**INSTITUTO TECNOLÓGICO DE COSTA RICA**

**ESCUELA DE INGENIERÍA EN COMPUTACIÓN**

**PRINCIPIOS DE SISTEMAS OPERATIVOS**

**II SEMESTRE**

**LABORATORIO #3**

**ESTUDIANTES**

**KATHY BRENES GUERRERO 2013012213**

**BARNUM CASTILLO BARQUERO 2013008696**

**PROFESOR**

**ESTEBAN ARIAS MENDEZ**

**GRUPO 40**

**fecha**

**21 de Octubre**

**Curso Lectivo 2015**

*Actividades*

*Formato archivo sudoers*

El archivo de sudoers esta compuesto de dos principales entradas que corresponden al:

*a) Aliases:* Son basicamente las variables.

*b) User specifications:* Especifica quien va realizar cada tarea.

Puede darse el caso en el que varias entradas coincidan para un mismo usuario, por lo que cada una de ellas deben ser aplicadas en el orden especificado por el archivo mencionado previamente. [1]

Este archivo puede ser leido y editado por medio del siguiente comando:

|  |
| --- |
| *$ sudo visudo* |

*Reglas que conforman el archivo sudoers*

Las reglas especificadas en este archivo se construyen como las reglas utilizadas para describir una gramatica de un lenguaje como la Extended Backus-Naur Form, donde cada regla de produccion puede hacer referencia a otra regla definida dentro del conjunto, ademas podrian incluir operandos como el ? , + , \* que se utilizan para reconocer expresiones regulares. Los simbolos anteriores especifican respectivamente que simbolo que lo precede es opcional, puede aparecer una vez o ninguna del todo (?), luego que el simbolo precedido puede aparecer cero o mas veces (\*), finalmente el simbolo podria aparecer una o mas veces (+). [1]

*Aliases*

Existen cuatro tipo de aliases que corresponden a: User\_Alias, Runas\_Alias, Host\_Alias and Cmnd\_Alias. Cada definicion de las anteriores siguen con la forma:

|  |
| --- |
| *Alias\_Type Name= item1, item 2, …*  ***Alias\_Type:*** *Se indica si es User\_Alias, Runas\_Alias, Host\_Alias o Cmnd\_Alias.*  ***Name:*** *Es una cadena de caracteres conformado de letras mayusculas, numeros y guion bajo, sin embargo siempre debe de iniciar con una letra mayuscula.* |

1. *User Aliases:* Se utilizan para especificar grupos de usuarios, se pueden indicar nombres de usuarios, grupos de sistemas con el prefijo % e incluso grupos de red con el prefijo +. Algunos ejemplos podrian ser [2]:

|  |
| --- |
| *# Everybody in the system group "admin" is covered by the alias ADMINS*  *User\_Alias ADMINS = %admin*  *# The users "tom", "dick", and "harry" are covered by the USERS alias*  *User\_Alias USERS = tom, dick, harry*  *# The users "tom" and "mary" are in the WEBMASTERS alias*  *User\_Alias WEBMASTERS = tom, mary*  *# You can also use ! to exclude users from an alias*  *# This matches anybody in the USERS alias who isn't in WEBMASTERS or ADMINS aliases*  *User\_Alias LIMITED\_USERS = USERS, !WEBMASTERS, !ADMINS* |

2. *Runas Aliases:* Es muy similar a los user aliases pero se diferencian porque se pueden especificar los usuarios por medio de los ids. Es muy util para cuando dos usuarios poseen el mismo nombre de usuario. Ejemplos [2]:

|  |
| --- |
| *# UID 0 is normally used for root*  *# Note the hash (#) on the following line indicates a uid, not a comment.*  *Runas\_Alias ROOT = #0*  *# This is for all the admin users similar to the User\_Alias of ADMINS set earlier*  *# with the addition of "root"*  *Runas\_Alias ADMINS = %admin, root* |

3. *Host Aliases:* Corresponde a una lista de nombres de host, direcciones ip, redes y grupos de red. En caso de que no se especifique la mascara de subnets con la red, se utilizaran las interfaces ethernet. Ejemplos [1]:

|  |
| --- |
| *# This is all the servers*  *Host\_Alias SERVERS = 192.168.0.1, 192.168.0.2, server1*  *# This is the whole network*  *Host\_Alias NETWORK = 192.168.0.0/255.255.255.0*  *# And this is every machine in the network that is not a server*  *Host\_Alias WORKSTATIONS = NETWORK, !SERVER*  *# This could have been done in one step with*  *# Host\_Alias WORKSTATIONS = 192.168.0.0/255.255.255.0, !SERVERS*  *# but I think this method is clearer.* |

4. *Command Aliases:* Conformado por la lista de los comandos y directorios, se puede utilizar para especificar un grupo de comandos. Ejemplos [1]:

|  |
| --- |
| *# All the shutdown commands*  *Cmnd\_Alias SHUTDOWN\_CMDS = /sbin/poweroff, /sbin/reboot, /sbin/halt*  *# Printing commands*  *Cmnd\_Alias PRINTING\_CMDS = /usr/sbin/lpc, /usr/sbin/lprm*  *# Admin commands*  *Cmnd\_Alias ADMIN\_CMDS = /usr/sbin/passwd, /usr/sbin/useradd, /usr/sbin/userdel, /usr/sbin/usermod, /usr/sbin/visudo*  *# Web commands*  *Cmnd\_Alias WEB\_CMDS = /etc/init.d/apache2* |

*User Specifications*

Esta es la parte fundamental del archivo, ya que es donde se especifica quien puede ejecutar que, las aliases deben de estar definidas previamente, dado que para este punto unicamente vamos asignar los permisos para los conjuntos de usuarios o los usuarios especificados en las aliases. Los user specifications deben de seguir el siguiente comando [1].

|  |
| --- |
| *<user list> <host list> = <operator list> <tag list> <command list>* |

***Formatos de los archivos***

*/etc/passwd*

Es un archivo de texto que almacena la informacion esencial requerida para la ejecucion del login, como la informacion de la cuenta de usuario. Esta conformado por una linea por cada cuenta de usuario registrado en la lista de cuentas del sistema, donde se almacenansta informacion como: id del usuario, id del grupo, home directory, shell, etc. Se deben tener permisos generales para poder leer el archivo. Solo funciona para usuarios locales Cada linea del archivo debe tener el siguiente formato [3]:

|  |
| --- |
| *Oracle (1) : x (2) : 1021 (3) : 1020 (4): Oracle user (5): [/data/network/oracle] (6): [/bin/bash] (7)*  *(1)* ***Username:*** *Debe contener entre 1 y 32 caracteres.*  *(2)* ***Password:*** *Un caracter x que indique que la contrase;a encriptada se localiza en el archivo /etc/shadow.*  *(3)* ***User ID (UID):*** *Cada usuario debe tener asignado un id, que pertenece al rango de 1 a 99. El id 0 esta reservado para* ***root*** *y en el rango de 100-999 se encuentra reservado para el sistema.*  *(4)* ***Group ID (GID):*** *El id del grupo principal (almacenado en el archivo /etc/group).*  *(5)* ***User ID Info:*** *Campo de comentarios, permite agregar informacion adicional sobre los usuarios como nombre completo o numero telefonico.*  *(6)* ***Home directory:*** *Toda la ruta del directorio en el que se ubicar el usuario una vez que haya iniciado sesion. Si no existiera el usuario se dirige a /.*  *(7)* ***Command / shell:*** *La ruta completa de la linea de comandos (bin/bash).* |

*/etc/shadow*

La contrase;a encriptada se almacena en este archivo, dado a que en los viejos tiempos no existia el problema de los permisos de lectura, sin embargo, este archivo no va poder ser leido por cualquier usuario regular. Cada linea del archivo contiene 9 campos que son separados por “:”, estos campos corresponden a [5]:

- **Login name:** Debe de corresponder a un nombre de cuenta valido que exista en el sistema.

- **Encrypted passoword:** Se refiere a la cadena de caracteres que contiene la contrase;a encriptada, eventualmente podria encontrarse vacio.

**- Date of last password change:** Corresponde a la fecha del ultimo cambio de contrase;a, expresado en la cantidad de dias restantes para que el usuario tenga que cambiar la contrase;a, en caso de que este valor sea 0 quiere decir que la proxima vez que el usuario se loguee este debe de realizar el cambio.

**- Minimum password age:** Es el numero de dias que el usuario tendra que esperar para poder cambiar su contrase;a de nuevo. Si el valor es 0 quiere decir que no existe una cantidad de dias establecido.

**- Maximum password age:** Numero de dias despues de cambiar la contrase;a que el usuario tendra para poder cambiarla.

**- Password warning period:** Numero de dias previos a que la contrase;a expire, tiempo en el que el usuario recibira recordatorios.

**- Password Inactivity period:** Cantidad de dias despues de que la contrase;a ha expirado en el que la contrase;a seguira siendo aceptada, antes de estar en estado inactivo.

**- Account Expiration date:** Fecha de vencimiento de la cuenta, que se expresa como la cantidad de dias que faltan para que llegue esa fecha.

**- Reserved field:** Es un espacio reservado para usos futuros.

*/etc/group*

Es un archivo de texto en el que se definen los grupos a los que pertenece el usuario en los sistemas operativos Linux y Unix. Los permisos se subdividen en tres clases: el usuario, el grupo y otros. El uso de grupos permite funcionalidades adicionales para delegar y organizarse de mejor manera como el acceso a discos, impresoras o bien acceso a otros perifericos. En este archivo se definen los grupos en cada linea, con el siguiente formato[6]:

* **Group name:** Es el nombre que se le asignara al grupo.
* **Password:** Generalmente no se utiliza la contrase;a, por lo que se deja vacia o con un espacio en blaco. En este espacio se puede almacenar la contrase;a encriptada. Es muy util para implementar grupos privilegiados.
* **Group id (GID):**  A cada usuario se le debe asignar el id del grupo al que pertenece. Este nombre se puede ver en el archivo /etc/passwd.
* **Group list:** Es la lista que contiene todos los nombres de usuario de aquellos usuarios que pertenecen al grupo. Los nombres de usuario, seran separados por comas.

*/etc/profile*

*Es el archivo que o*

*~/.profile*

Explique en el documento a entregar con sus propias palabras las secciones que componen el archivo sudoers y la forma en que deben construirse las reglas. De esta forma podrá darle permisos al usuario de trabajo “alumno” o el usuario que usa en su máquina para realizar las actividades requeridas. Documente además el formato de los archivos de configuración de usuarios para cuentas locales: /etc/passwd, /etc/shadow y /etc/group, /etc/profile y ~/.profile ; indicando su propósito y el orden de los campos que guardan la información dentro del archivo.

1. Verifique si el usuario normal de trabajo “alumno” (o el usuario de su máquina) tiene permiso de ejecutar ‘sudo’. Indique ¿cómo puede probar esto? Es decir, ¿por qué tiene permiso de ejecutar sudo?

2. a - Si el usuario de trabajo “alumno” (o su usuario) tiene acceso a ejecutar ‘sudo’. Indique, examinando el archivo /etc/sudoers, ¿cómo se le concedió permiso al usuario de trabajo para ejecutar ‘sudo’?. Indique ¿cuáles comandos puede ejecutar con ‘sudo’ dicho usuario?

2. b - Si el usuario NO tiene acceso a ejecutar ‘sudo’. Investigue cómo darle acceso a dicho usuario “alumno”  (o su usuario) para que pueda ejecutar ’sudo’. Y la configuración requerida en el archivo /etc/sudoers. En este caso cree reglas específicas para que el usuario “alumno”  (o su usuario) pueda ejecutar con sudo solamente los comandos y acceder los archivos de configuración listados previamente.

Indique en el documento a entregar, las reglas previamente definidas en sudoers si es la opción 2.a o bien las reglas que agregó al archivo si es la opción 2.b.

Nota:

En la máquina virtual del laboratorio que usa el usuario “alumno”, es posible que requiera convertirse en el usuario root o un usuario con privilegios como “soporte”. Para esto, ingrese como el usuario “soporte”, haciendo $ su - soporte y usando la clave “linux”, así ingresará como el usuario administrativo “soporte” el cual puede ejecutar comandos con “sudo”. Si requiere convertirse en root: una vez que se ha convertido en el usuario “soporte”, puede hacer $ sudo su - , para convertirse en el usuario root, sudo pedirá nuevamente la clave del usuario soporte la cual es “linux” como se indicó. Recuerde que la clave del usuario "alumno" es "so".

3. Una vez que el usuario de trabajo “alumno” (o su usuario) puede ejecutar ’sudo’ trabaje con dicho usuario y NO como root. Realice las siguientes actividades.

+ Escriba un programa script de Shell para BASH, que despliegue al usuario un menu usando el comando “select” para las siguientes opciones:

- crear usuario

- modificar usuario

- borrar usuario

- establecer contraseña usuario

- crear grupo

- borrar grupo

- salir

+ Dicho programa debe implementar cada una de las opciones listadas. Todas las opciones deben implementarse para ejecutarse en la máquina LOCAL así como en una máquina REMOTA que el usuario indique mediante IP por ejemplo. El usuario elige si la cuenta es LOCAL o REMOTA. Para los accesos remotos podrá usar SSH para conectarse entre máquinas y ejecutar dichos comandos.

+ La información que se debe solicitar a la persona para agregar un usuario es toda la requerida por el archivo /etc/passwd, es decir: el login-name, el texto comentario, el UID, GID principal, grupos adicionales (si los hay, sino vacío), el shell default, el home directory default. Estos mismos valores son los que podrá cambiarse al usuario, los datos que el comando usermod permita alterar para un usuario dado.

+ Su programa debe crear un archivo de reporte tipo log local que almacene la información de las opciones realizadas por el usuario y un resumen de los datos ingresados y los comandos requeridos.

+ Para cada una de las opciones el programa deberá preguntar por toda la información requerida para poder ejecutar internamente las opciones indicadas.

4. Muestre en el documento reporte en PDF a entregar los comandos ejecutados para tal fin en todos los pasos.

5. Muestre pruebas de ejecución con las salidas y entradas de su programa, el archivo log generado y las líneas de los archivos de configuración de los usuarios, grupos y claves, donde se muestre los usuarios creados y sus detalles tanto para una máquina LOCAL como para máquinas REMOTA

*Bibliografia*

[1] Sudo.ws,. (2015). *Sudoers Manual*. Retrieved 16 October 2015, from <http://www.sudo.ws/man/1.8.14/sudoers.man.html>

[2] Help.ubuntu.com,. (2015). *Sudoers - Community Help Wiki*. Retrieved 16 October 2015, from <https://help.ubuntu.com/community/Sudoers>

[3] Cyberciti.biz,. (2015). *Understanding /etc/passwd File Format*. Retrieved 16 October 2015, from <http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/>

[4] Manpages.ubuntu.com,. (2015). *Ubuntu Manpage: passwd - the password file*. Retrieved 16 October 2015, from <http://manpages.ubuntu.com/manpages/hardy/man5/passwd.5.html>

[5] Manpages.ubuntu.com,. (2015). *Ubuntu Manpage: shadow - shadowed password file*. Retrieved 16 October 2015, from <http://manpages.ubuntu.com/manpages/vivid/man5/shadow.5.html>

[6] Cyberciti.biz,. (2015). *Understanding /etc/group File*. Retrieved 15 October 2015, from <http://www.cyberciti.biz/faq/understanding-etcgroup-file/>