre órdenes de LINUX.

Condición AND
comando1 && comando2
comando2 es ejecutado si, y solo si, comando1 retorna un estado de salida cero.

Condición OR
comando1 || comando2
comando2 es ejecutado si y solo si comando1 retorna un estado de salida distinto de cero.
Lógica en la Shell

1 -true
0 –false

Bourne Again Shell es poseedor de una lógica inversa. Cuando una operación en linux se termina con éxito el estado de la variable $? será 0.

Ejemplo:

```
[root@localhost~]#cat loco.txt
cat: loco: No existe ese archivo o directorio
[root@localhost~]#echo $?
1
[root@localhost~]#
```

3.10 Operadores de comparación

s1 = s2	s1 coincide con s2
s1 != s2	s1 no coincide con s2
s1 < s2	s1 es alfabéticamente anterior o menor a s2
s1 > s2	s1 es alfabéticamente posterior o mayor a s2
-n s1	s1 no es nulo (contiene uno o más caracteres)
-z s1	s1 es nulo

Ejemplo
Comparando dos cadenas.

```
#!/bin/bash
S1='cadena'
S2='Cadena'
if [ $S1!=$S2 ];
then
    echo "S1('$S1') no es igual a S2('$S2')"
fi
if [ $S1=$S1 ];
then
```

```
        echo "S1('$S1') es igual a S1('$S1')"
    fi
```

Para ejecutar el archivo se utiliza **./**:
[root@localhost~]# ./nombre-archivo

Esto no es buena idea, porque si $S1 o $S2 son vacíos, aparecerá un parse error.
Es mejor: x$1=x$2 or "$1"="$2"

3.11 La construcción if –then

Ejemplo:

```
if [condición]; then
        ordenes
        ....
        ultima orden
fi
```

- La sentencia if finaliza con la palabra reservada fi (if escrito al revés).
- El sangrado no es necesario, pero hace lucir al código más elegante.

Nota: Los corchetes que están alrededor de las condiciones son necesarios y deben estar rodeados por espacios en blanco.

Ejemplo:

```
        if [condición]
        then
        ordenes_en_caso_de_condicion_verdadera
        ....
        else
        ordenes_en_caso_de_condicion_falsa
        ....
        Fi
```

Ejemplo:

```
if [ "petete" = "petete" ]; then
        echo expresión evaluada como verdadera
else
        echo expresión evaluada como falsa
fi
```

El código que se ejecutará si la expresión entre corchetes es verdadera se encuentra entre la palabra **'then'** y la palabra **'fi'**, que indica el final del código ejecutado condicionalmente.

Ejemplo:

```
if [condicion_1]
then
ordenes
....
elif [condicion_2]
then
ordenes
....
elif [condicion_3]
then
ordenes
....
else
ordenes
....
fi
```

3.12 El bucle while

El bucle **while** ejecuta un trozo de código si la expresión de control es verdadera, y sólo se para cuando es falsa (o se encuentra una interrupción explícita dentro del código en ejecución).

Ejemplo:

```
while [condicion]
do
ordenes
mas ordenes
done
```

Ejemplo:

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

3.13 El bucle until

El bucle **until** es casi idéntico al bucle loop, excepto en que el código se ejecuta mientras la expresión de control se evalúe como falsa.

Ejemplo:

```
until [condicion]
do
ordenes
mas ordenes
done
```

Ejemplo:

```
CONTADOR=20
until [ $CONTADOR -lt 10 ]; do
echo CONTADOR $CONTADOR
let CONTADOR-=1
```

```
done
```

3.14 Estructura for – in

El bucle **for** es distinto a los de otros lenguajes de programación. Básicamente, le permite iterar sobre una serie de `palabras' contenidas dentro de una cadena.

Ejemplo:

```
for variable in (lista de valores)
do
ordenes
mas ordenes..
done
```

Ejemplo:

```
for VARIABLE in `/etc/rc.d/rc.*`
do
        echo "$VARIABLE start" # Arranca todos mis demonios
done

for i in $( ls ); do
        echo item: $i
done
```

3.15 Estructura select

Ejemplo:

```
select variable in (lista de valores)
do
lista de ordenes
done
```

Ejemplo:

```
select VARIABLE in `ls`
do
echo "Cadena escogida $VARIABLE "
echo "Numero de respuesta $REPLY"
break # Rompe el ciclo
done
```

La línea leída es salvada en la variable REPLY. La lista es ejecutada después de cada selección, hasta que se aplique el comando *break* o un EOF.

Ejemplo:

```
OPCIONES="Hola Salir"
   select opt in $OPCIONES; do
      if [ "$opt" = "Salir" ]; then
       echo done
       exit
      elif [ "$opt" = "Hola" ]; then
       echo Hola Mundo
      else
       clear
       echo opción errónea
      fi
   done
```

Si ejecuta este script verá que es el sueño de un programador para hacer menús basados en texto. Probablemente se dará cuenta de que es muy similar a la construcción 'for', sólo que en vez de iterar para cada 'palabra' en $OPCIONES, se lo pide al usuario.

3.16 Construcción case

La estructura case escoge entre varias alternativas posibles.

Ejemplo:

```
case $OPCION
patron1)
ordenes

;;
patron2)
ordenes
;;
*)
ordenes
;;
esca
El * hace coincidencia con cualquier patrón
```

3.17 Funciones

Como en casi todo lenguaje de programación, puede utilizar funciones para agrupar trozos de código de una manera más lógica, o practicar el divino arte de la recursión.

Declarar una función es sólo cuestión de escribir function mi_func { mi_código }.

Llamar a la función es como llamar a otro programa, sólo hay que escribir su nombre.

Ejemplo:

```
function salir {
        exit
    }
    function hola {
       echo    Hola!
    }
    hola
    salir
    echo petete
```

3.18 La orden test

La orden test que es interna al shell evalúa la expresión que se le da como argumento y devuelve verdadero si la expresión así lo es. Test puede usarse de dos maneras:

Ejemplo:

```
if test "$VARIABLE"=valor
then
o
if ["$VARIABLE"=valor]
then
```

Sintaxis test numérico

```
test expresion_1 operador_logico expresion_2
INTEGER1 -eq INTEGER2
INTEGER1 es igual a INTEGER2
INTEGER1 -ge INTEGER2
INTEGER1 mayor que o igual a INTEGER2
INTEGER1 -gt INTEGER2
INTEGER1 es mayor que INTEGER2
INTEGER1 -le INTEGER2
INTEGER1 es menor que o igual a INTEGER2
INTEGER1 -lt INTEGER2
INTEGER1 es menor que INTEGER2
INTEGER1 -ne INTEGER2
INTEGER1 es distinto de INTEGER2
```

Sintaxis test cadenas comparación

```
test expresion_1 operador_logico expresion_2
STRING1 = STRING2
Las cadenas son iguales
STRING1 != STRING2
Las cadenas son diferentes
```

Sintaxis test cadenas comprobación

test operador "$VARIABLE"

3.19 Expresiones aritméticas

Pruebe esto en la línea de comandos (o en una shell):

echo 1 + 1

Si esperaba ver '2', quedará desilusionado. ¿Qué hacer si quiere que BASH evalúe unos números? La solución es ésta:

echo $((1+1))

Esto producirá una salida más 'lógica'. Esto se hace para evaluar una expresión aritmética.
También puede hacerlo de esta manera:

echo $[1+1]

Si necesita usar fracciones, u otras matemáticas, puede utilizar bc para evaluar expresiones aritméticas.

Si ejecuta "echo $[3/4]" en la línea de comandos, devolverá 0, porque bash sólo utiliza enteros en sus respuestas. Si ejecuta "echo 3/4|bc -l", devolverá 0.75

3.20 Operaciones Lógicas con expresiones

! EXPRESSION
NOT lógico
EXPRESSION1 -a EXPRESSION2
AND lógico
EXPRESSION1 -o EXPRESSION2
OR lógico

3.21 Capturando la salida de un comando

Este pequeño script muestra todas las tablas de todas las bases de datos (suponiendo que tenga MySQL instalado). Considere también cambiar el comando 'mysql' para que use un nombre de usuario y clave válidos.

```
#!/bin/bash
DBS=`mysql -uroot -e"show databases"`
for b in $DBS ;
do
mysql -uroot -e"show tables from $b"
done
```

3.22 Operadores para el manejo de cadenas

-z	Prueba si la cadena está vacía
-n	Comprueba el valor de una cadena
str	Verifica que no sea una cadena nula

3.23 Operadores para el manejo de archivos

FILE1 -ef FILE2
FILE1 y FILE2 tienen mismo manejador y números de inodo
FILE1 -nt FILE2
FILE1 es mas nuevo (fecha de modificación) que FILE2
FILE1 -ot FILE2
FILE1 es más viejo que FILE2

Sintaxis test archivo comprobación

test operador "$FILE"

-f $FILE El fichero existe y es un archivo regular.
-L $FILE El nombre de fichero es un vinculo simbólico
-s $FILE El fichero no esta vació
-r $FILE El fichero se puede leer.
-w $FILE El fichero puede ser modificado y se puede escribir en el.

-x $FILE El fichero es ejecutable
-d $FILE El nombre de fichero es un directorio
-c $FILE El nombre de archivo hace referencia a un dispositivo de carácter
-b $FILE El nombre de archivo hace referencia a un dispositivo de bloque
-O $FILE El archivo existe y es propietario del mismo
-p $FILE El archivo existe y es fue nombrado tubería
-S $FILE El archivo es un socket
-u $FILE El archivo existe y tiene activado el bit set-user-ID
-t [FD] El descriptor de archivo FD (stdout por default) esta abierto sobre una terminal
-e $FILE El archivo existe
-k $FILE El archivo existe y tiene activado el bit sticky.
-G $FILE El archivo existe y es propietario efectivo por ID de grupo.

3.24 Operadores para el manejo de parámetros

El shell proporciona la posibilidad para sustituir parámetros, lo que permite comprobar su valor y cambiarlo de acuerdo a una opción especificada. Esto es útil en la programación de shell, cuando necesita verificar si una variable es igual a algo. Por ejemplo, cuando emite una orden read en un guión, necesita asegurarse de que el usuario ha introducido alguna cosa antes de realizar ninguna acción.

El formato consiste en un signo de dólar ($), un conjunto de llaves ({y}), una variable, dos puntos (:), un carácter y una palabra de la forma siguiente:

${variable: caracter de opción palabra}

El carácter opción determina lo que hay que hacer con la palabra. Los cuatro caracteres de opción se especifican mediante los signos + - = ?. Estas cuatro opciones funcionaran de manera diferente, dependiendo si la variable esta vacía o no.
Una variable esta vacía, solo si su valor es una cadena vacía.

${parámetro}: Colocando la variable (parámetro) dentro de las llaves evita que se origine conflicto con el carácter que sigue al nombre de la variable. El ejemplo siguiente clarifica esta cuestion.

Suponga que desea cambiar el nombre de un archivo llamado izquierdo, especificado en la variable denominada ARCHIVO a izquierdoX.

```
[root@localhost~]# echo $ARCHIVO
izquierdo
[root@localhost~]# mv $ARCHIVO $ARCHIVOX
Usage: mv [-fi] source-file
[root@localhost~]#
```

Esta orden no funciona porque el shell considera que $ARCHIVOX es el nombre de la variable que no existe.

```
[root@localhost~]# mv $ARCHIVO ${ARCHIVO}X
[root@localhost~]# ls pl*izquierdoX
```

Esta orden funciona porque el shell considera que $ARCHIVO es el nombre de la variable y sustituye su valor, en este caso izquierdo.

${parametro:-cadena} La opción -(guión) significa que si la variable relacionada (parámetro) tiene asignado un valor y no esta vacía (no nula), se usa su valor. Si no es así, es decir, si la variable esta vacía (nula) o no tiene asignado valor, se sustituye su valor con cadena.

Por ejemplo:

```
bash-2.05b$ VAR=
bash-2.05b$ echo ${VAR:-/etc/X11/XF86Config}
/etc/X11/XF86Config
bash-2.05b$ echo $VAR
bash-2.05b$
```

La variable VAR permanece como una variable vacía.

${parametro:-cadena}: La opción + es opuesta a la opción -.

```
bash-2.05b$ HELPME="help me"
bash-2.05b$ echo ${HELPME:+"Ayuda va en camino"}
Ayuda va en camino
```

```
bash-2.05b$ echo $HELPME
help me
bash-2.05b$
```

La variable HELPME permanece inalterada.

${parámetro:=cadena}: La opción = significa que si a la variable relacionada (parámetro) no tiene asignado un valor o esta vacía (nula), se sustituye su valor con cadena. Si no, la variable no esta vacía y su valor permanecerá inalterado.

Por ejemplo:

```
bash-2.05b$ MSEG=
bash-2.05b$ echo ${MSEG:="Hola estoy aquí"}
Hola estoy aquí
bash-2.05b$ echo $MSEG
Hola estoy aquí
bash-2.05b$
```

La cena puede ser una cadena con espacios en blanco entre comillas. Funciona mientras se coloquen entre comillas.

El valor de MSEG se cambia y deja de ser una variable vacía.

${parametro:?cadena}: La opción ? significa que si la variable relacionada (parámetro) tiene asignado un valor y no esta vacía, entonces se sustituye su valor. Si no, si la variable esta vacía se imprime la palabra y se sale del guión actual. Si se omite cadena y se muestra el mensaje prefijado parameter null or not set.

Por ejemplo:

```
bash-2.05b$ MSEG=
bash-2.05b$ echo ${MSEG:?"Error"}
bash: MSEG: Error
bash-2.05b$
```

El shell evalúa la variable MSEG que esta vacía. De forma que la opción? provocara la sustitución de la cadena *Error;* que pasa a la orden echo para visualizarla

3.25 Ejercicios

1.- Muestre la siguiente cadena de argumentos "Programación Bash"

2.- Crear una variable de nombre MSG y asignarle el siguiente mensaje "Ingeniería de sistemas", crear otra variable NOMBRE y asignar su primer nombre. Mostrar ambos mensajes en la misma línea.

3.- Mostrar el siguiente mensaje "estos son caracteres especiales * $ \" '"

4.- Crear un archivo darle los permisos necesarios luego mediante la entrada estándar ingresar el nombre y que se almacene en una variable, luego ingresar el apellido y se almacene en otra variable, a continuación mostrar ambos en una sola línea.

5.- Crear un archivo que permita ingresar dos números y luego muestre su suma, resta, multiplicación y división darle los permisos necesarios.

6.- Crear un script de SHELL que liste únicamente los nombres de los directorios que se encuentran a partir del directorio actual.

7.- Realizar un script que espere hasta que un determinado proceso se ejecute. Y cuando este proceso se ejecute matarlo (utilizar el comando killall).

8.- Crear un script que reciba un directorio como primer parámetro, y a continuación una lista de archivos. EL script debe validar que los parámetros recibidos sean realmente archivos y luego copiarlos al directorio recibido.

9.- Crear el archivo PRUEBA darle permisos para el propietario del archivo de escritura lectura y ejecución, para el grupo tendría de lectura y ejecución y por último para el resto de usuarios tendría los mismos permisos que para el grupo antes mencionado. Editar el archivo pedir que ingrese un número entre "1 y 5",

ingresar número mediante la entrada estándar, preguntar si el número es igual a 5 mostrar “ganaste” si no mostrar “sigue intentando”.

10.-Crear el archivo EJEMPLO darle permisos de escritura, lectura y ejecución para todos los usuarios, recibir un nombre de archivo como parámetro e indicar, imprimiendo todas las leyendas que correspondan, si el archivo es legible, modificable y ejecutable por el usuario.

11.- Crear el archivo EJEMPLO2 darle permisos para el propietario del archivo de escritura lectura y ejecución, para el grupo tendría de lectura y ejecución y por último para el resto de usuarios tendría los mismos permisos que para el grupo antes mencionado. Editar el archivo para que permita ingresar 2 números, permita ingresar la suma de estos si es correcta mostrar un mensaje de suma correcta caso contrario mostrar el resultado válido de esta todo este procedimiento se repetirá mientras se escoja la opción s.

12.-Crear un archivo de nombre EJEMPLO4 darle todos los permisos. Editar el archivo para que muestre al usuario el calendario del mes que él mismo decida. El programa acepta un parámetro en el que el usuario indica el mes que quiere ver ya sea en formato numérico o usando las tres primeras letras del nombre del mes en cualquier combinación de mayúsculas o minúsculas. Si el mes seleccionado no es correcto se muestra un mensaje de error en la pantalla. En este programa usaremos el comando set ‘date` para obtener el año actual.

13.-Crear un archivo con los permisos del anterior ejemplo desarrollar un programa que solicita al usuario un número hasta que este entre 1 y 10.

14.- Crear un archivo darle los permisos necesarios luego ingresar dos números y mediante dos funciones Suma y Resta realice estas operaciones.

15.- Crear un script que permita saber si existe un archivo darle los permisos necesarios.

16.- Crear un archivo que permita mediante una funcion mostrar un mensaje de HOLA, luego mediante otra función salir del programa (utilizar exit).

17.- Utilizando el bucle until crear un archivo que permita mostrar los números del 10 al 20, darle los permisos necesarios.

3.26 Conclusión

La utilización de lenguaje Bash es de mucha importancia para el manejo del Shell, el aprendizaje de este nos será de mucha importancia para la manipulación y configuración de nuestros archivos y para entender como está funcionando nuestro sistema

CAPITULO 4: SEGURIDADES EN SERVIDORES LINUX

4.1 Introducción

La seguridad en un sistema Linux es un tema muy importante y sobre todo cuando nuestro sistema actúa como un Servidor de Comunicaciones, es difícil dejar inexpugnable un servidor, pero es bueno saber que dependiendo de qué tipo y valor tenga la información va a ser el empeño que coloquen los atacantes para ingresar al sistema, es por eso que en este capítulo se describe como mantener actualizado nuestro sistema y ciertas configuraciones para mantenerlo más seguro.

4.2 Manteniendo actualizado el sistema mediante YUM (Yellow dog Updater, Modified)

Un paso importante en combatir los accesos indeseados al equipo es mantenerlo siempre actualizado este procedimiento se lo puede automatizar con el programa yum que es un gestor automático de paquetería rpm, para realizar la automatización se realizan los siguientes pasos:

Para que yum se conecte al mirror más cercano y más rápido por región de un listado de 10 mirrors se instala el siguiente paquete:

yum install yum-plugin-fastestmirror

Luego se edita el archivo /etc/yum.conf y se aumenta la línea plugins=1

Para activar las actualizaciones automáticas se pone:

chkconfig –level 2345 yum on
service yum-updatesd start

Para que se inicie el servicio automáticamente la próxima vez q se encienda el computador se pone en el terminal.

ntsysv

Aparecerá la siguiente ventana (Gráfico 4.1), en la cual se activa el servicio utilizando barra espaciadora y para moverse entre las opciones de ok y cancelar usamos tabulador.

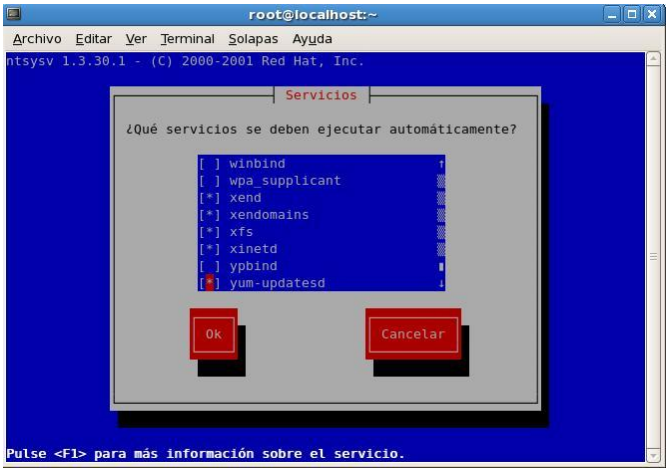

Gráfico 4.1

Si el equipo está detrás de un Proxy se debe configurar la variable de entorno http_proxy como se muestra en el ejemplo siguiente:

http_proxy=http://168.0.0.1
export http_proxy

Esto se lo puede poner en el archivo archivo /etc/rc.d/rc.local para que se configure siempre esta variable de entorno.

Existen gran cantidad de repositorios en donde se pueden encontrar programas ya compilados en formato rpm para adicionar más repositorios a yum se realiza lo siguiente:

Se edita el archivo /etc/yum.repos.d/CentOS-Base.repo y se aumenta las siguientes líneas. Los URL y los nombres pueden cambiar de acuerdo al repositorio que uno desee. El repositorio siguiente se muestra como ejemplo de repositorio pero debido a que ya no existe este repositorio no va incluido en la práctica.

[mailscanner- clamav]
name=MailScanner Linux Para Todos para Enterprise Linux 4.0
baseurl=h[mailscanner- clamav]

name=MailScanner Linux Para Todos para Enterprise Linux 4.0
baseurl=http://www.linuxparatodos.net/lpt/whitebox/4.0/mailscanner/
gpgkey=http://www.linuxparatodos.net/lpt/LPT-RPM-KEY

Otro repositorio famoso es dag (http://dag.wieers.com) este sitio provee de un rpm para instalar su repositorio. Los pasos para instalar el repositorio para la versión 5 de Centos son:

wget http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.i386.rpm

rpm -Uhv rpmforge-release-0.3.6-1.el5.rf.i386.rpm

4.3 Instalación del Repositorio AL Desktop

Se Instala la llave pública
wget http://www.alcancelibre.org/al/AL-RPM-KEY
rpm --import AL-RPM-KEY

Se edita el archivo /etc/yum.repos.d/CentOS-Base.repo y se aumenta las siguientes líneas.

Para Centos 4
[AL-Desktop]
name=Enterprise Linux $releasever - $basearch - AL Desktop
mirrorlist=http://www.alcancelibre.org/al/el4/al-desktop
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY

Para Centos 5
[AL-Desktop]
name=Enterprise Linux $releasever - $basearch - AL Desktop
mirrorlist=http://www.alcancelibre.org/al/el5/al-desktop
gpgkey=http://www.alcancelibre.org/al/AL-RPM-KEY

Se debe tener en cuenta que si en el momento de realizar alguna actualización mediante yum se da un error se debe borrar el repositorio que muestra como error.

Comandos útiles de yum:

yum update	actualiza el sistema en forma manual
yum install nombre del paquete	instala un paquete
yum check-update	verifica si hay actualizaciones
yum search nombre del paquete	busca un paquete
rpm --import http://rpm.livna.org/RPM-LIVNA-GPG-KEY	importa una llave de un repositorio

También se puede crear un repositorio desde el cual se pueden actualizar varios servidores de la red local de la siguiente forma:

4.4 Crear un repositorio YUM

mkdir /home/yum
ln -s /home/yum /var/www/html/yum
Se colocan los rpm en la carpeta /home/yum
cd /home/yum
yum-arch .
createrepo . esto para las versions nuevas de yum

Luego se configura el archivo yum de las otros servidores editando el archivo /etc/yum.repos.d/CentOS-Base.repo

Alli se pone lo siguiente

[repositorio]
name=interno
baseurl=http://www.repositoriointerno.com/yum/
gpcheck=0

En name no se debe poner lo mismo que se puso en [repositorio]

4.5 Cerrando los puertos no necesarios

Para ver los puertos abiertos se utiliza la instrucción nmap –v 127.0.0.1. Para ver los programas asociados a los puertos se utiliza netstat -ltunp , netstat -pel, o netstat -anp | grep 953.
A continuación se da un listado de algunos puertos que se deben apagar o que se está ejecutando en ese puerto.

Portmap	puerto 111 se desactiva con ntsysv y luego service portmap stop
Cups	puerto 631 desactiva con ntsysv y luego service cups stop
Auth	puerto 113 esto en ntsysv se reinicia el xinetd
Rndc	puerto 953 administra el dns para pararlo hay editar el archivo /etc/named.conf y comentar la línea 29 o 23 de la siguiente manera // inet 127.0.0.1 allow { localhost; } keys { rndckey; };
http-alt	puerto 8000 puerto del mapserver
ajp13	puerto 8009 puerto para comunicar apache con tomcat
rexec	puerto 512 se lo para en ntsysv se reinicia el xinetd
ssh	puerto 21 es para el servicio sshd
ipp	puerto 631 es el servicio cups que hay que desactivar con ntsysv es para impresion
rpc.statd	puerto 614 hay que desactivar portmap y reiniciar el servidor para que desaparezca
PERL	puerto 1212 Librería de Perl Net::SSLeay para usar OpenSSL kill del proceso o reiniciar el equipo una vez instalado el módulo

4.6 El sistema de Archivos Virtual PROC

Son los archivos que están en el directorio /proc estos archivos permiten la comunicación entre el usuario y el núcleo del sistema (kernel). Modificando algunos de estos archivos se puede dar mayor seguridad a Linux.

Las siguientes líneas son ejemplos de cómo modificar el sistema para que **ignore las peticiones de respuesta de ping.** Esto también se aplica para las siguientes opciones que se verán a continuación.

Se manda un echo 1 para activar que no responda el ping y un echo 0 para que si responda

echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all

También se puede utilizar el comando sysctl para realizar la misma acción
sysctl -w net.ipv4.icmp_echo_ignore_all=1

Las instrucciones anteriores no son permanentes o sea que cuando el equipo se reinicialice todo volverá a la normalidad. Para que esta y otras opciones siempre estén permanentes se edita el archivo /etc/sysctl.conf y allí se coloca la siguiente sentencia:

net.ipv4.icmp_echo_ignore_all = 1

4.7 No atender a las peticiones enviadas mediante Broadcast

Cuando una máquina envía un paquete a la dirección de broadcast (por ejemplo, 192.168.1.255), éste es entregado a todas las máquinas existentes en la red local. A continuación, todas las máquinas deben enviar un mensaje ECHO del protocolo ICMP. Esto puede provocar una congestión de la red, a la vez que permite determinar que sistemas están activos en la red.

Para desactivar la recepción de paquetes enviados a la dirección de broadcast:

sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1

4.8 Protección ante mensajes de error mal formateados

Es posible que una red se transmita mensajes de error mal formateados. Para evitar que éstos sean procesados por el sistema:

sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1

4.9 Deshabilitar la aceptación de redirecciones

Cuando el ordenador utiliza una ruta extinta o no-óptima para enviar un paquete a un destino particular, los rotures por donde circula el paquete envían al origen un mensaje de redirección del protocolo ICMP para informar de la ruta correcta a utilizar en el futuro.

Si un atacante tiene la capacidad de enviar mensajes de redirección puede modificar las tablas de direccionamiento del ordenador, haciendo por ejemplo que todo el tráfico fluya a través de una vía concreta.

Para evitar el proceso de estos mensajes en el sistema:

```
sysctl -w net.ipv4.conf.all.accept_redirects=0
sysctl -w net.ipv4.conf.default.accept_redirects=0
```

4.10 Protección contra ataques DoS de inundación SYN

El ataque de denegación de servicio (DoS) por inundación SYN ("SYN Flood") consigue consumir todos los recursos de la máquina, haciendo que sea necesario reiniciarla para volver a funcionar con normalidad.

Cada vez que se realiza una conexión TCP/IP existe una negociación de tres pasos:

1. El cliente envía un paquete (paquete 1) al servidor con el bit SYN activado y permanece a la escucha.
2. El servidor responde al cliente con un paquete de confirmación (paquete 2) y permanece a la escucha.
3. El cliente envía un tercer paquete (paquete 3) que consolida la conexión.

La información recibida en el paquete 1 se conserva dentro de una cola para que pueda ser comparada con los datos recibidos en el paquete 3 y dar por establecida la conexión. Esta cola es de un tamaño limitado y tiene un tiempo de latencia muy elevado.

El ataque de inundación SYN consiste en llenar esa cola, mediante el envío de un gran número de paquetes 1 y nunca respondiendo con un paquete 3. En el momento en que se llena la cola, el sistema es incapaz de atender cualquier otra petición de conexión que reciba.

La protección contra este ataque consiste en añadir información en el paquete 2, de forma que no sea necesaria conservar en el servidor ningún dato sobre el cliente.
Para activar esta protección:

```
sysctl -w net.ipv4.tcp_syncookies=1
```

Con este valor, el sistema utilizará el método de incluir la información en el paquete 2 siempre que la cola de paquetes por procesar esté saturada.

4.11 Protección contra direcciones IP no válidas

Esta protección permite que la máquina no pueda utilizarse para el envío de paquetes con direcciones IP no válidas. Este tipo de paquetes son habitualmente enviados cuando la máquina está intentando realizar una acción potencialmente ilegítima, como puede ser la suplantación de una conexión o el envío de paquetes en un ataque de denegación de servicio.

Para activar esta protección:

```
sysctl -w net.ipv4.conf.all.rp_filter=2
sysctl -w net.ipv4.conf.default.rp_filter=2
```

El valor de los parámetros puede ser 0 (valor por omisión, no realizar ninguna comprobación), 1 (rechazar únicamente las suplantaciones evidentes) y 2 (realizar una comprobación exhaustiva). Se aconseja seleccionar la opción de comprobación exhaustiva.

Esta opción no debe utilizarse en aquellos sistemas que actúen como cortafuegos o routers.

4.12 Redireccionamiento IP

El redireccionamiento IP es que en un sistema con diversos interfaces activos, se acepten paquetes en un interfaz con destino al otro. Si la opción de rediccionamiento está activa, la máquina podrá actuar como un router para el tráfico entre las redes existentes en cada uno de los interfaces.

Únicamente aquellos sistemas que actúan como cortafuegos o routers o bien en circunstancias muy especiales deberían tener esta opción activa.

Para verificar que se encuentra desactivada:

sysctl -w net.ipv4.ip_forward = 0

En caso de activar con el valor 1 esta opción, también se deberia modificar el valor de net.ip4.conf.all.rp_filter y net.ipv4.conf.default.rp_filter.

4.13 Control de rutas

Habitualmente un sistema no tiene ningún control sobre la ruta utilizada por los paquetes en su camino hacia su destino. El protocolo TCP/IP permite establecer la ruta exacta a seguir. Excepto en circunstancias muy especiales, este soporte deberá ser desactivado para evitar que un atacante pueda utilizar un sistema concreto como paso para saltarse las protecciones establecidas en el tráfico.

Para desactivar esta opción:

sysctl -w net.ipv4.conf.all.accept_source_route = 0
sysctl -w net.ipv4.conf.default.accept_source_route = 0

4.14 Registro de actividades sospechosas

Un último valor de interés nos permite registrar en los archivos de actividad del sistema aquellas situaciones potencialmente sospechosas: intento de envío de paquetes con dirección no válida, paquetes con cambio de rutas y otras situaciones

similares.

Se trata de una serie de situaciones que en un funcionamiento normal de la red no pueden producirse en ninguna circunstancia. Un ejemplo puede ser la recepción de un paquete a través de un interfaz Ethernet con dirección origen igual a 127.0.0.1

Para activar el registro de esta actividad:
sysctl -w net.ipv4.conf.all.log_martians = 1
sysctl -w net.ipv4.conf.default.log_martians = 1

Ejemplo del Archivo /etc/sysctl.conf

```
# Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled. See sysctl(8) and
# sysctl.conf(5) for more details.

# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1

# Disables packet forwarding
net.ipv4.ip_forward=0

# Disables IP source routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.lo.accept_source_route = 0
net.ipv4.conf.eth0.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

# Enable IP spoofing protection, turn on source route verification
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.lo.rp_filter = 1
net.ipv4.conf.eth0.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

```
# Disable ICMP Redirect Acceptance
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.eth0.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0

# Enable Log Spoofed Packets, Source Routed Packets, Redirect Packets
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.lo.log_martians = 1
net.ipv4.conf.eth0.log_martians = 1

# Disables the magic-sysrq key
kernel.sysrq = 0

# Decrease the time default value for tcp_fin_timeout connection
net.ipv4.tcp_fin_timeout = 15

# Decrease the time default value for tcp_keepalive_time connection
net.ipv4.tcp_keepalive_time = 1800

# Turn off the tcp_window_scaling
net.ipv4.tcp_window_scaling = 0

# Turn off the tcp_sack
net.ipv4.tcp_sack = 0

# Turn off the tcp_timestamps
net.ipv4.tcp_timestamps = 0

# Enable TCP SYN Cookie Protection
net.ipv4.tcp_syncookies = 1

# Enable ignoring broadcasts request
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Enable bad error message Protection
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

```
# Increases the size of the socket queue (effectively, q0).
net.ipv4.tcp_max_syn_backlog = 1024

# Increase the tcp-time-wait buckets pool size
net.ipv4.tcp_max_tw_buckets = 1440000

# Allowed local port range
net.ipv4.ip_local_port_range = 16384 65536
```

Una ves modificado el archivo /etc/sysctl.conf para que los cambios surtan efecto ejecutar la instrucción /sbin/sysctl -p

4.15 Seguridad en las Contraseñas

Hay que establecer una política en cuanto a cuantos caracteres como mínimo tendrá la contraseña, y cuanto tiempo el usuario estará con la misma. Una vez pensado esto se realizan los cambios de la siguiente manera:

Se edita el archivo /etc/login.defs y se modifica las siguientes variables

```
#       PASS_MAX_DAYS   Máximo número de días que una contraseña se puede usar.
#       PASS_MIN_DAYS   Mínimo número de días permitidos para cambiar la contraseña.
#       PASS_MIN_LEN    Mínimo numero de caracteres para la contraseña.
#       PASS_WARN_AGE   Número de días de mensaje de alerta indicando que la contraseña expira.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
```

4.16 No permitir acceso a root mediante el comando su

Se modifica el archivo /etc/passwd y se cambia el shell del root de /bin/bash a /sbin/nologin, de esta forma cuando se ejecute **su root** este comando no funcionara

4.17 Asegurando el Sistema de Ficheros

Cuando se crean las particiones en forma automática cuando se instala el sistema operativo, este crea tres particiones la /boot, swap, / este es un sistema de particiones básico en el cual los usuarios no tienen acceso a carpetas pero si se quiere que los usuarios tengan acceso a ciertas carpetas es recomendable que estas carpetas se creen como otras particiones para después poder asegurar estas particiones de mejor manera. Por lo general la carpeta a la que los usuarios tienen acceso es /home. De esta forma las particiones del sistema quedaría de /boot, swap, /, /home.

Para asegurar una partición o file system se edita el archivo /etc/fstab, este archivo contiene todos los file system que monta el sistema

```
# This file is edited by fstab-sync - see 'man fstab-sync' for details
/dev/VolGroup00/LogVol00 /                ext3    defaults        1 1
LABEL=/boot              /boot            ext3    defaults        1 2
none                     /dev/pts         devpts  gid=5,mode=620  0 0
none                     /dev/shm         tmpfs   defaults        0 0
none                     /proc            proc    defaults        0 0
none                     /sys             sysfs   defaults        0 0
/dev/VolGroup00/LogVol01 swap             swap    defaults        0 0
/dev/hda          /media/cdrom     auto    pamconsole,exec,noauto,managed 0 0
/dev/fd0          /media/floppy    auto    pamconsole,exec,noauto,managed 0 0
```

Las opciones que se pueden poner son:

NOSUID No permite la Ejecución de programas con el bit suid, es decir, que se ejecutan como root y son potencialmente peligrosos para el sistema.

NODEV no permite la creación de dispositivos de sistema en esa partición

librándonos así de la posible instalación de programas potencialmente peligrosos para el sistema.

NOEXE no permite que ejecuten aplicaciones en esa partición.
NOATIME no permite que se escriba en la bitácora del sistema los accesos a los archivos de la partición. Con esta opción activa también acelera el acceso al disco ya que no tiene el sistema que escribir cosas adicionales al mismo.

Todas estas opciones se ponen separadas por coma luego de la palabra defaults. Para ver el estado actual de las particiones se ejecuta el comando mount sin parámetros. Para realizar cualquier cambio se debe desmontar primero antes de realizar los cambios.

4.18 Conclusión

En este capítulo se muestra la forma de mantener actualizado nuestro sistema mediante el uso de yum y la creación y manejo de repositorios, así como el uso de ciertas seguridades para ayudar a proteger nuestro servidor, estas configuraciones servirán como base para seguir optimizando nuestro servidor en los próximos capítulos.

CAPITULO 5. INSTALACIÓN Y CONFIGURACIÓN DEL PROGRAMA VNC PARA ADMINISTRACIÓN REMOTA DE EQUIPOS

5.1 Introducción

La administración remota de un equipo es de mucha utilidad gracias a esta el administrador puede gestionar desde otro equipo en nuestro caso desde un equipo Windows el servidor.

Es por esto que el objetivo principal de la práctica es el de aprender a configurar y utilizar el programa de libre distribución llamado VNC, para administrar en forma remota y gráfica un servidor de Linux.

5.2 Conocimientos Previos

En esta práctica se utilizara el programa VNC desde un maquina con Windows para administrar un servidor Linux utilizando un entorno gráfico. Este programa también puede ser utilizado para administrar un equipo Windows desde otro equipo Windows en forma remota.

VNC (Virtual Network Computing) es un software cliente/servidor que permite acceder remotamente a sesiones X-Windows. Con este programa se puede acceder desde cualquier ordenador conectado a Internet que tenga el cliente (vncviewer) a una sesión que se ha abierto en el ordenador.

VNC es software libre, con licencia GPL y disponible para la mayoría de las plataformas. Este programa se lo puede conseguir en la siguiente dirección http://www.realvnc.com/

Otro programa que también sirve para administración remota es TightVNC que es una versión mejorada de VNC, optimizada para conexiones lentas ya que comprime el tráfico usando un algoritmo de compresión propio. En redes donde VNC es lento porque la conexión no es lo suficientemente rápida, TightVNC puede funcionar prácticamente en tiempo real. Este programa se lo puede conseguir en la siguiente dirección http://www.tightvnc.com/

La utilización del programa VNC en la práctica es debido a que Red Hat viene ya instalado con el servidor VNC.

5.3 Desarrollo de la Práctica

5.3.1 Configuración del Servidor de Linux

Para realizar los siguientes pasos ingrese en modo de instrucciones.

1.- Ejecute la instrucción vncserver, le pedirá la clave de acceso al servidor ponga como clave la palabra uda. Lo que le aparecerá en la pantalla será lo siguiente:

```
You will require a password to access your desktops.

Password:

Verify:

xauth:  creating new authority file /root/.Xauthority

New 'pruebas:1 (root)' desktop is pruebas:1

Creating default startup script /root/.vnc/xstartup

Starting applications specified in /root/.vnc/xstartup

Log file is /root/.vnc/pruebas:1.log
```

Esta instrucción además de poner una clave al servidor VNC crea una carpeta oculta llamada .vnc en donde están los archivos de configuración del servidor.

2.- Se tiene que editar el archivo /root/.vnc/xstartup que es el archivo de configuración del servidor, para esto tiene que utilizar el entorno gráfico de Linux, de un click en el icono carpeta de inicio de root

Gráfico 5.1

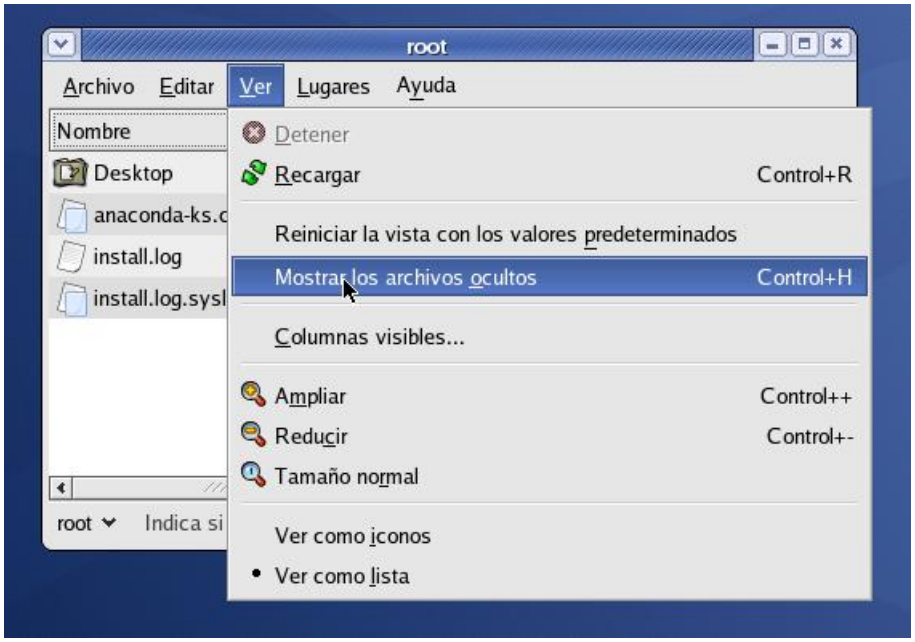

Gráfico 5.2

Vaya al menú de ver y escoja mostrar los archivos ocultos para poder ver la carpeta .vnc

Busque la carpeta .vnc y de dos click sobre esta le aparecerá el contenido de la carpeta busque el archivo xstartup de dos click sobre esta para poder editarla.

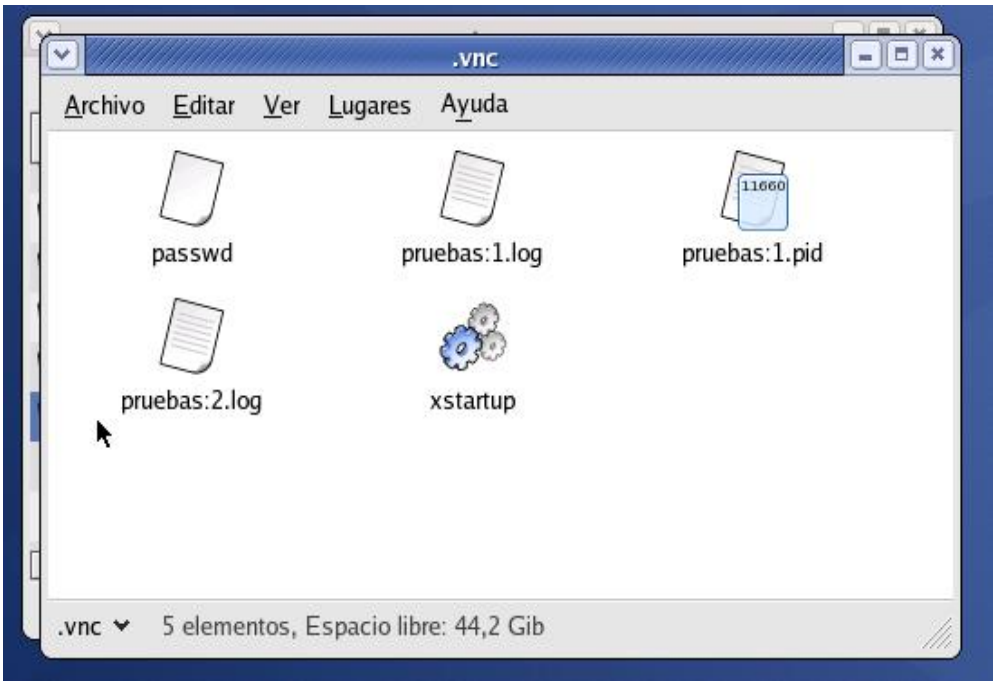

Gráfico 5.3

Le aparecerá la siguiente pantalla pulse en el botón de mostrar.

Gráfico 5.4

Haga los cambios necesarios para que el archivo quede de la siguiente forma:

```
#!/bin/sh

# Uncomment the following two lines for normal desktop:

 unset SESSION_MANAGER

 exec /etc/X11/xinit/xinitrc

#[ -x /etc/vnc/xstartup ] && exec /etc/vnc/xstartup

#[ -r $HOME/.Xresources ] && xrdb $HOME/.Xresources

#xsetroot -solid grey

#vncconfig -iconic &

#xterm -geometry 80x24+10+10 -ls -title "$VNCDESKTOP Desktop" &

#twm &
```

Las líneas que comienzan con # son comentarios, unset es una instrucción que sirve para borrar variables de entorno, exec es una instrucción para ejecutar programas.

3.- Regrese a la ventana de modo de instrucciones y mate el proceso VNC de la siguiente forma:

- Vea cual es el nombre del equipo con la instrucción hostname
- Luego escriba la siguiente instrucción reemplazando los signos de interrogación con el nombre del equipo

```
vncserver -kill ??????????:1
```

El uno es el número de sesiónvncserver -kill ??????????:1 n abierta. El servidor puede abrir varias sesiones VNC

4.- Ejecute nuevamente el Servidor VNC con:

```
Vncserver
```

5.3.2 Configuración del Cliente

Para realizar esto tiene que arrancar la computadora en Windows, luego ejecute el programa cliente de VNC (vnc-4_1_2-x86_win32_viewer.exe) el cual está en la página Web del curso de Linux. Le aparecerá la siguiente pantalla:

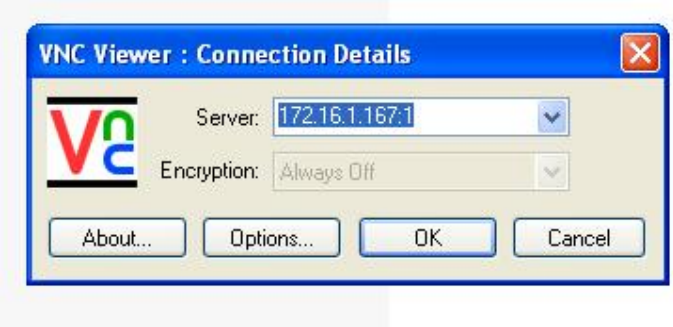

Gráfico 5.5

La ip 172.16.1.167 tiene que ser reemplazada por la ip de algún compañero que ya tiene configurado el servidor VNC y actualmente tiene arrancado Linux en el equipo. Luego presione el botón de OK. Le pedirá una contraseña que es la que puso cuando configuro el servidor de VNC. Si todo esta correcto aparecerá el ambiente gráfico de Linux de la computadora remota.

5.3.3 Configuraciones Adicionales

1.- Si quiere tener variase sesiones VNC ejecute varias veces vncserver y para conectarse cambie el número 1 por 2 o 3 o 4 etc.

2.- Si quiere terminar una sesión ejecute la siguiente instrucción:

vncserver -kill {nombre del computador} : {número de la sesión}

Ejemplo

vncserver -kill pruebas:2

vncserver -kill pruebas:3

3.- Para cambiar el password del servidor ejecute la instrucción:

vncpasswd

5.3.4 Para que arranque el servidor cada vez que se encienda la máquina:

1.- Se edita el archivo /etc/sysconfig/vncservers y se pone al final del archivo lo siguiente:

VNCSERVERS="1:root"

Donde 1 es el número de la sesión y root el usuario que se desea que arranque el servicio.

2.- Se activa el vncserver cada vez que arranque el servidor con la instrucción ntsysv del listado que aparece escoja vncserver y pulse el botón de ok.

3.- Para comprobar que está funcionando reinicie el equipo con la instrucción reboot o puede arrancar el servidor con la instrucción service vncserver start sin reiniciar el equipo.

4.- Deshabilite el cortafuegos tanto de Linux como de Windows.

En Linux abriendo el terminal y poniendo:

#service iptables stop

En Windows:

Ingresando al panel de control, luego escogemos la opción firewall de Windows y desactivamos el firewall.

5.- Conéctese con el cliente VNC al servidor.

5.4 Ejercicios

1) En el Cliente VNC en el momento de conectarse hay un botón de opciones. Describa brevemente las opciones que se puede configurar.
2) Cual piensa que son las mejores opciones de configuración del cliente VNC

5.5 Conclusión

En esta práctica se mostro la configuración de VNC que es un programa para la administración remota de equipos con el fin de poder gestionar un servidor Linux desde un equipo remoto Windows, esta práctica es de mucha importancia ya que en un gran número de ocasiones el administrador pasa en otro equipo que no es el servidor.

CAPITULO 6. INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR WEB (APACHE) CON UN CERTIFICADO DIGITAL

6.1 Introducción

La instalación de un servidor web que implementa el protocolo HTTP, nos permite crear nuestra página web sin necesidad de contratar hosting, probar nuestros desarrollos vía local, acceder a los archivos de nuestro equipo desde un PC remoto, entre otras cosas, es de mucha utilidad pero la información a través de la web puede ser fácilmente capturada y entendida por algún atacante, es por eso que es imprescindible encriptarla con el fin de que los atacantes no logren entender esta información, es por eso que el objetivo principal de esta práctica es la instalación del servidor Web Apache en el cual los datos transmitidos estarán encriptados, para esto se verá la utilización de un certificado digital.

6.2 Conocimientos Previos

6.2.1 Servidor Web

Un servidor Web es un programa que implementa el protocolo HTTP (HyperText Transfer Protocol). Este protocolo está diseñado para transferir lo que se llama hipertextos, páginas Web o páginas HTML (Hypertext Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

Sin embargo, el hecho de que HTTP y HTML estén íntimamente ligados no debe dar lugar a confundir ambos términos. HTML es un formato de archivo y HTTP es un protocolo.

Cabe destacar el hecho de que la palabra servidor identifica tanto al programa como a la máquina en la que dicho programa se ejecuta. Un servidor Web se encarga de mantenerse a la espera de peticiones HTTP llevadas a cabo por un cliente HTTP que se lo conoce como navegador.

6.2.2 Apache

Servidor Web de distribución libre. Fue desarrollado en 1995 y ha llegado a ser el más usado de Internet.

6.2.3 Certificado Digital

Hay ocasiones en las que se hace necesario recibir/enviar información sensible desde/a un servidor de Web. La información que se transmite por un servidor Web no está cifrada normalmente, para cifrarla hay que instalar un certificado digital.

Aunque los datos viajen cifrados por la Red, se tiene que estar seguro en que portales Web se deposita información sensible como números de tarjetas de crédito. Se hace imprescindible el contar con un mecanismo que dé fe de si un servidor seguro es quien creemos que es y podemos confiar en él a la hora de transmitirle nuestra información. La forma como se hace es mediante las Autoridades de Certificación (AC), conocidas informalmente como notarios electrónicos, encargadas de autenticar a los participantes en transacciones y comunicaciones a través de la Red. Su función es emitir certificados a los usuarios, de manera que se pueda estar seguro de que el interlocutor (cliente o servidor) es quien pretende ser, garantizando así la seguridad de las transacciones.

El certificado de seguridad se concede a una entidad después de comprobar una serie de referencias, para asegurar la identidad del receptor de los datos cifrados. Se construye a partir de la clave pública del servidor solicitante, junto con algunos datos básicos del mismo y es firmado por la autoridad de certificación (Verisign, GlobalSign, GTE CyberTrust, etc.) correspondiente con su clave privada.

Para ver si un servidor es seguro en la parte izquierda del navegador o browser verifique que haya un candado cerrado

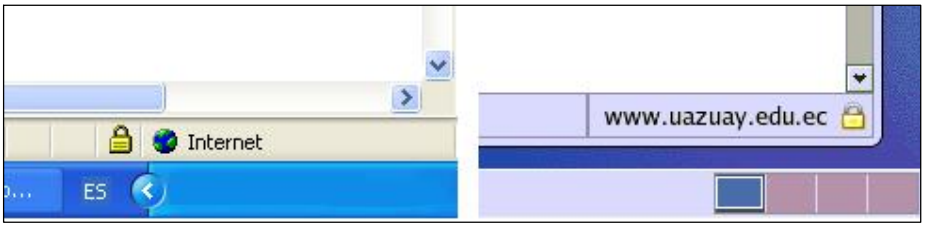

Gráfico 6.1

Para estar completamente seguros hay que ver los detalles del certificado para esto de doble click en el candado, aparecerá los detalles del certificado verifique que haya una entidad certificadora y que el nombre de la empresa coincida con el de la página Web.

Otro detalle que se tiene que ver es que la dirección del portal Web no comience con http:// sino con https:// (HyperText Transmission Protocol Secured) https es una URL creada por Netscape Communications Corporation para designar documentos que llegan desde un servidor WWW scentOS5eguro. Esta seguridad es dada por el protocolo SSL (Secure Sockets Layer) basado en la tecnología de encryptación y autentificación desarrollada por la RSA Data Security Inc.

6.3 Desarrollo de la Práctica

6.3.1 Configuración del Servidor Apache

1) El archivo de configuración del servidor apache es httpd.conf la ubicación exacta del archivo es:

   /etc/httpd/conf/httpd.conf

2) Instrucciones para Iniciar, Parar y Reiniciar el servidor web apache:

   service httpd start Ini cia el Servidor Web
   service httpd stop Apa ga el Servidor Web
   service httpd restart Rei nicia el Servidor Web

3) El archivo de configuración tiene muchas opciones de configuración pero las que se van a indicar son las básicas, (para probar estas opciones puede

hacer el cambio y luego ejecutar la instrucción service httpd restart para ver los cambios) para hacerlas edite el archivo httpd.conf y realice las siguientes modificaciones:

a) La carpeta o directorio donde se almacenarán los archivos html del servidor Web esta indicado en la instrucción DocumentRoot en la línea 265. En este caso es /var/www/html. Ejemplo:

   DocumentRoot "/var/www/html"

b) Si el archivo HTML tiene palabras con tildes estas saldrán como símbolos raros en el navegador esto es debido a que el set de caracteres que viene por defecto (UTF-8) no soporta tildes el set correcto es ISO-8859-1 modifique la línea 730 para que quede de la siguiente forma:

Cambie: AddDefaultCharset UTF-8 **por** AddDefaultCharset ISO-8859-1

c) Cuando uno pone un URL y no especifica un archivo sino únicamente la carpeta el servidor Web busca la instrucción DirectoryIndex esta instrucción tienes los nombres de los archivos que debe buscar en la carpeta para ser mostrados. El orden en esta lista es importante porque es el orden con el cual buscara y mostrara el archivo. En el caso de no existir los archivos del listado el servidor mostrara el contenido de la carpeta. Si lo desea puede aumentar la lista que viene por defecto con el nombre de los archivos que crea conveniente en la línea 375 por ejemplo:

Cambie: DirectoryIndex index.html index.html.var
Por: DirectoryIndex home.php home.htm home.html index.htm index.html index.html.var

d) en el punto b) si no se encontraba el archivo mostraba el contenido de la carpeta, pero esto por razones de seguridad no se recomienda para impedir que se liste el contenido de una carpeta vaya a la línea 304 y elimine la palabra Indexes.

Cambie: Options Indexes FollowSymLinks **por** Options FollowSymLinks

4) El nombre del servidor se lo define en la instrucción ServerName aquí se debe poner el nombre que se le asignara. Vaya a la línea 249 y realice los siguientes cambios:

Cambie en CentOS5:
#ServerName new.host.name:80
Por:
ServerName practicas.uazuay.edu.ec:80

El símbolo de # indica que la línea es un comentario el número 80 es el puerto que utilizará para conectarse.

6.3.2 Generando certificados SSL para apache:

La creación de certificados SSL es uno de los puntos más interesantes al trabajar con servidores web. Estos certificados nos permiten que la conexión entre el cliente (browser) y el servidor web viaje encriptada minimizando o mitigando la posiblidad de un ataque de hombre en el medio que tienda a descubrir nuestras claves.
¿Cómo hacerlo? se resume en 3 pasos (con uno adicional opcional), que son:

- Creación de una clave privada (KEY)
- Generación de una solicitud de certificado (CSR) Creación de un certificado autogenerado
- Instalación del certificado (CRT)

Luego crear una carpeta en la que se va a guardar los archivos.

- El **primer paso** es crear la clave RSA privada. Esta clave es del tipo RSA de 1024 bits y estará encriptada usando Triple DES y guardada en formato PEM de forma tal que sea visible como texto ASCII.

Aquí un ejemplo real:
openssl genrsa -rand /usr/bin/lsattr:/bin/cat -out server.key 1024

Aquí está generada la server.key, la clave privada:

ll server.key

-rw-r--r-- 1 root root 963 Apr 1 16:08 server.key

Es muy importante mantener una copia de ésta clave pues es la base para la encriptación usando un certificado. De ser posible mantener un respaldo en un disquete o cinta.

- El **segundo paso** es generar una petición de certificación (Certificate Signed Request).

Con esta podremos realizar la petición de un certificado a la entidad certificadora de nuestra elección.

Este es el archivo que se les envía cuando las entidades certificadoras solicitan el CSR. Sin embargo, también podemos hacer que nuestro sistema genere un Certificado AutoGenerado el cual nos permitirá operar de forma segura, pero siempre les sacará a los clientes una advertencia de que el certificado no puede ser validado en una entidad certificadora.

En negrita está lo que nosotros debemos ir escribiendo. El ejemplo es para Cuenca, Azuay, Ecuador, pero debe ponerse los datos de la organización propiamente dichos.

Abrimos el terminal y ponemos:

openssl req -new -key server.key -out server.csr

Nos mostrará lo siguiente:

Enter pass phrase for server.key: **(poner la frase con que generamos la clave privada)**

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [CA]:**EC**

State or Province Name (full name) [Some-State]:**Azuay**

Locality Name (eg, city) [Some-Locality]:**Cuenca**

Organization Name (eg, company) [Some-Organization Ltd]:**Internet**

Organizational Unit Name (eg, section) [Some-Organizational]:**IT**
Common Name (eg, YOUR name) [www.domain.com]:**localhost**
Email Address [admin@domain.com]:**art_izq@hotmail.com**
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Aquí se nos generará el CSR(server.csr):

ll server*
-rw-r--r-- 1 root root 765 Apr 1 16:22 server.csr
-rw-r--r-- 1 root root 963 Apr 1 16:08 server.key

Cuando vayamos a comprar un certificado, sólo enviaremos éste archivo server.crt a la entidad certificadora.
Ahora, como esto de comprar un certificado toma un tiempo y cuesta dinero, podemos nosotros generar un certificado autogenerado a partir de estos datos y seguir operando.
Este certificado de ejemplo será válido por 60 días, podemos poner más (1400 o algo así) si es que nunca vamos a pedir un certificado válido a una entidad certificadora.

openssl x509 -req -days 60 -in server.csr -signkey server.key -out server.crt
Signature ok
subject=/C=EC/ST=Azuay/L=Cuenca/O=internet/OU=IT/CN=Arturo Izquierdo/emailAddress=art_izq@hotmail.com
Getting Private key
Listo.. ya tendremos nuestro certificado autogenerado.
ll server*
-rw-r--r-- 1 root root 969 Apr 1 16:27 server.crt
-rw-r--r-- 1 root root 765 Apr 1 16:22 server.csr
-rw-r--r-- 1 root root 963 Apr 1 16:08 server.key

En el caso de que hayamos solicitado un certificado de autenticidad a una entidad certificadora:

Es éste certificado el que nos enviaría una entidad certificadora para que usemos.

Cuando lo envían, normalmente lo hacen en el cuerpo del mensaje, lo que tenemos que hacer realmente es crear un nuevo archivo llamado **server.crt** y pegarle todos los datos que nos indiquen.
Ahora procedemos a instalar el certificado en el apache:
Primero verificar que apache esté instalado:

rpm -q httpd

Probemos que el apache arranque:

service httpd restart

Copiamos los archivos creados de la siguiente manera:

 # cp server.crt /etc/pki/tls/certs/
 # cp server.key /etc/pki/tls/private/

Luego editamos el archivo
vi /etc/httpd/conf.d/ssl.conf

En la linea 111 modificamos lo siguiente:
SSLCertificateFile /etc/pki/tls/certs/localhost.crt

Reemplazamos por:
SSLCertificateFile /etc/pki/tls/certs/server.crt

En la línea 119, modificamos lo siguiente:

SSLCertificateFile /etc/pki/tls/private/localhost.key

Reemplazamos por:
SSLCertificateFile /etc/pki/tls/private/server.key

Y guardamos los cambios luego reiniciamos el servicio apache

#service httpd restart

Luego probamos en el browser

https://127.0.0.1/

Nos aparecerá la siguiente pantalla

Gráfico 6.2

Damos un click en examinar certificado.

Si se carga con la información que creamos los archivos anteriores como se muestra en la siguiente pantalla está listo el certificado.

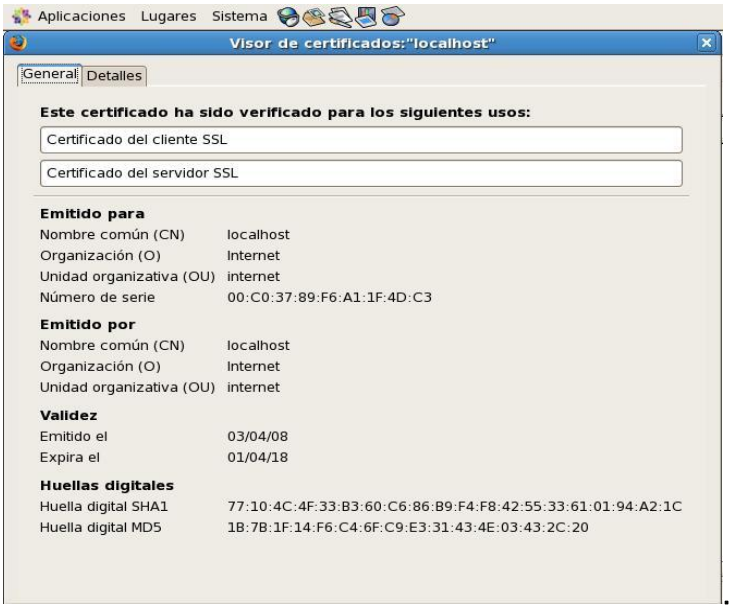

Gráfico 6.3

6.3.3 Instalación de un Certificado Digital de Verisign

1) Vaya a la página de Verisign http://www.verisign.com escoja la opción Go Free SSL Trial Llene los datos del formulario y de un click en submit. Le aparecerá una página con los pasos que tiene que realizar para obtener el certificado.

2) Llene los datos que le pide en las páginas siguientes hasta llegar a la página que muestra el gráfico que esta a continuación. Allí seleccione la plataforma de servidor como Apache, en la parte inferior del formulario pegue allí el contenido del archivo **/etc/pki/tls/certs/server.crt** de tal forma que quede como se muestra en el gráfico como dato opcional al final del formulario escoja en que va a usar el certificado digital. Pulse el botón de **Continue**.

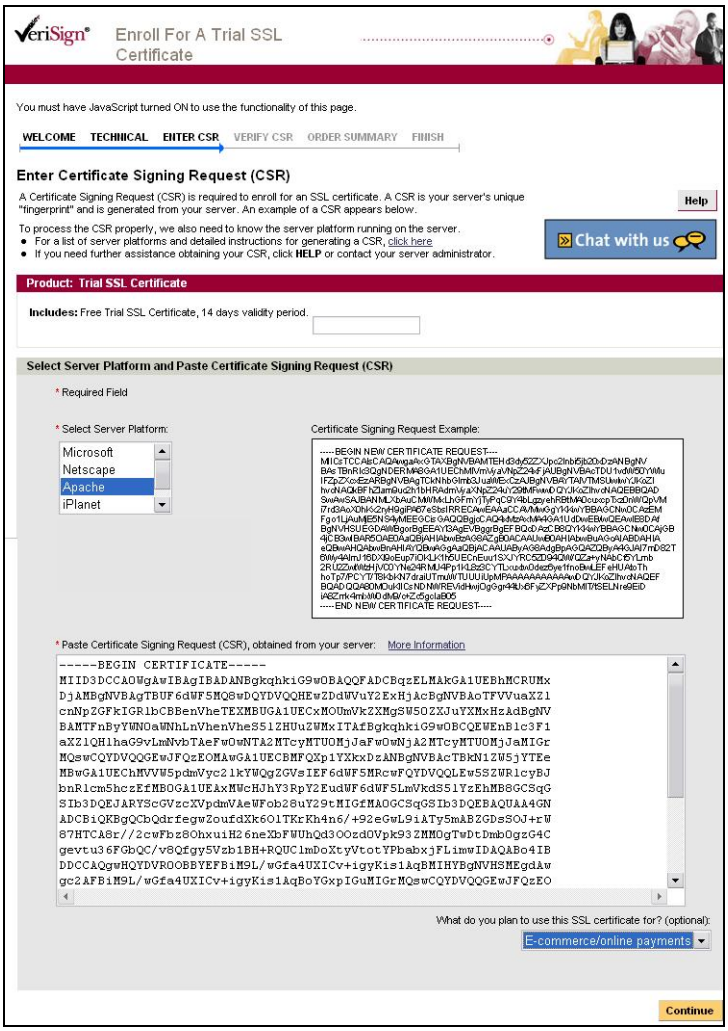

Gráfico 6.4

3) Le aparecerá los siguientes datos en donde le pedirá una clave que servirá para renovar el certificado.

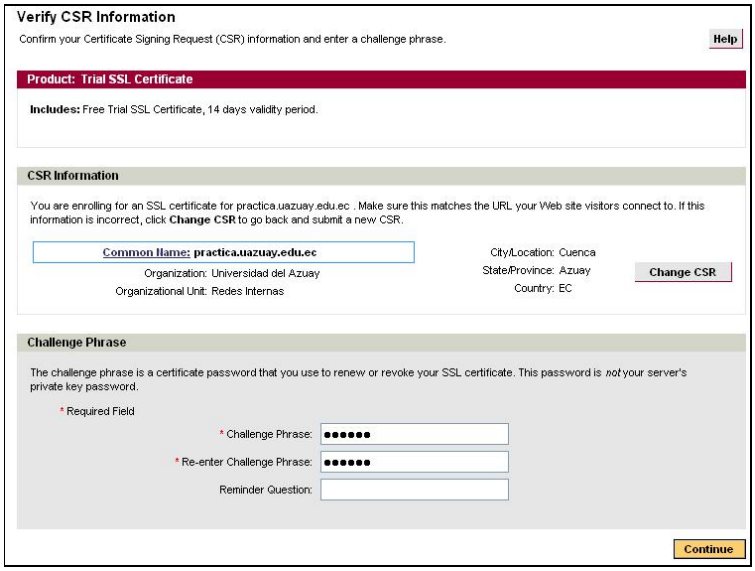

Gráfico 6.5

4) El siguiente paso le pedirá confirmar los datos que a llenado. De un click en aceptar para confirmar los datos. A continuación le saldrá la siguiente página:

Gráfico 6.6

Está página muestra el número de la orden, el tiempo de duración del certificado que es de 14 días y también que el certificado será enviado a la cuenta de correo electrónico en la próxima hora (realmente llega en un par de minutos).

5) Para instalar el nuevo certificado que le va a llegar por el correo electrónico saque un respaldo del certificado que creo anteriormente de la siguiente forma.

cd /etc/pki/tls/certs/
cp server.crt server.crt.bak2
rm server.crt

6) Vaya a la cuenta de correo electrónico que puso en el momento de registrarse y grabe el certificado que le llego con el nombre de server.crt en la carpeta **/etc/pki/tls/certs/server.crt** el contenido del archivo debe ser el siguiente.

-----BEGIN CERTIFICATE-----
MIIETjCCA7egAwIBAgIQcOZ6ude520TUuZljfBh/3DANBgkqhkiG9w0BAQUF
ADCB
jDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMT
AwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xMj
AwBgNV
BAMTKVZlcmlTaWduIFRyaWFsIFNlY3VyZSBTZXJ2ZXIgVGVzdCBSb290IE
NBMB4X
DTA1MDYyMDAwMDAwMFoXDTA1MDcwNDIzNTk1OVowgcQxCzAJBgNV
BAYTAkVDMQ4w
DAYDVQQIEwVBenVheTEPMA0GA1UEBxQGQ3VlbmNhMR4wHAYDVQQ
KFBVVbml2ZXJz
aWRhZCBkZWwgQXp1YXkxFzAVBgNVBAsUDlJlZGVzIEludGVybmFzMTo
wOAYDVQQL
FDFUZXJtcyBvZiB1c2UgYXQgd3d3LnZlcmlzaWduLmNvbS9jcHMvdGVzdG
NhIChj
KTA1MR8wHQYDVQQDFBZwcmFjdGljYS51YXp1YXkuZWR1LmVjMIGfMA
0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQCbQdrfegwZoufdXk6OlTKrKh4n6/+92eGw
L9iATy5m
ABZGDsSOJ+rW87HTCA8r//2cwFbz8OhxuiH26neXbFWUhQd3OOzd0Vpk9
3ZMM0gT

wDtDmb0gzG4Cgevtu36FGbQC/v8Qfgy5Vzb1BH+RQUCImDoXtyVtotYPba
bxjFLi
mwIDAQABo4IBdTCCAXEwCQYDVR0TBAIwADALBgNVHQ8EBAMCBaAw
RwYDVR0fBEAw
PjA8oDqgOIY2aHR0cDovL1NWUlNlY3VyZS1jcmwudmVyaXNpZ24uY29tL1
NWUlRy
aWFsUm9vdDIwMDUuY3JsMEoGA1UdIARDMEEwPwYKYIZIAYb4RQEHF
TAxMC8GCCsG
AQUFBwIBFiNodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYTAdB
gNV
HSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwNAYIKwYBBQUHAQEEK
DAmMCQGCCsG
AQUFBzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wbQYIKwYBBQUHA
QwEYTBf
oV2gWzBZMFcwVRYJaW1hZ2UvZ2ImMCEwHzAHBgUrDgMCGgQUj+XTG
oasjY5rw8+A
atRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nby5
naWYw
DQYJKoZIhvcNAQEFBQADgYEAJ3O5nS+B9cY3CLjTf31neBOXYoz156aw
KCSmYyFL
FZKWX6xT1hO40PzgeBZFr2UkoFYfMh57sdnA5hOR2ot3bKZKA8imQ7Omi
NjOZCe4
TKA01yQpUfEUtEcentOS5ap2HFv3bIer3jDhV9ueoafeZH0pz2HXrjtXHc71G
L8xJwHyHy1
GPA=
-----END CERTIFICATE-----

Nota:

En el caso de tener algún problema en la obtención del certificado digital vaya a la página del foro y baje el certificado que se encuentra allí.

7) Reinicie el servidor web con la instrucción **service httpd restart**. Pruebe que este el certificado digital instalado correctamente viendo la información del certificado.

6.3.4 Para que el servidor Web se inicie cuando se encienda el computador

Para que el servidor centOS5 se inicie cada vez que se inicializa el servidor ejecute la instrucción ntsysv y seleccione del listado el servicio httpd pulsando la barra espaciadora, con la tecla TAB sitúese en el botón de ok y púlselo dando un **enter**. La próxima vez que se reinicie el servidor también se iniciara el servidor Web.

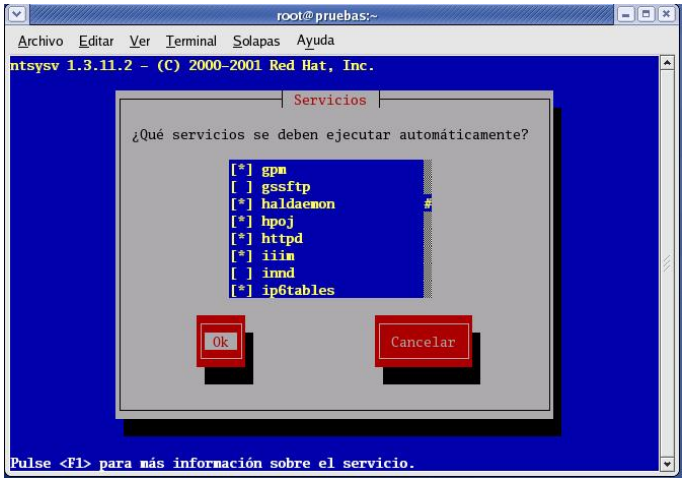

Gráfico 6.7

6.4 Ejercicios

1. En la práctica anterior se crearon dos certificados nuevos a más del que viene con el servidor apache. Reinstale los certificados digitales y vea cuales son las diferencias entre ellos. Haga un pequeño cuadro comparativo de las diferencias encontradas.

2. Con la experiencia obtenida en la práctica, indique cuales son los puntos que hay que fijarse para saber que un certificado digital sea considerado válido y poder confiar en el portal Web de dicho certificado.

6.5 Conclusión

En esta práctica se expuso la configuración de un servidor web en nuestro caso Apache y la creación de certificados digitales tanto gratuitos como otorgados por

una empresa certificadora todo esto con el fin de mantener segura nuestra información en la web mediante la encriptación de la misma.

CAPITULO 7. CONFIGURACIONES ADICIONALES DE UN SERVIDOR WEB

7.1 Introducción.

Como ya se vio en el capítulo anterior, un servidor web es un programa que implementa el protocolo HTTP (hypertext transfer protocol). Y esto sirve para transferir lo que llamamos hipertextos, páginas web o páginas HTML (hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música.

Este capítulo trata sobre ciertas configuraciones adicionales para optimizar su funcionamiento con el fin de adecuarlo para nuestras necesidades.

7.2 Configuraciones Adicionales

Se puede encontrar la cantidad de conexiones a Apache con estos comandos:

netstat -nt | grep :80 | wc -l
ps -A | grep httpd | wc -l (esto demostrará la cantidad de procesos)
ps -aux | grep httpd (esto mostrará los actuales procesos)

Para modificar los parámetros del servidor apache el archivo a modificar es /etc/httpd/conf/httpd.conf los parámetros a cambiar son:

- Numero de segundos antes de enviar un time out.

Timeout 120

- Permite que se establezcan conexiones HTTP persistentes. facilitan la posibilidad de que se establezcan sesiones HTTP de larga duración que permiten que se puedan enviar múltiples peticiones sobre la misma conexión TCP. En algunos casos, esto tiene como resultado una reducción de casi el 50% en los tiempos de retardo en el caso de documentos con muchas imágenes.

KeepAlive On

- Número de peticiones permitidas en una conexión persistente. Poniéndole 0 acepta un ilimitado número de conexiones

MaxKeepAliveRequests 100

- Tiempo que el servidor esperará peticiones subsiguientes en conexiones persistentes. Es el tiempo en segundos que Apache esperará peticiones subsiguientes antes de cerrar una conexión persistente. Una vez que una petición ha sido recibida, se aplica el valor especificado en la directiva Timeout para cerrar la conexión. Especificar un valor alto para KeepAliveTimeout puede provocar un menor rendimiento en servidores con mucha carga. Cuanto mayor sea el valor de timeout, mayor será el número de procesos del servidor se mantendrán ocupados esperando en conexiones con clientes no activos.

KeepAliveTimeout 3

- Número de procesos hijo del servidor que se crean al iniciar Apache. Como el número de procesos está controlado dinámicamente según la carga del servidor, no hay normalmente ninguna razón para modificar el valor de este parámetro.

StartServers 8

- Número mínimo de procesos hijo en espera. Si hay menos procesos hijo en espera que MinSpareServers, entonces el proceso padre crea nuevos procesos hijo a un ritmo máximo de uno por segundo. Ajustar este parámetro debe ser necesario solo en sitios Web con muchas visitas. Fijar un valor alto para este parámetro es una mala idea casi siempre.

MinSpareServers 10

- Número máximo de procesos hijo en espera que puede tener el servidor. Un proceso en espera es aquel que no está atendiendo ninguna petición. Ajustar este parámetro debe ser necesario solo en sitios Web con muchas

visitas. Fijar un valor alto para este parámetro es una mala idea casi siempre.

MaxSpareServers 20

- Máximo número de conexiones simultáneas. Cualquier intento de conexión por encima del límite MaxClients se pondrá en cola, hasta llegar a un límite basado en el valor de la directiva ListenBacklog. Una vez que un proceso hijo termina de atender una petición y queda libre, se atenderá una conexión en cola.

MaxClients 256

- Límite en el número de peticiones que un proceso hijo puede atender durante su vida. Después de atender MaxRequestsPerChild peticiones, el proceso hijo se eliminará. Si el valor especificado en esta directiva MaxRequestsPerChild es 0, no habrá límite. Especificar en la directiva MaxRequestsPerChild un valor distinto de cero tiene dos ventajas:

  Limita la cantidad de memoria que un proceso puede consumir en caso de que haya una fuga (accidental) de memoria;

  Establece un límite finito a la vida de los procesos, lo que ayuda a reducir el número existente de procesos cuando se reduce la carga de trabajo en el servidor.

MaxRequestsPerChild 4000

- Activa la resolución de DNS de las direcciones IP de los clientes. Esta directiva activa la resolución de DNS de manera que los nombres de host puedan ser guardados en los archivos log

HostnameLookups Off

- Para que no salga información sobre la versión del servidor Web se cambia esta directiva a Off para probar esto ponga una URL que no exista para que le dé un error

ServerSignature Off

- Permite indicar que archivo se cargara cuando se escriba el nombre de la carpeta. El orden de preferencia es el orden en el que se escribe los archivos.

DirectoryIndex index.html index.htm home.htm home.html home.php

- Cuando se crean archivos html en el cual las tildes no se escriben con los caracteres especiales de html se debe cambiar la directiva AddDefaultCharset de UTF-8 a ISO-8859-1

AddDefaultCharset ISO-8859-1

- Para que no se listen el contenido de las carpetas en el servidor web se modifica la directiva Options quitandole la palabra Indexes

<Directory "/var/www/html">
#Options Indexes FollowSymLinks por
Options FollowSymLinks

- Nombre de host y número de puerto que el servidor usa para identificarse. Cuando se quiere utilizar un servidor web la primera vez que se arranca da error en la directiva ServerName para quitar este error se descomenta la linea y se pone 127.0.0.1

#ServerName new.host.name:80
ServerName 127.0.0.1

- Para que cuando se accede a una carpeta del servidor le pida usuario y contraseña se realizan los siguientes pasos:

Se modifica las siguientes líneas

<Directory "/var/www/html">
AllowOverride controls what directives may be placed in .htaccess files.
It can be “All”, “None”, or any combination of the keywords:

```
#   Options FileInfo AuthConfig Limit
#
    AllowOverride None se cambia por    AllowOverride All

</Directory>
```

Para activar el acceso mediante clave a la carpeta se crea el archivo .htaccess en la carpeta que se quiere restringir el acceso con los permisos 755 y el archivo con las claves se lo debe poner fuera del sitio web en este caso es /var/www/claves.txt. El archivo .htaccess debe contener:

```
AuthName "Practica Web"
AuthType Basic
AuthUserFile /var/www/claves.txt
require valid-user
```

Para crear el archivo con las claves y usuarios se utiliza el comando htpasswd. de la siguiente forma:

```
htpasswd –bc [nombre del archivo]  [usuario] [clave]
```

- En un servidor web se puede dar acceso a los usuarios para que tengan su propio espacio Web y que ellos ingresen poniendo una url con el siguiente formato htt://nombre del sitio/~nombre del usuario. Para activar esto se realizan los siguientes pasos: Se modifica las directivas del modulo mod_userdir.c para que quede de la siguiente forma:

```
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    Se pone comentario
    #UserDir disable
    #
    # To enable requests to /~user/ to serve the user's public_html
```

```
    # directory, remove the "UserDir disable" line above, and uncomment
    # the following line instead:
    #
    Se Quita el comentario
    UserDir public_html

</IfModule>
```

Se descomenta todas estas líneas

```
<Directory /home/*/public_html>
    AllowOverride FileInfo AuthConfig Limit
     Options FollowSymLinks
    Esto se quita para que no puedan listar los directories y se deja como esta en la
línea     anterior
    #Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
        <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
```

Se crea en la carpeta del usuario la carpeta public_html (Ej: /home/usuario/publi_html) con permisos 755. Los archivos para el sitio web del usuario se lo tienen que pasar a esta carpeta.

7.3 Creación de Servidores Virtuales

Un servidor virtual es aquel en el cual dos direcciones URL distintas apuntan hacia un único servidor. Existen dos tipos de servidores virtuales los que tienen una sola ip para todos los dominios que maneja y la que tiene ip virtuales para cada uno de los dominios que maneja.

```
#############################################################
###  Para crear un servidor virtual con una sola IP se pone ##
###  Como requisito las URLs deben apuntar hacia la misma    ##
###  IP (esto se coloca al final del archivo httpd.conf      ##
###  combined en los logs es el formato que usa el log       ##
#############################################################
NameVirtualHost *:80

<VirtualHost *:80>
    ServerAdmin pruebas@uazuay.edu.ec
    DocumentRoot /var/www/html/pruebas
    ServerName www.pruebas.com
    ErrorLog /var/www/html/pruebas/logs/error_lo
    CustomLog /var/www/html/pruebas/logs/access_log combined
    DirectoryIndex index.htm
</VirtualHost>
<VirtualHost *:80>
    ServerAdmin virtual@uazuay.edu.ec
    DocumentRoot /var/www/html/virtual
    ServerName www.virtual.com
    ErrorLog /var/www/html/virtual/logs/error_lo
    CustomLog /var/www/html/virtual/logs/access_log combined
    DirectoryIndex home.htm
</VirtualHost>

#####################################################################
###  Para crear servidores virtuales cada uno con diferente IP ###
###  Como requisito se debe crear IP virtuales como eth0:1     ###
#####################################################################
# NameVirtualHost *:80
<VirtualHost 172.16.1.4>
    ServerAdmin pruebas@uazuay.edu.ec
    DocumentRoot /var/www/html/pruebas
    ServerName www.pruebas.com
    ErrorLog /var/www/html/pruebas/logs/error_lo
    CustomLog /var/www/html/pruebas/logs/access_log combined
```

```
    DirectoryIndex index.htm
</VirtualHost>

<VirtualHost 192.188.47.5>
    ServerAdmin virtual@uazuay.edu.ec
    DocumentRoot /var/www/html/virtual
    ServerName www.virtual.com
    ErrorLog /var/www/html/virtual/logs/error_lo
    CustomLog /var/www/html/virtual/logs/access_log combined
    DirectoryIndex home.htm
</VirtualHost>
```

7.4 Conclusión

En esta práctica se vieron ciertas configuraciones con el fin de optimizar nuestro servidor web y la forma como crear servidores virtuales que representan una alternativa económica y eficiente para aquellos que desean disfrutar los beneficios de un servidor dedicado pero aun no poseen el presupuesto para hacerlo.

CAPITULO 8. CONFIGURACIÓN DE UN SERVIDOR DNS

8.1 Introducción

Este capítulo trata sobre la configuración de un Servidor DNS o Sistema de Dominio de Nombres que es de mucha utilidad para resolver nombres de dominio, direcciones IP y para poder ubicar hosts de redes lejanas. Ya que es más fácil recordar nombres en vez de cifras. Sobre todo cuando se trata de una cantidad de direcciones tan inmensa como la que hay en Internet.

8.2 DNS

DNS (acrónimo de **D**omain **N**ame **S**ystem) es una base de datos distribuida y jerárquica que almacena la información necesaria para los nombre de dominio. Sus usos principales son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico correspondientes para cada dominio. El **DNS** nació de la necesidad de facilitar a los seres humanos el acceso hacia los servidores disponibles a través de Internet permitiendo hacerlo por un nombre, algo más fácil de recordar que una dirección **IP**.
Los **Servidores DNS** utilizan **TCP** y **UDP** en el puerto 53 para responder las consultas. Casi todas las consultas consisten de una sola solicitud **UDP** desde un **Cliente DNS** seguida por una sola respuesta **UDP** del servidor. **TCP** interviene cuando el tamaño de los datos de la respuesta excede los 512 bytes, tal como ocurre con tareas como **transferencia de zonas**.

8.3 NIC (Network Information Center).

NIC (acrónimo de **N**etwork **I**nformation **C**enter o Centro de Información sobre la Red) es una institución encargada de asignar los nombres de dominio en Internet, ya sean nombres de dominios genéricos o por países, permitiendo personas o empresas montar sitios de Internet mediante a través de un **ISP** mediante un DNS. Técnicamente existe un **NIC** por cada país en el mundo y cada uno de éstos es responsable por todos los dominios con la terminación correspondiente a su país.

Por ejemplo: NIC Ecuador es la entidad encargada de gestionar todos los dominios con terminación **.ec**, la cual es la terminación correspondiente asignada a los dominios de Ecuador.

8.4 FQDN (Fully Qualified Domain Name).

FQDN (acrónimo de **F**ully **Q**ualified **D**omain **N**ame o Nombre de Dominio Plenamente Calificado) es un Nombre de Dominio ambiguo que especifica la posición absoluta del nodo en el árbol jerárquico del DNS. Se distingue de un nombre regular porque lleva un punto al final.

Como ejemplo: suponiendo que se tiene un dispositivo cuyo nombre de anfitrión es «maquina1» y un dominio llamado «dominio.com», el **FQDN** sería «**maquina1.dominio.com.**», así es que se define de forma única al dispositivo mientras que pudieran existir muchos anfitriones llamados «maquina1», solo puede haber uno llamado «**maquina1.dominio.com.**». La ausencia del punto al final definiría que se pudiera tratar tan solo de un prefijo, es decir «**maquina1.dominio.com**» pudiera ser un dominio de otro más largo como «**maquina1.dominio.com.ec**».

La longitud máxima de un **FQDN** es de 255 bytes, con una restricción adicional de 63 bytes para cada etiqueta dentro del nombre del dominio. Solo se permiten los caracteres A-Z de ASCII, dígitos y el carácter «-». No se distinguen mayúsculas y minúsculas.

Desde 2004, a solicitud de varios países de Europa, existe el estándar **IDN** (acrónimo de **I**nternationalized **D**omain **N**ame) que permite caracteres no-ASCII, codificando caracteres **Unicode** dentro de cadenas de bytes dentro del conjunto normal de caracteres de **FQDN**. Como resultado, los límites de longitud de los nombres de dominio **IDN** dependen directamente del contenido mismo del nombre.

8.5 Componentes de un DNS.

Los DNS operan a través de tres componentes: Clientes DNS, Servidores DNS y Zonas de Autoridad.

8.5.1 Clientes DNS.

Son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Básicamente preguntan por la dirección IP que corresponde a un nombre determinado.

8.5.2 Servidores DNS.

Son servicios que contestan las consultas realizadas por los **Clientes DNS**. Hay dos tipos de servidores de nombres:

- **Servidor Maestro**: También denominado **Primario**. Obtiene los datos del dominio a partir de un fichero hospedado en el mismo servidor.

- **Servidor Esclavo**: También denominado **Secundario**. Al iniciar obtiene los datos del dominio a través de un Servidor Maestro (o primario), realizando un proceso denominado **transferencia de zona**.

Un gran número de problemas de operación de servidores DNS se atribuyen a las pobres opciones de servidores secundarios para las zonas de DNS. De acuerdo al RFC 2182, el DNS requiere que **al menos tres servidores existan** para todos los dominios delegados (o zonas).

Una de las principales razones para **tener al menos tres servidores** para cada zona es permitir que la información de la zona misma esté disponible siempre y forma confiable hacia los **Clientes DNS** a través de Internet cuando un servidor DNS de dicha zona falle, no esté disponible y/o esté inalcanzable.

Contar con múltiples servidores también facilita la **propagación** de la zona y mejoran la eficiencia del sistema en general al brindar opciones a los **Clientes DNS** si acaso encontraran dificultades para realizar una consulta en un **Servidor DNS**.

En otras palabras: tener múltiples servidores para una zona permite **contar con redundancia y respaldo del servicio**.

Con múltiples servidores, por lo general uno actúa como **Servidor Maestro o Primario** y los demás como **Servidores Esclavos o Secundarios**. Correctamente configurados y una vez creados los datos para una zona, no será necesario copiarlos a cada **Servidor Esclavo o Secundario**, pues éste se encargará de transferir los datos de manera automática cuando sea necesario.

Los **Servidores DNS** responden dos tipos de consultas:

- **Consultas Iterativas (no recursivas)**: El cliente hace una consulta al **Servidor DNS** y este le responde con la mejor respuesta que pueda darse basada sobre su caché o en las zonas locales. Si no es posible dar una respuesta, la consulta se reenvía hacia otro Servidor DNS repitiéndose este proceso hasta encontrar al **Servidor DNS** que tiene la **Zona de Autoridad** capaz de resolver la consulta.

- **Consultas Recursivas**: El **Servidor DNS** asume toda la carga de proporcionar una respuesta completa para la consulta realizada por el **Cliente DNS**. El **Servidor DNS** desarrolla entonces **Consultas Iterativas** separadas hacia otros **Servidores DNS** (en lugar de hacerlo el **Cliente DNS**) para obtener la respuesta solicitada.

8.5.3 Zonas de Autoridad.

Permiten al **Servidor Maestro o Primario** cargar la información de una zona. Cada **Zona de Autoridad** abarca al menos un dominio y posiblemente sus sub-dominios, si estos últimos no son delegados a otras zonas de autoridad.
La información de cada **Zona de Autoridad** es almacenada de forma local en un fichero en el **Servidor DNS**. Este fichero puede incluir varios tipos de registros:

Tipo de Registro.	Descripción.
A (**A**ddress)	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección **IPv4** de 32 bits.
AAAA	Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección **IPv6** de 128 bits.
CNAME (**C**anonical **Name**)	Registro de nombre canónico que hace que un nombre sea alias de otro. Los dominios con alias obtiene los sub-dominios y registros DNS del dominio original.
MX (**M**ail E**x**changer)	Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio, así como la prioridad entre éstos.
PTR (**P**oin**t**er)	Registro de apuntador que resuelve direcciones **IPv4** hacia el nombre anfitriones. Es decir, hace lo contrario al registro **A**. Se utiliza en zonas de **Resolución Inversa**.
NS (**N**ame **S**erver)	Registro de servidor de nombres que sirve para definir una lista de servidores de nombres con autoridad para un dominio.
SOA (**S**tart **o**f **A**uthority)	Registro de inicio de autoridad que especifica el **Servidor DNS** Maestro (o Primario) que proporcionará la información con autoridad acerca de un dominio de Internet, dirección de correo electrónico del administrador, número de serie del dominio y parámetros de tiempo para la zona.
SRV (**S**er**v**ice)	Registro de servicios que especifica información acerca de servicios disponibles a través del dominio. Protocolos como **SIP** (**S**ession **I**nitiation **P**rotocol) y **XMPP** (E**x**tensible **M**essaging and **P**resence **P**rotocol) suelen requerir registros **SRV** en la zona para proporcionar información a los clientes.
TXT (**Tex**t)	Registro de texto que permite al administrador insertar texto arbitrariamente en un registro DNS. Este tipo de

Tipo de Registro.	Descripción.
	registro es muy utilizado por los servidores de listas negras **DNSBL** (**DNS**-based **B**lackhole **L**ist) para la filtración de Spam. Otro ejemplo de uso son las VPN, donde suele requerirse un registro **TXT** para definir una llave que será utilizada por los clientes.
Registro HINFO:	Éste registro especifica los recursos de información del host, es decir, especificala CPU de la máquina y el SO (sistema operativo).

Las zonas que se pueden resolver son:

8.6 Zonas de Reenvío.

Devuelven **direcciones IP** para las búsquedas hechas para nombres **FQDN** (**F**ully **Q**ualified **D**omain **N**ame).

En el caso de dominios públicos, la responsabilidad de que exista una **Zona de Autoridad** para cada **Zona de Reenvío** corresponde a la autoridad misma del dominio, es decir, y por lo general, quien esté registrado como autoridad del dominio tras consultar una base de datos **WHOIS**. Quienes compran dominios a través de un **NIC** (por ejemplo: www.nic.mx) son quienes se hacen cargo de las **Zonas de Reenvío**, ya sea a través de su propio **Servidor DNS** o bien a través de los **Servidores DNS** de su **ISP**.

Salvo que se trate de un dominio para uso en una red local, todo dominio debe ser primero tramitado con un **NIC** como requisito para tener derecho legal a utilizarlo y poder propagarlo a través de Internet.

8.7 Zonas de Resolución Inversa.

Devuelven nombres **FQDN** (**F**ully **Q**ualified **D**omain **N**ame) para las búsquedas hechas para **direcciones IP**.

En el caso de segmentos de red públicos, la responsabilidad de que exista de que exista una **Zona de Autoridad** para cada **Zona de Resolución Inversa** corresponde a la autoridad misma del segmento, es decir, y por lo general, quien esté registrado como autoridad del segmento tras consultar una base de datos **WHOIS**.

Los grandes **ISP**, y en algunos casos algunas empresas, son quienes se hacen cargo de las **Zonas de Resolución Inversa**.

8.8 Práctica

El servicio que maneja el DNS es named para arrancar el servicio es **service named start** otras opciones son service named stop, service named restart. El puerto que utiliza es el 53.

El primer paso es editar el archivo **/etc/resolv.conf** aquí se pone el nombre del servidor de DNS en nuestro caso es el mismo equipo por lo tanto allí ira

nameserver 127.0.0.1

En la versión de centos 5.0 no existen los archivos de configuración así que deben ser creados de la siguiente manera:

yum install caching-nameserver

Instalando este paquete se instalarán los archivos para crear un DNS de cache y estos archivos se podrán modificar luego para personalizar la configuración

Se borra el archivo /etc/named.caching-nameserver.conf y también el archivo /var/named/chroot/etc/named.caching-nameserver.conf

Se crea el archivo /var/named/chroot/etc/named.conf con la siguiente información:

```
//
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};

options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        statistics-file "/var/named/data/named_stats.txt";
        allow-query { "reduda";};
        allow-re//
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};
cursion { "reduda";};
        allow-transfer { "reduda";};
        version "No disponible";
//
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};

options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        statistics-file "/var/named/data/named_stats.txt";
        allow-query { "reduda";};
        allow-re//
// named.conf for Red Hat caching-nameserver
//
```

```
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};
cursion { "reduda";};
        allow-transfer { "reduda";};
        version "No disponible";
        /*
         * If there is a firewall between you and nameservers you want
         * to talk to, you might need to uncomment the query-source//
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};

options {
        directory "/var/named";
        dump-file "/v/ named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};

options {ar/named/data/cache_dump.db";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        statistics-file "/var/named/data/named_stats.txt";
        allow-query { "reduda";};
        allow-recursion { "reduda";};
        allow-transfer { "reduda";};
        version "No disponible";

        /*
         * directive below.  Previous versions of BIND always asked
         * questions using port 53, but BIND 8.1 uses an unprivileged
         * port by default.
         */
         // query-source address * port 53;
};

//
```

```
// a caching only nameserver config
//
controls {
//      inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

logging {
category lame-servers { null; };

};

zone "." IN {
        type hinlogging {
category lame-servers { null; };

};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localdomain" IN {
        type master;
        file "localdomain.zone";//
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};

options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        statistics-file "/var/named/data/named_stats.txt";
        allow-query { "reduda";};
        allow-re//
```

```
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};
cursion { "reduda";};
        allow-transfer { "reduda";};
        version "No disponible";

        /*
         * If there is a firewall between you and nameservers you want
         * to talk to, you might need to uncomment the query-source//
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};

options {
        directory "/var/named";
        dump-file "/v/ named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};

options {ar/named/data/cache_dump.db";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        statistics-file "/var/named/data/named_stats.txt";
        allow-query { "reduda";};
        allow-recursion { "reduda";};
        allow-transfer { "reduda";};
        version "No disponible";

        /*
         * directive below.  Previous versions of BIND always asked
         * questions using port 53, but BIND 8.1 uses an unprivileged
         * port by default.
         */
         // query-source address * port 53;
```

```
};

//
// a caching only nameserver config
//
controls {
//      inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

logging {
category lame-servers { null; };

};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localdomain" IN {
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
```

```
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};
zone "." IN {
        type hint;
        file "named.ca";
};

zone "localdomain" IN {
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
```

```
        type master;
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};

include "/etc/rndc.key";

zone "localhost" IN {zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};
zone "." IN {
        type hint;
        file "named.ca";192.188.47.2
};

zone "localdomain" IN {
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
```

```
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};

include "/etc/rndc.key";

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
```

```
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};
```

Se hace un link simbólico a este archivo de la siguiente forma:

```
cd /etc
ln -s /var/named/chroot/etc/named.conf  -f
```

Se crea el archivo /etc/rndc.conf con el siguiente contenido:

```
/*
 * Copyright (C) 2004  Internet Systems Consortium, Inc. ("ISC")
 * Copyright (C) 2000, 2001  Internet Software Consortium.
 *
 * Permission to use, copy, modify, and distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
 * copyright notice and this permission notice appear in all copies.
 *
 * THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
 * REGARD TO TH*
 * Copyright (C) 2004  Internet Systems Consortium, Inc. ("ISC")
 * Copyright (C) 2000, 2001  Internet Software Consortium.
 **
 * Copyright (C) 2004  Internet Systems Consortium, Inc. ("ISC")
 * Copyright (C) 2000, 2001*
 * Copyright (C) 2004  Internet Systems Consortium, Inc. ("ISC")
 * Copyright (C) 2000, 2001  Internet Software Consortium.
 *
 * Permission to use, copy, modify, and distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
 * copyright notice and this   Internet Software Consortium.
```

```
 *
 * Permission to use, copy, modify, and distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
 * copyright notice and this
 * Permission to use, copy, modify, and distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
 * copyright notice and this IS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
 * AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
 * INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
 * LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
 * OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
 * PERFORMANCE OF THIS SOFTWARE.
 */

/* $Id: rndc.conf,v 1.7.2.1 2004/03/09 06:09:27 marka Exp $ */

/*
 * Sample rndc configuration file.
 */

options {
        default-server  localhost;
        default-key     "rndckey";
};

server localhost {
        key     "rndckey";
};

include "/etc/rndc.key";
```

Se da permisos al archivo /etc/rndc.conf

```
chgrp named rndc.conf
chmod 640 rndc.conf
```

Otro ejemplo de configuración del archivo named.conf para resolver las direcciones q llegan al equipo.

```
//
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1;};

options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        statistics-file "/var/named/data/named_stats.txt";
        allow-query { "reduda";};

// named.conf for Red Hat caching-nameserver
//
        allow-transfer { "reduda";};
        version "No disponible";
//
// named.conf for Red Hat caching-nameserver
};
logging {
category lame-servers { null; };

};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localdomain" IN {
        type master;
```

```
        file "localdomain.zone";//
// named.conf for Red Hat caching-nameserver
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};

include "/etc/rndc.key";
```

8.9 Explicación de algunas líneas del archivo named.conf

Se pone permisos para que solo acepte peticiones de nuestra LAN el archivo que se debe modificar es /etc/named.conf:

Permisos para que solo la red Nuestra consulte el DNS

acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16; 192.188.47.0/24;};

```
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        qua
```

acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16; 192.188.47.0/24;};

```
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
```

directorcl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16; 192.188.47.0/24;};

```
optionsery-source    port 53;
        query-source-v6 port 53;
        //allow-query     { localhost; };
```

allow-query { "reduda";};

allow-recursion { "reduda";};

allow-transfer { "reduda";};

version "No disponible";

```
192.188.47.2};options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
```

```
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";192.188.47.2
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        query-source    port 53;
        query-source-v6 port 53;
        //allow-query     { localhost; };
        allow-query { "reduda";};
        allow-recursion { "reduda";};
        allow-transfer { "reduda";};
        version "No disponible";

};
```

Realizados estos cambios ya se puede iniciar el servicio named. Lo que se acabo de configurar es un servidor DNS de cache, con esto las IPS de los sitios se almacenaran en la memoria del servidor y de esta manera no se consultara a los servidores raíz.

También se puede crear un servidor DNS con los nombres de las maquinas de nuestra red de esta forma si el enlace de Internet se cae la red puede seguir resolviendo los nombres de nuestra red. Para realizar esto se siguen los siguientes pasos:

Se deben crea la zona del dominio que se quiere manejar al final del archivo /etc/named.conf en este caso uazuay.edu.ec

```
zone "uazuay.edu.ec" {
        type master;
        file "uazuay.edu.ec.hosts";
        };
```

También se debe crear la zona del dominio inverso en este caso 47.188.192.in-addr.arpa (47.188.192 es la red a la que pertenece pero al revés)

```
zone "47.188.192.in-addr.arpa" {
        type master;
```

```
    file "47.188.192.in-addr.arpa";
};
```

A continuación se crear dos archivos en la carpeta /var/named/chroot/var/named con el siguiente contenido.

Archivo uazuay.edu.ec.hosts (archivo que da la ip basado en el nombre)

```
$ttl 38400
uazuay.edu.ec.  IN      SOA     uazuay. root.uazuay.edu.ec. (
                        1157674723      ; Serial Number
                        10800           ; Refresh (4 horas)
                        3600            ; Retry (2 horas)
                        604800  ; Expire (30 dias)
                        38400 ) ; Minimum TTL (8 horas)
uazuay.edu.ec.          IN      NS      uazuay.edu.ec.
www.uazuay.edu.ec.      IN      A       192.188.47.11
servicios.uazuay.edu.ec.        IN      A       192.188.47.12
uazuay.edu.ec.          IN      MX      10 192.188.47.2
```

Archivo 47.188.192.in-addr.arpa (archivo que da el nombre basado en la ip)

```
@       IN SOA  auzuay.edu.ec. root.uazuay.edu.ec. (
            1998022601              ; Serial Number
            14400                   ; Refresh (4 horas)
            7200                    ; Retry (2 horas)
            2592000                 ; Expire (30 dias)
            28800 )                 ; Minimum TTL (8 horas)

        IN NS   uazuay.

2       IN PTR  uazuay.edu.ec.
11      IN PTR  www.uazuay.edu.ec.
```

Realizado esto se reinicializa el servicio named. Para probar que funciona el servidor DNS se utiliza el comando nslookup:

```
nslookup        uazuay.edu.ec
nslookup        192.188.47.2
```

También hay que realizar unos cambios en el script del service para que funcione correctamente para esto se edita el archivo /etc/init.d/named y se va a la línea del procedimiento de stop y se modifica todo el procedimiento cambiándolo por el siguiente código

```
    # Stop daemons.
    echo -n $"Stopping $prog: "
    /usr/sbin/rndc stop >/dev/null 2>&1
    RETVAL=$?
    if [ $RETVAL -eq 0 ]; then
       rm -f /var/lock/subsys/named
       rm -f /var/run/named.pid
    elif pidof named >/dev/null; then
192.188.47.2        killproc named -TERM >/dev/null 2>&1
       RETVAL=$?
       if [ $RETVAL -eq 0 ]; then
          rm -f /var/lock/subsys/named
          rm -f /var/run/named.pid
       fi;
    fi;
    if [ $RETVAL -eq 0 ]; then
       success
    else
       failure
    fi;
    echo
    return $RETVAL
```

8.10 URL de sitios para revisar la correcta configuración de un servidor DNS

http://www.squish.net/dnscheck

http://www.dnsstuff.com/
http://centralops.net/co/

8.11 URL en donde se puede registrar gratis un dominio en un servidor DNS

http://www.everydns.net/index.php
http://www.no-ip.com

8.12 Configuración UDA

/etc/named.caching-nameserver.conf

```
//
// named.conf for Red Hat caching-nameserver
//
acl "reduda" {127.0.0.1; 200.93.222.0/24; 192.168.1.0/24; 172.16.0.0/16;
192.188.47.0/24;};

options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        allow-query { "reduda";};
        allow-recursion { "reduda";};
        allow-transfer { "reduda";};
        version "No disponible";

        /*
         * If there is a firewall between you and nameservers you want
         * to talk to, you might need to uncomment the query-source
         * directive below.  Previous versions of BIND always asked
         * questions using port 53, but BIND 8.1 uses an unprivileged
         * port by default.
         */
         // query-source address * port 53;
```

```
};

//
// a caching only nameserver config
//
controls {
//      inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

logging {
category lame-servers { null; };

};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localdomain" IN {
        type master;
        file "localdomain.zone";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
```

```
zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};

include "/etc/rndc.key";
```

/var/named/chroot/var/named/ 47.188.192.in-addr.arpa

```
@       IN SOA  auzuay.edu.ec. root.uazuay.edu.ec. (
                1998022601              ; Serial Number
                14400                   ; Refresh (4 horas)
                7200                    ; Retry (2 horas)
                2592000                 ; Expire (30 dias)
                28800 )                 ; Minimum TTL (8 horas)

        IN NS   uazuay.

2       IN PTR  uazuay.edu.ec.
11      IN PTR  www.uazuay.edu.ec.
```

/var/named/chroot/var/named/uazuay.edu.ec.hosts

```
$ttl 38400
```

```
uazuay.edu.ec.  IN      SOA     uazuay. root.uazuay.edu.ec. (
                        1157674723      ; Serial Number
                        10800           ; Refresh (4 horas)
                        3600            ; Retry (2 horas)
                        604800  ; Expire (30 dias)
                        38400 ) ; Minimum TTL (8 horas)
uazuay.edu.ec.          IN      NS      uazuay.edu.ec.
www.uazuay.edu.ec.      IN      A       192.188.47.11
servicios.uazuay.edu.ec.        IN      A       192.188.47.12
uazuay.edu.ec.          IN      MX      10 192.188.47.2
```

/etc/rndc.conf

```
/*
 * Copyright (C) 2004  Internet Systems Consortium, Inc. ("ISC")
 * Copyright (C) 2000, 2001  Internet Software Consortium.
 *
 * Permission to use, copy, modify, and distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
 * copyright notice and this permission notice appear in all copies.
 *
 * THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
 * REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
 * AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
 * INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
 * LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
 * OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
 * PERFORMANCE OF THIS SOFTWARE.
 */
```

```
/* $Id: rndc.conf,v 1.7.2.1 2004/03/09 06:09:27 marka Exp $ */

/*
 * Sample rndc configuration file.
 */

options {
	default-server  localhost;
	default-key     "rndckey";
};

server localhost {
	key     "rndckey";
};

include "/etc/rndc.key";
```

8.13 Conclusión

En este capítulo se vio conceptos de DNS, NIC, FQDN, Componentes, Zonas de Reenvió, Zonas de Resolución Inversa, etc., con el fin de obtener los conceptos necesarios para realizar la práctica, también se muestra la configuración de la Universidad con el fin de tener una idea para la configuración de nuestro propio servidor DNS.

CAPITULO 9: CONFIGURACIÓN DE TELNET Y FTP

9.1 Introducción

En este capítulo se describe el uso de dos herramientas muy potentes denominadas FTP y telnet, y aunque esta última es poco usada debido a los avances informáticos en otros campos sigue siendo muy útil. Se explicara la configuración de estos protocolos que son usados para transferencia de archivos y para acceder en forma remota a otro equipo con el fin de conocer su funcionamiento.

9.2 TELNET

Telnet es el nombre de un protocolo que sirve para acceder en forma remota a otro equipo. Utiliza el puerto 23 para establecer la comunicación con el equipo. Toda la información que se trasmita con este protocolo no está encriptado por lo que no se recomienda su uso.

Se borra o renombra el archive /etc/securetty en el archivo
Archivo de configuración de telnet es /etc/xinetd.d/telnet

Se aumenta la línea **only_from** para que solo esas direcciones ip tengan acceso

```
service telnet
{
	disable = no
	flags		= REUSE
	socket_type	= stream
	wait		= no
	user		= root
	server		= /usr/sbin/in.telnetd
	only_from	= 168.0.0.3 168.0.0.4 168.0.0.5
	log_on_failure	+= USERID
```

}

Si se desea que el usuario root se conecte se debe borrar o renombrar el archivo /etc/securetty

Para activar el servicio se ejecuta ntsys y se activa el servicio telnet, luego se reinicia el servicio xinetd de la siguiente forma service xinetd restart

9.3 FTP

FTP es el protocolo que se utiliza para la transferencia de archivos (File Transfer Protocol). Por defecto utiliza los puertos 20 y 21. El puerto 20 es el utilizado para el flujo de datos entre el cliente y el servidor y el puerto 21 para el flujo de control, es decir, para enviar las órdenes del cliente al servidor. Igual que el protocolo TELNET tampoco encripta la información que transmite.

El servicio que controla el servidor ftp se llama vsftpd para iniciarlo ejecutar service vsftpd start.

El archivo de configuración del servidor vsftpd es /etc/vsftpd/vsftpd.conf allí se hacen los siguientes cambios:

1.- Para que en los archivos log marque la hora local y no la GMT se agrega al archivo

use_localtime=YES

2.- La siguiente línea se des comenta para que se genere los log

xferlog_file=/var/log/vsftpd.log

3.- Se aumenta la siguiente línea para registrar en el archivo de log todos los protocolos de conexión

log_ftp_protocol=YES

4.- Se pone a No esta opción para que registre en los archivo de lo las fallas de acceso y los accesos correctos

xferlog_std_format=NO

5.- Se desactiva el servicio de anonymous con:

anonymous_enable=NO

6.- Para que aparesca un mensaje cuando se conecte

ftpd_banner=Bienvenido a la UDA

7.- Para configurar la tasa máxima de transferencia de los usuarios anónimos y locales

a 5 Kb se pone:

anon_max_rate=5120

local_max_rate=5120

8.- Número máximo de clientes que podrán acceder simultáneamente al servidor

max_clients=5

9.- Número máximo de conexiones desde una misma ip

max_per_ip=5

10.- Para que los usuarios solo se desplacen en su carpeta y no se puedan hacer un cd a otras carpetas

#se aumenta la línea esto hace que los usuarios no se desplacen a otra carpeta

chroot_local_user=YES

chroot_local_user=YES

9.4 Conclusión

Podemos concluir acerca de estas dos herramientas que:

Telnet sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. También se usaba para

consultar datos a distancia, como datos personales en máquinas accesibles por red , información bibliográfica, etc.

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.

Es por este motivo que se vio necesario hacer una práctica acerca de estas herramientas para tener una idea de su funcionamiento.

CAPITULO 10. CONFIGURACIÓN DE UN SERVIDOR PROXY (SQUID)

10.1 Introducción

En la navegación por internet se ha vuelto de suma importancia el ahorro de ancho de banda y esto ahora lo podemos lograr mediante la configuración de un servidor proxy. En este capítulo se realizarán las configuraciones necesarias con el fin de facilitar el rápido acceso a las páginas ya antes visitadas y a la vez como ya se menciono ahorrar ancho de banda.

10.2 Servidor Proxy

Un servidor Proxy actúa de cache de navegación para sus clientes si un cliente de la red local ya navego en la página que otro cliente quiere navegar el servidor Proxy le envía la página almacenada en su cache de esta forma el segundo cliente no ocupa ancho de banda del Internet y su navegación es más rápida. Se puede con un servidor Proxy ahorrar hasta un 40 % de ancho de banda.

El servidor Proxy mas utilizado es Squid soporta muchos protocolos, aunque se usa principalmente para HTTP y FTP. Se añade soporte también a TLS, SSL, Internet Gopher y HTTPS.

10.3 Acerca de Squid.

Squid es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo equipamiento lógico libre, está disponible el código fuente para quien así lo requiera.

Entre otras cosas, Squid puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS,

Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y y herramientas para clientes. Al iniciar Squid da origen a un número configurable (5, de modo predefinido a través del parámetro dns_children) de procesos de búsqueda en servidores DNS, cada uno de los cuales realiza una búsqueda única en servidores DNS, reduciendo la cantidad de tiempo de espera para las búsquedas en servidores DNS.

Para que un cliente de una red pueda utilizar el servidor Proxy se lo tiene que configurar. En el Internet Explorer esta opción esta en Herramientas, Opciones de Internet, Conexiones, Configuración de Lan, se activa la casilla de Servidor Proxy y se pone la dirección IP del servidor Proxy y el puerto en el cual se lo configuró.

El archivo de configuración de Squid es /etc/squid/squid.conf se lo edita y se realizan los siguientes cambios:

- Puerto por el cual va a funcionar el servidor. Por defecto esta en el 3128 se lo cambia al 8080 que es el puerto por defecto para servidores Proxy

```
# http_port 3128
http_port 8080
```

- El parámetro cache_mem establece la cantidad ideal de memoria para, Objetos en tránsito, Objetos frecuentemente utilizados (Hot), Objetos negativamente almacenados en el caché.

```
# cache_mem 8 MB
cache_mem 16 MB
```

- El parámetro cache_dir se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para Squid. El valor por defecto que ocupa Squid para almacenar sus datos es 100 MB se lo puede cambiar con este

parámetro a 700 MB. Los números 16 y 256 significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno. No se debe modificar esos valores.

```
# cache_dir ufs /var/spool/squid 100 16 256
cache_dir ufs /var/spool/squid 700 16 256
```

- Para impedir que de otras redes utilicen nuestro servidor Proxy se maneja las listas de control de acceso (ACL) allí se ponen las IP o las redes permitidas que se pueden comunicar con nuestro servidor.

acl localhost src 127.0.0.1/255.255.255.255 esta línea se modifica por
acl localhost src 127.0.0.1/255.255.255.255 172.16.0.1 - 172.16.254.254/255.255.255.255 192.168.1.1-192.168.1.254/255.255.255.255 192.188.47.1-192.188.47.254/255.255.255.255

Donde localhost es el nombre del ACL y 172.16.0.1 – 172.16.254.254 es el rango de IP a las cuales se les da acceso e igual para el resto de valores. Para aceptar esta ACL se utiliza el parámetro http_access allow manager localhost donde manager y localhost son los ACL que se les da permiso. Si se quiere denegar el acceso a esta lista se cambiaria la palara allow por deny.

Otro ejemplo de utilización de ACL para impedir la utilización del MSN seria:

```
acl msn_messenger req_mime_type -i ^application/x-msn-messenger$
http_access deny msn_messenger
```

Por ultimo agregar al archivo de configuración la instrucción

```
visible_hostname localhost
```

Para arrancar el servicio la primera vez se utiliza la instrucción **squid –z** esta instrucción crea todos los archivos y carpetas necesarias para almacenar la información de cache. Luego de esto se activa el servidor squid con la instrucción **service squid start**.

10.3.1 Recomendaciones:

Los archivos de Log del squid situados en /var/log/squid no deben sobrepasar los 2Gb si esto sucede en el archivo de /var/log/messages aparecerá un mensaje de error como el siguiente; **Squid Parent: child process XXXX exited due to signal 25** y el servidor squid no arrancara. Lo que se debe hacer es borrar los logs del squid y se arreglará el problema.

10.4 Conclusión

En esta práctica vimos como configurar un Servidor Proxy utilizando squid que es una de las herramientas más utilizadas, todo esto con el fin de optimizar el acceso a las páginas más visitadas y ahorrar el ancho de banda.

CAPITULO 11. CONFIGURACIÓN DE SSH

11.1 Introducción.

En muchas ocasionas es indispensable poder acceder a maquinas remotas a travez de una red con el fin de consultar información o manipular un ordenador. En una práctica anterior vimos el uso de telnet que nos permitía hacer esto pero el problema consistía en que la información que era capturada usando esta herramienta no era encriptada y los atacantes podían hacer uso de ella.

Es por eso que en este capítulo se describe la configuración de SSH que nos permite acceder y manipular información de un equipo remoto pero con la diferencia que esta información se haya encritada por lo que no tendrá utilidad para algún atacante.

11.2 SSH

SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red, utilizando el puerto 22. Permite manejar por completo el ordenador mediante un intérprete de comandos. Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas). SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya encriptada de tal forma que si se captura la información esta sea ilegible.

El archivo de configuración de ssh es /etc/ssh/sshd_config allí se tiene que realizar los siguientes cambios:

- Se cambia el puerto de defecto a uno que este libre con el parámetro Port de esta forma se hace mas difícil para un atacante descubrir que está en ese puerto

#Port 22

Port 5678

- Se cambia la versión del protocolo que se utiliza por defecto viene para que funcione con la versión 1 y 2 se le deja solo la 2 ya que la 1 tiene fallas

#Protocol 2, 1
Protocol 2

- Si el equipo tiene más de una tarjeta de red se puede configurar para que ssh solo atienda peticiones de una de las tarjetas para esto se le indica la ip de la tarjeta de red por la cual se desea escuchar peticiones. Si se pone 0.0.0.0 se escucha en todas las tarjetas de red

ListenAddress 168.0.0.2

- Si se desea que el usuario root se pueda conectar se descomenta el parámetro PermitRootLogin

#PermitRootLogin yes
PermitRootLogin yes

- Para permitir solo a ciertos usuarios que puedan conectarse se utiliza el parámetro AllowUsers en este ejemplo se permite conectarse como root solo desde el equipo 168.0.0.2 y 168.0.0.3 y los usuarios aizquierdo y xizquierdo se pueden conectarse desde cualquier equipo

AllowUsers root@168.0.0.2 root@168.0.0.3 aizquierdo xizquierdo

- En este otro ejemplo se permite conectar solo al usuario xavier

AllowUsers root xavier

- Para conectarse a un equipo mediante ssh se utiliza el formato usuario@ip_del_equipo. Para transferencia de archivos se utiliza sftp. Ejemplo:

  ssh aizquierdo@168.0.0.3

sftp xizquierdo@168.0.0.3

- Otra forma de conectarse para el caso que se haya cambiado el puerto de conexión es la siguiente:

  ssh -p 5678 root@192.168.1.201

  En ambos casos si es la primera vez saldrá el siguiente mensaje:

  The authenticity of host '168.0.0.3 (168.0.0.3)' can't be established.
  RSA key fingerprint is a1:74:1f:28:48:34:97:bf:ca:55:64:b3:26:ba:c1:14.
  Are you sure you want to continue connecting (yes/no)?
  Se tiene que contestar que yes para que acepte la llave publica de encriptación y establezca la conexión.

11.3 Conclusión

En esta práctica se realizó la configuración del SSH que consistió en el cambio del puerto de conexión, protocolo, configuración de usuarios, etc., con el fin de optimizar el uso de esta herramienta y volverla más segura.

CAPITULO 12. CONFIGURACIÓN DE UN SERVIDOR DHCP

12.1 Introducción

Dentro de una red es posible asignar direcciones ip a los equipos automáticamente, para ello en este capítulo se desarrollara la configuración de un servidor DHCP, esto con el fin de evitar duplicados en la red.

Es muy útil este tipo de configuración en el caso de una red que se encuentre formada por una gran cantidad de equipos, la cual si no contara con un servidor DHCP se tendría que configurar equipo por equipo asignando una dirección ip a cada uno y una máscara lo que provocaría pérdida de tiempo, confusión ya que puede asignar a otro equipo una dirección que ya fue asignada.

12.2 DHCP

DHCP son las siglas en inglés de Protocolo de configuración dinámica de servidores (Dynamic Host Configuration Protocol). Este protocolo asigna dinámicamente las direcciones de IP, mascara de red, servidor DNS y gateway a las máquinas a quien sirve.

Sin DHCP, cada dirección IP debe configurarse manualmente en cada ordenador y, si el ordenador se mueve a otro lugar en otra parte de la red, se debe de configurar otra dirección IP diferente. El DHCP le permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias y, automáticamente, asignar y enviar una nueva IP si el ordenador es conectado en un lugar diferente de la red.

El protocolo DHCP incluye tres métodos de asignación de direcciones IP:

Asignación manual: donde la asignación se basa en una tabla con direcciones MAC (pares de direcciones IP ingresados manualmente por el administrador). Sólo las computadoras con una dirección MAC que figure en dicha tabla recibirá el IP que le asigna dicha tabla.

Asignación automática: donde una dirección de IP libre obtenida de un rango determinado por el administrador se le asigna permanentemente a la computadora que la requiere.

Asignación dinámica: el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de direcciones IP y cada computadora conectada a la red está configurada para solicitar su dirección IP al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo controlable. Esto facilita la instalación de nuevas máquinas clientes a la red.

El archivo que se debe configurar es /etc/dhcpd.conf allí se deben realizar los siguientes cambios:

Se requiere instalar el paquete dhcp, el cual deberá estar incluido en los discos de instalación de la mayoría de las distribuciones.

yum -y install dhcp

12.3 Ejemplos de configuraciones DHCP

- El siguiente ejemplo asigna direcciones ip desde la 192.168.1.205 hasta192.168.1.210 entre dos equipos;

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style interim;
ignore client-updates;

subnet 192.168.1.0 netmask 255.255.255.0 {

# --- default gateway
#       option routers                  192.168.0.1;192.168.1.205 192.168.1.210;
       option subnet-mask              255.255.255.0;
```

```
        option nis-domain           "domain.org";
        option domain-name          "domain.org";
        option domain-name-servers      192.168.1.201;

        option time-offset          -18000; # Eastern Standard Time
#       option ntp-servers          192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.1.205 192.168.1.210;
        default-lease-time 21600;
        max-lease-time 43200;
        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
```

En el caso de usar una máquina virtual para que se pueda asignar una dirección mediante DHCP a la misma máquina en el otro sistema operativo (Windows) fuera de la maquina virtual debe estar conectado el cable.

Para probar la asignación de DHCP se coloca en **panel de control**, luego en **conexiones de red**, luego **conexión de área local**, en **propiedades del protocolo tcp-ip**, en **obtener una dirección automáticamente**.

Para revisar la asignación damos doble clic en **conexión de área local** y escogemos la opción **soporte** y revisamos la conexión asignada.

- Para asignar una dirección ip mediante la dirección mac añadimos la siguiente línea al final del archivo dentro de /etc/dhcpd.conf

host EQUIPO10_INTERNET { option host-name "EQUIPO10_INTERNET"; hardware ethernet 00:10:B5:F9:C4:38; fixed-address 192.168.1.206; }
En donde EQUIPO10_INTERNET es el nombre del equipo al cual se le va a asignar una dirección, 00:10:B5:F9:C4:38 y192.168.1.206 es la ip a asignarse

- El siguiente ejemplo asigna direcciones ip desde la 168.0.0.3 a la 168.0.0.254

```
authoritative;
one-lease-per-client on;
server-identifier 168.0.0.2;
ddns-updates on;
ddns-update-style ad-hoc;
default-lease-time 86400;
max-lease-time 86400;
option domain-name-servers 168.0.02;
option broadcast-address 168.0.255.255;
option subnet-mask 255.255.0.0;
option routers 168.0.0.1;
# Configuración de la Red a quien sirve en este caso asignara direcciones ip desde la
# 168.0.0.0 hasta la 168.0.0.254
subnet 168.0.0.0 netmask 255.255.0.0 {
    range 168.0.0.3 168.0.0.254;
    }
```

- El siguiente ejemplo asigna direcciones desde la ip 172.30.1.3 hasta la 172.30.1.254 y asigna direcciones ip median la direccion mac a las mac 00:0d:88:ca:35:da , 00:D0:09:D5:3B:12 , 00:E0:4C:94:B6:C5 , 00:0a:e6:43:45:85

```
host EQUIPO10_INTERNET { option host-name "EQUIPO10_INTERNET"; hardware ethernet 00:10:B5:F9:C4:38; fixed-address 192.168.1.206; }
ddns-update-style interim;
ignore client-updates;

shared-network uda {
```

```
subnet 192.188.47.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.188.47.3;
        option subnet-mask              255.255.255.0;
        option nis-domain               "uazuay.edu.ec";
        option domain-name              "uazuay.edu.ec";
        option domain-name-servers      192.188.47.2;
        option time-offset              -18000;         # Eastern Standard Time

        option root-path            "192.188.47.9:/opt/ltsp/i386";

#       range dynamic-bootp 192.188.47.233 192.188.47.247;
        default-lease-time 21600;
        max-lease-time 43200;

host JGUILLEN { option host-name "JGUILLEN"; hardware ethernet
00:0d:88:ca:35:da; fixed-address 192.188.47.136; }
host ASO-ELEC2 { option host-name "ASO-ELEC2"; hardware ethernet
00:D0:09:D5:3B:12; fixed-address 192.188.47.84; }
host ASO-ELEC3 { option host-name "ASO-ELEC3"; hardware ethernet
00:E0:4C:94:B6:C5; fixed-address 192.188.47.85; }
host REACUDAFE { option host-name "REACUDAFE"; hardware ethernet
00:0a:e6:43:45:85; fixed-address 192.188.47.61; }
}

subnet 172.30.0.0 netmask 255.255.0.0 {

# --- default gateway
      one-lease-per-client on;
      option routers                172.30.1.1;
      option subnet-mask              255.255.0.0;
      option nis-domain             "wlan.uazuay.edu.ec";
      option domain-name              "wlan.uazuay.edu.ec";
      option domain-name-servers      172.30.1.1;
      range dynamic-bootp 172.30.1.3 172.30.1.254;
```

```
    default-lease-time 86400;
    max-lease-time 86400;
}

}
```

12.4 Descripción de las Opciones del Archivo

authoritative Cuando hay dos servidores DHCP en la red el que tenga este parámetro es el que va a servir a la red y cuando este servidor este caído servirá a la red el otro servidor.

ddns-updates Activa la actualización DNS mediante los valores asignados por DHCP.

ddns-update-style Define el método de actualización automática de las DNS. Los valores pueden ser ad-hoc, interim y none.

default-lease-time Especifica la cantidad de tiempo, en segundos, que será mantenida una asignación de direcciones, siempre y cuando el cliente no haya especificado algo concreto.

ignore allow / client-updates Permite la actualización de las asignaciones (allow) de un cliente a requerimiento de este, o bien las asignaciones se actualizan cuando el servidor así lo requiera (ignore).

max-lease-time Especifica la cantidad máxima de tiempo, en segundos, que será mantenida una asignación de direcciones. No está sujeta a esta especificación la asignación dinámi/var/lib/dhcp/dhcpd.leasesca BOOTP.

netmask Define la máscara de red de la Subred

not authoritative La función de este parámetro es justo la contraria del anterior. Es decir: la configuración del servidor de DHCP no es

concluyente y los clientes mal configurados que sean detectados por el servidor, seguirán con su configuración intacta.

one-lease-per-client Cuando la opción se iguala a on y un cliente solicita una asignación de dirección (DHCPREQUEST), el servidor libera de forma automática cualquier otra asignación asociada a dicho cliente. Con esto se supone que si el cliente solicita una nueva asignación es porque ha olvidado que tuviera alguna, luego tiene un sólo interfaz de red. No dándose esta situación entre los clientes no es muy aconsejable el uso de esta opción.

option broadcast-address Define la dirección de broadcast de la Red.

/var/lib/dhcp/dhcpd.leases

option domain-name-servers Define el nombre de los servidores DNS.

option nis-servers Define la lista de servidores NIS (Sun Network Information Server) disponibles. Los servidores se /var/lib/dhcp/dhcpd.leaseslistan en orden de preferencia. Para establecer el nombre del dominio NIS, se usará option nis-domain <nombre>.

option routers Define el router , gateway o pasarela de enlace listadas en orden de preferencia.

option subnet-mask Definición de la máscara de subred general.

range ip-menor ip-mayor En una declaración de subred, este parámetro define el rango de direcciones que serán asignadas. Pueden darse dos instrucciones range seguidas del modo:

range 192.168.0.11 192.168.0.100;
range 192.168.0.125 192.168.0.210;

server-identifier	Identifica la máquina donde se aloja el servidor de DHCP. Su uso se aplica cuando la máquina en cuestión tiene varias direcciones asignadas en un mismo interfaz de red.
shared-network	Declaración de Subred compartida.
subnet	Declaración de Subred.

Nota:

La ubicación del archivo donde están las IPS que están asignadas es /var/lib/dhcp/dhcpd.leases y para ver los logs del dhcpd se ejecuta el comando tail -f /var/log/messages | grep dhcp

12.5 Conclusión

En este capítulo se vio conceptos básicos de DHCP, ejemplos de asignación de direcciones ip entre un rango de direcciones, asignación de direcciones ip mediante dirección MAC, esto con el fin de dar una idea del funcionamiento y utilidad de esta herramienta.

CAPITULO 13: CONFIGURACIÓN DE SENDMAIL

13.1 Introducción

Un Agente de Transporte de Correo es indispensable para enviar correos electrónicos, es por esta razón que en este capítulo se describe como configurar Sendmail que es un popular agente de transporte de correo, también se realizará configuraciones pop e imap con el fin de que el usuario obtenga sus mensajes.

13.2 Sendmail

Sendmail es un popular "agente de transporte de correo" (MTA - Mail Transport Agent) en Internet, cuya tarea consiste en "encaminar" los mensajes correos de forma que estos lleguen a su destino. Se afirma que es el más popular MTA, corriendo sobre sistemas Unix y el responsable del envió del 70% del correo de Internet, aunque se le critica su alto número de alertas de seguridad (la mayoría de ellas parchadas a las pocas horas), además de no ser sencillo de configurar. Sendmail utiliza el puerto 25. Para arrancar el servicio se utiliza la instrucción **service sendmail start.** Se puede ver los mails que están en la cola de salida utilizando la instrucción **mailq**, si se desea que estos emails que están en la cola salgan se utiliza la instrucción **sendmail –q**.

Los archivos que se deben configurar son:

Archivo /etc/mail/ sendmail.mc

Cambiar para que el spam no verifique la existencia de la cuenta (deshabilita comandos como EXPN y VRFY)

dnl define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
Cambiar por
dnl define(`confPRIVACY_FLAGS',`goaway')dnl

Se aumenta la siguiente línea para que el tamaño de la cabecera no sea muy grande, una cabeceras puede ser generada por correo spam

Luego de dnl define(`confCONNECTION_RATE_THROTTLE', 3)dnl se escribe la siguiente línea que define un máximo de cabecera de 16kb.

dnl define(`confMAX_HEADERS_LENGTH', `16384')dnl

Para define el tamaño máximo del mensaje a 3MB se cambia la siguiente línea.

dnl define(`confMAX_MESSAGE_SIZE', `3145728')dnl

Para definir cuantos procesos hijos se permitirán simultáneamente en el servidor.

dnl define(`confMAX_DAEMON_CHILDREN', 20)dnl

Para definir el número máximo de destinatarios por defecto es 256 en este caso es 20.

dnl define(`confMAX_RCPTS_PER_MESSAGE', `20')dnl

Para limitar el número de conexiones máximas por segundo.

dnl define(`confCONNECTION_RATE_THROTTLE', 3)dnl

Para que de un mensaje sin la versión de sendmail se aumenta la línea al final del archivo.

dnl define(`confSMTP_LOGIN_MSG',`$j ; $b')dnl

Se comenta la siguiente línea esto es para que se pueda enviar correo desde otras pc y no solo desde el servidor.

dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
Se cambia por
dnl # DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl

Si se desea que Sendmail solo trabaje con una red específica por ejemplo solo correo interno se aumenta la siguiente línea:

DAEMON_OPTIONS(`ClientPortOptions=Family=inet, Address=192.168.0.0/24')

Se comenta la siguiente línea de esta forma no aceptara email de dominios que no se puedan resolver.

FEATURE(`accept_unresolvable_domains')dnl
dnl # FEATURE(`accept_unresolvable_domains')dnl

Todos los emails que salgan saldrán con el dominio especificado en mydomain.com en este ejemplo saldrán con el de la Universidad del Azuay (uazuay.edu.ec)

dnl MASQUERADE_AS(`mydomain.com')dnl
se cambia por
dnl MASQUERADE_AS(`uazuay.edu.ec')dnl

La opción "Timeout.queuewarn" determina el lapso que permanece un mensaje en cola para generar un mensaje de alerta al redactor del mismo. Esta alerta le permite saber que el mensaje no pudo ser enviado en 4 horas este es el valor por defecto.

La opción "Timeout.queuereturn" determina el tiempo máximo que el sistema mantendrá el mensaje en la cola (intentando enviarlo.) Cuando este tiempo se cumple, el mensaje es eliminado de la cola y se envía una alerta al redactores valor por defecto son 5 días.

Por consistencia, Timeout.queuewarn debe ser menor que Timeout.queuereturn. ya que si Timeout.queuewarn es mayor nunca dará un mensaje de alerta (aunque en algunos casos se configura así)

A fin de que los mensajes "reboten" más aprisa (y la cola se libere más aprisa), es conveniente en ciertos casos reducir estos valores, por ejemplo:

dnl define(`confTO_QUEUERETURN',`1d')
dnl define(`confTO_QUEUEWARN',`2h')

El ordenamiento de la cola en base a la prioridad es la política por omisión de Sendmail; para hacer esto sendmail ordena los mails que recibe por la prioridad que

tienen antes de enviarlo esto toma tiempo, y lo aconsejable es cambiar este valor a la opción QueueSortOrder permite alterar esto.

priority.	Ordena por prioridad
hosts	Ordena por Host de destino solo habré una conexión una sola vez
filename	Envia los archivos a medida que llegan, si el archivo esta bloqueado por otro proceso continua con el siguiente
random	Con la opción filename puede dar colisiones en el momento de leer el archivo para evitar esto se puede utilizar la opción random que es la recomendada

dnl define(`confQUEUE_SORT_ORDER',`random')http://29.212.78.4/

Tiempo de espera para la respuesta a una consulta IDENT se debe poner en 0 segundos ya que aumentar un valor aquí lo que hace es que se demore en enviar el mail. El valor por defecto es cero

dnl define('confTO_IDENT', '0')dnl

Se puede bloquear el correo spam con el parámetro dnsblde servidores que estén listados en las listas negras aquí un ejemplo de servidores que tienen listas de servidores que emiten spam se aumenta

dnl FEATURE(`dnsbl', `dnsbl.njabl.org', `Rejected - see http://dnsbl.njabl.org')dnl
dnl FEATURE(`dnsbl', `dnsbl.sorbs.net', `Rejected - see http://dnsbl.sorbs.net')dnl
dnl FEATURE(`dnsbl', `list.dsbl.org', `Rejected - see http://dsbl.org/')dnl
dnl FEATURE(`dnsbl', `multihop.dsbl.org', `Rejected - see http://dsbl.org/')dnl
dnl FEATURE(`dnsbl', `unconfirmed.dsbl.org', `Rejected - see http://dsbl.org/')dnl
dnl FEATURE(`dnsbl', `dnsbl.ahbl.org',`Rejected - see http://www.ahbl.org/')dnl
dnl FEATURE(`dnsbl', `rhsbl.ahbl.org',`Rejected - see http://www.ahbl.org/')dnl

Una vez configurado todos estos parámetros se compila el archivo para que genere el archivo sendmail.cf que es el verdadero archivo de configuración que lee sendmail para realizar esto se utiliza la siguiente instrucción.

m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf

Archivo /etc/mail/ access

Este archivo tiene las redes a las cuales se les da acceso para que envien correo (opcion RELAY) desde el servidor. Aquí debe estar la red de la LAN. También aquí se pone las redes y las cuentas de email que se desea bloquear (REJECT).

localhost.localdomain	RELAY
localhost	RELAY
127.0.0.1	RELAY
192.188.47	RELAY
172.16	RELAY
abuse@hotmail.com	REJECT
168.0	REJECT

Se debe compiler este archive con la siguiente instrucción:

makemap hash /etc/mail/access.db < /etc/mail/access

Archivo /etc/mail/ local-host-names

En este archivo se pone el nombre de dominio del servidor en donde se esta configurando el sendmail si no se pone el correcto sendmail rechazara el correo. El contenido del archivo quedara como el siguiente ejemplo:

local-host-names - include all aliases for your machine here.
uazuay.edu.ec

Archivo /etc/mail/ hosts

El archive hosts tiene la IPS y los nombres de la red LAN aquí se debe poner la ip del servidor y su nombre de dominio. El archivo quedaría de la siguiente forma:

Do not remove the following line, or various programs
that require network functionality will fail.

127.0.0.1 localhost.localdomain localhost
168.0.0.4 uazuay uazuay.edu.ec

13.3 Configuración de POP y IMAP

Para que los clientes (Microsoft Outlook, y otros) se puedan conectar al servidor de correo se debe habilitar el protocolo POP o el protocolo IMAP. La diferencia entre estos dos protocolos es que el protocolo POP pasa al cliente las cabeceras del correo y su contenido, mientras que IMAP solo pasa las cabeceras y si el cliente habré la cabecera que le llego se pasa el contenido de esa cabecera. En clientes con líneas dial–up seria aconsejable utilizar IMAP ya que la conexión sería más rápida.

Para activar estos protocolos se utiliza el programa dovecot el archivo de configuración de este archivo es /etc/dovecot.conf

Se modifica la línea.

#protocols = imap imaps
por
protocols = imap imaps pop3 pop3s

pop3s y imaps son los protocolos pop3 y imap encriptados es la opción que se debería ocupar.

Para activar el servicio se utiliza la instrucción **service dovecot start**

SSL con dovecot

Generando clave y certificado.

La creación de la llave y certificado para Dovecot es simple, pero requiere utilizar una clave con algoritmo RSA de 1024 octetos, con estructura X.509. En el ejemplo a continuación, se establece una validez por 730 días (dos años) para el certificado.

mkdir /etc/ssl
cd /etc/ssl

openssl req -x509 -nodes -newkey rsa:1024 -days 730 -out dovecot.crt -keyout dovecot.key

Se contestan las preguntas como en el siguiente ejemplo:

Generating a 1024 bit RSA private key
....++++++
.....++++++
writing new private key to 'dovecot.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:EC
State or Province Name (full name) [Berkshire]:Azuay
Locality Name (eg, city) [Newbury]:Cuenca
Organization Name (eg, company) [My Company Ltd]:Universidad del Azuay
Organizational Unit Name (eg, section) []:Universidad del Azuay
Common Name (eg, your name or your server's hostname) []:uazuay.edu.ec
Email Address []:webmaste@uazuay.edu.ec

Luego se da permisos a los archivos con el comando chmod 400 dovecot.*

-r-------- 1 root root 1407 abr 3 15:32 dovecot.crt
-r-------- 1 root root 887 abr 3 15:32 dovecot.key

Para instalar los certificados copiamos la llave pública que el archivo dovecot.crt en la carpeta /usr/share/ssl/certs/ con el nombre de dovecot.pem recuerde sacar un respaldo de este archivo antes de realizar la copia

cp dovecot.crt /etc/pki/dovecot/certs/dovecot.pem
realizamos el mismo procedimento con la llave privada

cp dovecot.key /etc/pki/dovecot/private/dovecot.pem
reiniciamos el servicio con service dovecot restart

13.4 Recolectar Correo de Otra cuenta pop3

Si se desea recolectar el correo de otra cuenta pop y ponerla en la cuenta local se utiliza fetchmail.

Se crea el archivo en /root/.fetchmailrc con el siguiente contenido:

set syslog
set logfile "/var/log/fetchmail.log"
poll 192.168.1.200 with protocol POP3, with options user "aizquierdoout" there with password "clave" is aizquierdo here with options rewrite mimedecode pass8bits

donde 192.168.1.200 es el servidor al cual se va a conectar
aizquierdoout es el nombre del usuario de la cuenta externa
clave la clave del usuario externo
aizquierdo el usuario local

Esto se puede poner varias veces con todos los usuarios que se necesite recuperar el mail externo

fetchmail –q para cancelar cualquier demonio activo de fetchmail

fetchmail -d 60 para activar fetchmail y que revise cada 60 segundos

13.5 Herramientas para Revizar un servidor de Correo

Prueba para ver si se puede hacer relay en el servidor
http://www.antispam-ufrj.pads.ufrj.br/test-relay.html

Para ver si el servidor (ip) está en las listas negras
http://rbls.org/?q=200.63.209.231
http://www.robtex.com/r/200.63.209.231.html

http://www.declude.com/Articles.asp?ID=97
http://relays.osirusoft.com/cgi-bin/rbcheck.cgi
http://www.spamhaus.org/query/bl?ip=190.12.31.141

Para revisar los DNS
http://www.squish.net/dnscheck
http://www.dnsstuff.com/

13.6 Conclusión

Se pudo comprobar que sendmail es una herramienta muy útil y popular entre los agentes de transporte de correo, pero a la vez su configuración es compleja es por esto que en esta práctica se configuro sendmail, se configuro pop e imap, se vio como recolectar correo de otras cuentas todo esto con el fin de optimizar esta herramienta y aprender su uso.

CAPITULO 14. CONFIGURACIÓN DE OPENWEBMAIL

14.1 Introducción

Con el fin de manejar grandes archivos de correo en una forma eficaz se vio necesario realizar una práctica de uso y configuración de Open WebMail que posee un gran número de características adicionales para adiministrar eficientemente nuestro correo.

14.2 Open WebMail

Open WebMail es un sistema webmail basado en la version 1.14 de Neomail de Ernie Miller. OpenWebMail esta diseñado para manejar grandes archivos de mail con un manejo de memoria muy eficiente. También tiene gran cantidad de opciones para facilitar el manejo al usuario dentro de esas opciones esta la migración de las listas de contacto de Microsoft Outlook a OpenWebMail. La última versión del software se lo encuentra en:

http://www.openwebmail.org/openwebmail/download/current/openwebmail-current.tar.gz

Para que funcione el Openwebmail previamente debe estar funcionando el servidor web en el equipo que se quiere instalar el OpenWebMail (OWM).

14.3 Pasos para instalarlo y configurar Open WebMail

- Se ejecuta tar –zxvf openwebmail-current.tar.gz

- Se mueve las carpetas a los directorios en los cuales debe funcionar

mv data /var/www/html
cd cgi-bin
mv openwebmail /var/www/cgi-bin

- Se instalan las librerías de Perl necesarias para que funcione:

Text::Iconv
perl-Text-Iconv-1.7-1.el5.rf.i386.rpm
que se encuentra en:
http://dag.wieers.com/rpm/packages/perl-Text-Iconv/

suidperl
perl-suidperl-5.8.8-10.el5_0.2.i386.rpm
que se encuentra en:
http://rpm.pbone.net/index.php3/stat/4/idpl/6031292/com/perl-suidperl-5.8.8-10.el5_0.2.i386.rpm.html

- Se configura OWM para que funcione con las cuentas del sistema operativo

cp /var/www/cgi-bin/openwebmail/etc/defaults/auth_unix.conf /var/www/cgi-bin/openwebmail/etc/auth_unix.conf

vi var/www/cgi-bin/openwebmail/etc/auth_unix.conf

Este archivo debe quedar con las configuraciones que están a continuación:

```
passwdfile_plaintext  /etc/passwd
passwdfile_encrypted  /etc/shadow
passwdmkdb    none
check_expire    yes
check_nologin   no
check_shell   no
check_cobaltuser  no
change_smbpasswd  no
```

- Configuración de la Base de Datos que utiliza OWM

vi /var/www/cgi-bin/openwebmail/etc/defaults/dbm.conf

Este archivo debe quedar como lo que sigue:

```
dbm_ext              .db
dbmopen_ext          .db
dbmopen_haslock      no
```

- Se cambian los Path de los archivos de OpenWebMail a los correctos en el archivo de configuración de OWM

vi /var/www/cgi-bin/openwebmail/etc/openwebmail.conf

```
ow_cgidir            /var/www/cgi-bin/openwebmail
ow_htmldir           /var/www/html/data/openwebmail
ow_htmlurl           /data/openwebmail
```

- Para cambiar el idioma predeterminado que es el ingles al español y también para cambiar los iconos de default a español se agrega o modifican las siguientes líneas en el archivo de configuración

```
default_locale       es_AR.ISO8859-1
default_language     es_AR
default_iconset      Cool3D.Spanish
default_style        Adjunct
```

- Configuraciones Adicionales de OpenWebMail

```
# Nombre del dominio del servidor lo que va a ir luego de la @
domainnames          uazuay.edu.ec

# Crea automáticamente el archive de configuración del usuario
auto_createrc        yes

#Configuración de la Zona Horaria el no es para que no aumente una hora en
verano
default_timeoffset           -0500
default_daylightsaving       no

#Configuración de tamaño de la letra, formato de la fecha y formato de la Hora
default_fontsize             10pt
```

```
default_dateformat          dd/mm/yyyy
default_hourformat          24
default_fscharset           is0-8859-1
default_sendcharset         iso-8859-1
default_charset             iso-8859-1
abook_addrperpage           1000
default_sessiontimeout      1440
default_msgsperpage         20

<default_autoreplytext>
Hola,
Este momento no puedo leer mi correo.
Tu email '$SUBJECT' lo leere cuando regrese.
</default_autoreplytext>

<default_signature>
--------------------------
 Universidad del Azuay
(http://www.uazuay.edu.ec)
</default_signature>

<page_footer>
<hr>
<center>
 <font size=2>
  <b>Universidad del Azuay</b> Av. 24 de Mayo 7-77 Cuenca-Ecuador
<b>Tel&eacute;fono</b>
    (593)7288-1333 <br>
  <b> Internet</b> Ext (279)<b> Apartado</b> 01.01.981<b>Sugerencias o
Comentarios a: </b>
     <a href="webmaste@uazuay.edu.ec">webmaste@uazuay.edu.ec</a><br>
  <b>&copy;</b> Todos los derechos Reservados<b> <br>
   http://www.uazuay.edu.ec</b>
  </font>
</center>
</page_footer>
```

```
########################################
# Desactiva Webdisk y Telnet
########################################
enable_webdisk              no
enable_sshterm              no

################################################
# Cambios para el Diccionario del mail
# no hay que instalar aspell ya viene en centos
################################################
spellcheck                  /usr/bin/aspell -a -S -w "-" -d @@@DICTIONARY@@@ -p
@@@PDICNAME@@@
spellcheck_dictionaries  spanish, english, american
default_dictionary       spanish

# Formato de la pantalla de Mensajes botón de envió arriba y abajo
default_sendbuttonposition       both

# Para las desactivar las ventanas de envió y nuevo mail
default_newmailwindowtime        0
default_mailsentwindowtime       0
default_refreshinterval          3
```

- Se inicializa el programa con la instrucción

/var/www/cgi-bin/openwebmail/openwebmail-tool.pl --init

- Para ingresar a OpenWebMail se pone en el Navegador la siguiente URL

http://localhost.localdomain/cgi-bin/openwebmail/openwebmail.pl

Nota: Todas estas configuraciones se almacenan en la carpeta del usuario /home/usuario/.openwebmail si se desea usar otra carpeta en donde almacenar los correos se debe modificar el archivo de configuración con los siguientes parámetros:

```
#################################################################
# Lineas que se aumentan  para crear archivos en otra carpeta
#################################################################
use_syshomedir                no
create_syshomedir             yes
use_syshomedir_for_dotdir     no
ow_usersdir                   /var/openwebmail/users

#####################################
# Esto para conexión mediante pop3
#####################################
#auth_module           auth_pop3.pl
#use_homedirspools     no
#enable_changepwd      no
#enable_autoreply      no
#enable_setforward     no
#authpop3_server       127.0.0.1
#authpop3_port         110
#authpop3_getmail      no
#authpop3_delmail      no
#authpop3_usessl       no
```

14.4 Creación de La Libreta de Direcciones para OpenWebMail

La libreta de direcciones para todos los usuarios se encuentra en /var/www/cgi-bin/openwebmail/etc/addressbooks y allí se crea un archivo con permisos solo para el root. En ese archivo el formato de las direcciones es el siguiente:

```
BEGIN:VCARD
VERSION:3.0
N:cuenta 1;*Todo;en;;
EMAIL:cuenta1@uazuay.edu.ec
REV:20051222T221546Z
X-OWM-UID:20051222-221546-YTJQBZKNCQLE-SCIU
END:VCARD
```

```
BEGIN:VCARD
VERSION:3.0
N:cuenta 2;*Todo;en;;
EMAIL:cuenta2@uazuay.edu.ec
REV:20051222T221547Z
X-OWM-UID:20051222-221547-U0YGZEDL6Y8F-U8C0
END:VCARD
```

Para general el valor de X-OWM-UID que es único para cada una de las cuentas se utiliza el siguiente programa en Perl:

uid.pl

```
sub make_x_owm_uid {
    my ($uid_sec,$uid_min,$uid_hour,$uid_mday,$uid_mon,$uid_year) =
gmtime(time);
                my @chars = ( 'A' .. 'Z', 0 .. 9 );
                my $longrandomstring = join '', map { $chars[rand @chars] } 1..12;
                my $shortrandomstring = join '', map { $chars[rand @chars] } 1..4;
                my $uid =
($uid_year+1900).sprintf("%02d",($uid_mon+1)).sprintf("%02d",$uid_mday)."-".

sprintf("%02d",$uid_hour).sprintf("%02d",$uid_min).sprintf("%02d",$uid_sec)."-".
                        $longrandomstring."-".$shortrandomstring;
                                return $uid;
                                }
print make_x_owm_uid;
```

Se ejecuta utilizando la instrucción **Perl uid.pl**

14.5 Configuración de OpenWebMail por Usuario

Si se desea que solo algunos usuarios tengan mas o menos opciones que otros usuarios se copia el archivo .openwebmailrc de la carpeta del usuario en este caso /home/usuario/.openwebmail

A la carpeta /var/www/cgi-bin/openwebmail/etc/users.conf con el nombre del usuario.

Se edita el archivo y se realizan los cambios respectivos para este usuario.

14.6 Configuración de OpenWebMail con SpeedyCGI

SpeedyCGI es un programa que aumenta la velocidad de ejecución de OpenWebMail la forma de cómo realiza esto es manteniendo en memoria el programa de esta forma no tiene que ejecutarlo cada vez que lo necesita. Se lo baja desde la URL http://daemoninc.com/SpeedyCGI/CGI-SpeedyCGI-2.22.tar.gz los pasos para instalarlo son:

- tar -zxvf CGI-SpeedyCGI-2.22.tar.gz
- cd CGI-SpeedyCGI-2.22
- perl Makefile.PL se contesta no en la creación del módulo
- vi Makefile
- se aumenta la línea DEFINE = -DIAMSUID luego de la línea FULL_AR = /usr/bin/ar
- Se sale del archivo Makefile grabando los cambios
- make
- make test
- Si todo esta ok se instala con make install
- cp /usr/bin/speedy /usr/bin/speedy_suidperl
- chmod 4555 /usr/local/bin/speedy_suidperl
- se cambia la primera línea de los archivos *.pl de #!/usr/bin/suidperl -T a #!/usr/bin/speedy_suidperl se puede ejecutar el siguiente script para cambiar estas líneas:

```
for name in open*.pl ; do
    cp -a $name ${name}.old
    echo $name
    sed -e "s/suidperl -T/speedy_suidperl/" <  ${name}.old > ${name}
done
```

14.7 Conclusión

Open WebMail está diseñado para manejar grandes archivos de la carpeta de correo en una memoria eficaz. Proporciona herramientas para ayudar a los usuarios a migrar sin problemas de Microsoft Outlook a Open WebMail.

En este capítulo se hizo práctica de cómo instalarlo, configurarlo, como crear una libreta de direcciones, configurar por usuario, configurarlo con SpeedyCGI el cual aumenta la velocidad de ejecución de Open WebMail esto con el fin de dar una idea de manjeo de un sistema de correo.

CAPITULO 15. CONFIGURACIÓN DE MAILSCANNER CON EL ANTIVIRUS CLAMAV

15.1 Introducción

El manejo de un sistema de correo trae consigo varios problemas entre ellos correo masivo no solicitado (Spam), así como también los fraudes electrónicos (Phishing. Es por esto que en este capitulo veremos la configuración de MailScanner combinado con Clamav, un poderoso y versátil anti-virus libre para GNU/Linux y otras versiones de Unix, resultan una de las soluciones más robustas para la protección contra correo masivo no solicitado, fraudes electrónicos, virus, gusanos y troyanos desde el servidor de correo electrónico.

15.2 MailScanner

MailScanner, es un robusto servicio que examina el correo electrónico e identifica y etiqueta correo masivo no solicitado (Spam) y fraudes electrónicos (Phishing). Combinado con ClamAV, un anti-virus gratuito, resulta una de las soluciones más robustas para la protección contra virus, gusanos y troyanos en un servidor de correo electrónico. La última versión de MailScanner se puede encontrar en http://www.mailscanner.info/downloads.html . La última versión Clamav se puede encontrar en http://www.clamav.net/.

15.3 Instalación de MailScanner

Ejecutar tar -zxvf MailScanner-4.55.10-3.rpm.tar.gz
Ejecutar cd MailScanner-4.55.10-3
Ejecutar ./install.sh

15.4 Instalación de Clamav

Ejecutar rpm -ivh clamav-0.88.4-1.9.el4.lpt.i386.rpm
Los archivos con las definiciones de los virus se instalan en /var/lib/clamav/*.cvd

15.5 Configuración de MailScanner

El archivo de configuración de MailScanner es /etc/MailScanner/MailScanner.conf se edita este archivo y se realizan los siguientes cambios:

%org-name% = UDA
%org-long-name% = Universidad del Azuay
%web-site% = http://www.uazuay.edu.ec
%report-dir% = /etc/MailScanner/reports/es
Incoming Work User = clamav
Incoming Work Group = 0640
Virus Scanning = yes
Virus Scanners = clamav
Monitors for ClamAV Updates = /var/lib/clamav/*.cvd
Quarantine Infections = yes // para mantener copias de los archivos infectados
Notify Senders Of Viruses = yes //Notifica si el mail es infectado a quien envía
Virus Subject Text = {Virus Eliminado?}
Content Subject Text = {Contenido Peligroso?}
Disarmed Subject Text = {Revisado HTML}
Phishing Subject Text = {Posible intento de Fraude?}
Notices To = virus@uazuay.edu.ec // cuenta en donde se recibe los mensajes de los mails que están infectados
Local Postmaster = virus@uazuay.edu.ec // igual que el anterior
Spam List = ORDB-RBL spamhaus.org spamhaus-XBL SBL+XBL spamcop.net NJABL //para habilitar las listas negras de SPAM

Nota: Si se configuro Sendmail con listas negras, no se debe activar esta funcionalidad en MailScanner para no duplicar las consultas hacia los DNSBL. Si se desea aumentar mas listas negras se debe modificar el archivo /etc/MailScanner/spam.lists.conf

Spam Actions = delete

Si se desea que se acepten archivos .exe se modifica el archivo /etc/MailScanner/filetype.rules.conf

deny executable No executables No programs allowed

por

allow executable No executables No programs allowed

Si se desea que se acepten archivos .exe se modifica el archivo /etc/MailScanner/filename.rules.conf

deny \.exe$ Windows/DOS Executable

por

allow \.exe$ Windows/DOS Executable

15.6 Se inician los servicios de CLAMAV

chkconfig clamd on

chkconfig freshclam on

service clamd start

service freshclam start

15.7 Se inician los servicios de MailScanner

Se apaga el servicio de sendmail ya que MailScanner va a manejar esto

chkconfig sendmail off

service sendmail stop

Se activa el servicio de MailScanner

chkconfig MailScanner on

service MailScanner start

15.8 Para revisar si MailScanner se esta ejecutando

Se ejecuta la instrucción /usr/sbin/check_mailscanner y saldrá

MailScanner running with pid 20360 20361 20366 20368 20374 20375

15.9 Probando el funcionamiento del Antivirus

Todos los antivirus tienen un test de pruebas con un archivo llamado eicar en diferentes formatos estos archivos se encuentran en http://www.eicar.org/anti_virus_test_file.htm baje cualquiera de ellos y mande un mail con esos archivos si todo esta correcto mailscanner le enviara un mail con un mensaje indicando que el mail que mando esta con virus. (Mediante la consola también se puede probar con la instrucción **mail –v cuenta@uazuay.edu.ec < eicar.com**). La actualización del antivirus es automática por lo tanto no hay que preocuparse de que las definiciones de virus estén viejas.

Si se esta detrás de un firewall los puertos que se deben habilitar son:
• SMTP, puerto 25 a través de TCP (entrada y salida).
• DNS, puerto 53 a través de TCP y UDP (salida).
• Razor23, puerto 2703 a través de TCP y puerto 7 a través de UDP (salida).
• DCC, puerto 6277 a través de UDP (salida).
• Pyzor, puerto 24441 a través de UDP (salida).
• HTTP, puerto 80 (salida).

15.10 Configuraciones Adicionales

Bloqueando el envió de mail según su tamaño y por usuario

Para bloquear que un determinado usuario no envie correo que tenga un tamaño mayor que X se modifica el archivo MailScanner.conf cambiando la línea Maximum Message Size = 0 por Maximum Message Size = %rules-dir%/messagesize.rule. Luego se crea el archivo /etc/MailScanner/rules/messagesize.rule con la siguiente información:

```
FromOrTo:  usuario1@*  100000
FromOrTo:  usuario2@*  200000
FromOrTo:  usuario3@*  300000
FromOrTo:  default 0
```

El usuario1 esta limitado a 100 Kb, el usuario2 a 200 Kb y el usuario3 a 300Kb para el resto de usuarios no se les limita nada (eso indica el valor 0).

15.11 Conclusión

En este capítulo se explicó como instalar MailScanner junto con el antivirus Clamav ambas herramientas de mucha utilidad para verificar que nuestro sistema de correo no sea afectado por spam o virus. La configuración de cada una de estas herramientas va de acuerdo a nuestras necesidades y cabe recalcar que las actualizaciones de antivirus son automáticas.

CAPITULO 16. CONFIGURACIÓN DE SPAMASSASSIN CON MAILSCANNER Y OPENWEBMAIL

16.1 Introducción

Con el fin de proteger aún más nuestro sistema de correo, sobre todo de mensajes no solicitados se desarrollará en este capítulo la configuración de Spamassassin que junto con MailScanner y Clamav volverán más seguro nuestro sistema de correo Open WebMail.

16.2 Spamassassin

SpamAssassin (http://spamassassin.apache.org/) es un filtro de correo electrónico usado para identificar spam. Es un proyecto open source ampliamente utilizado, maneja una variedad de mecanismos incluyendo análisis de cabeceras y texto, filtrado bayesiano, bases de datos de filtrado, etc. SpamAssassin funciona filtrando los mails que llegan al servidor antes de pasarlos al destinatario.

Esta configuración de Spamassassin necesita de MailScanner y OpenWebMail. Además se lo configuro solamente para que el administrador de la red pueda enseñarle a la base de datos bayesiana ya que los usuarios por lo general no utilizan bien esta opción.

16.3 Configuración de MailScanner

Se edita el archivo /etc/MailScanner/MailScanner.conf y se realizan los siguientes cambios:
Always Include SpamAssassin Report = yes
Spam Checks = yes
Use SpamAssassin = yes
Required SpamAssassin Score = 7
High SpamAssassin Score = 12

Always Include SpamAssassin Report = yes //para que en el correo que no es spam salga el puntaje asignado y los test realizados por spamassassin de esta forma se puede ver como esta funcionando para poderlo afinar.
Spam Actions = notify //envia un mail indicando que no llego el mail por ser spam
Spam Actions = store forward spam@uazuay.edu.ec reenvia el spam a un mail
High Scoring Spam Actions = delete //borrara el spam
Antes estaba High Scoring Spam Actions = deliver header "X-Spam-Status: Yes"
Log Spam = yes // activa los log para el Spam

Nota: El log para mailscanner es el mismo que para el mail /var/log/maillog

Se edita el archivo /etc/MailScanner/rules/spam.whitelist.rules en este archivo se ponen las ips de la red local o la dirección de la red para que no se lo considere como spam.

```
# This is where you can build a Spam WhiteList
# Addresses matching in here, with the value
# "yes" will never be marked as spam.
#From:          152.78.         yes
#From:          130.246.        yes
FromOrTo:       default         no
From:           192.168.1.0.    yes
From:           172.16.0.       yes
From:           200.31.26.241   yes
From:           127.0.0.1       yes
```

Se edita el archivo /etc/MailScanner/spam.assassin.prefs.conf y se realizan los siguientes cambios:

```
trusted_networks 192.188.47/24 172.16/16 172.30/16
use_bayes 1
bayes_path  /etc/MailScanner/bayes/bayes

score BAYES_99 0 0 4.5 4.5
score HTML_30_40 0
score URIBL_JP_SURBL 0
score URIBL_OB_SURBL 0
```

score HABEAS_SWE 0
score SUBJ_ILLEGAL_CHARS 1 1 2 2
score UPPERCASE_75_100 0
score MSGID_FROM_MTA_ID 2 2 2 2
score UNPARSEABLE_RELAY 2 2 2 2
score FORGED_RCVD_HELO 3 3 3 3
score HTML_SHORT_LENGTH 0
score UPPERCASE_50_75 0
score DOMAIN_4U2 0
score HTML_MIME_NO_HTML_TAG 0
score HTML_TINY_FONT 0
score EXTRA_MPART_TYPE 3.10
score MIME_HTML_ONLY 1 1 1 1
score RCVD_IN_NJABL_DUL 2.5 2.5 2.5 2.5

bayes_auto_learn 0
bayes_auto_learn_threshold_nonspam 0.1
bayes_auto_learn_threshold_spam 3.9
use_razor2 0
use_dcc 0
use_pyzor 0

Nota:

- trusted_networks no reviza los mails de estas redes.
- use_bayes 1 activa el uso de redes bayesianas
- Si bayes_auto_learn es 1 la base bayesiana va a aprender automáticamente y se debe configurar los parámetros bayes_auto_learn_threshold_nonspam 0.1 y bayes_auto_learn_threshold_spam 3.9, de esta forma cualquier mail que spamassassin marque con un valor de 0.1 o menor lo considerara como no spam y un valor de 3.9 o mayor lo considerará como spam.
- En la opción bayes_path va el directorio donde están las bases bayesianas la palabra bayes es el comienzo del nombre de los archivos de las bases bayes.mutex, bayes_seen, bayes_toks
- score UPPER_75_100 0 indica una reasignación de puntaje a cero sobre aquellos correos que contengan entre el 75% y 100% de su cuerpo en letras mayúsculas, esto evita que al ser inspeccionados mensajes de este tipo su

puntaje se eleve considerablemente. Las líneas de score que vienen a continuación es para desactivar otros test o darles otro puntaje al que viene por defecto y no de falsos positivos**. El primer puntaje** es usado cuando la red bayesiana y los test de red están desactivados, **el segundo puntaje** es cuando la red bayesiana esta deshabilitada y el test de red activado, **el tercer puntaje** es cuando la red bayesiana esta habilitada y el test de red deshabilitado, **el cuarto puntaje** es cuando la red bayesiana esta habilitada y el test de red también esta habilitado (razor, pyzor, dcc son los test de red soportados por spamassassin en el ejemplo anterior están desactivados). Una lista completa de todos los test que realiza spamassassin esta en la URL http://spamassassin.apache.org/tests_3_1_x.html

- use_razor2 0 , use_dcc 0 , use_pyzor 0 desactivan los test de red razor, dcc y pyzor

16.4 Configuración de Spamassassin

Se renombra el archivo /etc/mail/spamassassin/local.cf ya que esto va a manejar con MailScanner mediante el archivo /etc/MailScanner/spam.assassin.prefs.conf

mv local.cf local.cf.bak

16.5 Creando bases bayesianas la primera vez

La primera vez se crea ya carpeta /etc/MailScanner/bayes y se ejecuta la instrucción sa-learn --sync –p /etc/MailScanner/spam.assassin.prefs.conf para crear las bases bayesianas en /etc/MailScanner/bayes. Luego de esto se dan los siguientes permisos:

El directorio bayes debe pertenecer al usuario root y al grupo apache y debe tener los permisos chmod 755 y los archivos dentro de este directorio también deben pertenecer al usuario root y al grupo apache y tener los permisos chmod 764

Se puede hacer que aprenda la base bayesiana ejecutando las siguientes instrucciones:

- Para que aprenda que no es spam

/usr/bin/sa-learn --ham --mbox -p /etc/MailScanner/spam.assassin.prefs.conf /var/mail/archivo_con_mails_que_no_son_spam

- Para que aprenda que es spam

/usr/bin/sa-learn --spam --mbox -p /etc/MailScanner/spam.assassin.prefs.conf /var/mail/archivo_con_mails_que_si_son_spam

Nota: Como mínimo se necesita entrenarle a la base bayesiana con 200 mensajes spam y 200 mensaje no spam.

16.6 Configuración de OpenWebMail

Se crea un archivo con el nombre del usuario que va alimentar la base bayesiana en /var/www/cgi-bin/openwebmail/etc/users.conf el contenido de ese archivo debe tener lo siguiente:

#desabilita el chequeo con Spamassassin ya que esto lo realiza MailScanner
enable_spamcheck no
#habilita el aprendizaje de spam
enable_learnspam yes
#Sentencia que aprende que es spam
learnspam_pipe /usr/bin/sa-learn --spam -p /etc/MailScanner/spam.assassin.prefs.conf
#Sentencia que aprende que NO ES spam
learnham_pipe /usr/bin/sa-learn --ham -p /etc/MailScanner/spam.assassin.prefs.conf

16.7 Probando el Funcionamiento de Spamassassin

Para probar si esta aprendiendo la base bayesiana desde openwebmail se ingresa a openwebmail con el usuario que se configuro en el paso anterior este usuario tendrá un icono para aprendes spam se selecciona un correo y se presiona el boton de aprender spam si todo es correcto el tamaño de los archivos de la carpeta /spam cambiarán o se modificaran las fechas o horas de los mismos.

Para probar el funcionamiento del mailscanner con la funcionalidad de spamassassin activada se modifica el archivo MailScanner.conf en la línea **High Scoring Spam Actions = delete** cambiándola por High Scoring Spam Actions = deliver header "X-Spam-Status: Yes" para que no elimine el spam sino que llegue pero modificada la cabecera (luego se debe poner como estaba). Se envía una mail con la siguiente cadena en el contenido del mensaje:

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

Se ingresa en el usuario a donde se envió el mail y en la cabecera del mensaje enviado se vera lo siguiente:

X-UDA-MailScanner-SpamCheck: spam, SpamAssassin (puntaje=996.288, requerido 3.9, ALL_TRUSTED -3.30, BAYES_00 -2.60, GTUBE 1000.00, TO_MALFORMED 2.19)
X-UDA-MailScanner-SpamScore:
sssssssssssssssssssssssssssssssssssssssssssssssssssssss
X-UDA-MailScanner-From: pesquive@uazuay.edu.ec
X-Spam-Status: Yes
Status: R

La línea marcada con rojo es la importante allí esta la calificación que se le da al mail enviado. Si no aparece esto esta mal configurado el spamassassin.

También se puede ver el funcionamiento de spamassassin ejecutando la siguiente instrucción **spamassassin -D --lint** -p /etc/MailScanner/spam.assassin.prefs.conf con esta instrucción mostrará los warning o errores de spamassassin.

Se puede ver también si las bases bayesianas están funcionando con la instrucción:

spamassassin -p /etc/MailScanner/spam.assassin.prefs.conf --lint -D 2>& 1 | grep -i bayes

Deberá salir algo como lo siguiente:

[22549] dbg: config: read file /usr/share/spamassassin/23_bayes.cf
[22549] dbg: bayes: tie-ing to DB file R/O /spam/bayes_toks
[22549] dbg: bayes: tie-ing to DB file R/O /spam/bayes_seen
[22549] dbg: bayes: found bayes db version 3
[22549] dbg: bayes: DB journal sync: last sync: 1159540471
[22549] dbg: bayes: DB journal sync: last sync: 1159540471
[22549] dbg: bayes: corpus size: nspam = 96297, nham = 416016
[22549] dbg: bayes: score = 0.885017415134888
[22549] dbg: bayes: DB expiry: tokens in DB: 148495, Expiry max size: 150000, Oldest atime: 1159307909, Newest atime: 1159540863, Last expire: 1159480624, Current time: 1159541132
[22549] dbg: bayes: DB journal sync: last sync: 1159540471
[22549] dbg: bayes: untie-ing
[22549] dbg: bayes: untie-ing db_toks
[22549] dbg: bayes: untie-ing db_seen
[22549] dbg: rules: ran eval rule BAYES_80 ======> got hit
[22549] dbg: check:
tests=BAYES_80,MISSING_SUBJECT,NO_REAL_NAME,NO_RECEIVED,
NO_RELAYS,TO_CC_NONE

Nota: Si no sale lo anterior es que las bases bayesianas están mal entrenadas.

16.8 Respaldando y Restaurando las Bases Bayesianas

Para respaldar su base bayesiana utilice la instrucción:
sa-learn --backup -p /etc/MailScanner/spam.assassin.prefs.conf > backup.txt

Para restaurar su respaldo utilice la instrucción:
sa-learn --restore -p /etc/MailScanner/spam.assassin.prefs.conf backup.txt

Nota: La opción de restore borra los datos anteriores de la base bayesiana. Si no quiere que suceda esto utilice la opción import con esta opción aumentará los datos sin borrar los anteriores ya que esta opción sirve para migrar datos de versiones antiguas de spamassassin.

Cuando se les manda a aprender a las bases temporalmente se pasa la información al archivo bayes_journal y luego se actualizan las bases bayesianas con la instrucción sa-learn --sync para que esto se realice cada 5 minutos se debe colocar la siguiente linea en el archivo /etc/crontab

5 * * * * root /usr/bin/sa-learn –sync -p /etc/MailScanner/spam.assassin.prefs.conf

16.9 Aumentando opciones a Spamassassin

Se pueden utilizar bases de datos bayesianas externas mediante programas adicionales como:
Dcc (http://wiki.apache.org/spamassassin/UsingDcc)
Pyzor (http://wiki.apache.org/spamassassin/UsingPyzor)
Razor2 (http://wiki.apache.org/spamassassin/UsingRazor),

- Sistema DCC (Distributed Checksum Clearinghouse) de clientes y servidores que recolecta y cuenta los checksums de los mensajes de email para la detección de Spam (Puerto de salida que utiliza es el 6277)
- Pyzor es un sistema en red para la detección y bloqueo de Spam utilizando resúmenes identificativos de mensajes (Puerto de salida que utiliza es el 24441)
- Razor2 es un detector de Spam y un filtro de red distribuido y colaborador (Puerto de salida que utiliza es el 2703 y 7)

16.10 Conclusión

La configuración de Spamassassin es compleja junto con su configuración hay que configurar las bases bayesianas las cuales aprenden que es spam y que no lo es pero para eso hay que entrenarlas, también hay que configurar el Open WebMail para que acepte al Spamassassin. Pero todo esto será de mucha utilidad para la buena administración de nuestro sistema de correo.

CAPITULO 17. CONFIGURACIÓN DE UN ANALIZADOR DE MAILSCANNER (MAILWATCH)

17.1 Introducción

En toda práctica resulta mucho más fácil de entender la información si esta va acompañada por resultados mediante gráficos y tablas. Con el propósito de conocer la actividad o lo que sucede con nuestro correo para nuestro caso lo que pasa con el MailScanner se vuelve imprescindible la utilización de un analizador de MailScanner en nuestro caso MailWatch el cual muestra la actividad de nuestro sistema de correo de la forma antes descrita volviéndose más fácil de entender esta información.

17.2 MailWatch.

MailWatch es un front-end basado en Web para MailScanner que permite analizar la actividad de MailScanner. Esta escrito en PHP, MYSQL y JpGraph bajo licencia GNU. Se lo puede bajar de http://mailwatch.sourceforge.net/doku.php

17.3 Requisitos

Se verifica que estén instalados los paquetes necesarios

rpm -q php-gd
rpm -q mysql

Si no están instalados estos paquetes hay que instalarlos

17.4 Configurando php

Se edita el archivo /etc/php.ini para que las sentencias queden de la siguiente forma:

short_open_tag = On
safe_mode = Off
register_globals = Off
magic_quotes_gpc = On
magic_quotes_runtime = Off
session.auto_start = 0
allow_url_fopen = On

17.5 Configurando y arrancando Mysql

Se ejecutan los siguientes comandos:
mysql_install_db
mysqladmin –u root password yyyyy donde yyyyy es la clave del usuario root
chkconfig mysqld on
service mysqld start

17.6 Instalación de MailWatch

tar -xfz mailwatch-1.0.3.tar.gz
cd mailwatch

mysql -p < create.sql pedirá una clave la clave es la de la base de datos

Se crea el usuario para administrar MailWatch mediante los siguientes pasos:

mysql mailscanner -u xxxxx -p
Enter password: yyyyy
use mailscanner

INSERT INTO users VALUES ('xxxxx',md5('yyyyy'),'Administra','A','0','0','0','0','0');
EXIT

Donde xxxxx es el usuario para administrar mailwatch y yyyyy la clave del usuario

cp mailscanner/conf.php.example mailscanner/conf.php

vi mailscanner/conf.php

Se va a la línea 30 y se realiza los siguientes cambios:

```
define(DB_USER, 'root');
define(DB_PASS, '');
```

Se cambia por

```
define(DB_USER, 'xxxxx');
define(DB_PASS, 'yyyyy');
```

Donde xxxxx es el usuario de la base de datos por lo general root de mysql y yyyyy es la clave de ese usuario.

En la línea 73 se realiza el siguiente cambio:

```
define(QUARANTINE_USE_FLAG, false);
```

Se cambia por

```
define(QUARANTINE_USE_FLAG, true);
```

vi MailWatch.pm

Se va a la línea 43 y se modifica para que quede de la siguiente forma:

```
my($db_user) = "root";
my($db_pass) = "";
```

se cambia por

```
my($db_user) = "xxxxx";
my($db_pass) = "yyyyy";
```

Donde xxxxx es el usuario de la base de datos y yyyyy su clave.

Se va a la línea 173 y se modifica para que quede de la siguiente forma:

MailScanner::Log::InfoLog("$$message{id}: Logged to MailWatch SQL");

se cambia por
MailScanner::Log::DebugLog("$$message{id}: Logged to MailWatch SQL");

Se va a la línea 326 y se modifica para que quede de la siguiente forma:

MailScanner::Log::InfoLog("Logging message $msg{id} to SQL");

Se cambia por
MailScanner::Log::DebugLog("Logging message $msg{id} to SQL");

vi mailscanner/mailq.php

Se va a la línea 15 y se modifica para que quede de la siguiente forma:

case default:

se cambia por
default:

Se mueve al archivo de MailWatch.pm

mv MailWatch.pm /usr/lib/MailScanner/MailScanner/CustomFunctions

Se mueve la carpeta mailscanner a la carpeta para el Web
mv mailscanner /var/www/html

Se da permisos a las carpetas
chown root:apache /var/www/html/mailscanner/images
chmod ug+rwx /var/www/html/mailscanner/images
chown root:apache /var/www/html/mailscanner/images/cache
chmod ug+rwx /var/www/html/mailscanner/images/cache
chown apache /var/www/html/mailscanner/temp
chmod gu+wr /var/www/html/mailscanner/temp

17.7 Configuración de MailScanner

vi /etc/MailScanner/MailScanner.conf

Quarantine User = root
Quarantine Group = apache (this should be the same group as your web server)
Quarantine Permissions = 0660

Quarantine Whole Message = yes
Quarantine Whole Message As Queue Files = no
Detailed Spam Report = yes
Include Scores In SpamAssassin Report = yes
Always Looked Up Last = &MailWatchLogging
Detailed Spam Report = yes
Include Scores In SpamAssassin Report = yes

17.8 Permisos a las bases bayesianas

chown root:apache /etc/MailScanner/bayes
chmod g+rws /etc/MailScanner/bayes

17.9 Para ingresar a ver el monitoreo

http://www.xxxx.com/mailscanner

Donde xxxx es el nombre del servidor donde se instalo el Mailwatch.

En este url pedirá un usuario y una clave esto son lo que se ingreso en la base de datos con el comando Insert.

17.10 Conclusión

MailWatch es una herramienta de mucha utilidad para monitorear nuestro analizador de correo tiene muchas utilidades entre ellas informes personalizables con los filtros y gráficos de JpGraph, herramientas para ver la condición de anti-virus, base de datos MySQL y para ver los ficheros de configuración MailScanner, además muestra los entrantes, salientes y tamaño de cola de correo entre otras utilidades más.

CAPITULO 18. CONFIGURACIÓN DE RSYNC

18.1 Introducción

En muchas ocasiones es muy importante respaldar archivos y directorios de un equipo a otro esto con la finalidad de asegurar nuestra información. Es por eso que en este capítulo se vera el uso de Rsync que nos permite sincronizar la información entre dos equipos.

18.2 Rsync

Rsync es una aplicación que permite sincronizar los archivos y directorios entre dos equipos o en el mismo equipo. Para realizar dicha tarea únicamente transfiere los cambios realizados en el archivo y no todo el archivo. El puerto que utiliza es el 873.

18.3 Configuración en el equipo que se quiere respaldar

- Se crea el archivo /etc/rsyncd.conf que tiene la configuración de las carpetas que se quiere respaldar. El contenido de este archivo es:

```
#Opciones Generales de Configuración de Rsync
#Usuario y grupo con el que se ejecutara rsync
uid = nobody
gid = nobody
#Activa el entorno chroot para rsync
use chroot = yes
#Número máximo de conexiones que acepta el servidor
max connections = 1
#Log de rsync
log file = /var/log/rsyncd.log
#Archivo donde se graba el número pid del proceso rsync
pid file = /var/run/rsyncd.pid
```

```
#Nombre del modulo que se quiere configurar
[cgi]
#Path de la carpeta que se quiere respaldar
path = /var/www/cgi-bin
comment = CGI-BIN  Universidad del Azuay
use chroot = true
max connections = 1
#Se activa solo para lectura
read only = true
#No permite listar archivos del servidor
list = false
uid = root
gid = root
#Usuario con el que se conectara a rsync
auth users = usuario1
#Path y nombre del archivo donde esta la clave del usuario definido en auth users
secrets file = /etc/rsyncd.secrets
#Verifica que el archivo con la clave sea solo de lectura
strict modes = trae
#IP desde la cual se puede conectar al servidor rsync
hosts allow = 192.168.1.30

[www]
path = /var/www/html
comment = Web Universidad del Azuay
use chroot = true
max connections = 1
read only = true
list = false
uid = root
gid = root
auth users = usuario1
secrets file = /etc/rsyncd.secrets
strict modes = true
hosts allow = 192.168.1.30
```

- Se da permisos al archivo rsyncd.conf con chmod 644 rsyncd.conf
  -rw-r--r-- 1 root root 1987 oct 12 18:52 rsyncd.conf

- Se crea el archivo /etc/rsyncd.secrets y el contenido del archivo debe tener el nombre del usuario y la contraseña del mismo separado por dos puntos ejemplo:

  usuario1:clave

- Se da permisos al archivo rsyncd.secrets con chmod 700 rsyncd.secrets
  -rwx------ 1 root root 19 oct 11 11:33 rsyncd.secrets

- Se activa el servicio rsync service rsync start

18.4 Configuración en el equipo donde se grabara el respaldo

- Se crea el archivo /etc/password.rsync allí se pone la clave del usuario que se creo en el archivo /etc/rsyncd.secrets en este ejemplo se pondría la palabra clave como contenido de este archivo.

- Se da permisos al archivo password.rsyn con chmod 600 password.rsync
  -rw------- 1 root root 9 oct 11 11:13 password.rsync

- Se crea el archivo respaldo.sh en la carpeta /etc/cron.hourly para que se ejecute cada hora con el servicio cron. Este archivo debe contener:

```
#Ejemplo para respaldar toda una carpeta
/usr/bin/rsync --delete -arzvpl --password-file=/etc/password.rsync rsync://usuario11@192.168.1.1/www /respaldos/www

#Ejemplo para respaldar solo un archivo
/usr/bin/rsync --delete -arzvpl --password-file=/etc/password.rsync rsync://usuario1@192.168.1.1/cgi/prueba.pl /respaldos/cgi
```

18.5 Explicación de las Opciones

--delete Si se borra un archivo en el servidor a respaldar también se borra en el respaldo

--password-file Path y nombre del archivo donde esta la clave del usuario

rsync://usuario1@192.168.1.1/cgi/prueba.pl /respaldos/cgi

Nombre del usuario con el que se conecta en este caso usuario1. IP del servidor al cual se va a conectar en este caso 192.168.1.1. Nombre del modulo en este caso cgi. Nombre del archivo a respaldar en este caso prueba.pl. Nombre de la carpeta donde van a grabarse el respaldo en este caso /respaldos/cgi

-arzvpl

a (archive) La opción -a indica que preserve los enlaces simbólicos y demás archivos "extraños" igual que -rlptgoD
r (recursive) Respalda en forma recursiva
z (compress) Comprime los datos durante la transferencia
v (verbose) Muestra información detallada de lo que esta haciendo
p (perms) Conserva los permisos de los archivos
l (link) Respalda enlaces a archivos
t (times) Conserva la fecha y hora del archivo
g (group) Conserva el grupo del archivo
o (owner) Conserva el usuario del archivo
D Igual que --devices y --specials
--devices Respalda archivos de dispositivos (device)
--specials Respalda los archivos especiales
--rsh=ssh Respalda utilizando ssh

18.6 Configuración para que funcione mediante SSH

- Como usuario root se genera una llave pública y privada el servidor donde se va a respaldar la información con el comando ssh-keygen -t rsa (para ssh2) todos las preguntas se las contesta con los valores por defecto.

```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
c3:de:3c:46:d2:dd:87:34:ec:63:ed:09:c5:55:07:c9 root@uda
```

- Se copia el contenido del archivo root/.ssh/id_rsa.pub en el archivo /root/.ssh/authorized_keys (debe tener permisos chmod 600)del servidor al cual queremos respaldar.

- En las opciones del archivo respaldo.sh se aumenta la opcion --rsh=ssh para que rsync funcione bajo ssh.

18.7 Conclusión

En este capítulo se mostro como respaldar archivos de un equipo a otro mediante la herramienta Rsync que sincroniza archivos y directorios entre dos equipos, debido a su gran utilidad se vio necesario realizar esta práctica.

CAPITULO 19. CONFIGURACIÓN DE UN FIREWALL (IPTABLES)

19.1 Introducción

Con el fin de lograr cierta protección y seguridad en nuestro sistema se vio necesario en este capítulo dar una introducción y configuración acerca de Iptables que es una utilidad de linux que se encarga de darle directivas al kernel, acerca del filtrado de paquetes TCP/IP.

19.2 Iptables

Iptables es el nombre de la herramienta por medio de la cual el administrador crea reglas para filtrado de paquetes (Firewall). Iptables es una parte standard de todas las distribuciones Linux actuales. El Archivo donde se deben definir las reglas del Firewall es /etc/sysconfig/iptables si no existe se los debe crear. Debe tener solo permisos de escritura (w) y lectura (r) para el usuario root, y el archivo también debe pertenecer al grupo root. Para arrancar el servicio del Firewall se ejecuta **service iptables start**. Para grabar las reglas que están en memoria a un archivo se utiliza la instrucción **iptables-save > archivo.txt**. Para restaurar las reglas grabadas en un archivo a memoria se utiliza la instrucción **iptables-restore < archivo.txt**. Para ver las reglas que están cargadas en memoria se utiliza la instrucción **iptables –L**.

Un Ejemplo de Archivo de Configuración sería:

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
```

```
#Acepta conexiones localmente y desde eth0 y eth1
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i eth0 -j ACCEPT
-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT
# PROTECCION CONTRA PORT SCANNERS (nmap, etc...)
-A RH-Firewall-1-INPUT -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s
-j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -j REJECT --reject-with icmp-port-unreachable  --syn
-A RH-Firewall-1-INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
# PROTECCION CONTRA WORMS
-A RH-Firewall-1-INPUT -p tcp --dport 135:139 -j REJECT
-A RH-Firewall-1-INPUT -p udp --dport 135:139 -j REJECT
# PROTECCION CONTRA SYN-FLOODS
-A RH-Firewall-1-INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT
# PROTECCION CONTRA PING DE LA MUERTE
-A RH-Firewall-1-INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -j
ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
#Acepta conexiones http,https,ftp,smtp,ssh,proxy,pop,dns,webmin
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state -m tcp --dport 8080 --state NEW -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state -m tcp --dport 110 --state NEW -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state -m tcp --dport 53 --state NEW -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m state -m udp --dport 53 --state NEW -j ACCEPT
-A RH-Firewall-1-INPUT -p tcp -m state -m tcp --dport 10000 --state NEW -j
ACCEPT
-A RH-Firewall-1-INPUT -p udp -j ACCEPT  --source-port 53
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

19.3 Comandos de Iptables

Los comandos de iptables son:

Las cadenas internas para la tabla filtro son las siguientes:

INPUT — Aplica a los paquetes recibidos a través de una interfaz de red.

OUTPUT — Esta cadena sirve para paquetes enviados por medio de la misma interfaz de red que recibió los paquetes.

FORWARD — Esta cadena sirve para paquetes recibidos en una interfaz de red y enviados en otra.

Las cadenas internas para la tabla nat son las siguientes:

PREROUTING — Altera los paquetes de red cuando estos llegan.

POSTROUTING — Esta cadena altera paquetes antes de que sean enviados por medio de una interfaz de red.

POSTROUTING — Altera los paquetes de red cuando estos son enviados.

PREROUTING — Esta cadena altera paquetes recibidos por medio de una interfaz de red cuando llegan.

OUTPUT — Esta cadena altera paquetes generados localmente antes de que sean dirigidos por medio de una interfaz de red.

POSTROUTING — Esta cadena altera paquetes antes de que sean enviados por medio de una interfaz de red.

Las cadenas internas para la tabla mangle son las siguientes:

PREROUTING — Esta cadena altera paquetes recibidos por medio de una interfaz de red antes de que sean dirigidos.

POSTROUTING — Altera los paquetes de red cuando estos son enviados.

Independientemente de su destino, cuando un paquete cumple una regla en particular en una de las tablas, se les aplica un objetivo (target) o acción a ellos. Si la regla especifica un objetivo ACCEPT para un paquete que coincida, el paquete se salta el resto de las verificaciones de la regla y se permite que continúe hacia su destino. Si una regla especifica un objetivo DROP, a ese paquete se le niega el acceso al sistema y no se envía nada de vuelta al servidor que envió el paquete. Si una regla especifica un objetivo QUEUE, el paquete se pasa al espacio del usuario. Si una regla especifica el objetivo opcional REJECT, el paquete es descartado, pero se envía un paquete de error al que envió el paquete.

Cada cadena tiene una política por defecto de ACCEPT, DROP, REJECT, o QUEUE. Si ninguna de estas reglas en la cadena se aplica al paquete, entonces el paquete es tratado de acuerdo a la política por defecto.

19.4 Estructura de las opciones iptables

Muchos comandos iptables tienen la siguiente estructura:

iptables [-t <table-name>] <command> <chain-name> <parameter-1> \ <option-1> <parameter-n> <option-n>

- ### 19.4.1 Opciones de comandos

Las opciones de comandos le dicen a iptables que realice una acción específica. Solamente una opción de comando se permite por comando iptables. Excepto el comando de ayuda, todos los comandos se escriben en mayúsculas.

Los comandos de iptables son los siguientes:

-A — Añade la regla iptables al final de la cadena especificada. Este es el comando utilizado para simplemente añadir una regla cuando el orden de las reglas en la cadena no importa.

-C — Verifica una regla en particular antes de añadirla en la cadena especificada por el usuario. Este comando puede ser de ayuda para construir reglas iptables complejas pidiéndole que introduzca parámetros y opciones adicionales.

-D — Borra una regla de una cadena en particular por número (como el 5 para la quinta regla de una cadena). Puede también teclear la regla entera e iptables borrará la regla en la cadena que corresponda.

-E — Renombra una cadena definida por el usuario. Esto no afecta la estructura de la tabla.

-F — Libera la cadena seleccionada, que borra cada regla de la cadena. Si no se especifica ninguna cadena, este comando libera cada regla de cada cadena.

-h — Proporciona una lista de estructuras de comandos, así como también un resúmen rápido de parámetros de comandos y opciones.

-I — Inserta una regla en una cadena en un punto especificado por un valor entero definido por el usuario. Si no se especifica ningún número, iptables colocará el comando en el tope de la cadena.

- 19.4.2 Atención

Tenga en cuenta que al utilizar las opciones -A o -I el orden de las reglas dentro de una cadena es importante para determinar cuál regla aplica a cuáles paquetes.

-L — Lista todas las reglas de la cadena especificada tras el comando. Para ver una lista de todas las reglas en todas las cadenas en la tabla por defecto filter, no especifique ninguna cadena o tabla. De lo contrario, la sintaxis siguiente deberá utilizarse para listar las reglas en una cadena específica en una tabla en particular: iptables -L <chain-name> -t <table-name>

-N — Crea una nueva cadena con un nombre especificado por el usuario.

-P — Configura la política por defecto para una cadena en particular, de tal forma que, cuando los paquetes atraviesen la cadena completa sin cumplir ninguna regla, serán enviados a un objetivo en particular, como puedan ser ACCEPT o DROP.

-R — Reemplaza una regla en una cadena particular. El número de la regla debe ser especificado después del nombre de la cadena. La primera regla en una cadena corresponde a la regla número uno.

-X — Borra una cadena especificada por el usuario. No se permite borrar ninguna de las cadenas predefinidas para cualquier tabla.

-Z — Pone ceros en los contadores de byte y de paquete en todas las cadenas de una tabla en particular.

19.5 Opciones de parámetros de iptables

Una vez que se especifiquen ciertos comandos iptables, incluyendo aquellos para añadir, anexar, eliminar, insertar o reemplazar reglas dentro de una cadena, se requieren parámetros para construir una regla de filtrado de paquetes.

-c — Resetea los contadores de una regla en particular. Este parámetro acepta las opciones PKTS y BYTES para especificar qué contador hay que resetear.

-d — Configura el nombre de la máquina destino, dirección IP o red de un paquete que coincide con la regla. Cuando se coincida una red, se soportan los siguientes formatos de direcciones IP o máscaras de red:

N.N.N.N/M.M.M.M — Donde N.N.N.N es el rango de direcciones IP y M.M.M.M es la máscara de la red.

N.N.N.N/M — Donde N.N.N.N es el rango de direcciones IP y M es la máscara de bit.

-f — Aplica esta regla sólo a los paquetes fragmentados.

Usando la opción ! después de este parámetro, únicamente se harán coincidir los paquetes no fragmentados.

-i — Configura la interfaz de red entrante, tal como eth0 o ppp0. Con iptables, este parámetro opcional puede ser usado solamente con las cadenas INPUT y FORWARD cuando es usado con la tabla filter y la cadena PREROUTING con las tablas nat y mangle.

Este parámetro también soporta las siguientes opciones especiales:

El carácter de exclamación! — Invierte la directriz, es decir, se excluye de esta regla cualquier interfaz especificada.

El caráter de suma + — Un caracter tipo comodín utilizado para coincidir todas las interfaces con una cadena de caracteres especificada. Por ejemplo, el parámetro -i eth+ aplicará esta regla a cualquier interfaz Ethernet pero excluirá cualquier otra interfaz, tal como, ppp0.

Si el parámetro -i se utiliza sin especificar ninguna interfaz, todas las interfaces estarán afectadas por la regla.

-j — Salta a un objetivo particular cuando un paquete coincide con una regla particular. Los objetivos válidos a usar después de la opción -j incluyen las opciones estándar (ACCEPT, DROP, QUEUE y RETURN) así como también las opciones extendidas que están disponibles a través de los módulos cargados por defecto con el paquete RPM de Red Hat Enterprise Linux iptables, como LOG, MARK y REJECT, entre otros. Consulte la página del manual de iptables para más información sobre esto y otros objetivos.

Puede también dirigir un paquete coincidiendo esta regla a una cadena definida por el usuario fuera de la cadena actual, para aplicar otras reglas al paquete.

Si no especifica ningún objetivo, el paquete pasa la regla sin llevar a cabo ninguna acción. A pesar de todo, el contador para esta regla se sigue incrementando en uno.

-o — Configura la interfaz de red de salida para una regla y puede ser usada solamente con las cadenas OUTPUT y FORWARD en la tabla de filtro y la cadena POSTROUTING en las tablas nat y mangle. Estos parámetros de opciones son los mismos que aquellos de la interfaz de entrada (-i).

-p — Configura el protocolo IP para la regla, el cual puede ser icmp, tcp, udp, o all, para coincidir todos los protocolos soportados. Además, se puede usar cualquier protocolo listado en /etc/protocols. Si esta opción es omitida cuando se esté creando una regla, la opción all es la opción por defecto.

-s — Configura la fuente para un paquete particular usando la misma sintaxis que el parámetro (-d).

19.6 Protocolo TCP

Estas opciones de identificación están disponibles en el protocolo TCP (opción -p tcp):

--dport — Configura el puerto de destino para el paquete. Use bien sea un nombre de servicio (tal como www o smtp), número de puerto, o el rango de números de puertos para configurar esta opción. Para hojear los nombres y alias de los servicios de red y los números que ellos usan, visualice el archivo /etc/services. La opción --destination-port es sinónimo con --dport.

Para especificar un rango de números de puertos, separe los dos números con dos puntos (:), tal como -p tcp --dport 3000:3200. El rango más grande aceptable es 0:65535.

Use un caracter de exclamación (!) después de la opción --dport para coincidir todos los paquetes que no utilizan el servicio de red o puerto.

--sport — Configura el puerto fuente del paquete usando las mismas opciones que --dport. La opción --source-port es sinónimo con --sport.

--syn — Provoca que todos los paquetes designados de TCP, comúnmente llamados paquetes SYN, cumplan esta regla. Cualquier paquete que esté llevando un payload de datos no será tocado. Si se sitúa un punto de exclamación (!) como bandera tras la opción --syn se provoca que todos los paquetes no-SYN sean seleccionados.

--tcp-flags — Permite a los paquetes TCP con bits específicos o banderas, ser coincididos con una regla. La opción --tcp-flags acepta dos parámetros. El primer parámetro es la máscara, la cual configura banderas a ser examinadas en el paquete. El segundo parámetro se refiere a la bandera que se debe configurar para poder coincidir.

Las banderas posibles son:

ACK,FIN,PSH,RST,SYN,URG,ALL,NONE

Por ejemplo, una regla iptables que contenga -p tcp --tcp-flags ACK,FIN,SYN SYN tan sólo seleccionará los paquetes TCP que tengan la bandera SYN activo y las banderas ACK y FIN sin activar.

Usando el caracter de exclamación (!) después de --tcp-flags reversa el efecto de la opción de coincidencia.

--tcp-option — Intenta seleccionar con opciones específicas de TCP que pueden estar activas en un paquete en particular. Esta opción se puede revertir con el punto de exclamación (!).

19.7 Protocolo UDP

Estas opciones de selección están disponibles para el protocolo UDP (-p udp):
--dport — Especifica el puerto destino del paquete UDP, usando el nombre del servicio, número de puerto, o rango de números de puertos. La opción de coincidencia --destination-port es sinónimo con --dport.

--sport — Configura el puerto fuente del paquete UDP, usando el nombre de puerto, número de puerto o rango de números de puertos. La opción --source-port es sinónimo con --sport.

19.8 Protocolo ICMP

Las siguientes opciones de coincidencia están disponibles para el Protocolo de mensajes de Internet (ICMP) (-p icmp):

--icmp-type — Selecciona el nombre o el número del tipo ICMP que concuerde con la regla. Se puede obtener una lista de nombres válidos ICMP tecleando el comando iptables -p icmp -h.

19.9 Módulos con opciones de coincidencias adicionales

Opciones adicionales de coincidencia están disponibles a través de los módulos por el comando iptables. Para usar un módulo de opciones de coincidencia, cargue el módulo por nombre usando la opción -m, tal como -m <module-name> (reemplazando <module-name> con el nombre del módulo).

Un gran número de módulos están disponibles por defecto. Hasta es posible crear sus módulos para proporcionar funcionalidades de opciones de coincidencia adicionales.

Lo siguiente, es una lista parcial de los módulos usados más comúnmente:

limit module — Permite colocar un límite en cuántos paquetes son coincididos a una regla particular. Esto es especialmente beneficioso cuando se usa en conjunto con el objetivo LOG, pues puede prevenir que una inundación de paquetes coincidentes sobrecarguen el registro del sistema con mensajes repetitivos o usen los recursos del sistema. Para más información sobre el objetivo LOG, refiérase a la Sección 18.3.5.

El módulo limit habilita las opciones siguientes:

--limit — Configura el número de coincidencias en un intervalo de tiempo, especificado con un número y un modificador de tiempo ordenados en el formato <número>/<tiempo>. Por ejemplo, si usamos --limit 5/hour sólo dejaremos que una regla sea efectiva cinco veces a la hora.

Si no se utiliza ningún número ni modificador de tiempo, se asume el siguiente valor por defecto: 3/hour.

--limit-burst — Configura un límite en el número de paquetes capaces de cumplir una regla en un determinado tiempo. Esta opción deberá ser usada junto con la opción --limit, y acepta un número para configurar el intervalo de tiempo (threshold).

Si no se especifica ningún número, tan sólo cinco paquetes serán capaces inicialmente de cumplir la regla.

módulo state — Habilita la coincidencia de estado.

El módulo state tiene las siguientes opciones:

--state — coincide un paquete con los siguientes estados de conexión:

ESTABLISHED El paquete seleccionado se asocia con otros paquetes en una conexión establecida.

INVALID El paquete seleccionado no puede ser asociado a una conexión conocida.

NEW El paquete seleccionado o bien está creando una nueva conexión o bien forma parte de una conexión de dos caminos que antes no había sido vista.

RELATED El paquete seleccionado está iniciando una nueva conexión en algún punto de la conexión existente.

Estos estados de conexión se pueden utilizar en combinación con otros separándolos mediante comas como en -m state --state INVALID, NEW.

módulo mac — Habilita la coincidencia de direcciones MAC de hardware.

El módulo mac activa las opciones siguientes:

--mac-source — Coincide una dirección MAC a la tarjeta de red que envió el paquete. Para excluir una dirección MAC de la regla, coloque un símbolo de exclamación (!) después de la opción --mac-source.

Para visualizar otras opciones disponibles a través de los módulos, consulte la página del manual de iptables.

19.10 Opciones del objetivo

Una vez que un paquete ha coincidido con una regla, la regla puede dirigir el paquete a un número de objetivos diferentes que deciden su suerte y, posiblemente, toman acciones adicionales. Cada cadena tiene un objetivo por defecto, el cual es usado si ninguna de las reglas en esa cadena coinciden con un paquete o si ninguna de las reglas que coinciden con el paquete especifica un objetivo.

Los siguientes son los objetivos estándar:

<user-defined-chain> — Reemplace <user-defined-chain> con el nombre de una cadena definida por el usuario dentro de la tabla. Este objetivo pasa el paquete a la cadena objetivo.

ACCEPT — Permite que el paquete se mueva hacia su destino (o hacia otra cadena, si no ha sido configurado ningún destino para seguir a esta cadena).

DROP — Deja caer el paquete sin responder al solicitante. El sistema que envia el paquete no es notificado de esta falla.

QUEUE — El paquete se pone en una cola para ser manejado por una aplicación en el espacio de usuario.

RETURN — Para la verificación del paquete contra las reglas de la cadena actual. Si el paquete con un destino RETURN cumple una regla de una cadena llamada desde otra cadena, el paquete es devuelto a la primera cadena para retomar la verificación de la regla allí donde se dejó. Si la regla RETURN se utiliza en una cadena predefinida, y el paquete no puede moverse hacia la cadena anterior, el objetivo por defecto de la cadena actual decide qué acción llevar a cabo.

Además de estos objetivos standard, se pueden usar otros más con extensiones llamadas módulos de objetivos (target modules). Para obtener más información sobre los módulos de opciones de coincidencias, mire en la Sección 18.3.4.4.

Existen varios módulos extendidos de objetivos, la mayoría de los cuales tan sólo se aplican a tablas o situaciones específicas. Un par de estos módulos, de los más populares e incluidos por defecto en Red Hat Enterprise Linux son:

LOG — Registra todos los paquetes que coinciden esta regla. Puesto que los paquetes son registrados por el kernel, el archivo /etc/syslog.conf determina dónde estas entradas de registro serán escritas. Por defecto, son colocadas en el archivo /var/log/messages.

Se pueden usar varias opciones adicionales tras el objetivo LOG para especificar la manera en la que tendrá lugar el registro:

--log-level — Configura el nivel de prioridad del registro de eventos. Una lista de los niveles de prioridad se puede encontrar en la página del manual de syslog.conf.

--log-ip-options Cualquier opción en la cabecera de un paquete IP se guarda en el registro.

--log-prefix — Coloca una cadena de hasta 29 caracteres antes de la línea de registro cuando es escrita. Esto es muy útil para la escritura de filtros de syslog para usarlos en conjunto con el registro de paquetes.

--log-tcp-options — Cualquier opción colocada en la cabecera de un paquete TCP es registrada.

--log-tcp-sequence Escribe el número de secuencia TCP del paquete en el registro del sistema.

REJECT — Envia un paquete de error de vuelta al sistema remoto y deja caer el paquete.

El objetivo REJECT acepta --reject-with <tipo> (donde <tipo> es el tipo de rechazo) el cual permite devolver información más detallada con el paquete de error. El mensaje port-unreachable es el <tipo> de error por defecto dado si no se usa otra opción. Para una lista completa de los <tipo>s de opciones que se pueden usar, consulte la página del manual de iptables.

Otras extensiones de objetivos, incluyendo muchas que son útiles para el enmascaramiento de IP usando la tabla nat o con alteración de paquetes usando la tabla mangle, se puede encontrar en la página del manual de iptables.

19.11 Opciones de listado

El comando predeterminado para listar, iptables -L, proporciona una vista muy básica de los filtros por defecto de las cadenas actuales de la tabla. Las opciones adicionales proporcionan más información:

-v — Muestra la salida por pantalla con detalles, como el número de paquetes y bytes que cada cadena ha visto, el número de paquetes y bytes que cada regla ha encontrado y qué interfaces se aplican a una regla en particular.

-x Expande los números en sus valores exactos. En un sistema ocupado, el número de paquetes y bytes vistos por una cadena en concreto o por una regla puede estar abreviado usando K (miles), M (millones), y G (billones) detrás del número. Esta opción fuerza a que se muestre el número completo.

-n Muestra las direcciones IP y los números de puertos en formato numérico, en lugar de utilizar el nombre del servidor y la red tal y como se hace por defecto.

--line-numbers — Proporciona una lista de cada cadena junto con su orden numérico en la cadena. Esta opción puede ser útil cuando esté intentando borrar una regla específica en una cadena o localizar dónde insertar una regla en una cadena.

-t — Especifica un nombre de tabla.

19.12 Configuración de una herramienta cortafuegos Firestarter

Firestarter es uno de los cortafuegos más sencillos de utilizar y configurar que podemos encontrar para GNU/Linux. Es una muy buena opción para tener de forma rápida y cómoda un cortafuegos que satisfacerá la mayoría de nuestras necesidades.

En esta URL podemos encontrar esta herramienta:

http://rpm.pbone.net/index.php3/stat/4/idpl/5781621/com/firestarter-1.0.3-17.el5.kb.i386.rpm.html y descargamos el archivo

firestarter-1.0.3-17.el5.kb.i386.rpm

19.12.1 Primeros pasos: Asistente de configuración

La primera vez que iniciemos *Firestarter* se nos abrirá un asistente que nos configurará los parámetros básicos del cortafuegos. Nos preguntará lo siguiente:

Dispositivo de red en el que vamos a filtrar el tráfico.
Si queremos iniciar el cortafuegos al iniciar la conexión.
Si obtenemos la dirección IP por DHCP.
Si queremos activar la conexión compartida a Internet (por si queremos que otros PCs salgan a Internet a través de este.
Si queremos iniciar el cortafuegos al finalizar el asistente.

Una vez seleccionadas las opciones que creamos convenientes, llegaremos a la pantalla principal de *Firestarter* y tendremos el cortafuegos con una configuración por defecto, denegando el tráfico entrante.

19.12.2 Configurando el cortafuegos: creando reglas para abrir puertos

En la ventana principal tenemos las tres pestañas desde las que se administra este cortafuegos:

Gráfico 19.1

Eventos: Muestra las conexiones que el cortafuegos ha rechazado. **Normativa:** Muestra las reglas que hemos definido para configurar el cortafuegos. Como lo que queremos es configurar las reglas necesarias para que el cortafuegos permita el acceso a través de ciertos puertos, iremos a la pestaña Normativa para crear nuestras reglas personalizadas.

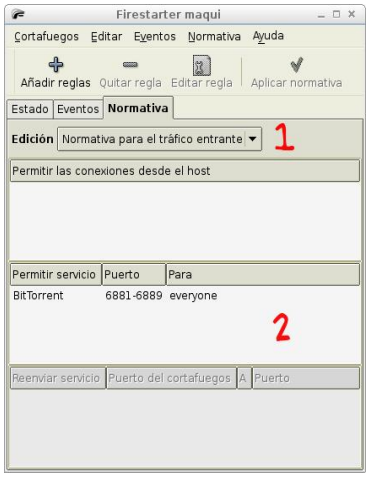

Gráfico 19.2

Para crear nuestras reglas, primero dejaremos seleccionada la opción **Normativa para el tráfico entrante**.

La normativa de tráfico saliente no la tocaremos, ya que por defecto permite todo el tráfico de nuestra máquina al exterior, y en principio este será tráfico permitido.

Una vez seleccionada esa opción, pincharemos con el botón derecho en el panel

inferior, y en el menú contextual que se nos abrirá, seleccionaremos la opción **Añadir regla**.

Gráfico 19.3

Se nos abrirá una ventana en la que introduciremos la información del puerto que queremos abrir:

Nombre: Nombre descriptivo para el puerto que abriremos.
Puerto: Puerto a abrir (si queremos abrir un rango, pondremos algo del estilo: 6881-6889).
Origen: Si queremos abrirlo sólo para lo que provenga de una IP concreta.
Normalmente querremos dejar esta opción en **cualquiera**.
Comentario: Un comentario (opcional) que describa para qué se usa ese puerto.

Una vez introducidos los datos, le damos al botón **Añadir** y la regla quedará aplicada.

19.12.3 Abriendo puertos a partir de conexiones registradas

Si no sabemos qué puertos utiliza una aplicación y ésta no funciona correctamente, es probable que el cortafuegos esté denegándole el tráfico, al no tener configurada una regla explícita para ella.

En este caso, en la pestaña Eventos veremos las conexiones de dicha aplicación:

Gráfico 19.4

Si damos clic con el botón derecho del ratón sobre la conexión correspondiente a nuestra aplicación, se nos abrirá un menú contextual que nos mostrará las opciones:

Gráfico 19.5

Para abrir el puerto correspondiente a dicha aplicación, seleccionaremos la opción **Permitir tráfico de servicio entrante para todo el mundo**.

19.12.4. Permitir el tráfico de nuestra red

Como el firewall por defecto es muy restrictivo, seguramente nos rechazará la mayoría de tráfico que proviene de nuestra red local. Si se quieren compartir ficheros entre las máquinas, etc, es posible que queramos configurar una regla para permitir el acceso a nuestra máquina desde los PCs de nuestra LAN.

Para ello iremos a la pestaña **Normativa** y daremos un clic con el botón derecho del ratón en el recuadro Permitir las conexiones desde el host (teniendo seleccionada en el estado la opción de Normativa para el tráfico entrante).

Gráfico 19.6

En la pantalla que se nos abre podremos introducir la ip, nombre de la máquina o red (ip junto con la máscara) a la que queramos permitir el acceso completo a nuestro PC.

Una vez introducidos los valores (el comentario es opcional), le daremos al botón **Añadir**.

Siguiendo estos pasos pueden configurarse las reglas típicas que necesitaremos en nuestros PCs de escritorio para utilizar las aplicaciones más comunes, y a la vez tener el acceso bien restringido.

19.13 Conclusión

Este capítulo trato sobre firewall (iptables) que sirve para filtrar paquetes tcp/ip, es decir controlar el trafico de información o paquetes que pasan por nuestro ordenador e internet, se vio un ejemplo de configuración y los conceptos necesarios para poder crear un achivo de configuración de acuerdo a nuestras necesidades.

CONCLUSIONES GENERALES

Se logro completar la instalación y configuración de los servicios de yum, vnc, web, dns, telnet, ftp, Proxy, ssh, dhcp, sendmail, openwebmail, mailscanner, Spamassassin, mailwatch, rsync, firewall.

Para la instalación de los servicios anteriormente descritos se necesito realizar un manual de los comandos básicos de Linux y de las instrucciones básicas de la programación en bash.

Linux es un sistema operativo que se presta para poder enseñar a configurar los servicios que necesita cualquier empresa, debido a que se puede manipular cualquier configuración de acuerdo a las necesidades propias de la práctica.

Las personas que lean el documento podrán al final del mismo realizar cualquier implementación de los servicios antes mencionadas sin ninguna dirección adicional.

Todos los servicios que se documentan son ampliamente usados y es ese el motivo por el cual fuerón escojidos.

RECOMENDACIONES GENERALES

Es importante en primera instancia hacer una correcta instalación del sistema operativo ya que de estar mal instalado, ciertas prácticas no funcionarán, es por eso que se debe poner atención en la parte de la instalación.

Revisar los requisitos de hardware para la instalación del software para las prácticas.

Otra cosa muy importante al momento de bajarse paquetes debemos comprobar que estos sean para la versión de Linux que estamos utilizando ya que de no ser así provocaría conflictos en la instalación.

Se debe comprender bien el manejo de comandos básicos ya que varios de estos se manejarán en todo el tutorial.

También se recomienda leer los conceptos para entender lo que estamos haciendo en cada práctica. Si es posible primero leer toda la práctica y entender para luego desarrollarla.

BIBLIOGRAFÍA

- WEBMIN http://www.webmin.com/ [consulta Abril 7 de 2008].
- DAG http://dag.wieers.com [consulta Abril 10 de 2008].
- Alcance Libre http://www.alcancelibre.org [consulta Abril 16 de 2008].
- Programación en BASH - COMO de introducciónhttp://es.tldp.org/COMO-INSFLUG/COMOs/Bash-Prog-Intro-COMO/ [consulta Abril 18 de 2008].
- Advanced Bash-Scripting Guidehttp://tldp.org/LDP/abs/html/ [consulta Abril 21 de 2008].
- Real VNC http://realvnc.com [consulta Abril 23 de 2008].
- TightVNC Softwarehttp://tightvnc.com [consulta Abril 24 de 2008].
- VeriSign http://verisign.com [consulta Mayo 5 de 2008].
- Squish http://www.squish.net [consulta Mayo 7 de 2008].
- Dnstuff.com http://dnstuff.com **[consulta Mayo 12 de 2008].**
- Centralops.net http://centralops.net [consulta Mayo 13 de 2008].
- Linux para Todos http://www.linuxparatodos.net [consulta Mayo 16 de 2008].
- Redhat http://www.redhat.com/ [consulta Mayo 20 de 2008].
- Rpm.pbone.net http://rpm.pbone.net/ [consulta Mayo 26 de 2008].
- Spamhaus http://www.spamhaus.org [consulta Mayo 29 de 2008].
- @pen Webmail http://www.openwebmail.org [consulta Junio 6 de 2008].
- MailScanner http://www.mailscanner.info/ [consulta Junio 12 de 2008].
- ClamAV http://www.clamav.net [consulta Junio 18 de 2008].
- ADSL Ayuda http://adslayuda.com/cortafuego/firestarter.html [consulta Junio 20 de 2008].

ANEXOS